2

THE INTERNET, TECHNOLOGY STUDIES, AND INTERNATIONAL RELATIONS

Learning Objectives

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

1. Compare and contrast three positions regarding the sources of a tool's meaning: technological determinism, designer's intent, and social construction of technology
2. Define terms: *dual use technology*, *export regime*, *affordances*, and *net neutrality*.
3. Describe the uniqueness debate and the three positions related to how norms and rules should be designed for the internet: the adoption of unique rules, grafting of old rules, and borrowing from other fields.

We know that many of the internet's original architects believed that the internet would inevitably be used for the extension of traditional freedoms such as freedom of information, freedom of assembly, and freedom of the press. Indeed, the international nongovernmental organization Reporters without Borders was established in 1985, and it has subsequently published an annual "internet enemies list," which calls attention to countries that are said to be violating the spirit of the internet through engaging in surveillance or censorship.[1]

In this chapter we consider two questions: How do new technologies in particular acquire meaning and who or what exactly determines what a technology should and should not be used for? That is, when one state accuses another of improperly or unlawfully deploying a technology, what is the basis for this understanding?

WHO DECIDES WHAT A TECHNOLOGY IS FOR?

Philosophers of technology have long struggled with the question of what a technology means and who is responsible for imbuing a technology with a specific meaning. Many of the political, social, and legal debates today about establishing norms for the use of the internet and its associated technologies (like social media, artificial intelligence, and big data analytics) are part of a broader conversation that takes place every time a new technology is introduced. Users often fear new technologies and tend to imbue them with certain types of power—to shape a society and its citizens. They may also create narratives about the threats and dangers inherent in new technologies. Think, for example, about the ways in which citizens were wary when a nuclear power plant was built in their community or even about current fears related to vaccines, which have led some people to choose not to vaccinate their children.

In thinking about what a technology means and how it acts, there are three major approaches or narratives to explain how technologies come about, how they function in society, and the threats they pose to society.

Technological Determinism

In the technological determinism narrative, agency—or the ability to exercise choice—can be said to belong to the technology itself. Here, technology is said to be "driving the train" because it appears to be capable of shaping and reshaping societies. These analysts argue that a new technology contains its own ideology or values—as well as built-in immutable characteristics—and that as a result, it evolves organically of its own volition, achieving an end point as it moves toward what it is meant to be.

In describing the internet's growth, philosophers like Luciana Floridi describe the evolution of our world—from the time in which humans invented writing until today—into a **mature information society** in which everyone and everything will be connected and there will be a constant source of good connectivity available in society in the same way that modern societies now can expect that there will be safe drinking water and food.

The technological determinism narrative suggests that humans themselves (including politicians) play only a limited role in steering the evolution of new technologies because control belongs to the technologies themselves. Indeed, the speed at which the internet penetrated our societies creates a sense of inexorability or inevitability. As early internet activists like Stewart Brand first stated in 1984, "Information wants to be free."[2] Therefore, they argued, information and the internet itself actually seek their own ends, moving toward transparency, freedom of speech, bottom-up organizing, and the overthrowing of autocracy.

They believed that the internet's development would cause real-world effects like the growth of freedom internationally. They thought that the internet

architecture would drive political events, thereby causing real-world effects on physical architecture or structures in the terrestrial world. Some internet optimists believed that the internet's growth would inevitably strengthen capitalism and free trade internationally. Some believed that the availability of connectivity would lead to unprecedented opportunities for individuals in the developing world. They would have more interaction with the developed world, better opportunities for education and employment, and if the digital divide could be overcome, surely states would then succeed in overcoming other divides, creating a more peaceful and stable world as a result.[3]

Technological determinists emphasize the internet's immutable characteristics because these characteristics (like openness, transparency, and interconnectivity) are seen to reside in the technology itself rather than what designers want or what users do with these technologies.[4]

However, analysts differ in their evaluations of these characteristics. Whereas one person regards the technology's emphasis on mobilizing users toward action as positive—noting its ability to create democracy through mobilizing users to vote or contribute to a political cause—others view this same capability as negative, pointing out that it also allows the coming together of like-minded individuals (like Nazis or white supremacists) to organize against democratic institutions.

Thus, analysts differed in their evaluations of what they saw as the inevitable effects of increased connectivity and internet penetration. Some analysts worried about the speed at which these changes were taking place because they seemed to be moving faster than states could create regulations and laws to affect the structures and practices that were emerging.[5]

Military analysts in particular argued that these new developments were creating new threats. Greater connectivity was said to lead to an "expansion of the threat surface." Others worried about the "weaponization of social media." These analysts argue that the internet is a technology that is not inherently democratic, open, or free. That is, they argued that it should be regarded as merely a tool. Just as a tool like a hammer could be used either for building a house or for bludgeoning someone to death, a tool like the internet could be either a tool of repression or one of emancipation depending upon whose hands it ends up in. Here Klimburg writes,

> Ultimately, we face the small but real prospect that in the not too distant future of the internet, a fabulous artifice of human civilization largely perceived today as a domain for advancing freedom and prosperity, could become instead a dark web of subjugation.[6]

Other analysts also voiced fears about the growth of a surveillance society in which individuals will have little privacy, with the waning of privacy seen as inevitable due to facets of the technology itself.[7]

The technological determinism argument regarding the internet's growth also led to the adoption in some societies of draconian measures to limit people's access to the internet. If one believes that the internet inevitably reshapes societies in a democratic fashion, then it is not surprising that an authoritarian society like North Korea would seek to establish what is in essence an intranet, which functions

only within the self-contained environment of North Korea while eschewing ties to the larger outside world through the internet. If technology is viewed as fundamentally uncontrollable, then the most logical reaction to that technology seems to be forbidding or controlling access to that technology. However, whereas a purely technological deterministic argument suggests that regulating technological access and use is best done from above, many individuals and groups believe that education and limits can enable individuals to speak back to technology.

The Role of the Designer

Not all internet architects were technological determinists, however. Instead, architects and analysts like Professor Lawrence Lessig emphasized the roles that designers or inventors themselves play in determining what a technology becomes.

