1 The Emergence of Cyberspace and Its Implications

> We no longer have to debate whether we will fight wars in cyberspace, and to some, it may seem crazy that we ever had to have that discussion in the first place. Cyberspace is a recognized domain of warfare, and for better or worse, our service members and civilians are engaged with our adversaries on a daily basis.
>
> US Representative Jim Langevin (2022), Subcommittee on Cyber, Innovative Technologies, and Information Systems

Broadly speaking, subnational, transnational, and international actors are challenging the ability of sovereign governments to provide a secure environment for their citizens, the most basic function of the state. This is true on land, air, sea, space, and cyberspace. However, in democratic states, when it comes to security in cyberspace, government is either absent or follows information and communications technology (ICT) companies that generally pursue global business models for the benefit of its owners and corporate boards, rather than national interests. The gap between threats faced by ICT companies and government responses generates security deficits, which are evidenced through regular reports of cyber insecurity. And in nondemocratic countries, governments compel ICT companies to restrict basic rights of privacy and reinforce authoritarian rule through content moderation and disclosure of encryption keys.

These dynamics illustrate that the array of cyberspace threats is broad and vast. Transnational organized criminal groups steal identities and conduct financial crimes; terrorist organizations recruit fighters and promote their destructive deeds; countries employ cyber tools for domestic repression and international espionage while laying the groundwork for military operations in cyberspace; and nations worry about disruptions to their critical infrastructure imperiling society when basic services cease and disruptions of access to vital data result from cyber blockades (Russell, 2014) (see Table 1.1). The more devices individuals use to interact in society, the more

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

Table 1.1 US critical infrastructure sectors

Chemical	Commercial facilities
Communications	Critical manufacturing
Dams sector	Defense industrial base
Emergency services	Energy
Financial services	Food and agriculture
Government facilities	Healthcare and public health
Information technology	Nuclear reactors, materials, and waste
Transportation systems	Water and wastewater

vulnerabilities bad actors can exploit, thus creating a cycle of dependency and vulnerability.

Cyber challenges cut across all dimensions of society and simultaneously cross into technological, political, economic, and social realms. Reinforced by intelligence assessments, public opinion polling in democratic countries places cyber insecurity as a leading national security challenge and a pressing national security concern for many governments. Facebook founder Mark Zuckerberg captured the complexity of this problem, saying, "Security isn't a problem you ever completely solve. We face sophisticated and well-funded adversaries, including nation states, that are always evolving and trying new attacks. But we're learning and improving quickly too, and we're investing heavily to keep people safe" (McMillan & Seetharaman, 2018).

Zuckerberg's comments capture the threats that exist in cyberspace yet acknowledge that ICT corporations are expected to contribute actively to improving security in cyberspace – something governments do not expect from other industries. For example, while manufacturing cars is subject to government regulation requiring seat belts and safety recalls, unless there are significant safety concerns, car manufacturers are not expected to license drivers or compel owners to perform routine maintenance of their products. In contrast, ICT corporations are expected to find and fix vulnerabilities by routinely updating their products through patches and alerting the public about vulnerabilities to improve their products after they are installed.

As the online and physical worlds continue to merge, new threats will develop that take advantage of the vulnerabilities inherent in the relatively open system we call cyberspace. When it comes to security, there is tension between the common free space that is the Internet and governments' attempts to police it or exploit it for surveillance. In the People's Republic of China, internet security is a tenet of public safety. In contrast, since 1996: "The policy of the United States [is] … to promote the continued development of the Internet and other interactive computer services and other interactive media … [and] preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation" (Section 230 of the Communications Decency Act, n.d.-a, p. 230).

In short, hands-off or laissez-faire principles have guided the US federal government when addressing cybersecurity; Title 47 of the US Code (Telecommunications) addresses technical regulation such as the rules governing the laying of submarine cables, the granting of commercial licenses to use the electromagnetic spectrum, and the taxing of internet commerce. But there is no equivalent regulation for software standards akin to those that governments impose on auto manufacturing with fuel efficiency requirements, emissions limits, and safety features.

As think-tank scholar James Lewis and colleagues (Lewis et al., 2012, 113) wrote, "the original American view was that Internet governance should be weak and the role of government strictly proscribed, as this would empower innovation and allow an emerging global community to guide the new infrastructure. Security was largely ignored." However, there is a growing chorus within the US Congress to amend the law, but at the time of writing, outside of anti-hacking, generic anti-competitive laws, and limited breech disclosure requirements, cybersecurity regulation and law are sparse in the United States in deference to ICT companies.

There are privacy laws protecting citizens that are rooted in the US Constitution, but they are designed to protect individuals from government intrusion; constitutional protections do not apply between users and ICT companies. Yet privacy is too easily relinquished to corporations when users accept their terms of use when downloading an app or installing software, so there are some efforts to ensure users have the same basic rights in cyberspace that they enjoy in physical life.[1]

Responding to cybersecurity threats, Congress created the Office of the National Cyber Director within the Executive Office of the President in 2020.[2] This created a single voice on cybersecurity issues reporting to the president and confirmed by the Senate. Chris Inglis, who served as the deputy director of the National Security Agency, filled the post from 2021 to 2023 as the country's first national cyber director with responsibility to "coordinate the defense of civilian agencies and review agencies' budgets" (Nakashima, 2021). President Biden also appointed Anne Neuberger, formerly cybersecurity director at the

[1] Rising privacy concerns moved cybersecurity to the national security agenda, and presidents started to address cybersecurity in the 2000s (Obama, 2013; White House, 2018).

