1

A BRIEF HISTORY OF THE INTERNET

Learning Objectives

At the end of this chapter, students will be able to do the following:

- Describe the four major phases associated with the growth of the internet and the major technological, political, and economic developments associated with each.
- Define significant terms associated with the growth of the internet.
- Describe in basic terms the technical specifications of the internet as well as what unique facets distinguish it from other technologies.
- Describe key political issues that have arisen in the growth of the internet, and describe the ways in which technological closure has begun to occur regarding these issues.

WHAT IS THE INTERNET?

Students today probably do not remember a time when they lacked internet access. If you were born in the 1990s, you have always been able to send e-mail, access a library of resources online, and purchase products from all over the world. However, the internet has only been available to the average user since 1994, when commercial **internet service providers (ISPs)** like America Online began attracting large numbers of civilian subscribers. Thus, it is astounding to contemplate how this technology has reshaped our world and our relations with others in the space of fewer than thirty years.

Today, an estimated 4.2 billion of the world's 7 billion people have internet access. The **penetration rate** describes what percent of the population of a nation has personal access to at least some of the internet's features, either at work or in a private home. Penetration rates globally range from a high of 95 percent of North America's citizens to a low of 36 percent of Africa's citizens. If we look at the universe of internet users globally, we see that nearly half (48 percent) are in Asia, whereas 16 percent are in Europe, another 16 percent are in Latin America, and 10 percent are in Latin America. Eight percent are in North America, whereas nearly 4 percent are in the Middle East.[1]

The internet has been credited with launching or aiding in revolutions in the former Soviet Union and the Middle East. It has changed how people shop, how they search for information about whom to vote for, as well as changing how people are educated and trained worldwide. International recruitment sites like LinkedIn have aided in the recruitment and hiring of international staff, whereas e-government initiatives have changed how citizens think about and interact with their elected leaders and government agencies providing services.

E-commerce (or online shopping) has created a global marketplace. In 2016, more than half of all global internet users purchased something online, and nearly 70 percent of millennials prefer shopping online rather than in a store. In the United States, nearly half of all e-commerce sales are through Amazon.com, and this company is considered a driving force in e-commerce globally.[2] Through the wonders of e-commerce, users are as likely to buy something directly from a store in China as they are to purchase it locally.

The internet's expansion also introduced new players to the international system. Today, Amazon's annual revenue dwarfs the GNP of many smaller nations, and there are more citizens of Facebook than there are in any nation. Thus, as nations and international bodies like the United Nations and the International Telecommunications Union work to shape the rules and structures of the internet, players like Google and Twitter are gaining a seat at the table. Policies made on these platforms—such as a decision to disallow hate speech or to police news for factual content—have international effects. Thus, companies like Google are now shaping international policies in the ways that nations and international bodies did in the past.

The internet's growth also created new legal issues. From the beginning of widespread civilian use of the internet (beginning in the mid-1990s, with the e-commerce revolution taking place in 1998), states have been concerned about issues of jurisdiction in the online environment. Consider a situation in which, for example, a Canadian citizen logs onto the internet in his country, visits a Scandinavian website hosting child pornography, and downloads an image of a Brazilian child, uploaded by a user in Asia. Even if viewing, downloading, and storing child pornography is a crime in Canada, where exactly did the crime occur? Whose laws determine how the crime should be treated? Should the Canadian user be extradited to Brazil? Asia? Or Scandinavia?

In this chapter, we summarize the issues that the internet's creation poses for scholars of politics and international relations. We begin by describing the internet's origins. Initially, the internet had an "American flavor" due to the fact that American research dollars funded the internet and the fact that it developed in America. In the early years, American policy makers argued that this technology was associated with ideas like freedom of information or globalization due to the circumstances of its birth. However, today many nations dispute this contention, arguing that it is possible for Russia to have a "Russian internet," which looks quite different from the technology as it was envisioned by its American designers. Over time, the internet has become more divided, polarized, and militarized. This brief history illustrates how it got there.

A Brief History of the Internet

Barely fifty years have passed since the internet was first envisioned until today, when the internet is nearly ubiquitous—present in nearly every household in America, utilized daily by millions of people, and where at least two generations of individuals cannot even envision or conceptualize of life before the internet.

Major Policy Issues on the Internet

However, despite its ubiquity, there are still significant points of contention regarding the use and regulation of this technology today. First, some analysts see the internet as an arena for peace and cooperation, whereas others see it as a place defined by conflict. Analysts also disagree about particular aspects of cyber warfare—including what it is, how states that carry out acts of cyber warfare should be sanctioned or censored, and how acts of cyber warfare relate to the principles of traditional warfare.

Next, analysts disagree about the phenomenon of regulation. As the internet has developed, analysts disagree regarding which activities should be permitted or banned in cyberspace. Should states allow people to engage in online pornography, the deploying of viruses and cyberweapons, and identity theft? And if they do not wish to have individual citizens or groups engaged in such activities, how should they regulate the internet so that they do not occur? Indeed, the speed at which internet connectivity technologies have developed has outpaced the ability of governments to regulate them, both nationally and internationally. As a result, although states may think that they control many aspects of this "information revolution" and its ramifications, they do not actually do so. Harvard political scientist Karl Deutsch once said that "history sometimes amounts to nothing more than a litany of unintended consequences and unforeseen side effects."[3] That is, technological changes appear to be leading the policy component as well as the development of legal and other regulatory schemes.

Next, analysts and policy makers disagree about governance of the internet. They ask: Who should make rules regarding regulations on the internet—professionals, states, or the international community? Is the internet best understood as a self-regulating entity that has emerged and grown, developing its organic structures of governance through the work of those technology experts who have created it? Or is it more similar to a territory that has been discovered and that then needs to be colonized by preexisting states and integrated into their real territory? That is, should we think about Russian cyberspace and Chinese cyberspace, or should we instead think of the internet as a borderless territory and community—like outer space or the ocean—which belongs to all nations and therefore needs to be administered by an international body like the United Nations? Who governs the internet? Does anyone?

Analysts and policy makers also disagree about norms and values in cyberspace. They ask: Where do the norms governing behavior on the internet come from, and whose values should they reflect? Do these norms somehow emerge naturally or "organically" from the internet itself, or are they norms, values, and laws that already exist and apply to other areas of national and international politics that are then transferred onto the cyber realm and applied there? Should activities like censorship and surveillance (which might be forbidden or intensely regulated in a state's real territory) be allowed to occur on the internet? And if not, how might they be prevented?

Analysts and policy makers also disagree about sovereignty or control in the internet environment. They ask: How should we conceptualize the "territory" of the internet? Does it belong to a particular state (i.e., "the Russian internet"), or should it be considered some form of global commons? Is it a "world apart" from normal nation-state relations, or does it interact with existing forms of power like political, social, and economic power?

The Four Phases of the Internet's History

In this chapter, we divide the internet's history into four phases: The first, the infancy of the internet, spans the period from 1963, when plans for what was then known as ARPAnet were first articulated, until 1984, when it was released from US military control to become a utility open to civilians as well. The second phase of the growth of the internet can be termed the period of growth and early regulation. This phase proceeded from 1984 until 2000. Phase three is the securitization of cyberspace and growth of internet governance (2001–2012); Phase four is the era of surveillance and big data (2013–present).

This division is somewhat arbitrary. However, these four phases provide a useful shorthand for becoming familiar with the significant events that have occurred in cyberspace in the last 50 years. They also enable us to see a particular arc in the story of cyberspace from its infancy, in which both users and developers had almost a utopian vision of how the technology could develop as well as how it might change and shape our international system. We see how individuals have become more cynical or more realistic—aware of the harms that internet access can provide as well as good. States became aware of risks and security threats, the possibility of online crime, and the rise of events like online terrorist recruitment. The growth of hacking and computer viruses showed that cyberspace is not a world apart but rather a portal into the real world. Real-world harms can occur through the use of cyberspace.

Each era saw the emergence of new challenges and debates and had ramifications for social, political, and economic systems both nationally and internationally. The initial phase saw the creation of technological advances. Most of those who created this new technology had expertise that was technological rather than legal or policy related. They were interested in seeing how preexisting technological capabilities might be extended over the globe. Many individuals who were active in this initial phase now note that they were not completely aware of what they were creating or the role that it might come to play in today's world.