In this narrative, the meaning of a technology or tool comes from the person who creates it. The designer therefore has some agency or free will as he or she makes design decisions that can then structure and limit the ways in which a technology may be used. Thus, the designer helps determine what a technology becomes and what it means through the decisions that he or she makes.

This stance assumes that technologies are introduced into a world that already has politics and power distribution within it. Thus, designers may seek to uphold social, gender, or racial divisions through making decisions about who a technology is for and who may access it, or they may introduce a technology with the explicit intent of changing these power distributions. (For example, if we think about reading as a technology, then we can consider people denied the gift of literacy historically—from women, to slaves, to African Americans in the American South during the twentieth century. The decision by teachers and even printers to present reading as "not for you" had nothing to do with the technology and everything to do with the world into which the technology was introduced.) Bruno Latour has famously summarized this understanding with the phrase "artifacts have politics."[8]

The design perspective suggests that a tool's inventor clearly knows how people should and should not use a technology. This perspective posits that societies, organizations, and groups can determine objectively whether someone is misusing a technology and restrict technology use. In recent history we can identify examples of situations in which societies sanctioned those who are thought to be "misusing" a technology through ethical regimes like professional licensing requirements to legal, economic, and political sanctions. For example, many European pharmaceutical companies would not sell certain medications to American prisons when they knew these drugs would be used to carry out death sentences.[9] Here there is a legal, political, and ethical understanding in many nations and internationally regarding the right and wrong use of anesthetics and other pharmaceuticals in which using them for pain relief is sanctioned whereas using them for execution is not.

In his work, Lessig argues that the internet is a built environment, built by humans through the technology of writing code. The internet looks and behaves in particular ways because humans make programming decisions. Here the designer

is seen to have the ability to build norms and values into a technology, which he or she may do either consciously or unconsciously. A designer can discourage certain types of behaviors while encouraging others. Technology scholars refer to **affordances** to describe particular facets of technology that are interwoven in technology, affecting how people use it. For example, many social media and communications technologies (like Twitter) are designed in such a way that users must use transparency in their communications because they offer only limited faculties for communicating privately rather than publicly.[10]

In thinking about the internet, we see that ARPAnet's designers had clear ideas about how it should be used and the values by which it should be governed and organized. Computer scientists who invented tools for networking, messaging, and establishing connections believed that the internet should be international rather than national in character, that it should be as free of regulation by states and other entities as possible (libertarian in character), and that users should share information freely, without cost and without barriers for sharing and use. This philosophy is summed up in "A Declaration of the Independence of Cyberspace" by Paul Barlow, written in 1996. Barlow wrote,

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[11]

In this story, designers created an architecture with certain features associated with specific values. The resulting product was nonhierarchical, with information moving between nodes and hubs rather than up and down to a central location at the top of a hierarchy. Within this structure anyone could join the internet from anywhere. In the language of economics, the internet was a **free good**.

In addition, the internet was envisioned as a space without borders that would not belong to any particular nation and where no nation would have jurisdiction over the activities that occurred there. The designers believed that internet users would not be citizens of a particular nation. Instead they would be "netizens." They would not be governed by the rules and norms of their physical territorial residence but would rather be governed by rules and norms that resided in the technology itself (either because they were placed there by designers or because they spontaneously emerged either from the technology itself or from the interaction of people within that technology).

Next, no information was more important than other information. All information moved at the same speed, and no source (at least initially) stood above any other source. This principle is referred to as **net neutrality**.[12] Additionally, people could join without revealing their real names or any personal information and could thus browse and participate in conversations and other activities anonymously. Finally, it was initially regarded as largely "American" because it was invented in the United States. It was associated with freedom of information, freedom of association, and freedom of speech.

The notion that the internet thus meant freedom—of information and of access—either because of some inherent attribute of the technology or because of the designer's values, was prevalent during the first two phases of internet development. Indeed, in 2006 Reporters without Borders began publishing a list of what they term *enemies of the internet*, nations that they perceived to be using internet technology incorrectly through erecting "structures" like firewalls or filters that limited citizen access to the internet and information or by requiring citizens to register their identities online or to abide by national restrictions on freedom of speech and freedom of association.[13] Furthermore, the United Nations issued a resolution in 2012 that called upon states to recognize those international human rights granted in the real world as applying to the virtual world as well. This resolution asked states to "promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries."[14] There is thus a legal precedent for accusing those who violate established ideas like freedom of the press of abusing or misusing internet technology.

Cindy Cohn, director of the Electronic Frontier Foundation, takes this understanding further, arguing that "how we build our tools will determine our rights." She argues that "our digital world can be fair or unfair. Empowering or disempowering. Utopian or dystopian depending on the choices we make along the way."[15] Thus, she worries that companies like Google and Twitter have a disproportionate amount of power to determine the future of the internet and thus of human society. She writes,

> For the last decade . . . we've seen governments and companies take negative advantage of their positions in building and running the networks, architectures and tools that the rest of us rely on. They treat us as unimportant serfs in their mass spying systems, fodder for machine learning algorithms and treat our world like a cybersecurity battleground where our private lives are mere collateral.[16]

Similarly, Brooking and Singer reference the designer's role in describing social media, arguing that

> the engineers behind social media had specifically designed their platforms to be addictive. The brain fires off a tiny burst of dopamine as a user posts a message and it receives reactions from others, trapping the brain in a cycle of posts, "likes," retweets and "shares."[17]

Today, some critics worry that if design decisions constrain our individual behaviors, then users will have fewer opportunities to practice regulating our own behaviors. For example, designers could design a cell phone that can determine if it is inside a moving car and disable its texting feature in this situation. Instead of deciding not to text and drive, we would be robbed of the ability to do so. In the social media environment, we can ask whether it is better for people to learn to identify and avoid racist ideas and speech in their

own lives than for an algorithm to simply be deployed to identify and delete racist content once it is posted.