[2] See Section 1752 of the National Defense Authorization Act for Fiscal Year 2021 (Smith, 2021).

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

National Security Agency, as the deputy national security adviser for cyber and emerging technology (Riley, 2021). Finally, in 2022, the Department of Homeland Security created the Cyber Safety Board to examine significant cybersecurity incidents in a similar way to the National Transportation Safety Board, which investigates train derailments and plane crashes. These are initial signs that the US government may alter its laissez-faire approach, but there is still no national cybersecurity law comparable to the European Union's General Data Protection Regulation, adopted in 2018, or the Digital Services Act and Digital Markets Act, adopted in 2022.

We explore the ways governments around the world are active in regulating cyberspace, but suffice it to say, today the European Union protects individuals' privacy very deliberately. The European Union offers its citizens the right to be forgotten (excluded from search results) and imposes steep penalties for data loss. In contrast, China and Russia seek to isolate their networks and users from the global system and use technology as a form of authoritarian control. While there is some regulation in the United States, especially with respect to criminal uses of computers, the focus is on technical regulation. Content regulation runs against US civil liberties, such as free speech, and US foreign policy, which seeks a free and open cyberspace. Mathematician and cybersecurity scholar Susan Landau (2016a) underscores that "privacy versus surveillance in Internet communications can be viewed as a complex set of economic tradeoffs – for example, obtaining free services in exchange for a loss of privacy; and protecting communications in exchange for a more expensive, and thus less frequently used, set of government investigative techniques – and choices abound."

The absence of a comprehensive federal US cybersecurity law today relative to other democracies in Europe is striking since several US states have undertaken actions for their own residents. Traditional law applies in cyberspace, but some states have enacted new laws to reinforce applicability in cyberspace. For example, California enacted an internet privacy law in 2020, Washington State took legislative steps to protect against biases in facial recognition software, and Virginia followed California with a consumer privacy law. The new laws are grounded in the Constitution, which prohibits government from violating privacy rights, and are attempting to extend this principle to protect citizens from corporations who collect data on users with their unwitting participation when they agree to terms of use.

While this book presents general principles for cybersecurity, US actions and inactions on cybersecurity will have global effects since decisions made in Washington, DC, and the US technology sector will affect users around the world. However, the national policy gridlock as of 2023 that has forestalled a

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

Policy Matters 1.1 Internet privacy in California

The state of California has long played an important role in cyberspace. For example, several California universities were among the earliest sites to be connected to the ARPANET, an experimental packet-switched network launched by the US Department of Defense in 1969 and renamed the Internet in 1983. Silicon Valley in northern California emerged as a hotbed of innovation in cyberspace and is now home to such companies as Apple, Google, and Facebook. California passed the first US Consumer Privacy Act in 2018, which became operational in 2020. It allows individuals to request details on how companies use their individual data for commercial purposes and to opt out of a business's sale of their data.

Source: California (2018)

comprehensive cybersecurity law in the United States creates a vacuum filled by other governments that will affect US users because it is more efficient for Google and other Internet-based companies to apply European privacy standards globally rather than just to those living in the European Union. We explore various ways governments are regulating companies and users in cyberspace in Chapter 6, but it is first important to review how and why the Internet was conceived as a global network.

1.1 THE EMERGENCE OF PACKET-SWITCHING

The Internet is the *network of networks* that is the backbone of cyberspace. It is a packet-switched network designed to connect computers by sending data packets between them. For intermittent computer-to-computer communications, this is more efficient than the circuit-switched telephone networks that provide dedicated channels between pairs of endpoints. Circuit-switched networks worked well for voice calls in the analog era where call volume was low and data transfer or streaming did not exist, but they do not efficiently support intermittent communication in the digital era.

In 1962, J. C. R. Licklider was hired by the Advanced Research Projects Agency (ARPA) of the Department of Defense as the first head of the ARPA's Information Processing Techniques Office (IPTO).[3] He brought with him a

[3] The ARPA was created by President Eisenhower in 1958 in response to the Soviet launch of Sputnik I in 1957. It is now known as the Defense Advanced Research Projects Agency.

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

vision that networks were needed to connect the very large and expensive computers of the day. Independently, in the very early 1960s, when Paul Baran, a RAND employee, was asked to devise a method of communication that could survive a nuclear attack, he wrote a comprehensive study for the US Air Force entitled *On Distributed Communications* (1964). At the time, the primary communication method was through circuit-switched communication systems that were highly centralized and therefore vulnerable. Baran's solution was to digitize a message, group the message bits into blocks, add source and destination addresses, and launch the blocks on a network that was capable of rerouting them in the event of a disruption and assembling them in order. In 1965, Donald Davies at the National Physical Laboratory in the United Kingdom independently developed and implemented the same concept, using the word "packet" to describe his blocks.

In 1967 Lawrence (Larry) Roberts, an electrical engineer, was hired by ARPA to be the IPTO program manager for a new computer network to be called ARPANET. He was charged with realizing the vision of Licklider. Roberts incorporated ideas from Baran and Davies into his plan for the network and contracted with Bolt, Beranek and Newman Inc. (BBN) to implement his plan for the new network by designing the interface messaging processor (IMP), a precursor to routers. Bob Kahn was one of the engineers on the BBN project.