In the second phase, from 1984 until 2000, we see the development of e-commerce and the extension of the internet from a domain that mostly belonged to technology experts, scholars, and military officials to the larger civilian community. People could access a home internet, where they could read the news, participate in chat groups, and communicate globally. During this period, states began to struggle with questions like who could collect sales tax on goods sold across state borders in the United States and who should regulate international commerce on the internet. People also became aware of the internet's dark side as the US Congress convened hearings on issues like internet pornography. During this phase, the United States also sought to extend the internet reach internationally, optimistically believing that the spread of this technology would enhance values like freedom of information and democratic governance.

In the third phase, from 2001 until 2012, states became aware of the national security issues associated with this technology. In the aftermath of the 9/11 terrorist attacks, the US security community became aware that the internet could be used by extremist groups for organizing, recruiting members, and sharing information. This era also saw significant advances in the development of strategic military doctrines for "fighting in cyberspace." The US military described cyberspace as a "domain" that needed to be protected from enemies and intruders. Policy makers no longer viewed the internet as a utopian world apart that bears no connection to physical space. Analysts stopped describing cyberspace as a "global village," instead describing it as a "virtual battlefield" or arena for conflict.

The final phase that we examine in this work is the era of big data and surveillance, which dates from 2012 until the present day. In the aftermath of Edward Snowden's revelations to the international community about how US intelligence officials were collecting user data in cyberspace, individuals and states became aware of privacy issues and surveillance concerns. People became aware that they had a digital identity intimately connected to their real identity in the physical world. They became aware that users were the product that was being sold in cyberspace. Their data was being collected, analyzed, and packaged to monitor their activities, predict their actions, and manipulate their opinions and even their votes.

Later in this volume, we consider the advent of technologies like artificial intelligence to make some predictions about what the internet of the future might look like and how we as users might interact with it.

THE INFANCY OF THE INTERNET (1963–1984)

In this section, we focus on the theme of **path dependence** (defined later in this section) and built-in constraints. The internet was developed by skilled technical people who had their own values and visions of the internet. However, it was also primarily supported by US government funds, in particular, those of the military. As a result, later critics faulted the internet for being "too American" or "too Western." They stated that the United States has played an outsized role in the conduct and regulation of internet issues today due to advantages that accrued by virtue of the internet's birth in the United States. Some nations have also voiced suspicion of the internet being introduced into their societies, even going so far as to label it a "CIA plot." Here we consider how a technology's history (or birth) affects where it can go in the future and how it is understood by those inside and outside of that birth.

In a recent memoir, retired Air Force General Michael Hayden describes how the internet was built.[4] Today's internet began as a project of the Advanced Research Projects Association (ARPA, which is now the Defense Advanced Research Projects Association, or DARPA), and it was created to solve a particular technical problem. Department of Defense contractors working in the field of computer science wanted to be able to share data with one another simply and efficiently. Before the establishment of network connectivity, all of the contractors could communicate directly with the Department of Defense but not with one another. In attempting to solve this real technical problem, the Department of Defense did not have a grand vision of what would eventually emerge. They never foresaw a time when the technology would be international, available to civilians, or used as a **backbone** for the conduct of activities like e-commerce, e-governance, the dissemination of news, or the posting of social media. Even the internet's planners were unaware of how societies might someday depend on the internet for the provision of essential goods and services, nor were they aware of the vulnerabilities and threats that might surface as the result of this creation.

Hayden argues that people had no idea what they had built.[5] His story thus echoes an earlier story about the first public demonstration of the telegraph in 1844. In demonstrating his invention to members of Congress, Samuel F. B. Morse sent a message from the US Capitol in Washington, DC, to Baltimore, Maryland. The text that he chose was taken from the Bible's Old Testament (Numbers 23:23), and its text was "What hath God Wrought?"[6] Like Hayden, Morse did not foresee precisely what this technology was, how it might be used, or its eventual impact.

The technology that allowed the development of computer connectivity into a network that became the internet was something called packet switching. Packet switching refers to a process by which data is transferred over a connection (first a telephone line using a modem and later a cable). Your data (an e-mail message, a photo, or a social media post) is broken down into many parts, packaged into units called packets, and then transferred over a network that uses network switches or routers. Your data is then reassembled into its final form when it reaches its destination. Your packets are labeled with information that identifies the sender and the recipient address. The network then decides how best (most efficiently and quickly) to send your data on its journey.[7]

Funding for the creation of the network that would carry this data was allocated in 1966, and it was taken from the US Defense Department's Ballistic Missile Defense Program. Today some foreign nations, including US adversaries, believe that because the internet was born in the United States as part of a US Defense Department research project, other nations should be wary of allowing this technology into their societies because the US government may have created this technology to achieve aggressive or belligerent purposes, including destabilizing the governments of adversarial regimes. Most pointedly, in the wake of the 2013 revelations that the US National Security Agency had engaged in spying on US citizens and allies through the internet, Russia's President Vladimir Putin suggested that the US Central Intelligence Agency invented the internet for this purpose.[8]

Work on the internet connectivity project began in 1969, and the original ARPAnet connected four research facilities—the University of California at Los Angeles (UCLA), the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah School of Computing. In the 1970s, the ARPAnet was extended to the East Coast of the United States, and in 1973 it continued to grow, reaching research facilities in Norway and London. Ray Tomlinson invented the technology allowing us to send e-mails in 1971.

At the same time that the internet's physical structure was being created, advances in computing were creating much of the framework for the types of services and features that we see in today's internet. For example, in 1978, scientists developed **asymmetric cryptography** and the Rivest, Shamir, and Adelman (RSA) algorithm. This invention allowed for secure communications between two parties even over a nonsecure communications channel through the use of mathematically linked virtual keys. (This development allowed for the later growth of online services like e-commerce or filling out forms with confidential information.)

In 1984, those parts of ARPAnet that connected military facilities were broken off to create MILNET, which later became the internal Department of Defense "intranet," known as NIPRnet. In 1990, the US military turned over the bulk of the internet to civilian control. The US National Science Foundation, a government agency, became the entity administering the civilian internet that we know and utilize today.

The Birth of Hacking

Although most Americans were not even aware of the internet in the 1970s and 1980s (although many began to join the World Wide Web in the early 1990s), US government officials were already learning about threats that computer connectivity could pose. The well-known computer hacker Kevin Mitnick first achieved notoriety as a high school student in 1979, when he was able to gain unauthorized access to a California company, the Digital Equipment System. Mitnick, who served time in prison for his hacking exploits, and who went on to become an international security consultant, advising others in how to secure their computer systems and information against hacking, utilized **social engineering**, or the use of non-technical means to gain the trust of users in order to "con" them into providing confidential information[9] to convince individuals to provide him with information that allowed him to hack into computer systems without authorization.

And in 1984, the Hollywood movie *War Games* featured the story of a high school student who nearly caused a nuclear war when he accidentally hacked into the computer system belonging to NORAD, the North American Aerospace Defense Command.[10] In his memoir, General Hayden describes how US President Ronald Reagan saw the movie and immediately summoned members of the US defense community to ask them: "How much of this movie is real? Could this happen here?" As a result of events like hacking, the US government began to recognize the security threats posed by computer connectivity, eventually passing the Computer Security Act of 1987 and creating the first Computer Emergency Response Team (CERT) in 1988, to collect information and respond to unauthorized breaches of government computers.

At the same time, as computer connectivity began to grow, the US government moved to implement national standards in areas such as modem speeds so that data could be transferred quickly and efficiently among military and government facilities and academic institutions in the United States and throughout the world.

Path Dependence and the First-Mover Advantage

But why does it matter that internet connectivity technology developed in the United States and not elsewhere, and why does it matter that the initial blueprint for the technology as well as the initial impetus to govern and regulate this technology began in the United States and not elsewhere?

The term *path dependence* describes how technologies can become locked into specific pathways as the result of earlier design decisions. Those who develop new technologies may not even be aware of how their decisions at the early, developmental stages of technology affect how technology develops and looks many years later. In considering how path dependence affected the internet's development, we should remember that the United States was and is a wealthy nation with a highly developed technology sector. As a result, American telephone lines and later cables were quickly able to carry large amounts of data, and few people (except those in highly rural areas) were excluded from participation in the civilian internet as a result of technological shortcomings in America's existing communications infrastructure. In developing this technology, then, American defense planners were not cognizant or responsive to the needs of those in developing countries who might later find it difficult to connect to the internet due to communications shortfalls in their own. Also, America is a capitalist country with a highly developed private sector. As a result, the American internet grew from the bottom up as commercial ISPs were formed and as they engaged in competition with one another to sign up subscribers to the civilian internet. (In contrast, in many developing nations, the internet has grown in a top-down matter at the behest and with the support of government programs, often featuring a newly formed Ministry of Information Technology, which has taken responsibility for this effort.)