The design perspective does not, however, posit that an environment is static. Instead, we can conceptualize of a dynamic environment in which the internet's architecture and properties can change over time, depending on who has the power to design the environment. Here we can consider encryption technology. At first programmers worked to keep us and our identities and our information secret. (Anonymity was considered a nonnegotiable attribute of the internet, which was built into the environment.) Today, however, those same programmers work to make us traceable online.[18] Here, Lessig points to the 1994 Communications Assistance for Law Enforcement Act in the United States that required that networks be designed to preserve the ability of law enforcement to conduct electronic surveillance. This means that in the area of surveillance, the US Federal Communications Commission (FCC) gets to have a say in the types of systems that are designed and the types of uses to which they may be put—just as they have done previously with telephone networks.

In the same way, many analysts have queried the claim that the internet is inherently a borderless international place where concepts like nationality do not apply. They claim that the principle of nonterritoriality of the internet came about because of designers' choices and that it can be undone. Although programmers initially set up the internet without links to physical territory and territorial sovereignty, this does not mean that it has to be this way or that it cannot change.

However, as we saw with the technological determinism view of the internet, there are those who have critiqued and questioned the design view as well. One of the strongest critics of the design view of the internet was Evgeny Morozov, a journalist who grew up in Belarus, one of the most autocratic nations of the former Soviet Union. In the book *The Net Delusion: The Dark Side of Internet Freedom*, Morozov argued there is nothing inherently democratizing about the internet. Instead, he argues that internet technology is actually **dual use.** He believes that features like photo and voice recognition, in particular, could easily become instruments of surveillance and social control, depending on who deployed the technology. Morozov's ideas were later realized when participants in anti-state demonstrations in Ukraine received text messages from the government noting that their identities had been determined through facial recognition and that they would be punished if they engaged in further demonstrations. And the German company Lench IT was criticized by human rights organizations for selling its Finfisher surveillance software (intended to be used by democratic regimes for carrying out counterterrorism activities) to nations like North Korea and Belarus, who deployed it against their own citizens.

Critics like Morozov thus ask us to think about whether there is an entity such as "the design community." Back in the early days when most of the internet's architects were Western and US-based, these designers were a monolithic group who shared values, including a commitment to democratization. For most of the 1970–1990 period, the design community was unified in its support and vision of

an open and largely unregulated internet, the goal of growth of the internet, and the extension of it to all who desired to participate. Here, the Internet Engineering Standards Task Force (IETF), with its philosophy of making decisions by "rough consensus," played a leading role. This body worked to make design decisions about the internet's architectural forms and its growth in as transparent a fashion as possible.[19]

However, today, there are actually multiple design communities: There are the neoliberal academic designers of the internet; there are also members of the defense community, like the US military, which paid for the creation of the internet and had different aims in its creation, including the ability to create redundant capabilities for military command and control functions. And some argue that the role of internet architecture developers is arguably "owned" by the international corporations that administer the major online platforms. In addition, we can point to designers in Saudi Arabia, North Korea, and China, all of whom are working to create user experiences for their citizens reflecting the characteristics and values of their societies.

Currently, we can identify a multiplicity of players within the design community—democratic states, autocratic states, business interests, and technology experts. These individuals and groups do not always agree on what the internet should look like, who it should serve, or what it is for. Thus, analysts sometimes refer to a **standards war,** in which different factions within the design community have attempted to put into practice different or competing visions of what the internet's architecture will ultimately look like.

Case Study: Is China "Misusing" Internet Technology?

Here we pause briefly to consider at greater length the argument that a state is "misusing" internet technology by designing an experience for its own domestic users that differs from the internet experience as originally conceptualized by designers like Barlow and Cerf. Here we can think particularly of the creation by China's government of what has come to be known as the Great Firewall of China. Beginning in the 1980s, Chinese authorities began utilizing filters to control all internet traffic that travels to and from—as well as within—China. This firewall allows the state to filter out and make unavailable content based on the inclusion of keywords.

The US-based nongovernment organization Freedom House has reported on what it sees as the Chinese government's techniques to impose "information control" and censorship as well as their crackdowns on the use of social media to prevent citizens from organizing in anti-state demonstrations or activities online.[20] At times, China has blocked citizens' access to Google and Gmail and has also utilized cyber warfare to carry out attacks on the websites attached to Microsoft, Yahoo, and Apple. Because nearly a third of the world's internet users reside in Asia, including China, groups like Freedom House worry that the internet could lose its character as an international territory without borders where

information flows freely if one or two big players like China were to adopt different sets of norms and rules for how information should be treated in their territories. For this reason, they have sought to shame and sanction states whose orientations to the internet do not reflect this understanding of the internet as an international body.

Rather than denying censorship, China's government admitted to taking these actions and defended its right to do so. In April 2013, China's Communist Party issued "Document Nine," which listed seven perils presented to China by the growth of internet technology within their society. This list included threats created by exposure to Western constitutional democracy and the claim that there were "universal values" that all internet users should be in favor of. China's Ministry of Industry and Information Technology has similarly admitted to engaging in censorship and content blocking, arguing that doing so was necessary for the "healthy and lawful development of the internet."[21]

At the same time, the Chinese government used social media access to construct what many have described as a vast surveillance state. China is actively engaged in setting up a national video-surveillance network named xueliang, or "sharp eyes." This system will use facial recognition and other technologies to monitor the activities of China's citizens in schools, in public facilities, and while they are on city streets. Citizens also have monitoring software automatically installed on their smartphones. At the same time, China has created a **social credit system** that assigns citizens a score based on their past behavior, including whether they have committed actions like traffic offenses. This score can affect their credit ratings, including their ability to borrow money to take out a student loan or a mortgage.

The issue for international relations specialists is whether every country should have the right to utilize internet technologies—including new advances in artificial intelligence—to monitor their citizens in this way or whether actions like monitoring and filtering constitute a "misuse" of the internet technology as it was designed and envisioned. Within the international system, whose vision of the internet should prevail, and how much leeway do states have to decide how they will utilize these technologies internally within their own countries and perhaps against their own people?