Eventually, ARPANET became the first large-scale packet-switched network. With technical contributions from academia and the private sector, it became an important platform for experimentation on packet-based communication, bringing the ideas of Baran, Davies, BBN, and many others together. In the beginning, ARPANET was based on an open architecture where "the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level 'Internetworking Architecture'" (Leiner et al., 2009).

The primary ARPANET nodes were operational in 1969 when the first communication occurred between the University of California, Los Angeles, and the Stanford Research Institute. Other research nodes from California to Cambridge, Massachusetts, were later connected. Access to ARPANET had the effect of stimulating research on networking and network applications. New network protocols, that is, methods for organizing and transmitting data over networks, led to improved packet-switched networking. With the advent of personal computers in the mid-1970s, cyberspace began to grow and different networks in the United States and around the world emerged. Networks in other countries, however, did not attract the levels of funding the Department of Defense could provide. By 1980, ARPANET was widely available to

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

History Matters 1.1 Technology gap and the Cold War

At the end of World War II, the US economy accounted for a significant portion of all goods and services (gross domestic product) produced in the world. As Europe and Asia recovered, the lead slowly diminished and became evident in the Cold War. The Soviet Union shocked the world by orbiting the first satellite in space in 1957 (Sputnik I) and orbiting the first human in 1961. Both achievements, coupled with Soviet military modernization, signaled an apparent technology gap that became a major issue in the 1960 presidential election between Richard Nixon and John F. Kennedy, Jr.

When Kennedy assumed office in 1961, he pursued a national effort to revitalize US scientific and engineering activities built around the race to the moon. Kennedy told Congress on May 25, 1961, that the United States needed "to take a clearly leading role in space achievement" and "commit itself to achieving the goal, before this decade is out, of landing a man on the Moon and returning him safely to the earth" (Kennedy, 1961). While he did not see Neil Armstrong walk on the moon in 1969, Kennedy laid the groundwork with federal research and development spending that reached about 2 percent of gross domestic product in 1964 (Orszag, 2007). This had important impacts for the civilian space program led by the National Aeronautics and Space Administration, the defense industry, and ultimately the military establishment.

universities and research laboratories in the United States and a few other countries. The development of computers and the operation of the Internet are examined in detail in Chapters 2 and 3, but suffice it to say, the paradigm shift in the way data moved via packets rather than direct connections paved the way for the exponential growth in information technology (IT), new industries, and revolutions within old industries.

1.2 THE EXPERIMENTAL ARPANET PACKET-BASED NETWORK

The growth of cyberspace became important given the perception that the United States had fallen behind the Soviet Union in science and technology during the Cold War. As one of many efforts to revitalize US innovation, ARPA funded research on networking and time-shared computing, which is

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

a technology that allows multiple users to use a single computer. The costs of computing were substantial, and ARPA paid to have specialized ARPANET computer equipment assembled so that the research community could join the network.[4]

As hardware developed and an interconnected network was created, new ways of communicating evolved, creating potential diverging pathways that could have led to noncompatible networks. In an example relevant today, to ensure that a file could be opened within both Microsoft Windows and macOS would require computer users to adopt a standard file format, such as .jpg or .pdf, so that users could collaborate without needing to use a common operating system or computer. In the Internet's early days, the same problem arose when US researchers on an ARPA machine wanted to connect with European researchers using machines connected to other networks. It was solved through the creation of international standards and protocols.

In 1974, electrical engineer Robert Kahn and computer scientist Vinton Cerf published the Transmission Control Protocol/Internet Protocol (TCP/IP), which forms the basic architecture of the Internet. IP is used to specify the source and destination addresses that are used for routing while TCP ensures that every packet reaches its destination. TCP/IP became critical to reliably connecting networks around the world and reinforcing the goal of a compatible network of networks; both Kahn and Cerf were later recognized with Presidential Medals of Freedom as internet pioneers since their work played a central role in the development of the interconnected network or Internet (White House, 2005). On January 1, 1983, TCP/IP was fully incorporated into ARPANET, giving rise to what now we call the Internet.

Since ARPANET was rooted in military funding, the link to the Defense Department was severed by splitting ARPANET into MILNET for defense purposes and ARPANET for civilian use. The civilian-only ARPANET also made it more palatable for networks in other countries to join since it was not associated with the US military; funding gradually shifted away from the Defense Department to the National Science Foundation (NSF). Within a few years the NSF was involved in networking, and ARPANET was formally decommissioned on February 28, 1990, with its nodes transferred to NSFNET, which became the new backbone for the network of networks.

We return to internet architecture in Chapter 3, but by the early 1990s the Internet became commercialized with internet service providers assuming

[4] Janet Abbate noted in her history, "individuals and organizations interested in pursuing computer networking often found it necessary to join government-sponsored projects or to present their work as responsive to contemporary political agendas" (Abbate, 1999, 40).

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

responsibility for the internet backbone on April 30, 1995. With the creation of a simple-to-use interface through the Web, a proliferation of personal computers, and significant investment in telecommunications, these changes marked the transition to the modern Internet that paved the way for a robust commercial space largely free of government interference.

1.2.1 Transmission Control Protocol/Internet Protocol

The TCP/IP is designed to interconnect networks using multiple technologies as well as computers with different operating systems. This was an important innovation that enabled researchers around the world to connect their networks to other networks, paving the way for the network of networks, thereby creating the Internet as we know it.