Finally, because the internet grew up in the United States, it made sense for American policy makers to set up and fund the structures, like the Internet Society and the Internet Corporation for Assigned Names and Numbers (ICANN), which sought to resolve standards and connectivity issues as the internet proliferated in the United States and later internationally.

The internet thus came to have an "American flavor," as it was associated with and arguably carried the values of the nation in which it was born. In addition, America and American corporations enjoyed what is known as a first-mover advantage. Those actors who are first movers or early entrants to a field can accrue certain advantages over time, from having a significant market share of consumers to helping set the parameters within which later entrants must operate. Here we can think of the first online bookstore, Amazon.com. Being the first in that market allowed Amazon to condition customers to expect to receive goods in a rapid timeframe. Other bookstores that did not have that same capacity eventually went bankrupt. Amazon also captured a significant share of the market for e-readers, and later entrants to that field struggled to keep up and compete with the Amazon Kindle. Thus, Amazon came to control the e-reader market as the result of its first-mover advantage.[11] Many of the corporations that operate in cyberspace today—including Google, Microsoft, eBay, and Amazon—were able to develop a strong brand and significant market share in the United States, which later translated into economic and political power on a global scale.

Today, some nations are critical of America's position as a hegemon or leading player in cyberspace, suggesting that the extension of internet technology to their nations represents a new form of American colonialism. Here it is important to remember the circumstances under which internet technology grew, and how these circumstances both limited and shaped the internet's reach and policies today. Figure 1.1 provides a brief summary of the key events associated with these circumstances.

Timeline: Key Milestones in the History of the Internet

Figure 1.1 The Birth of the Internet

1865	International Telecommunication Union is established to regulate international dimensions of the telegraph industry.
1938	British science fiction author H. G. Wells conceptualizes of a "world brain" in a series of essays about a global encyclopedia.
1962	Central Intelligence Agency Analyst Orrin Clotworthy publishes an internal article that describes a possible future in which computers are linked and ubiquitous.

(*Continued*)

Figure 1.1 (Continued)

1963	Computer scientist J.C.R. Licklider produces memoranda discussing the concept of the "intergalactic computer network." That same year, Licklider comes to head a project at ARPA.
1966	The US Advanced Research Projects Agency funds a project to create a computer network to allow ARPA researchers to share information among themselves quickly.
1969	Work begins on ARPAnet, connecting four West Coast universities: UCLA, Stanford Research Institute, UC Santa Barbara, and University of Utah school of computing.
1970	ARPAnet reaches the US East Coast, at Cambridge, Massachusetts.
1971	Ray Tomlinson creates e-mail technology.
1973	Satellite links allow the US system to connect internationally to Norway and London.
1977	US Senator Abraham Ribicoff introduces the first federal legislation aimed at protecting federal computer systems and defining "computer crimes."
1978	Development of asymmetric cryptography and the RSA algorithm occurs.
1983	Teenage hackers break into several government computers, including a nonclassified computer at the Los Alamos National Lab in New Mexico.
1984	The parts of ARPAnet that connect military facilities are broken off to create MILNET (ARPAnet was decommissioned in 1990).
1985	The US National Science Foundation is tasked with creating a similar network for academic institutions (NSFNET). This later becomes the backbone of the civilian internet.
1986	The Internet Engineering Task Force (IETF) is formed by the US government to develop and promote internet standards.
1987	President Ronald Reagan signs the Computer Security Act of 1987, an attempt to protect federal agency computers.
1988	The first Computer Emergency Response Team (CERT) is created in the United States and serves as a reporting center for computer crimes and security problems.
1989	First large-scale computer "worm" infects 600,000 government computers.

THE PERIOD OF GROWTH AND EARLY REGULATION (1984–2000)

The second phase of the internet's growth is the period of growth and early regulation. This phase proceeded from 1984 until 2000. During this period, the internet spread internationally as well as penetrating households—moving beyond purely academic or think tank usage. In this period, ISPs began providing content, like news, to users—and early types of e-commerce were created. People spoke of "surfing the web" or traveling on the information superhighway.

A key development at this time was segmentation or fragmentation of the internet. Users were able to customize what they saw on the internet, subscribing to feeds about topics of interest and interacting with others with similar interests and values. MIT Media Lab Founder Nicholas Negroponte utilized the phrase "the daily me" to describe how internet users could choose which news stories and new sources they saw. At this point, customization was considered to be a positive development with no downside. Later on, however, this ability to customize one's internet experience would be blamed for the growth of political extremism and polarization, particularly in the United States.

This period also saw the advent of internet censorship and filtering, mostly on a state level. States became aware of how nongovernmental organizations could use the internet to organize and communicate with supporters. They saw how such an organization could prove detrimental to state control of the media and civil society. Thus, 1998 saw the beginning of a large-scale network of state surveillance of citizen activism on the web in Russia, implemented by the Russian FSB, the post-soviet version of the KGB. The law establishing this network of surveillance was officially accepted in Russia in July 2000.[12]

Globalization and the Internet

In considering the internet's development, we can consider the idea of technological momentum. New technologies do not develop in isolation but rather as part of a "large technical system" with both technology and social or human components. These social components may influence how technology develops.[13] In considering the internet's growth, we must consider the political and social climate in which the technology grew. Beginning in the mid-1980s, policy makers and academics began to describe a phenomenon called globalization. As Drezner writes, "Globalization is the cluster of technological, economic and political innovations that have drastically reduced the barriers to economic, political and cultural exchange."[14] As new technological innovations—such as cable television and 24-hour news—made it easier for citizens across the world to receive information about events that were happening, many analysts believed that these events would empower citizens and make it harder for authoritarian regimes to enforce top-down control of their citizens.

Also, with the collapse of the Soviet Union in 1989 and breakup of the Commonwealth of Independent States (CIS) in 1991, and the creation of fifteen new independent countries, Western politicians were euphoric. Policy makers and political analysts stated that the United States had won the Cold War against the Soviet Union and that the Soviet Union's abandonment of the economic system of communism showed that capitalism and democracy were triumphing everywhere in the world. An influential essay called "The End of History and the Last Man" by former Reagan policy adviser Francis Fukuyama, published in 1989,[15] reflected this worldview. Fukuyama argued that modernization was an inevitable process and that forces like globalization were allowing ideas to move through the world faster than ever before, leading to the breakdown of government control and the ultimate triumph of democracy, capitalism, and globalized institutions. As a result, he and others believed that modernizing nations would end up looking similar. To participate in a global economy, for example, states would find themselves adopting policies regarding monetary policy, regulation of utilities, and citizen rights that would look similar. They would also create similar structures and processes. The term *convergence* was utilized to describe this tendency.[16]

Thus, the internet's growth was embedded in larger forces like globalization, free trade, and the growth of markets, and it, therefore, seemed logical to envision the internet as an agent of that change. Both President Clinton and Vice President Al Gore spoke about the internet as a vehicle for the export of American ideas like democracy, freedom of information, and freedom of assembly. Policy makers utilized utopian language in describing how the internet could further equality between citizens and nations and further education internationally through making content available to users. They envisioned the United States playing a leading role in extending the internet's reach globally by offering both foreign aid and opportunities provided by US commercial interests internationally. The Clinton administration described how the US government would work to bridge what was termed the "digital divide," which separated developing nations from the promise of prosperity and education through a lack of the infrastructure necessary to connect to the internet.[17]

Internet enthusiasts spoke of a "global village" (or global commons) in which citizens might identify not as members of a particular nation but rather as "netizens" who lived in a world of cyberspace, which was borderless and open to all.[18] Also, at this time, most analysts believed that the norms that would exist in cyberspace would be a product of the internet environment, which was still mainly conceptualized as space apart from traditional governments and government structures. That is, people did not believe or speak of "Russian cyberspace" or "American cyberspace." They did not conceptualize of a future in which states might clash in cyberspace, and they did not imagine that states might someday differ about which nation's norms should prevail in cyberspace.