As we will see later in the textbook when we take up the subject of internet governance, not all states within the international system agree with the US and European positions that the internet contains its own values—including a commitment to openness and free speech—and that all states should attempt to comply with these values. As we will see, Russia in particular has sided with China, espousing the position that the United States is acting unfairly in stating that the internet must reflect American norms and values. Here Russia argues that it has a right to treat the internet as part of Russia's real territory, and therefore it has the ability to create its own Russian internet reflecting Russian norms and values. Other analysts have suggested that the internet is international, rather than American, in character and that if there is a prevailing set of norms and values attached to the internet, these values and norms should be created as the result of an international consensus rather than dictated by the United States simply because the United States "invented" the internet.

CRITICAL ISSUES

WHAT ARE DIGITAL HUMAN RIGHTS?

Early internet developers described the online environment as "a world apart" from regular, terrestrial space. They hoped that people would have complete freedom online to express their ideas, to interact with others from across the globe, and to share information freely. However, what they took for granted—the idea that people would have the same rights online that they had in real space—is actually a subject of contention among states today.

Analysts make three arguments regarding the sources of human rights. The United Nations, in the Universal Declaration of Human Rights, states that there are certain basic rights that everyone has by virtue of the fact that they are human. Such rights can be positive (the right to do something) and negative (the right to be protected from something). The Universal Declaration of Human Rights states that everyone everywhere has the right, for example, to live free from violence, to not be enslaved, and to be provided with basic living requirements like food and shelter.

Today, some activists suggest modifying the Universal Declaration of Human Rights to include an additional article. Article 19 would clarify that all humans have "digital human rights" by virtue of their humanity. If this codicil passed, then a state like North Korea or China could not deprive their citizens of internet access. Doing so would constitute a human rights violation, affecting their eligibility for international foreign aid and trade preferences. In severe cases, human rights violators can even be tried by an organization like the International Criminal Court.

Digital human rights are said to include positive rights: the freedom to express opinions, to "gather" digitally in groups, and to share information. They also contain negative rights like freedom from the possibility of government surveillance. Thus, just as people have a human right to own property, these activists suggest that people should have the right to own their own data that they produce, to determine how that data is used and shared, and to be made aware of situations in which others are accessing or utilizing their data.

However, Yakupitiyage and other analysts from the developing world have questioned whether any international body truly has the power to enforce the understanding, or norm, that digital rights are an important subset of human rights—particularly because there is not currently a global consensus regarding this issue. Traditionally, the United States has argued this position, advocating for the extension of internet access globally, particularly in the developing

world, because it can be seen as part of a larger "package" of human rights. However, in 2018, the United States withdrew as a member of the UN Human Rights Council, arguing that the body was both biased and heavily politicized in its aims. As a result, some policy makers in the developing world worry that in the absence of America's strong participation and advocacy of the digital human rights position, nations like Russia and China, which do not accept this position, will come to play a larger role globally, leading to a situation in which digital rights are seen as detached from broader human rights claims.[22]

However, others argue that individuals have rights not because of their basic humanity but because these rights are conferred upon them by the state. Such rights are conditional. A state can confer rights, or rescind them, and can also determine who receives such rights (e.g., stating that only men may vote).

Finally, the internet's architects claimed that people's rights derived from their positions within a certain environment (i.e., online). Tim Berners-Lee, an early internet developer, first argued for a separate Digital Bill of Rights in 2014.[23] He believes that there are universally right and wrong ways to use the internet and that states denying their citizens full access to cyberspace are misusing the internet. In addition, in the wake of the revelations by American whistle-blower Edward Snowden in 2015, activists have voiced concerns about government surveillance as well as the collection and analysis of user data. A digital Bill of Rights could thus help citizens protect their rights online through spelling out what those rights are (i.e., the ability to own your data and to protect your reputation online).

The Digital Freedom Fund has provided an extensive list of the rights that they feel users should have online. The schematic in Figure 2.1 outlines these rights

Figure 2.1 Digital Human Rights

Right	Examples
Right not to be profiled	Right to access information about your own data Right to keep your personal data protected Right to opt out of profiling Right to anonymous access and participation
Right not to be judged by a machine	Right to request a human override to algorithmic justice Right to delete the digital self

(*Continued*)

(Continued)

Figure 2.1 (Continued)

Right	Examples
Right to (digital) self-determination	Right to control your own data Right to object to the use of personal data Freedom to move providers Right to challenge or opt out of standard terms and conditions
Right to disconnect	Right to unplug from time to time Right to non-digital access to governmental services
Right to participate in the cultural life of one's community	Right to participate in digital expression Freedom to share and receive information Right to participate in online communities
Right not to be discriminated against	Freedom from discrimination
Right to personal safety and security	Right to digital security Right to bodily integrity Freedom from cyberbullying, trolling, and abuse
Right to political participation	Freedom from online manipulation Right to take part in political decision-making online
Right to privacy	Freedom form profiling Freedom from bulk surveillance Right to use strong encryption Right to private digital communications
Right to challenge the algorithm	Right to algorithmic transparency
Right to education and literacy	Right to digital literacy Right to understand the implications of technology

Sources

Article19.org. "#InternetofRights: Creating the Universal Declaration of Digital Rights." Last modified March 24, 2017, https://www.article19.org/blog/resources/internetofrights-creating-the-universal-declaration-of-digital-rights/.

Kaltenbach, L., and O. Le Guay. "Desperately Looking for a Data Ethic: The Importance of a Universal Declaration on Digital Human Rights." Digiworld Economic Journal 97 (2014): 102–105. https://www.thefreelibrary.com/Desperately+looking+for+a+data+ethic%3a+the+importance+of+a+Universal…-a0414693455.

Ojekunle, A. "African Governments Are Using Laws to Stifle Internet Freedom—Report." Pulse.ng. Last modified November 13, 2018, https://www.pulse.ng/bi/tech/tech-african-governments-are-using-laws-to-stifle-internet-freedom-report/prg88d6.

UN Office of the High Commissioner on Human Rights. "The Right to Privacy in the Digital Age." Last modified 2018, https://pp-international.net/2018/07/the-right-to-privacy-in-the-digital-age-for-the-report-of-the-high-commissioner-for-human-rights/.

Social Construction of Technology

Today, while many Western organizations still support either technological determinism or the design view to advance the claim that there are universal norms and values associated with internet technology that all states should comply with—unless they wish to risk being labeled "internet enemies"—there are many other states in the world who disagree.