The Internet is subdivided into subnetworks called autonomous systems (ASs), each of which may have many clients. Every computer on the Internet requires a unique IP address, which is assigned to a client by an AS. Internet Protocol version 4 (IPv4) assigns 32-bit IP addresses, of which there are about 4.3 billion. Almost all the IPv4 addresses have been allocated and Internet Protocol version 6 (IPv6) now assigns 128-bit IP addresses, of which there are about 3.4×10^{38}. Each AS must have a unique AS number by which it is known to other ASs. The Internet Corporation for Assigned Names and Numbers maintains a list of AS numbers, the organizations that manage them, and the block or blocks of IP addresses that they are authorized to allocate.

The operation of the domain name system (DNS), which acts like a telephone directory for the Internet, is explained in detail in Chapter 3, but it is important to note that its operation is based on trust, which can be abused. For example, an analysis of 303 supposed government websites providing

Exploit 1.1 Spoofing domain names

Malicious actors have learned to trick users into visiting a domain of their choosing by sending a domain name that may look like the one a user may want to visit, such as a bank, but which is slightly different. For example, instead of sending www.jpmorganchase.com, the bad actor might send www.jpmorganchaise.com. A tired customer at the end of a busy day may not see the difference between these two domain names and the malicious actor could trick the customer into disclosing personal information that can be exploited.

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

Exploit 1.2 Cybersquatting

When it became apparent in the 1990s that interest in the Internet was going to explode, domain names suddenly became very valuable. That's when *cybersquatting* emerged. This is the practice of registering a domain name that might have value to a major corporation, an institution, or a well-known person.

Mike Rowe, a 17-year-old Canadian high-school student, registered the domain name MikeRoweSoft.com in August 2003, which is phonetically the same as Microsoft.com. Microsoft took legal action against him, asserting to the World Intellectual Property Organization (WIPO) that Rowe had infringed their trademark. In January 2004, it was announced that the parties had settled out of court and that Microsoft had taken control of the domain.

Recording artist and composer Bruce Springsteen filed a complaint with WIPO against Jeff Burgar, asserting that he violated Springsteen's common law rights by registering BruceSpringsteen.com. A WIPO panel evaluated the case and ruled against Springsteen in 2001.

Source: WIPO Arbitration and Mediation Center (2001)

information on the COVID-19 pandemic suggested that nearly 80 percent were not verified as authentic but were a combination of commercial entities selling products or others engaged in domain name spoofing (Tombs & Fournier-Tombs, 2020).

1.3 THE WORLD WIDE WEB APPEARS

For about 20 years, until the early 1990s, the Internet and its precursors around the world were largely used by universities, colleges, and research institutes. But after Tim Berners-Lee and his colleagues announced the World Wide Web in 1990, commercial and social applications exploded.[5] Berners-Lee and his colleagues at the European Organization for Nuclear Research (Conseil

[5] The development of the Web was not preordained, as Janet Abbate notes: "[T]he Web did not spring from the ARPA research community; it was the work of a new set of actors, including computer scientists at [the Geneva, Switzerland-based research center] CERN, the staff of an NSF supercomputer center, and a new branch of the software industry that would devote itself to providing Web servers, browsers, and content" (1999, p. 214).

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

Européen pour la Recherche Nucléaire, CERN) used TCP/IP for the Web, thereby demonstrating its usefulness.

The Web is a public layer of indexed content that can be found with traditional search engines and browsers, as opposed to the dark web, where content is intentionally hidden, requiring users to know specific locations and have special software to access the hidden sites. Berners-Lee built upon the work of Ted Nelson, who coined the term hypertext and believed a computer's interface should be simple and be easily understandable by a basic user (Nelson, 1974). With the simple interface that the Web offered, computer users everywhere, regardless of programming expertise, could use the Internet for email, shopping, and recreation. Within a few short years, companies such as Amazon and eBay (1995), Wikipedia (2001), Facebook (2004), Twitter (2006), and Zoom (2011) created new industries and changed the way we live and work. Social media companies enabled individuals to connect with each other and share content, while the federal government shielded companies from liability from what is expressed on their platforms.

1.4 DEFINING CYBERSPACE

The development of cyberspace and the broader information environment have been influenced by science fiction, which offers both inspiration and anxiety for thinking about technological change. Writer William Gibson coined the term "cyberspace" in a short story published in 1982 where he described cyberspace as a "consensual hallucination." Professor of English and Cinema and Media Studies Patrick Jagoda (2012) notes the etymological roots from the Greek word "kybernetes," which means steersman, seeing "cybernetics was not only a theory of communication but also one of control. Once confined to the cyberpunk literature and science fiction like the movie *The Matrix*, the information environment entered the real world in the late 1990s. Early internet providers such as AOL, CompuServe, and Prodigy gave home users easy but slow access to the Internet.

In 2003, the Bush administration described cyberspace as the "nervous system – the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work" (White House, 2003). The National Institute of Standards and Technology later defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications network, computer systems, and embedded processors and controllers" (National Institute of Standards and

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

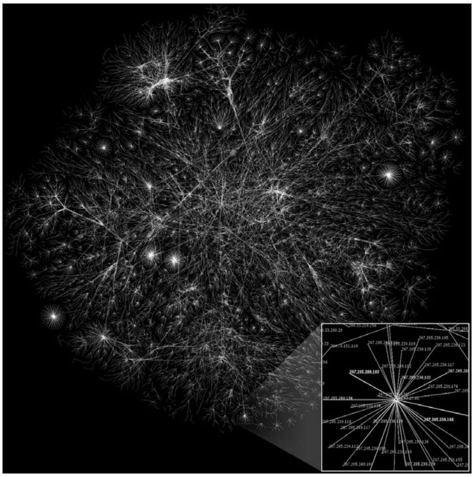

Figure 1.1 A map of internet routes by the Opte Project licensed under CC BY 4.0

Technology, 2012). A partial map of the Internet is contained within Figure 1.1. When we add people and the decisions they make to the cyberspace definition, we have the information environment.