However, at the same time, states like Russia and China, which had been characterized by tight state control over media, struggled with how to grapple with new phenomena like multiple independent news sources. Although Russia, in particular, had passed a media law in 1991 that allowed for the growth and creation of new, privately owned media outlets—rather than exclusively state-owned and -run enterprises—the transition to a free press had not been problem free. Independent media outlets were credited with playing a vital role in the opposition to a KGB-backed coup attempt in 1991, which led ultimately to the downfall of the Commonwealth of Independent States (CIS) and the extension of freedom to fifteen former Soviet republics. As we will see, throughout the 2000s, Russia began implementing a series of laws aimed at regulating independent activity in the "blogosphere," including extending existing legislation regarding libel and slander of individuals and public officials to blogs and other forms of informal media. In addition, they implemented measures requiring bloggers to register as journalists and eventually began banning certain types of online media outlets on the grounds that they were contributing to the growth of extremism (both nationalist and Islamic terrorism) in Russia.[19]

Thus, we can see how the internet came to be seen not as a "world apart" but rather an extension of existing physical spaces such as the media space, the legal space, and the economic space within nations. Despite its utopian origins, over time, it came to be regarded not as a separate, independently existing entity that did not conform to the constraints of the real physical world but rather as a technology that was born into a real-world environment and that would need to conform to that environment.

The Advent of E-Commerce

One way in which the real, physical world and the virtual world of the internet came together was through the advent of e-commerce, or online shopping. Many consumers today can scarcely imagine a world without e-commerce. However, when e-commerce arrived on the scene in the late 1990s, online shopping was a fundamentally new idea. It was seen as fraught with risk. Consumers struggled with whether to trust new online entities that did not have an established reputation and with which they did not have an existing history. How could they feel that their money was safe, that they would receive the goods that they had ordered, and that they would be satisfied with these goods? Initially, many consumers were uncomfortable giving personal information to a website and also did not trust websites to recommend additional products or services to them.[20] Consumers were uniformly confused by new business models like eBay, which required them to bid on goods or services and to carry out calculations that asked them to consider the probability that they would win an auction versus the risk that they might lose through being outbid. Also, particularly in the developing world, people often had a preexisting cultural inclination to wish to do business with vendors whom they knew personally or to physically feel and hold the garments or goods that they wished to purchase.

In addition, early e-consumers encountered technological barriers to engaging in online shopping such as low bandwidth, which caused pages to load slowly, or for connections to be dropped during the transaction. At the same time, e-commerce's advent required changes in many other industries—from banking systems that needed to develop protocols for tracking and clearing large numbers of international payments to legal regimes for carrying out online dispute resolution (ODR) between consumers and companies when there was a disagreement about goods or services rendered or ordered online.[21]

Like many novel or emerging technologies, e-commerce spawned many social, political, and economic developments, many of which were unexpected. Developing e-commerce could often require less of an initial investment than starting a bricks-and-mortar business did because one did not need to buy real estate for a showroom or a warehouse, as goods could often be shipped straight from the factory to a consumer. Therefore, economists expected that it would lead to a democratization of the marketplace and the growth of entrepreneurship. However, the first-mover advantage allowed for extremely large-scale marketplaces like Amazon.com in the West and Alibaba in China to capture a significant market share through investing in and patenting online commerce technologies.[22] In addition, online commerce has in some cases helped cause the bankruptcies of established physical store chains in the United States and abroad. Also, even now, many sectors of the world—including the Caribbean and Africa—are missing out on the economic advantages of participation in e-commerce due to lagging physical infrastructure and a less-educated workforce.[23]

Finally, whereas in the West, e-commerce giants like Amazon seem to function mainly as independent retailers who are free of government regulations and ties, Alibaba, the largest e-retailer in China, actually works quite closely with the Chinese government, sharing information about consumers and purchasers and benefitting from advantages conferred to it in the economic sector.[24] Today, some analysts argue that the international and regional competition for market shares between e-commerce giants such as Amazon and Alibaba is a new type of warfare, leading to increased conflicts in the international system rather than a new era of international prosperity as first promised.[25]

The Growth of Off-Shoring

As this period drew to a close, it was clear that despite its promise as a great leveler, enabling people throughout the world to have free access to information and education, the internet was not achieving this goal. Instead, critics argued that internet technology increased inequalities in the international system. They pointed to corporate decisions in the United States and Western Europe to outsource jobs to remote contractors located in developing countries. Beginning in the late 1990s, American and international corporations like Texas Instruments, American Express, and British Airways established remote call centers that took orders, made reservations, or provided technical support.[26] These centers, which utilized modern telephone and internet technology, were in nations like India, where wages were low and worker protection laws were less developed. "Off-shoring" refers to moving an activity that is produced within the firm to another country so that the activity is still associated with the same firm but performed elsewhere.[27] Trade economists argued that corporations' ability to outsource functions over the internet made it harder for skilled workers unions in the United States and Western Europe to bargain for favorable terms. If they asked for too much, the company might decide to take its business elsewhere. Simultaneously, internet technology was making individual workers more productive, which sometimes meant that corporations decided to employ fewer workers. The internet, combined with globalization, was thus implicated in the creation of precariousness or economic instability.[28] Workers worried that they could be replaced by someone in another country and eventually by a machine.

Critics also pointed to the wealth amassed by entrepreneurs like Mark Zuckerberg, the founder of Facebook, and Bill Gates, Microsoft's founder. Critics began to worry about the outsized influence of a global super-elite, especially because these individuals had not been elected and were not accountable to citizens in the same way that elected officials were. Critics worried about agreements being made between individual entrepreneurs and global states that might have repercussions on a state's citizens in ways that were opaque and lacked transparency. Comparisons were made to the so-called robber barons, the early 19th-century capitalists like Commodore Vanderbilt, Andrew Carnegie, and J. Paul Getty, who amassed fortunes while building American infrastructure in industries like railroads and manufacturing.[29]

Privatization of the Internet

Much of the initial impetus for the internet's creation came through the aegis of the US government. However, in this second period of the internet's growth, many actors participating in creating the internet's infrastructure—both the physical infrastructure or hardware as well as the internal infrastructure, known as software or code—were private corporations. That is, individual enterpreneurs created the internet's "architecture," from the search engines that allowed users to find what they wanted on the web to the sites, like eBay and Amazon, that they most wanted to reach.

One of the significant advances at this time was the advent of commercial search engines, like Google, WebCrawler, and Yahoo.[30] Prior to their invention, users could only find pages online if they knew the **Internet Protocol (IP) address** or the specific web address of another user. But in 1996, Stanford students Larry Page and Sergei Brin created a proprietary algorithm to rank and classify web pages. In essence, a page that was linked to many other pages was seen as being more important and credible than one that few other pages linked to. Therefore, the page with the highest number of links to it would appear first in a Google search. This algorithm, known as Google, was available to internet users for free but was financed through the sale of advertising links that appeared alongside web searches. Also, companies could pay to be a sponsored link, which would appear in a list of links called up through a web search.[31]

By 2006, policy makers were raising concerns about how private companies like Google could influence what information users saw. In countries like Germany, where strict laws adopted after the rise of the Nazi Party in World War Two prevent citizens from accessing neo-Nazi propaganda and neo-Nazi websites, policy makers expressed concern about materials that their citizens could access through a Google search. Google began asking questions internally about what its corporate foreign policy should be. Should this company always seek to cooperate with the national leadership in nations where citizens used Google? Alternatively, should Google, as a company that began in America, always seek to promote freedom of speech?[32] How should Google work with leaders in nations like China, which might ask it to engage in repression of information that Chinese citizens might desire? And as Google began to develop services like Google Earth, which allowed citizens to see satellite maps of locations across the world, it began to ask questions about its responsibility as a purveyor of security. Should Google comply with US requests not to offer users printouts that might reveal the location of military bases or troops?