These states often make a third argument for the source of a technology's values. This argument most closely aligns with the arguments set forth by proponents of the **social construction of technology** (SCOT) school, who argue that new technologies do not develop in a vacuum, nor do they necessarily have only one set of values and norms attached to them automatically. Rather, SCOT adherents argue, a technology's meaning is negotiated within a specific socioeconomic, political, and economic context. When a new technology is developed, its meaning may be contested. Different technology users may have conflicting visions of what the technology is for and who it is for, who may use it, and how. Over time, they argue, the debate may be settled with a specific version and meaning described as acceptable for the technology. (This process is referred to as **technological closure**.)

In this model, a technology may change from the period when it is invented, often assuming a new and unanticipated, novel form. In this model, even a designer may be surprised by what a technology eventually becomes because it may not be what even he or she anticipated.

Function creep describes how technology invented for one reason is found to be useful for other reasons as well, creating a situation in which it is used for other than the designer's intended purpose. In the United Kingdom, the 1939 National Registration Act led to the issuing of national identity cards for the purposes of rationing food during the war. By 1950, however, thirty different government agencies were using these cards for a variety of purposes—asking citizens to show such cards to pick up packages from the post office, to collect social welfare benefits, or to provide identification to police.[24]

Function creep explains why the internet has come to play such a vital role in the lives of citizens and the state today. Although initially envisioned largely as a way of sharing instant communications among citizens internationally, today the internet's function has "crept" so that it is now a news purveyor, a means of voting, a way of tracking pedophiles in a society, an advertising platform, and an engine

of commerce. Here we can again consider the story we encountered earlier in this volume, where General Michael Hayden stated that the ARPAnet designers actually had no grand vision of the internet's future. They had no idea how people would use this creation—how they might use it in creative ways, some of which were normative or condoned, while others were nonnormative or sanctioned.

More than any other explanation, the SCOT school illustrates the quirky and creative ways in which new technologies can be deployed and the inability of analysts and designers to predict what a technology becomes. In recent years, social theorists have pointed to the issues associated with so-called emerging technologies. An **emerging technology** is one characterized by a high degree of uncertainty regarding its potential, which also has a network effect. (That is, the technology's existence and deployment have the ability to affect developments in a variety of other fields and also have the ability to influence a society politically, economically, and socially.) Emerging technologies often come with (or create) unseen social and ethical concerns because they are so new or unexpected that there is little preexisting research about them and their effects. When we think about the internet's creation, we see that no one ever predicted that ARPAnet's existence would later lead to the creation of social problems like the existence of Pornhub, or legal issues related to intellectual property being created on sites like YouTube, or political issues like the online radicalization of teenagers toward terrorist groups.[25] It is often difficult to predict how such a technology will develop over a period of ten or fifteen years, and as a result, these types of technologies have been particularly difficult to regulate and oversee.

PEOPLE AND PLACES

The Great Firewall of China

The term *Great Wall of China* refers to a series of fortifications that runs in an East-to-West direction across much of China. They were built beginning in 700 BC to keep out foreign invaders and protect China's people and resources.

The Great Firewall of China is more recent. This term refers to a series of measures undertaken by China's national leaders to prevent Chinese citizens from accessing certain types of information on the internet. As a one-party state, China's leaders are concerned about domestic activism that might end in calls for the end of that one-party ruling arrangement and the establishment of democratic elections. Thus China's leaders have worked to censor information about previous attempts at democratization, such as the 1989 Tiananmen Square protests, in which up to 1 million Chinese students called for an end to one-party rule and the implementation of full freedom of speech and information in China. Fang Binxing, a former president of the Beijing University of Posts and Telecommunications, is seen as the "father" of China's

Great Firewall. He argues that online controls are necessary to "prevent chaos" domestically within China.[26]

The Great Firewall is not completely impenetrable, however. Currently, many users now use tools like **virtual private networks (VPNs)** to gain access to sites overseas. A VPN, which can be set up on a cell phone, can be configured to make it look as though a user is located somewhere else, outside of China. Between 2008 and 2012, the US Department of State spent nearly $100 million on the development of tools like VPNs to be used by dissidents and activists in repressive regimes to circumvent internet censorship in their countries.[27] China has reacted to US efforts in this arena, labeling such activities as a violation of China's sovereignty and their right to control what happens in their internet. The United States, in response, has listed China's internet controls to a list of barriers that they see as impeding trade between the United States and China.[28]

In recent years, Western-based internet service companies—like Google and GitHub—have clashed with Chinese authorities, who have required that companies comply with Chinese laws regarding censorship to do business in the region. Google, in particular, was criticized by American and international bodies when it established google.cn despite requests by Chinese authorities to, for example, provide them with data on what Chinese citizens were searching for online. (In particular, the Chinese government was interested in who was searching for information about the banned religious group Falun Gong.)[29] In 2010, Google shut down the google.cn search engine. Although they claimed that they were doing so because of their strong commitment to human rights internationally, some Chinese economists have suggested that Google was actually unable to compete with the domestic Chinese search engine Baidu and that their real motivation was economic.[30]

China's leadership argues that despite the existence of the Great Firewall of China, most citizens have benefited in numerous ways from the introduction of the internet in their nation. They point in particular to the ways in which citizens in rural areas now have access to a much wider range of consumer goods from clothing and baby items to entertainment.[31] Here, China's leadership demonstrates that they have a different idea regarding the utility and ideology that they attach to the internet. They see it largely as a vehicle for commerce and the extension of education through the establishment of online learning rather than as a vehicle of democratization and free speech. The fact that Western companies are now competing less in that market, and the fact that many of the sites that Chinese users rely on are now domestic Chinese companies, helps bolster the leadership's understanding that China should have a Chinese internet rather than seeking to join the international community online.

As we think about attempts by actors like the European Union or the United Nations to regulate and oversee internet technology, we should remember that today's internet may also not reflect the internet of tomorrow. Measures like the internet of things and wearable technologies and the development of artificial intelligence mean that the threats that nations face will look different in the future—and the internet may change in rapid and unpredictable ways.