Like the physical environment, the information environment is all-encompassing. It includes physical hardware such as routers, telecommunication lines, and servers, which are often the basis for governments to regulate cyberspace. Additionally, cyberspace includes information such as data and media, the mental or cognitive processes people use to comprehend their experiences, and the virtual world, where people connect socially through real and alternate personas. Democratic governments generally promote environments in which content (speech) is not regulated whereas authoritarian governments attempt to regulate access and content. Authoritarian governments also design content to reinforce political control. Cyberspace serves as a domain where people can adopt alternate personae on blogs, social networking sites, and virtual reality games.

Larry Johnson, chief executive officer of the New Media Consortium, predicted that we will experience the virtual world as an extension of the real one. Johnson concluded:

> Virtual worlds are already bridging borders across the globe to bring people of many cultures and languages together in ways very nearly as rich as face-to-face interactions; they are already allowing the visualization of ideas and concepts in three dimensions that is leading to new insights and deeper learning; and they are already allowing people to work, learn, conduct business, shop, and interact in ways that promise to redefine how we think about these activities – and even what we regard as possible. (Johnson, 2008)

1.5 CYBERSPACE CHALLENGES

Cyberspace is powered by algorithms, which are recipes for computations, and software, or code, that is, the implementation of algorithms. Software consists of instructions in a programming language that are translated into machine-level programs executable by computers.

There is an enormous gap between the machine-level instructions of a computer and the functionality that humans need to do serious work. For example, a modern operating system may require 50 million lines of code, which may take some tens of thousands of person-years to write, test, and document. Given the enormous size of the programming task, it is easy to imagine that programmers will make mistakes and replicate mistakes when reusing previously published open-source code. When mistakes are discovered, they can be exploited as vulnerabilities, providing unauthorized users access to networks that can be exploited for gain. Consequently, software companies regularly issue patches to remove the vulnerabilities from previous versions.

Industries as diverse as water resource management and nuclear power have embraced electronic supervisory control and data acquisition (SCADA) technologies. These operational technology (OT) networks are often separated from a company’s IT networks. On the one hand, this has led to developing infrastructures that would be unimaginable without technology. On the other hand, the shift from mechanical to electronic control creates new vulnerabilities that can be exploited when SCADA systems are connected to the Internet for remote access. For example, when remote access is used for nefarious purposes to target critical infrastructure, electricity can be shut off or water can be contaminated by increasing the volume of purifying chemicals to toxic levels, thereby having a widespread societal impact.

Essential Principle 1.1 Coding principles

The languages used to write programs have evolved over time. The first languages were machine-level and told machines explicitly what to do. Soon the concept of a process, a program with its data, was invented, followed by the virtual machine, which simulates a potentially infinite memory from a collection of individual memories, to today in which a program invokes an operating system to manage the memory of a computer, thereby creating a “virtual memory,” and reducing the number of errors programmers make and helping them to work more quickly.

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

Exploit 1.3 The Aurora Generator Test

Electricity is an essential resource on which the rest of a nation's critical infrastructure depends. To determine whether or not the US electrical grid is at risk of a cyberattack, the US Department of Energy conducted an experiment, the Aurora Generator Test, to see if a cyberattack could seriously damage an electricity generator and thereby threaten the grid.

In 2007 the US government installed a new diesel generator at its Idaho National Laboratory and invited computer scientists to see if the generator could be damaged. The computer scientists repeatedly opened and closed the circuit breakers on the generator so that it was out of synchronism with the synchronous North American electricity grid. This produced great stresses on the rotor of the generator and destroyed it.

Source: Greenberg (2020)

Interdependencies across computer networks exacerbate vulnerabilities when an exploited flaw within one network sector impacts another. For example, when the 2017 WannaCry ransomware attack exploited a vulnerability in the Microsoft Windows XP operating system, which was so old that it no longer received updates, the ransomware had a disproportionate effect on the British National Health System. WannaCry also affected companies around the world using the same antiquated XP operating system (Smart, 2018).

Countries have come to realize that their infrastructure is accessible to and possibly threatened by foreign actors, challenging a government's laissez-faire approach to cybersecurity. Recognizing this, the US government has identified 16 critical infrastructure sectors and works with industry to improve their cybersecurity. President Biden gave this list to Russian president Putin in 2021 with the warning to keep Russian intelligence and Russia-based organized criminal groups out of these sectors. In addition to stepped-up defenses, this redline might explain why there were limited cyberattacks when Russia escalated its invasion of Ukraine in 2022.

Obviously, computers and networks require electricity to operate. If the electricity supply fails, there is no cybersecurity. As discussed in Exploit 1.3, the Aurora Generator Test demonstrated that a hacker could destroy a generator by briefly disconnecting and reconnecting it to the electric grid, illustrating a key US electric grid vulnerability. The risk to the grid is made worse by the fact that US electricity suppliers are heavily dependent on

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

foreign manufacturers to replace damaged generators, transformers, and other equipment, subjecting replacement equipment both to foreign compromise at the root-level and to lengthy replacement waiting periods if global supply chains are slowed.