In the aftermath of the US 2016 presidential elections, policy makers are still grappling with these complicated issues. Congresspeople in the United States have asked whether Google is complicit in suppressing some types of news and information, and promoting other types of news and information, in instances where doing so may have altered people's votes. Similarly, some critics of private information sites like GreatSchools.net have asked if this platform's activity—making information about factors like the demographic and racial makeup of public schools in the United States—is actually leading to increased educational segregation as some families are using the information available to choose schools that are highly racially segregated. Is it enough for a website to claim that it is merely making a service available that people desire, or should it be required to buy into a particular set of social values? Should it have to consider possible social or political effects of providing a service?[33]

Finally, states are becoming aware of how they and their citizens are vulnerable when states do not control many aspects of today's internet directly themselves—from the building of physical infrastructure like data pipelines (the vast majority of which are privately owned and administered)[34] to the creation of the software that runs critical infrastructure like roads, bridges, and hospital records. To what degree should states be allowed to dictate how private businesses run their activities, mainly when these activities may have implications for a state's national security?

As noted earlier, rapid technological changes throughout the internet era mean that often legislation and the ability to regulate technologies lags far behind the technology itself. These issues, which first came to the forefront in the late 1990s, are far from resolved, even today.

The Issue of Intellectual Property

Just as the media community was struggling to integrate new types of media—like newsfeeds and blogs—into its space, and economists were struggling with how to regulate and structure e-commerce, the legal community was asking questions about how intellectual property rights apply online. Whereas initial internet "evangelists" believed that everything that resided on the internet should be free to everyone, over time, the notion that online information could be owned and sold gained strength. Media organizations erected paywalls and asked users to pay for content access, and groups like the World Intellectual Property Organization

(WIPO) worked to implement penalties for individuals and corporations trafficking online in stolen intellectual property—including movies, music, and books and manuscripts. WIPO defines **intellectual property** as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names, and images used in commerce."

However, the fact that files (including music, videos, and text) could easily and quickly be cloned or copied online meant that it was increasingly difficult for the creators of intellectual property to retain the rights to their materials. The advent of peer-to-peer network sharing programs like Napster also made it easier for users to directly connect to one another to share copies of materials off of their home computers without having to pass the material first through a central site or clearinghouse. As a result, in 1993, the US government set up the Working Group on Intellectual Property Rights to examine how legal concepts regarding the ownership of ideas and creative materials might be applied to what they termed the *National Information Infrastructure*.[35]

By the late 1990s, the US government had labeled groups like Napster (1999–2001) as "online pirates," and US legal cases sought to shut down websites that served as clearinghouses for **online piracy** activities. The Digital Millennium Copyright Law went into force in 1998. However, even today, not all nations agree with the notion that intellectual property laws apply the same way in cyberspace as they do in real-life situations, and not all agree that there should be a universal norm against pirating intellectual property online. Instead, they argue, the prohibition on network file sharing is an American norm that US and Western corporations are attempting to impose on those in the developing world who may struggle to afford access to Western publications and ideas.

States also began to realize that their national economies were becoming dependent on the internet, with the 2000 G8 Charter on the Global Information Society describing information technology as "a vital engine of growth for the world economy." The internet thus was no longer regarded as an organic entity that could be said to be "evolving" but instead began to be perceived as an extension of a state's physical space and economic, social, and military power in the world.

Policy makers and investors also worried that governments around the world, including in the United States, might not be sufficiently well equipped to face new developing problems in cyberspace, including the growth of viruses and hacking attacks on US institutions and businesses. At the same time, they became aware of the existence of cybercrimes, including the transmission of online pornography. The United States began considering how to regulate the "dark side" of the internet with the first hearings on online pornography called by the US Congress in 1995.[36] The Clinton administration also released the first American cybersecurity strategy in 2000.

And as the internet became more international in character, with Beijing joining the internet revolution and companies like eBay and Amazon becoming established, states within the international system also began to consider whether international structures were necessary to regulate and administer the internet. Here, the United States, as the founder and creator of the internet, still played a leading role. The United States worked to establish the Internet Corporation for Assigned Names and Numbers (ICANN), which although housed in the United States and funded through the Department of Commerce, in fact managed the allocation of IP addresses for organizations and individuals throughout the world, with the monetary proceedings going to the United States.

As this period of growth and change in cyberspace draws to a close, the first issues of economic volatility in cyberspace are becoming apparent. Although investors were initially euphoric about the growth of e-commerce, by 2000, it became apparent that many internet stocks were overvalued. Many internet companies went bankrupt, leading to the end of the dot-com "bubble" in 2000.

Figure 1.2 Timeline Phase Two: The Growth of Internet Threat and Regulation

1990	Englishman Tim Berners-Lee merges hypertext and browsing functionality to create the World Wide Web.
1992	**Governance:** • Fifty countries have access to the internet. • Ebone, a European version of the NSFNET backbone in the United States, is established. • The Internet Society (ISOC) is founded, with a mission to "assure the open development, evolution, and use of the Internet for the benefit of all people throughout the world."
1993	Mosaic, an early web browser, is created.
1994	**Cybersecurity:** • The first commercial spam is released. **E-Commerce:** • Amazon is established as an online retailer. • Beijing connects to the internet through CAINONET.
1995	**Governance:** • NSFNET ceases to be administered by the National Science Foundation and instead becomes public property. **Regulation:** • US Congress proposes first legislation aimed at regulating online pornography, including protecting children. **E-Commerce and Social Media:** • The first use of a webcam occurs. • The first item is sold on eBay. • MIT Media Lab Founder Nicholas Negroponte uses the term *the daily me* to refer to internet users' ability to receive a daily customized newsfeed tailored to their interests. **Cybersecurity:** • The US military begins to develop and define the doctrine of asymmetric warfare.

1996	**Cybersecurity:** • The first act of online piracy occurs (Metallica's "Until it Sleeps" becomes the first pirated track). • Russia opens an internet café.
1997	**Social Media:** The first social media (sixdegrees.com) is developed. The term *weblog* (later shortened to *blog*) is first used.
1998	**Censorship:** • China begins creating a filtering, censorship, and surveillance system that comes to be known as the Great Firewall of China. • Russia's internal security bureau begins establishing the system of state-run surveillance of electronic media and communications known as "SORM." **Governance:** • ICANN, a California nonprofit, is established by the US government and awarded a contract by the US Department of Commerce to administer the distribution of domain names in cyberspace. • Digital Millennium Copyright Law passes in the United States. **Cybersecurity:** • President Clinton introduces Presidential Directive PDD63, which defines and calls attention to critical infrastructure protection. • The US government creates the federal Computer Incident Response Center (US-CERT).
1999	**Intellectual Property:** • Napster's peer-to-peer network for file sharing begins. **Cybersecurity:** • Nations undertake extensive preparations for the Y2K problem, which does not materialize. **E-Commerce:** • China implements regulations limiting foreign capital investment in internet startups in China.
2000	**Cybersecurity:** • First large-scale cyberattacks: Distributed Denial of Service (DDOS) Attacks and "I love you" virus hit sites in the United States and internationally. • The US Congress convenes hearings about cybersecurity, and President Clinton releases cybersecurity strategy. **Governance:** • The United States joins Council of European Cybercrime Treaty to address issues of prosecution and jurisdiction for cybercrime and cybervandalism. • G8 adopts Charter on the Global Information Society. **E-Commerce:** • Dotcom "bubble" bursts with NASDAQ falling from 5,000 to 2,000 points.

THE SECURITIZATION AND MILITARIZATION OF CYBERSPACE (2000–2012)

The next period in the internet's development, the securitization of cyberspace and the growth of internet governance, spans the period from 2000 until 2012. At this time, states began speaking of the internet as part of their "strategic terrain," utilizing military language to speak about cyberspace as an extension of their physical territory. Policy makers also began to speak of **cyber sovereignty** as policy makers and citizens increasingly accepted the notion that one could identify American, Russian, and Chinese cyberspace. States also became aware of the vulnerabilities created by their dependence on the internet—for commerce, social communications, and military use. At the same time, international organizations developed for the governance of the internet, resolving physical problems that occurred such as how new undersea cables would be built and regulated and how new domain names would be assigned.

Following the terrorist attacks on the United States on September 11, 2001, a sea change took place as a sense of pessimism and threat replaced much of the initial optimism generated by the internet's founders. Many of the internet's features that had initially been seen as exciting and liberating—such as the ability to browse and participate in forums anonymously, the speed at which activities occur on the internet, and the ability of the internet to carry large volumes of information of uncertain or unregulated quality—came instead to be seen as liabilities.

The term **attribution problem** describes the difficulties that cybersecurity experts encountered in trying to trace a virus, worm, or another weapon back to its source to identify and sanction the hacker. The advent in 2002 of TOR, a program that internet users could use to disguise their IP addresses so that they could not be traced back to their online postings, activities, or attacks, made attribution particularly tricky.