As we examine policy developments regarding regulating and governing the internet's structures, as well as policies related to cyber warfare and cyber conflict, we see how all three discourses are present. In some instances, analysts argue that cyber arms control is necessary because the internet's existence will inevitably create new conflicts (echoing here the technological determinist viewpoint). In other instances, states argue about whether states can work together or whether international bodies can be created to shape the internet's architecture in ways that encourage cooperation and sharing rather than conflict (echoing the design viewpoint). And in other instances, states have contested the meaning of internet technology. Here it is likely that we have not yet achieved technological closure or arrived at a consensus about what the internet means. However, there is evidence already that the internet has not been deployed or constructed in the same way in all states and all societies.

Figure 2.2 summarizes the differences between the three schools of thought and their implications. We turn next to the uniqueness debate, again borrowing from technology studies, to consider whether internet policy issues differ fundamentally from policy issues in real space.

Figure 2.2 Three Schools of Thought and Their Implications

	Agency Belongs To	Norms Derive From	Threats	State Response
Technological Determinism	Technology	Technology itself (i.e., information wants to be free)	Technology changes human behavior and values	Limit access to technology —censorship, registration, and filtering
Role of Designer	Designer	Aims, values of designers (i.e., designing for security and privacy)	User abuse of technology; malignant designers who create bad code or destroy environment	Build in measures to preempt threats; punish those who violate the ethos of technology
Social Construction of Technology	Users	User community, preexisting rules and norms (state)	Unanticipated uses	Introduce surveillance, rules governing use

THE UNIQUENESS DEBATE

With the internet's advent, we saw an explosion of new words to describe phenomena occurring online. Analysts referenced cybercrime, cyberstalking, cybertheft, cybertrespass and cyberwar. Military analysts warned that the United States was not sufficiently armed with the latest cutting-edge cyberweapons and that as a result, the United States faced the possibility of a Cyber Pearl Harbor or a Cyber 911 situation in which the United States could be surprised by a large-scale attack for which they are insufficiently cognizant of the dangers that they face and as a result are unprepared to respond.

Here, an important question for academics—from social scientists who study conflict to philosophers who study ethics—revolves around the uniqueness debate. How do we understand these new phenomena that have emerged as the result of the internet's development? Are they best understood as variants of existing, often age-old problems (like bullying, violence, and conflict), or are they better understood as fundamentally new issues that have emerged in this new environment?[32]

The Internet as a Unique Environment

We can identify characteristics of cyberspace that are unique in comparison to terrestrial space, including the speed at which interactions occur and the "radical connectivity" that allows information and ideas to traverse physical borders, making it difficult if not impossible for states to exercise border control in cyberspace. This radical connectivity also presents issues of legal jurisdiction related to border control, whereas the international character of the space itself presents issues related to an absence of sovereignty. On the military front, conflict in cyberspace can look different from other types of terrestrial conflicts due to the fact that cyberweapons are virtual rather than material. They can thus be developed more cheaply and more quickly and can be much harder to track than material weapons such as a missile housed permanently in one location in a missile silo. We have also considered the ways in which anonymity may be a characteristic of cyberspace, although analysts disagree as to whether this is indeed an immutable characteristic. Finally, we have considered the ways in which the internet as a highly technical built environment—differs from terrestrial space—because the state alone has neither "discovered" it, built it, nor controlled it alone. Rather, states are particularly dependent on the roles played by international organizations, technical specialists, and the business community in creating, policing, and monitoring cyberspace.

As a result of these unique characteristics, then, many internet designers claimed that digital space differed fundamentally from terrestrial space. Terrestrial space had borders inside of which states had sovereign authority, and property and ideas could be owned in terrestrial space. However, they felt that the internet was radically different and governed by its own rules and norms.

Initially, internet pioneers claimed that all content available on the internet should be free of charge and able to be freely shared. **Open source software** was thought to be the model for how individuals could work together to create new programs and content on the internet, which would then be freely available to all users. (That is, because the internet itself was a free good, some users argued that everything contained within that environment should likewise be a free good.) These same utopian idealists also argued that one of the internet's greatest virtues was that it provided a space of radical transparency where information could be freely and infinitely shared. It was therefore

Figure 2.3 Comparing Terrestrial and Digital Space

Characteristic	Manifested in Real Space	Manifested in Digital Space
Speed	Interactions formalized or slow (i.e., treaties or alliances)	Interactions (including alliances) may be fleeting or temporary
Jurisdiction	Real borders in which states have sovereignty	Borderless space across which data and ideas migrate freely and unregulated
Private property, including intellectual property	Recognized as existing on national and international levels through treaties; with penalties for violating norms	Not always recognized; norms may favor sharing or open source solutions to problems
Anonymity	Actions are carried out by real people who can be disciplined by the state for violations	Actions not always traced to an individual or group due to attribution problem
Weapons	• Tangible • Can be tracked and governed by international community	• Intangible cyberweapons • Cheap
	• Understandings regarding use and tech specifications change slowly • Utility of weapons remains over the long term	• Difficult to track and govern • Strategies, tactics, doctrines, and tech specifications change quickly • Utility of weapons decays quickly

considered to be unique and a world apart from terrestrial space. (We see some of this sentiment still existing today in the manifestos of groups like the nonprofit organization WikiLeaks, which argues that internet users should not recognize legal understandings related to the dissemination of classified information, for example, but rather that people should strive to make government as transparent as possible, even if doing so involves making stolen and classified documents available.)[33]

Figure 2.3 illustrates the differences between real space and digital space with reference to the unique characteristics referenced earlier in this chapter.

A WORLD APART OR AN EXTENSION OF TERRESTRIAL SPACE?

Whereas designers described the internet as detached from physical territory, social theorists identified similarities between social phenomena occurring in the real world and those occurring in cyberspace. That is, initially, social theorists tended to describe cybercrime, cyberstalking, and other "cyber" problems as variations of those social problems that occurred in the terrestrial world. And in the beginning, something that occurred "in cyber" (from cyberbullying to cyber infidelity) was often viewed as a lighter or less serious, less real version of its real-world counterpart. In writing about criminology and sentencing guidelines, there was initially an assumption that cyber offenses were perhaps lesser offenses and that their treatment—including the penalties imposed—should be less because the severity of events did not rise to the same level as events that occurred in the terrestrial world.