Very little of modern life is excluded from critical infrastructure sectors. Industries in these sectors have come together with the US government to share security information through communities of interest called Information Sharing and Analysis Organizations (ISAOs) and Information Sharing and Analysis Centers (ISACs). ISACs collect, analyze, and disseminate actionable threat information to their members to mitigate risks and enhance resiliency. ISACs were started in 1998 to facilitate information-sharing among members; ISAOs were created in 2015 to share information across sectors.

The US Department of Homeland Security through the Cybersecurity and Infrastructure Security Agency (CISA) has several information-sharing programs including Automated Indicator Sharing, the Cyber Information Sharing and Collaboration Program, and Enhanced Cybersecurity Services. CISA recognized that information-sharing with industry is paramount and launched a new program in 2021 called the Joint Cyber Defense Collaborative. Finally, the Federal Bureau of Investigation (FBI) created a partnership called InfraGard to represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. If a company is being attacked, it can work with the FBI to stop it and possibly arrest the attacker(s). While these are important efforts, cybersecurity is very much a cat-and-mouse game; with every new product comes new vulnerabilities that get exploited until new software updates or patches are released. The limited law enforcement role in cybersecurity has resulted in a large cybersecurity industry where individuals and corporations must rely on themselves to stay ahead of attackers by bringing in third-party support.

1.6 THREATS TO THE INFORMATION ENVIRONMENT

As explored in subsequent chapters, there is a dark side of the cyber world wherein hackers, phishing scam artists, and transnational criminal groups harness technology for nefarious purposes. Through phishing, criminals and spies gain access to government and private computer networks. Through viruses and denial-of-service attacks, individuals and groups can steal intellectual property and disrupt governments and corporations with ransomware. And through spyware or government surveillance programs, the cherished civil liberty of

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

privacy is subverted. No longer only in fiction, the personal, professional, and financial records of one's life can be exposed or stolen for malevolent purposes. Thus, for many the ultimate human security threat comes from cyberspace.

Adding cybersecurity to the national security agenda has generated some controversy. While it is common for criminal enterprises to launch ransomware attacks and for foreign intelligence services to engage in economic espionage, governments are now concerned enough to include cyber warfare in their military planning and operations. For example, a cyber operation accompanied Russia's invasion of Ukraine in 2014 and in 2022. As Russian tanks and aircraft entered Ukrainian territory, cyber warriors attacked government websites and advanced Russian interests through the information sphere. In an attack in December 2015, the nightmare scenario became real as a cyberattack shut down power for some 230,000 Ukrainians (Zetter, 2016). In 2022, a similar attempt was made to disable the power infrastructure, but Ukrainian defenders prevented exploitation (Rundle & Stupp, 2022). Although it had a temporary effect, the attack was a harbinger; future conflicts will combine physical and online operations, as militaries continue to develop ways to combine cyber and conventional operations.

Consequently, cybersecurity analyst Kenneth Geers (2014) argued that "[n]ations today use computer network operations to defend sovereignty and to project power, and cyber conflicts may soon become the rule rather than the exception. Most cyber-attacks do not rise to the level of a national security threat, but in the post-Stuxnet era, the notion of 'cyber war' has moved closer to reality." (Stuxnet was an attack on Iran's nuclear infrastructure that produced physical destruction of centrifuges used to enrich uranium gas by targeting industrial control systems through cyber means, which was revealed in 2010 [Sanger, 2010].) Political scientist Erik Gartzke (2013, p. 59), however, maintains "the need to follow virtual force with physical force to achieve lasting political consequences suggests that the application of cyberwarfare independent of conventional forms of warfare will be of tertiary importance in strategic and grand strategic terms." While the challenge for analysts remains differentiating between espionage and preparation for a future attack, analysts do believe that there is a risk of an inadvertent escalation due to cyber capabilities (Buchanan & Cunningham, 2020). As mentioned earlier, this sentiment was echoed by President Biden in 2021.

It is important to realize that governments could use cyberspace operations the same way they use drone strikes, namely, to meet immediate security needs rather than produce long-lasting results. This can lead to long campaigns of tit-for-tat operations, creating an inherent instability in cyberspace and society but may also provide de-escalatory off-ramps for governments to express displeasure with foes without causing significant harm. Because traditional definitions

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

of war include use of violence to achieve political outcomes that produce battle deaths, Valeriano and Maness (2015, pp. 28–32) argue that cyber *conflict* is a better way than war to describe how governments interact with each other in cyberspace. War has specific meaning in law, doctrine, and academia; nevertheless, organizations that are responsible for war are developing military capabilities for cyberspace.

For its part, the United States developed US Cyber Command in 2010 with the explicit intent of defending military networks, supporting combatant commanders executing their missions around the world, and strengthening the country's ability to withstand and respond to cyberattacks. Dozens of other countries are developing similar military entities. As governments and militaries embrace technology for efficiency and effect, they also become vulnerable to cyberspace operations. And as more of society, government, and the economy move online, individuals in developed countries can no longer be isolated from the effects of conflict, which may explain why governments are largely restrained in their cyberspace operations. Former senior leaders in Defense and Homeland Security offered a sobering assessment of this situation: "Until the U.S. government makes significant strides on each of these issues, policymakers will have to accept that the offensive cyber-option isn't much of an option" since US society is so vulnerable to counterattacks through cyber means (Rosenbach et al., 2021).