Policy makers became aware of the many different types of vulnerabilities that our national computer systems were threatened by. Although some of these attacks might be regarded as merely nuisance behavior, the most significant attacks have the ability to paralyze a nation's economy (through an attack on the financial sector); to destabilize the transportation routes that carry food to, from, and throughout a nation; or to cause mass casualties through scenarios like an attack on a hospital that forbids health-care workers to access patient data or an attack on a nuclear power facility or hydroelectric dam. A report by the White House Council of Economic Advisors notes that currently, cyberattacks cost the US economy somewhere between $57 billion to $109 billion a year.[37] At the same time, they can have grave political effects—leading to rising tensions among the United States, its adversaries, and even its allies.

Beginning with 9/11, policy makers in the United States and abroad became aware of the ways in which national security systems were vulnerable as well as the fact that so many activities of daily life were now dependent upon access to internet technology. The term *critical infrastructure* was coined to describe all of the structures within a nation—from the agricultural sector to the carrying out of water and sewage treatment, to the running of transportation activities within a nation—that citizens count on their nation to be able to provide. And as a result of the 9/11 attacks on the United States, the first domestic attacks within the United States since Pearl Harbor in 1941, planners and policy makers within the United States became aware of the possibility that an adversary could attack these structures, causing significant damage and perhaps widespread panic to the US political, social, and economic systems.

Thus, the result of widespread internet penetration into nearly every sector of society has resulted in a paradoxical situation: Using the internet has made nations more productive and prosperous and has created unprecedented opportunities for citizens. However, the fact that individuals, corporations, and nations now rely on the internet to support so many of their traditional functions—from law enforcement to education to military warfighting—means that everyone now is also dependent on this technology and therefore vulnerable if the technology should fail.

On an international level, the international system is more connected than ever before—which presents opportunities for increased cooperation between states—but our international system is also more vulnerable due to the numbers of ways in which states and their people now interact both formally and informally. In many Western nations, citizens have become concerned about what they perceived as an increased amount of government surveillance of their activities and their lives. They have begun to voice concerns about actions by groups like the US National Security Agency, which has been capturing and storing data about American citizens' web searches, posts, and online activities to combat terrorism both domestically and abroad. In recent years, we have also seen data breaches in which state-sponsored and individual hackers have electronically broken into the computers of corporations and government agencies, releasing people's highly personal data. In some instances, individuals have been merely embarrassed, whereas in other instances they have experienced long-range financial hardships as the result of identity thefts. Law enforcement agencies have expressed concern about the so-called dark web, untraceable and hidden computer networks that harbor "black markets" where users can purchase illegal drugs and computer viruses or even order a service like an assassination. National security professionals also warn that unsavory groups, from white nationalists to neo-Nazis to terrorists, have mastered techniques to utilize the internet to organize, share information, and even recruit new members.

Militarizing the Internet

Particularly in the wake of the 9/11 terrorist attacks on the United States, optimism about the potential of the internet to create world peace and prosperity was replaced by cynicism. As Manjikian writes, "Realists saw cyberspace as an avenue for insurgents and national enemies to penetrate 'real' defenses. It was viewed as a frontier or border requiring protection and vigilance in contrast to less strategically significant territory."[38]

Indeed, as early as 1976, Boeing engineer Thomas Rona coined the phrase **information warfare,** describing the dangers presented by US dependency on information capabilities as a function of logistics in the conduct of warfare.[39] In this view, the internet is merely an extension of existing spaces (like radio waves) in which military personnel carry out electronic warfare or information warfare. The term *electronic warfare* refers here to all types of warfare in which one side targets the communications systems of others—whether by jamming or scrambling a radio signal, attempting to disrupt a satellite signal, or targeting another side's ability to access or utilize the internet.[40]

Moreover, in the aftermath of terrorist attacks against the United States, counterterrorism experts began to consider how terrorist groups could utilize the internet to organize or to launch attacks against developed nations that were increasingly coming to rely on the internet to carry out activities in political, economic, and social spheres. In 2004, terrorist analyst Marc Sageman described how terrorist groups were using cyberspace to organize. In his work, he described the internet not as space that was free and common to all but rather as a "failed space" that was anarchic, lacking a strong governing and regulating structure that was necessary to keep it safe.[41] The phrase "Cyber Pearl Harbor" was coined to describe the possibility that the United States might be taken by surprise by a large-scale cyberattack for which they were unprepared.

Features previously associated with media democratization and the growth of civil society—such as the ability of anyone to access the internet and to set up a site where they could share their ideas and perspectives cheaply and easily—began to be viewed differently. Analysts warned of asymmetric warfare, referring to "engagement between dissimilar forces" characterized often by the use of unconventional means of warfare and the element of surprise. US military doctrine experts had begun speaking of asymmetric warfare as early as 1995.[42] However, in the aftermath of 9/11, the concept received renewed attention, with particular reference to how terrorists engaged in asymmetric warfare, including through the use of social media and internet communications.

The US Cyber Command

As a result, beginning in 2002, the US military began to develop doctrines or plans for fighting in cyberspace, including the conduct of offensive cyber operations. Here, it was acknowledged that each state should seek "information dominance," or the ability to be the most technologically advanced, with the best ability to understand the cyberspace environment and to respond quickly to events occurring there. In 2006, the US government took the first steps toward the establishment of the US Cyber Command, which would be tasked explicitly with defending the "cyber domain."

The newest command, USCYBERCOM, was established in 2009. Its mission is to defend the Department of Defense's information networks (sometimes referred to as the DODIN) and to carry out both offensive (active) and defensive (passive) cyber operations. It also sets policies regarding US cyberspace strategy and has legal experts who work to reconcile existing legal understandings (including International Humanitarian Law and the Law of Armed Conflict) with the specific issues that may arise in an online environment. Finally, it plans for the creation of new cyberweapons and works to integrate cyberweapons policies with defense policies in other areas, including the use and deployment of conventional forces. USCYBERCOM is headquartered at Ft. Meade, Maryland, adjacent to the US National Security Agency.

Figure 1.3 Timeline Phase Three: Securitization of Cyberspace and the Growth of Internet Governance

2001	• President George Bush creates President's Critical Infrastructure Protection Board, to develop a national cybersecurity strategy. • First White House cybersecurity adviser is appointed. • Phrase "Cyber Pearl Harbor" is first used. • Internet Telecommunication Union proposes to United Nations the first World Summit on the Information Society (to be held in 2003 and 2005). • The Shanghai Cooperation Organization, a Eurasian political, economic, and security alliance that includes China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan, is created.
2002	**Cybersecurity and Cybercrime:** • BitTorrent, a tool used for pirating video and other types of media, is created. • President Bush publishes National Security Presidential Directive (NSPD) 16 on offensive cyber operations. **Social Media and E-Commerce:** • Wikipedia, the world's first online encyclopedia, which can be written and edited by anyone, is created. • iTunes is created. **Governance:** • The International Telecommunication Union, now part of the United Nations, proposes holding the first World Summit on the Information Society, leading to summits in 2003 and 2005. • Researcher Tim Wu coins term *net neutrality.* • Google's subsidiary in Hong Kong provides information about online activities by two Chinese political dissidents to the Chinese government.
2003	**Cybersecurity and Cybercrime:** • White House issues its first cybersecurity plan. • The United States houses many cybersecurity functions in the newly created Department of Homeland Security. • The public release of TOR, anonymizing software, occurs.

(*Continued*)

Figure 1.3 (Continued)

2004	**Social Media:** • Facebook is created. **Cybersecurity and Cybercrime:** • The Budapest Convention on Cybercrime is the first international treaty to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Participants include the Council of Europe members as well as observer states Canada, Japan, Philippines, South Africa, and the United States.
2005	**Governance:** • The United Nations of Internet Governance Forum, a dialogue group for stakeholders in internet governance, is created to establish terms and concepts.
2006	**Social Media:** • WikiLeaks is established as an international space for governmental whistle-blowing. • Twitter is created. **Governance:** • The US State Department establishes the Global Internet Freedom Task Force to monitor internet freedom worldwide, to respond to challenges on the internet, and to advance internet freedom through financial and technology support. **Censorship:** • Russia adopts a law that broadens the definition of extremist activity to include criticism of public officials, including in social media or online platforms. • Google establishes Google.cn—a filtered search engine for users in China.
2007	**Cybersecurity:** • Russia conducts international cyberwar against Estonia. • The *US Army and Marine Corps Counterinsurgency Manual* describes cyberspace as a "virtual sanctuary" for terrorists and criminals. **E-Commerce:** • Amazon invents the Kindle e-reader.
2008	**Governance:** • The first cloud computing technology is released. • Representatives from Google, Yahoo, Microsoft, and Cisco are asked to testify before the Senate Committee on the Judiciary. They are accused of helping China's government violate its citizens' human rights. **Cybersecurity:** • Russia conducts international cyberwar against Georgia.