At the same time, in the internet's early days, analysts assumed that events which occurred in cyberspace were confined only to cyberspace. However, by 2010, social analysts were aware that cyberbullying could in fact lead bullied teens to commit suicide in the real world. They began arguing that online behaviors—from participating in a pro-anorexia discussion board to discussing radical Islamic jihad online—had real-world repercussions.[34] In addition, the wall between people's online or digital identities and their real-world identities broke down. As individuals applied for jobs online, posted their résumés and creative work online, and paid taxes and bills online, it became clear that online activities could easily be traced back to real-world identities. In addition, with social media's emergence, platforms like Twitter and Facebook were being asked to police interactions among users, creating fewer and fewer places where anonymity was the rule for online interactions.

Today the idea that online information and activities are governed by different, unique rules is a minority position. By 2003, American courts established the understanding that the internet could be subject to proprietary control and that information and space on the internet could be privatized.[35] And analysts accepted that cyberspace and real space are intimately and deeply connected. Cyberspace

is said to have "leaky borders," and analysts note that cyberspace can be used as a vector or platform for launching attacks on physical targets, such as telecommunications and electrical grids. It can also be used to meddle in real-world events, like national elections. At the same time, analysts have developed an understanding that cyberwarfare and cybercrime are not lesser variants of real warfare or real crime but rather again that they are serious events.

PEOPLE AND PLACES

What Is the Dark Web?

Today, the web is commonly described as having three layers: the surface web, the deep web, and the dark web. The **surface web** encompasses all publicly identifiable and searchable sites (i.e., everything that comes up when you perform a Google search). However, the surface web is only the tip of the iceberg in terms of all of the information and activity that takes place on the web. **Deep web** refers to sites that may be "hidden" within either a legitimate or an illegitimate site and that do not come up during a standard search. Here you may need a password or to type the web address for this page directly into a server. (For example, the content you access when you use an online content management system like Desire 2 Learn or Blackboard is part of the deep web, as is information you encounter on your university's website after you log in as a student. We can also place the "Clearnet," a network of secure or encrypted channels through which individuals and corporations may make purchases using e-commerce, within the deep web.)

Dark web refers to material that is hidden intentionally and is inaccessible through a standard web browser. (The dark web is thus a subset of the deep web.) To access materials within the deep web, users have to have access to an anonymizing web browser like Tor, which encrypts the addresses from which information is sent or received as well as the pathways by which the information travels. In this way, the sites cannot be traced back to a particular user or even a particular computer. Readers may be familiar with the Silk Road, which was described as the world's largest marketplace for illegal drugs. This site was shut down by US law enforcement personnel in 2013.

Using an anonymizing browser is not always illegal. Someone might use Tor or a similar browser to engage in activities like whistle-blowing (i.e., reporting a violation of rules or protocol that has occurred at one's workplace in a situation where one fears retaliatory actions, like being fired, as a result of reporting the information) or engaging in social activism under a repressive regime. Such an instance would constitute a legitimate use of the dark web. In addition the dark web itself constitutes less than 1 percent of the web's overall geography with perhaps as few as 45,000 sites contained within it.

However, law enforcement personnel on local, state, and federal levels wish to enforce laws within the dark web—preventing activities like trafficking in illegal drugs, weapons, or human beings. Current law is unclear both in the United States and internationally regarding the methods that law enforcement can use in tracking and preventing criminal activity on the dark web or the laws that apply for indicting and sentencing those who engage in illegal activity on the dark web. Currently law enforcement personnel may use tools like adopting false identities to infiltrate such sites and may make purchases to gather evidence against those trading in illegal substances. Some lawyers believe that such activities constitute entrapment and that the rights of those who engage in dark web trafficking are therefore not being sufficiently respected. Others argue that such measures are necessary given the difficulty of pursuing criminals across the dark web.

Currently, China and Russia have both introduced regulatory measures within the international community aimed at eliminating citizen access to Tor. However, there is not a great deal of international support for this solution to the problem of how best to regulate the dark web.

Sources

Chertoff, Michael. "A Public Policy Perspective of the Dark Web." *Journal of Cyber Policy* 2, no. 1 (2017), 26–38.

Davis, C. "Addressing the Challenges of Enforcing the Law on the Dark Web." *Global Justice* (blog). Last modified December 11, 2017, https://www.law.utah.edu/addressing-the-challenges-of-enforcing-the-law-on-the-dark-web/.

Patterson, D. "How the Dark Web Works." Zdnet.com. Last modified September 1, 2016, https://www.zdnet.com/article/how-the-dark-web-works/.

How to Regulate the Internet

Although many internet characteristics have proved to be mutable, rather than immutable or unchanging characteristics, there are still certain facets of online interactions that are unusual and that present unusual challenges to policy makers and analysts today. For example, online interactions in the international community tend not to occur from a purely state-centric perspective. Rather, from the beginning, the technology community has played a major role in the development and evolution of the internet environment.

Thus, a major issue for policy analysts today is this: Do the differences between real and virtual space mean that the internet requires fundamentally different and unique structures and rules for governing and regulating it? Or can the governance and regulation of state and individual activity in online interactions—including cyber warfare—be carried out through widening existing regulations

and organizations to include the cybersphere? Here we can ask: Is there something so fundamentally unique about cyberwarfare, in comparison to traditional warfare, that we need to create brand-new doctrines and institutions to regulate and control it? And is cyberterrorism fundamentally different from terrorism, or are they related? Similarly, as we think about the internet as a venue for international relations among states, we may also wish to ask: Is every encounter between states online uniquely different from activities that occur in the real world?

In considering internet regulation, we can identify three approaches where each understands the uniqueness debate somewhat differently. First, some analysts believe that cyberspace is so different from terrestrial space that states and the international community need new organizations and institutions to govern it. These analysts describe the evolution of a new type of multistakeholder governance or regulation featuring a unique constellation of actors—including technology specialists (and specialized technology organizations like the Internet Society), states, multinational corporations, and international organizations.