As it relates to war, the Internet is both a means to support operations and a target for militaries to impose costs on their adversaries. Former US deputy defense secretary William Lynn underscored how important the information infrastructure is to national defense:

> Just like our national dependence [on the Internet], there is simply no exaggerating our military dependence on our information networks: the command and control of our forces, the intelligence and logistics on which they depend, the weapons technologies we develop and field – they all depend on our computer systems and networks. Indeed, our 21st century military simply cannot function without them. (Miles, 2009)

In contrast to traditional war-fighting domains such as land, air, or sea, governments are not the only powers in cyberspace. Rather, nonstate actors can readily harness technology to compete on a global scale. And it is worth noting that virtualization will continue this trend of democratizing the Internet, giving individuals tremendous power unthinkable even 10 years ago. Satellite imagery used to be highly classified and limited by the intelligence community, but now anyone can access imagery from an iPhone using Google Earth or contract with myriad commercial satellite imaging companies. Likewise, the complexity and cost of building a nuclear weapon limit their production

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

to governments, but the same cannot be said for malware that can destroy data and networks, undermine international credibility, and disrupt commerce. Consequently, governments are increasingly concerned with the cyber domain as a new feature within the national security landscape as individuals are exposed to the dangers of being connected.

A wired society offers many vulnerabilities. While it can take months or years to map a target's networks, speed of attack is beyond human perception, and malicious actors take advantage of human vulnerabilities through social engineering to elicit network access. Offense tends to dominate thinking in the information environment since there is an open architecture and protocols, but defense and resilient networks are important too.

While physical destruction dominates Western ways of thinking about war, it is possible cyberspace operations can be considered a use of force under international law if it is destructive, sustained, and attributed to a nation-state. Use of force through malware is rare, but since cybersecurity is occupying national security thinking, it may be better to rely on ideas of war as a bargaining model (Fearon, 1995) or use terms such as cyber conflict and cyber competition rather than war to connote disagreements among states since countries increasingly employ cyber operations as a unique tool of power (Valeriano & Maness, 2015).

As Herb Lin (2012, p. 41) wrote, "Cyber-attacks are particularly well suited for attacks on the psychology of adversary decision makers who rely on the affected computers, and in this case such effects can be regarded as indirect effects." Chamath Palihapitiya, who was a Facebook founder and a venture capitalist, sees that social media has been "used and abused in ways that we, their architects, never imagined" (Koh, 2018). Algorithms are used to amplify false or sensational messages. In other words, cyberspace operations can generate broad feelings of insecurity, which force both governments and social media companies to take users' actions more seriously and look to algorithms to identify content that is deliberately false or incendiary.

1.7 ATTRIBUTION

Attributing the source of a cyberattack, its point of origin, operator, and intent, can be difficult. Unlike a missile launch that has a discrete signature, geographic location, and obvious intent to kill, those who employ cyber tactics can easily hide their origin or conduct operations from servers inside the victim's borders, which makes attribution difficult but not impossible. The cybersecurity analyst at the prominent think tank Center for Strategic and International Studies James Lewis (2009) has argued, "Uncertainty is the most prominent aspect of cyber

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

Table 1.2 Malicious actors and motivations

Threat source	Motivation
Governments	Information gathering and espionage activities
Criminal groups	Monetary gain
Hackers	Thrill of the challenge
Hacktivists	Politically motivated attacks to send for monetary gain
Disgruntled insiders	Cause damage to the system or steal for monetary gain
Terrorists	Propaganda, fund-raising, recruiting, and reconnaissance

conflict – in attribution of the attackers [*sic*] identity, the scope of collateral damage, and the potential effect on the intended target from cyberattack."

Thus, when trying to analyze cyber threats, it is best to take a comprehensive approach. Accordingly, we can classify threats by the actor, such as individual and government, by the target, such as a financial sector or defense department, or by the means, such as a virus, a bot, a denial of service, or social engineering. The actors include individual hackers, organized criminal groups, intelligence services, and agencies of governments. Patterns of cyber operations among governments resemble interstate rivalries where it would be more common to observe Iran attack Israel than Iran attack China (see Table 1.2).

As the diversity of actors illustrates, the barriers to entry for cyberspace are low, which helps explain why cyberattacks have become commonplace. There are differences of opinion about the power to cause disruption or damage by various individuals, groups, or nation-states. For example, the head of the International Telecommunications Union noted, "[T]he next world war could happen in cyberspace and that would be a catastrophe. … Loss of vital networks would quickly cripple any nation, and none is immune to cyberattack." (Hui, 2009). While a cyberspace superpower, such as China, Russia, France, Israel, and the United States, should be capable of causing massive damage to computers, networks or attached equipment, it is highly unlikely that a single individual could do it. Analyses of significant disruptions caused by NotPetya and Stuxnet illustrate that much planning and effort must go into designing malware to have a significant impact. It remains easier to order a missile strike than a cyberattack, so a future characterized by Cybergeddon is not certain (Healey, 2011).