2009	**E-Commerce and Cryptocurrency:** • The first Bitcoins are mined. **Cybersecurity:** • The US Cyber Command is created as a US military entity charged with conducting offensive and defensive cyber operations.
2010	**Governance:** • The first Cyrillic domain is created, ending the monopoly of Latin characters on the internet. **Cybersecurity:** • Evidence is uncovered that US intelligence agencies have deployed the Stuxnet virus against Iran to damage its nuclear program. • The US government crafts the National Cyber Incident Response Plan. **Social Media:** • The Arab Spring begins throughout the Middle East and North Africa. Many analysts credit social media as a driving force behind the events that destabilize and replace governments throughout the region.
2011	**Cybersecurity:** • The North Atlantic Treaty Organization (NATO) defines the concept of "hybrid warfare."
2012	**Cybersecurity:** • The Shamoon virus wipes out the computer system of Saudi Aramco, a major oil company located in Saudi Arabia. The virus is traced back to Iran. **Governance:** • Russian President Putin is reelected and puts into place a blacklist of banned websites in Russia. • The International Telecommunication Union facilitates the World Conference on International Telecommunications 2012 (WCIT-12) in Dubai. WCIT-12 is a treaty-level conference to address international telecommunications regulations and international rules for telecommunications, including international tariffs. • The US government drafts legislation opposing US participation in the WCIT treaty.

THE ERA OF SURVEILLANCE AND BIG DATA (2008–PRESENT)

In this final phase, we focus on developments from 2013, when the Snowden revelations about National Security Agency spying on the internet became public, until the present day. Some of the major issues that have emerged during this last period include issues of privacy and data sovereignty or data governance. In short, many internet users became aware that they themselves were the product being produced and sold on the internet because each user creates a profile of himself or herself as he or she uploads information, creates information, and searches for information online. In the aftermath of the 2016 US presidential election, citizens also became aware that websites and search engines had begun selling access to that data, including selling targeted ads that only some subsets of users would see based on user characteristics.

During this period, then, many states, including the European Union, took steps in the aftermath of the Snowden revelations to safeguard their citizens' data online. This often meant passing legislation mandating that data produced by European citizens within Europe be housed and stored within Europe and not shared with those outside of Europe without the knowledge and permission of the users themselves.

In considering how citizens themselves had become the product, states and citizens also became aware of the large role that private corporations like Google, Facebook, and WikiLeaks had come to play in politics, both on a national and a global level. Thus, many nations, including the United States, convened congressional and parliamentary hearings aimed at better understanding and regulating the role played by private actors in national and international affairs. During these hearings, observers also became aware that a private person like Mark Zuckerberg, the founder of Facebook, is not as accountable to American citizens as an elected official might be. His actions may be less transparent, and he may not conceptualize his personal role or the role of his corporation in relation to goals like preserving American democracy in the same way that an elected official might.

During this period, pundits and analysts also began asking some variant of the question "Can the internet be saved?" Here, they were asking if those who use the internet could still be said to have a role in steering the internet or weighing in on what this technology should and should not be used for. In 2014, one of the internet's original founders, Tim Berners-Lee, proposed the adoption of a Magna Carta for the internet, echoing earlier rhetoric about a Declaration of Independence for the internet.[43] Although these issues are far from resolved, it is important to consider the events of this last period to understand how we have arrived at the present moment.

At the same time, new technological developments—such as the advent of social media like Facebook and Twitter—were also drawing the world closer together. Here social media is defined as "any electronic medium where users may create, share or view user-generated content which can include videos, photographs, speech or sound."[44] The state began to seem like a porous entity that national governments could not completely control. Analysts pointed to the role that these technologies played in the so-called Arab Spring in 2010 as well as in protests in Iran and Moldova in 2009 and in the United States during the 2009 G-20 summit and Occupy movements.[45] In response to mounting protests, some governments, like the government of Egypt, have ordered cell phone providers in their nations to shut down service so that people can no longer access social media.[46]

However, at this time, analysts were also starting to voice concerns about the ways in which internet media was being used by consumers who were learning to "curate" their own news and information. By the mid-2000s, blogging was a feature of American life, with individuals subscribing to and visiting blogs about issues of importance to them from lifestyles (like dating or having children) to politics and economics. The growth of services like the AdSense advertising platform enabled individuals to make money through selling access to their readers to advertisers who placed ads on their blog platforms.[47] Although consumers appreciated the ability to hone in on the information most important to them, academic Cass Sunstein began voicing concerns about the ways in which individuals now had the ability to "consume only content which aligns with our beliefs."[48] He warned that individuals were now able to "isolate ourselves in ideological and partisan enclaves" in which we were not challenged to understand others' perspectives or indeed to even encounter facts that might conflict with pre-established worldviews. In this way, he argued, online media tended not to change individuals' minds as they learned more about the topic but rather to reinforce their preexisting prejudices and subjective biases that they might bring to their exploration of a topic online. Here, he noted that search engines like Google were implicated in this process through a mechanism by which Google's artificial intelligence programs learned which types of news you liked and then proceeded to show you more of it. In this way, search engines engaged in a type of censorship, shielding readers from ideas that they might find to be harmful or distressing rather than exposing them to a full range of views on a subject.[49]

Political scientists noted a polarization of the American electorate, describing the fact that individuals often did not interact with others who had different ideological views online or that when they did interact, interactions sometimes became hostile or abusive. Political scientists note that the degree of distance between the attitudes of Democratic and Republican voters on a variety of social issues became significantly larger beginning in 2002 or 2003, at the same time that social media and social media segmentation became common among internet users.[50]

The End of American Hegemony?

The sense of animosity that many nations felt toward the United States in particular—due to its behaving as a sort of internet hegemon with a preponderance of power and rule-making ability within the international community—was exacerbated with the revelations by Edward Snowden in 2013. (A hegemon is an actor that exercises a preponderance of power within a system, with the result that this actor acts as a leader, influencing other actors as well as the structure of the system itself.)[51]

Edward Snowden, an American computer scientist working on contracts with the US National Security Agency and the US Central Intelligence Agency, became aware that in the aftermath of 9/11, the US government had begun engaging in large-scale surveillance and data collection. In particular, these agencies were utilizing computer programs that allowed them to scan and store users' e-mails as well as information about the people and organizations with which they were interacting in cyberspace. The National Security Agency was accused of having spied on American citizens both at home and abroad as well as on both private citizens and public figures internationally. They were found to have hacked into phone records and conversations as well as electronic communications of individuals working at the United Nations and individuals like German Chancellor Angela Merkel.

Although the US government claimed that these types of surveillance were a necessary part of its counterterrorism activities and that it was necessary to monitor suspected terrorists to keep America safe, other nations reacted by accusing the United States of hypocrisy in its foreign policy and cybersecurity policies. Although America had claimed to be an avid supporter of internet freedom, they claimed, in reality it had engaged in the sorts of activities typically undertaken by authoritarian regimes. Snowden, who sought and received political asylum in Russia, has remained a firm critic of US surveillance policies.

At this point, many of the related international policy arguments about the internet were not focused so much on the specifics of how the international cyberspace architecture might look and function. Rather, they focused on the newly emerging idea that data (both individual data and large-scale data sets that showed how people behaved in cyberspace) was a vital resource. Most internet users did not understand the economics behind the internet, nor had they thought much about how it was that services like Twitter or Facebook were available to them for free. They were also unaware of the ways in which their online activities could be tracked or the types of data that they were producing by browsing, shopping online, or logging activities like going for a run. That is, they were unaware that they were producing a digital footprint, which is defined as "a combination of activities and behavior when the entity under consideration (a person or something else) is acting in the digital environment." These may be log-on or -off records, addresses of visited web pages, open or developed files, e-mail, or chat records.[52]

At this point, computer users were only starting to become aware of the phenomenon of ubiquitous computing, which is defined as "the practice of embedding technology within everyday objects so that they can store and collect data, sharing it with other objects within the Internet of Things to which they are connected."[53] That is, users didn't always realize that they were producing data streams due to signals being emitted and stored from objects like cell phones that they carried while driving, shopping, or engaging in physical activity.