The second set of analysts argues that what needs to occur is **grafting**. In this scenario, some existing regulations and organizations can successfully broaden their mission to absorb new, related missions and goals for regulating the online environment. We can identify grafting in the push to widen our understanding of international law—particularly in the areas of war or conflict—such that key international law principles can also be used to explain and regulate conflicts in the cyber arena. The publication of the *Tallinn Manual* in 2012 represents an attempt to do just that. This manual, created by an international team of experts and created at the NATO Center for Excellence in Tallinn, Estonia, asked whether, for example, NATO's Article 1, which requires a NATO member to interpret an act of aggression against a fellow member state as an act of aggression against itself, could be widened such that a cyberattack against a member state would also require a response by all other NATO member states.

We can also point to the decision in 2013 to broaden the provisions of the international **Wassenaar Arrangement**, which prevails upon signatory states to consider how dual-use technologies in biology and chemistry might be used before granting export licenses to developers wishing to sell them abroad. (Here, for example, we would consider whether a laboratory that creates cultures used to test vaccines might be considered responsible if these cultures are instead used by an adversary nation to create a biological or chemical weapon.) In 2013 signatory members agreed to broaden the agreement so that states would also be asked to police and regulate the export of computer code that might be used to create cyberweapons or instruments of state surveillance.[36]

Finally, we can point to discussions regarding whether the United Nations Declaration of Human Rights should be expanded to include an Article 19, which would focus specifically on the role of the United Nations in safeguarding so-called digital human rights, including freedoms like freedom to assemble, freedom of speech, and freedom from surveillance online.[37]

A third approach to regulating the online environment is borrowing. These analysts believe that the internet is a unique strategic environment—borderless, international, and amorphous. However, there are other existing terrestrial environments that share some of these characteristics. Garett suggests viewing the online environment as similar to the ocean, arguing that "laws that have succeeded in the ocean take into account the unique characteristics of the ocean. The result is maritime law."[38] In addition, there are other areas of international governance and rule making that are highly specialized and that involve a number of players, including business interests and international corporations.[39] For example, firms may play a leading role in crafting legislation and creating structures of governance in sectors like environmental law, public health law, and even in the area of product liability.

CONCLUSION

In this chapter we have considered several vital questions that are the subject of fierce debate within the international community. We have asked where the use rules and meanings attached to a technology derive from and whether technologies should be seen as having a universal meaning and set of use rules or whether each state should feel free to steer and define a technology's role within their own society in accordance with their own values and history.

We have considered whether technology has a life of its own or whether technologies can ultimately force changes in individuals or societies. Here, we have asked how effective it is ultimately for states to attempt to create use rules and place constraints upon the use of this technology.

Finally, we have attempted to integrate the story of the internet within a larger set of issues. In the last section of this chapter, we have considered the degree to which policy making in regard to the internet should be considered as a unique set of questions that will require unique policy solutions or whether many policy issues related to the internet can be either grafted onto existing rules and structures. We have also considered the ways in which many of the qualities that allow us to describe the internet's evolution as unique—including the fact that this "territory" is unowned and global in scope as well as the fact that technical specialists and business interests have been highly involved in its creation—can actually be found to parallel developments in other areas of policy making from the fields of maritime and securities law.

As this chapter has shown, cyber policy making is rapidly evolving and highly conflictual. Compared to other sectors in which states make policies (such as working together to overcome a pandemic disease), it appears that states do not share a consensus regarding how to regulate cyberspace, what a good or healthy cyberspace might look like, or whose responsibility it is to create that space. We take up this issue again in Chapter 6 on internet governance.

QUESTIONS FOR DISCUSSION

1. Visit this site to download a copy of the 2018 United States National Cyber Strategy: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

   Respond to the following questions after reading through the document:

   a. How does the US vision of cybersecurity describe the relationship between security in real space and security in the online environment?
   b. What are some values that the US national cybersecurity strategy ascribes to the online environment (i.e., free and open)? Do you think that other nations would agree with this US vision? Why or why not?
   c. Can you find any phrases in the document that suggest that the United States is laying claim to the internet as belonging to or controlled by the United States? Write them down. Do you agree with these ideas? Why or why not?

2. Consider China's example as it struggles with how and when to use surveillance tools. In an article published in the *Financial Times* called "Inside China's Surveillance State," the authors quote a German minister who suggests that any nation would wish to keep its citizens safe, and therefore, it would be foolish for a nation to refuse to use facial recognition technology if it were available.

   a. What do you think? Can we have a strong state that acts internationally in the online environment that won't feel compelled to turn these same technologies inward to monitor and police their own citizens?
   b. Should there be an international norm against using the internet to spy on your nation's citizens? And how easy or difficult would it be for the international community to enforce that norm?

3. Read the essay "Can the Internet Be Saved?" found at this website: https://mondediplo.com/outsidein/can-the-internet-be-saved.

   a. Does this article reproduce the technological determinist view? Do you agree with it?
   b. Can states change the internet's meaning and parameters, or must it exist in its present form?
   c. What types of measures might you come up with to reform this technology, and what facets of its current form might you eliminate—anonymity, net neutrality?

KEY TERMS

Affordances 37
Dark web 52
Deep web 52
Dual use 39
Emerging technology 46
Free good 37
Function creep 45
Grafting 54
Mature information society 34
Net neutrality 37
Open source software 50
Social construction of technology 45
Social credit system 41
Standards war 40
Surface web 52
Technological closure 45
Virtual private network (VPN) 47
Wassenaar Arrangement 54

FOR FURTHER READING

Klimburg, A. *The Darkening Web: The War for Cyberspace* (New York, NY: Penguin, 2017).

Morozov, E. *The Net Delusion: The Dark Side of Internet Freedom* (New York, NY: Public Affairs, 2016).

Schmitt, M, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York, NY: Cambridge University Press, 2017).

Singer, P. W., and E. Brooking. *Likewar: The Weaponization of Social Media* (New York, NY: Houghton Mifflin, 2018), 3.