Web-based attacks are a common source of malicious activity, which often happens by exploiting a vulnerable Web application or exploiting some vulnerability present in the underlying host operating system. A single individual or

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

criminal enterprise can do a lot of damage through denial-of-service attacks or ransomware, but to produce a serious incident, such as turning off the electricity supply for a week or more over a large portion of a large country, requires either a lot of luck or a high level of skill in discovering vulnerabilities and designing malware that can cause failure across many subsystems. It is more likely that a nation-state would have the resources, the motivation. and the will to attempt such a serious attack.

Governments such as China, Russia, France, Israel, the United Kingdom, and the United States have significant cyber capabilities and are superpowers in cyberspace.[6] The US Defense Department predicts, "Strategic attacks will likely focus on disrupting elements of the US financial infrastructure, where trust and data integrity are paramount" (CISA, 2021a). What is important, however, is governments are not alone in using malware to further their interests. This fundamentally changes thinking about national security, which is no longer the exclusive domain of governments. To be sure, governments are still leading efforts to seek advantage in cyberspace and are the only cyber actors capable of existential operations, but now multinational companies, nongovernmental organizations, and transnational organized criminal groups are important actors in cyberspace as well. Defense is grounded in public–private partnerships where ICT companies work with governments to improve cybersecurity (see Table 1.3).

Table 1.3 Types of malware and cyberattacks

Denial of service (blockade): accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users

Trojan: malware that, once implanted in a computer, provides remote access to an attacker

Phishing: an email or text-based social engineering attack that can trick users into providing attackers access to a targeted system

Ransomware: malware that blocks access to a computer until a ransom is paid

Virus: malware designed to replicate itself for the purpose of infecting other computers

Wiper: malware designed to corrupt or erase a significant portion of memory, usually to make a computer inoperable

Worm: malware that behaves as a standalone virus and does not need to infect an application to copy itself but does need to exploit a vulnerability in an operating system

[6] To measure cyber power of states, see Schwarzenbach et al. (2021).

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

1.8 ETHICS, NORMS, REGULATIONS, AND LAW

As with all domains in which humans operate, not all participants in cyberspace subscribe to the same moral principles (ethics) or the same rules of behavior (norms). Similarly, cyberspace has made available new violations of confidentiality, integrity, and availability of data. Thus, new laws and regulations are required to protect such data.

For example, the theft of an owner's identity can impose exorbitant costs on that owner as well as damage his/her/their reputation. Other violations, such as denial of access to information, can impose costs on users of that information. It could be as simple as having to wait to withdraw funds from a checking account to incurring costs for failure to pay bills on time.

A website that hosts a user's postings without examining the content of such postings might endanger a community by publishing inflammatory information or injure an individual's reputation by publishing defamatory information. The former might produce damaging political polarization. The latter could destroy the reputation of an innocent person. Similarly, when historical data is used to train an artificial intelligence system to be used in making decisions, if the data reflects bias, systems trained on that data will perpetuate that bias when used to make similar decisions. Novel issues arise in cyberspace that require thoughtful and informed action by individuals, organizations, and governments.

1.9 CYBERSPACE IS UNIQUE

No single entity owns the Internet, yet individuals, companies, and governments use it. Anyone with a phone, tablet, or computer with an internet connection can connect to the Internet and can operate there. And, making it more challenging for governments, most of the IT expertise resides in the commercial sector. Israeli Defense Force cyber chief of staff Brig. Gen. Yaron Rozen said, "This whole front resides in the civilian world, not in the military one. Look how long it took nations across the globe to sign the Kyoto Treaty, which deals with global warming and affects everyone. The Cyber nations are not just the superpowers, but huge international corporations like Google, Facebook, and Kaspersky" (quoted in Zitun, 2017). Likewise, international agreements can be rescinded when the political party in power changes, which further complicates trust and efforts to reach international agreement on law and norms. This may explain why corporations such as Microsoft have been promoting norms and even established an office at the United Nations Headquarters.

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press

Cyberspace is more tightly integrated than one might expect. For example, a computer virus that infects an airline in South America can also affect a logistics company in North America since users across the world use the same software and malware can readily spread beyond the intended target. Furthermore, as Harvard Law professor Lawrence Lessig (1998) reminds us, cyberspace "architecture is inherently political. In the world of cyberspace, the selection of an architecture is as important as the choice of a constitution."

Cyberspace also reflects the culture of the locale where the code is written, hardware is designed, and rules are implemented. Thus, it matters that today's Internet is dominated by developed democracies where anonymity prevails, social spaces can be safe spaces, and users find affection with each other rather than loyalty to a particular government. While never realized, poet John Perry Barlow (1996) captured this aspiration for a cyberspace "where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."

As Chapter 6 discusses, however, countries are attempting to regulate cyberspace within their borders in ways that reflect their national cultures. Consequently, China and Russia attempt to apply authoritarian principles in cyberspace, depriving users of anonymity and free speech. Alternatively, the European Union has applied human rights laws in cyberspace granting users significant privacy protections vis-a-vis ICT companies. Chapters 2 and 3 provide a foundation in thinking about computing and networking before returning to these issues and exploring ways to make cyberspace more secure for everyone.

1.10 DISCUSSION TOPICS

1. Explain the origins of the general laissez-faire approach the US government takes to the IT sector and defend the position that it is likely or unlikely to change.
2. Identify the nature of cybersecurity incidents that you believe would rise to national security incidents. Consider the possibility of cascading effects.
3. Explain why you believe that the open architecture of cyberspace is or is not a source of strength and weakness.

https://doi.org/10.1017/9781009308564.003 Published online by Cambridge University Press