If users didn't know they were producing all of this information, they were also unaware that companies like Facebook were collecting this information, storing it, and selling it to other entities—like companies that might decide to target you with advertising for a specific product based on your digital footprint. Advertisers began to state that "data is the new oil" because it was a resource produced by users that once unearthed, had value. It could be exploited, stored, or traded to others for a price.

In this way, the Snowden revelations showed computer users just how little online privacy they actually had. They also showed how the internet had changed since its inception. Whereas in the 1990s users may have had a reasonable expectation of anonymity and privacy when they went online to participate in conversations or to search for information, the advent of more sophisticated ways of collecting and tracking data (including the use of facial recognition software in social media sites like Facebook), as well as aggregating data from multiple data streams, meant that corporations and advertisers as well as the government often knew a great deal more about individual users than they might have suspected.[54] Writing in 2012, philosopher Danah Boyd described the advent of **big data**, or the ways in which researchers were able to search, aggregate, and cross-reference large data sets (such as all of the messages sent on a particular topic on Twitter during a particular day).[55]

Users were similarly unaware of the extent to which artificial intelligence was used to analyze data about citizens and to make decisions that affected them as a result. Corporations and state entities were able to deploy artificially intelligent agents or bots to run programs—called **algorithms**—which sought to analyze and identify patterns in user data and as a result to arrive at statistical generalizations about groups of users. For example, a bank might use an artificially intelligent agent to decide whether or not you were a good credit risk, affecting your ability to purchase a home or automobile. An employer might also use intelligent agents to sort through résumés and decide which individuals should be interviewed for a job opening.[56]

By the mid-2010s, analysts and policy makers were beginning to query the extent to which algorithms had begun to govern citizens' daily lives. Professional groups like the Association for Computing Machinery (ACM) acknowledged that such algorithms often reflected the inherent, even unconscious, biases of their creators—or biases that existed within society.[57] (For example, an artificially intelligent program might conclude that only women can be secretaries or nurses because most images found in Google Images of secretaries and nurses are female.) Thus, they called for greater transparency and accountability in how algorithms were utilized and deployed. At this point, new regulations began to be passed regarding the preservation of user privacy. In particular, the Council of Europe passed the Directive on Privacy and Electronic Communications (E-Privacy Directive), which required that citizens be informed of situations in which their data was being collected (such as browsing a website) and that they confirmed their agreement with the conditions of that data collection. (This principle is known as informed consent.)

Figure 1.4 Timeline Phase Four: Rise of Big Data and Social Media Analytics

2013	**Cybersecurity:** • US citizen and Central Intelligence Agency contractor Edward Snowden utilizes internet technology and social media to publicize his claims that the US National Security Agency has engaged in unauthorized surveillance of US and other citizens. • The NATO-supported *Tallinn Manual*, a document spelling out the applicability of international law in the area of warfare to the conduct of cyber warfare, is published.

(*Continued*)

Figure 1.4 (Continued)

2014	**Cybersecurity:** • US Office of Personnel Management networks that contain information on thousands of applicants for top secret clearances are breached. • Russia conducts cyber warfare against Ukraine. **Governance:** • Tim Berners-Lee, one of the internet's original founders, proposes a "magna carta" to protect the internet as a neutral system free from government and corporate manipulation. • European Court of Justice rules that "Right to Be Forgotten" is valid within the European Union, allowing European Union citizens to request the removal of personal information from search results.
2015	**Cybersecurity:** • A US teenage hacker successfully uses phishing and social engineering to gain access to the personal e-mail account of US CIA Director John Brennan.
2016	**Cybersecurity:** • Russia is accused of having carried out social media hacking to affect the outcome of US presidential elections including hacking into the files of the US Democratic National Committee and releasing e-mails on WikiLeaks. • Computer hackers believed to be linked to North Korea carry out the Bangladesh Bank Heist through hacking into the financial transfer system (SWIFT). Bangladesh's Central Bank loses $100 million. **Governance:** • The General Data Protection Regulation establishes data protection and privacy rights for European Union citizens.
2017	• Google launches first fully autonomous (self-driving) car, utilizing advances in the internet of things (IoT) and artificial intelligence.
2018	**Cybersecurity:** • The Cambridge Analytica scandal breaks—Facebook is accused of having knowingly sold advertising space and user data analytics to Russian agents seeking to affect the outcome of US presidential elections. • The Department of Homeland Security confirms that Russian hackers have broken into voter registration files in several US states prior to 2016 elections.

CONCLUSION

As this whirlwind history of the internet has shown, some facets of internet technology are still the same as they were when the technology first began, back in the 1980s. The internet is still fast and borderless, with information traveling quickly and cheaply all over the world.

At the same time, we have seen vast changes in this environment. The original domination of this space by state actors, including those associated with the military, has given way to a new environment where private corporations today play a leading role in affecting events that happen in cyberspace.

And the United States has, arguably, lost its privileged position as the leader in cyberspace. Today, the term *race* is often invoked to describe the competitive interactions between other states that seek to take a lead in defining and administering events in the online environment, including China and Russia.

And we have seen how the internet—which began as a world apart from traditional political dealings, including interstate conflicts and legal understandings of issues like private property—has instead become part of that same world. The borders of cyberspace have become leaky, with events occurring online having real-world repercussions—from the theft of classified and proprietary information by adversary nation spies to the ability of adversaries to affect events like the outcome of elections.

Today, providing cybersecurity for a nation's critical infrastructure is a multibillion-dollar industry, with states devoting vast resources to keeping their citizens and information safe online. Yet citizens today may trust the online environment less than they did in the past, and they may also doubt the ability of their governments to keep them safe online. They may also doubt the intentions of those corporations that provide goods and services online.

In the following chapters, we begin to ask what the internet means and who decides where that meaning is derived from. We also ask what it means to "misuse" the internet and whether states can be said to be violating the spirit of the internet somehow as they develop sophisticated policies for cyber espionage, cyber defense, and critical infrastructure protection.

QUESTIONS FOR DISCUSSION

1. How does America's place in the history of the internet's development influence current international cyber-related debates?
   a. Does the internet "boost" US hegemony, and if so, then how exactly?
   b. Is the internet inherently democratic or liberal?
2. How has the privatization of the internet changed or altered its development?
   a. Would Twitter, Facebook, or other popular social media platforms, e-commerce, and so on have been possible without a privatized internet?

   b. How does a privatized internet affect states as actors in the international system?

3. Is there something inherent about the progress of technology that made the internet the logical next step to communication?

4. Is there something inherent about democracy (especially in America—consider its size) that implied or required a means for mass communication and interconnectivity?

KEY TERMS

Algorithm	29
Asymmetric cryptography	7
Attribution problem	20
Backbone	6
Big data	29
Cyber sovereignty	20
Information warfare	22
Intellectual property	17
Internet Protocol (IP) address	15
Internet service provider (ISP)	1
Online piracy	17
Path dependence	5
Penetration rate	1
Social engineering	7

FOR FURTHER READING

Ems, Lindsay. "Twitter's Place in the Tussle: How Old Power Struggles Play Out on a New Stage." *Media, Culture and Society* 36, no. 5 (2014): 720–731.

Kwak, J., Zhang, Y., and Yu, J. "Legitimacy Building and E-Commerce Platform Development in China: The Experience of Alibaba." *Technological Forecasting and Social Change* (2018): 1–10. Accessed June 20, 2019. https://doi.org/10.1016/j.techfore.2018.06.038.

Leiner, Barry, Vinton Cerf, David Clark, Robert Kahn, Leonard Kleinrock, Daniel Lynch, Jon Postel, Larry Roberts, and Stephen Wolff. "A Brief History of the Internet." Last modified 1997. Accessed June 20, 2019. https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

Manjikian, M. "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik." *International Studies Quarterly* 54, no. 2 (2010): 381–401.

Shah, R. C., and J. F. Kezan. "The Privatization of the Internet's Backbone Network." *Journal of Broadcasting & Electronic Media* 51 (2007): 93–109.