Learning Objectives

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

1. Define governance, and relate it to ideas of power, sovereignty, and rule making.

2. Describe multistakeholder governance in internet regulation.

3. Name major agreements and events in the evolution of multistakeholder governance.

4. Describe the players who participate in multistakeholder governance in the internet area and how this differs from other types of international governance.

As we have seen previously, the internet can be viewed as an international "territory" that brings together a variety of actors to carry out a variety of functions in the online environment—from participating in commerce to sharing resources like information, data, and entertainment. It has also been described as an international common in which participants from nations and groups come together to share resources as well as to share in the risks that might arise in this environment. In the liberal internationalist lens, the internet is seen as a vehicle that fosters interdependence through creating situations in which states need to work together cooperatively, both relying upon and creating an atmosphere of trust.
At the same time, as we have noted, the realist view suggests that the internet is fundamentally a space of anarchy. Risks arise and are challenging to deal with precisely because there is no one central governing authority whose job it is to regulate this environment. For this reason, the internet was initially described as a frontier, or even as the Wild West.

In this chapter, we consider several questions related to the structure of the internet as an international space. As noted previously, in the “real world,” the global system has emerged over a period of hundreds of years, evolving structures of organization, agreement, and cooperation among its members. In some narratives, the creation of consensus among states about what constitutes right or ethical behavior in the international system is described as “evolving”—or emerging naturally from the bottom up as a result of political development. For example, those who write about human rights often tell a story about how, as people have become more educated and scarcity has lessened, people and states have reached a consensus internationally regarding the fact that all humans have individual rights.¹ In this view, states can cooperate in, for example, observing human rights agreements like the United Nations Universal Declaration of Human Rights on the basis of these shared values and norms. Similarly, analysts describe how states naturally, over time, evolved the notion of state sovereignty, or the idea that a state can control what happens in its territory. Finally, customary international law, which forms the legal basis for the resolution of many disputes among states in the global system, is a system of legal understandings that has evolved over hundreds of years. States may accept that a legal obligation—or a constitutional prohibition—exists regarding carrying out a specific action in the international community because doing so has become a “custom,” and there thus exists an expectation that an issue will be handled in a particular fashion. Such customs evolve as legal suits are undertaken, legal rulings take place, and problems are resolved. The Universal Declaration of Human Rights is an example of customary international law because it serves as a codification of a consensus about the meaning and place of human rights in the global system that has evolved gradually over time.²

However, as noted in Chapter 1, the internet environment differs from real territorial space because this technology has emerged and expanded so rapidly, quickly becoming a vital part of our lives today. Many of the critical building blocks of the international system in the real world appear absent in cyberspace. Currently, there is a lack of consensus in three areas: Not all actors in the international system agree that states should be the primary organizing unit for cyberspace, as they are in the global order. Also, states disagree about whether or not the internet should be construed as territory that can
and should be subdivided along state lines. Is it reasonable to speak about Russian cyberspace or American cyberspace, or is cyberspace better understood as a global commons or international territory like the ocean or outer space? Thirdly, states disagree about whether there are norms and values that states should be compelled to observe in cyberspace.

**NORMS AND CYBERSPACE NORMS**

Here, we can also point to a disagreement about where a norm comes from. Norms are “collective understandings of the proper behavior of actors.” Norms can be either informal or formal. Formal norms are codified into law and are enforceable, whereas informal norms do not have the force of law. An informal norm or rule of behavior might be something like “world leaders can expect that other world leaders will not publicly call them names,” whereas a formal norm would be something like a prohibition on torturing prisoners of war, which is codified and enforced by the Geneva Convention. Both informal and formal norms together, in the words of Barnett, form a “normative web that constrains (a state’s) foreign policy in general and its use of force in particular.”

Although some analysts have argued that norms about how states should behave (e.g., in regard to conflict and respect for one another’s borders) emerge organically in the international system, other analysts believe that norms can be imposed upon states from the top down and that wealthy and powerful states may act to impose those norms upon less affluent, less powerful states. Because the internet is so new in comparison to the international system (with an age of only forty, as opposed to nearly four hundred years for the Westphalian state system), analysts disagree about whether norms truly exist in cyberspace and whether it is possible to either create formal cyber norms from the top down or bring about their creation from the bottom up. Finally, we can return to the uniqueness debate that we introduced in Chapter 2 to ask about whether international laws should be expanded to also apply to cyberspace or whether new rules and regulations need to be created in this new space.

Thus, a central question in this chapter is: If structures of governance and organization for cyberspace have not yet emerged organically, then can they (and should they) be created and imposed from the top down? That is, can the major players in cyberspace today—from states to international organizations to corporations—come together to agree on what sorts of regulatory frameworks should exist in cyberspace, and can humans thus act to build cyberspace, not merely as a technical entity but as a political entity as well?

This chapter considers three issues: First, is it feasible or desirable to create some form of international institution or international structure (or structures) to regulate the internet? Here, we consider the concept of governance. Next, in the absence of an overarching governance structure for cyberspace, can states still engage in policy coordination in cyberspace on regional and international levels?
Finally, we consider the matter of norms and values. Is it reasonable to expect that a consensus will emerge regarding the norms and values that states and other actors should adhere to in resolving conflicts in cyberspace?

Creating Structures of Governance

We begin by considering how creating a governance structure for cyberspace is and is not a unique problem. Although some arrangements of governance (like customary international law) have emerged or evolved organically, rather than being steered from above, states have also routinely sought to explicitly create structures of governance in a variety of arenas, particularly in the period since the eighteenth century. That is, states do regularly cooperate to regulate activities and actions within the international community. They engage in rule making and standards setting—establishing normative understandings regarding how states should treat other countries within the global system as well as how states should treat their citizens within their territory. International organizations like the United Nations and the World Trade Organization exist to create and enforce both formal and informal standards in the areas of conflict, conflict resolution, human rights, and free trade.

Here, some authors argue that states engage in rule making when a consensus already exists. In this way, regulation can be seen as merely the formal acknowledgment of an agreement that has already been made or that already exists. (Here, analysts may speak of a convergence of standards and concepts regarding what a good or right order would look like.)

However, critics of international organizations ask whether organizations like the United Nations are acknowledging a preexisting consensus or imposing Western standards upon other nations under the guise of behaving as though such norms and values are universal values. Some states, particularly in the developing world, have argued that wealthy nations like the United States, who contribute the majority of funding to the United Nations, actually play an outsized role in the events that occur in this policy body. They argue that the United Nations often seems to impose its agenda and its values upon other nations, who then comply because they need foreign aid rather than because they necessarily agree with the policies. For example, current initiatives within the United Nations to guarantee and uphold the rights of women, as well as the LGBT community, are fiercely opposed by many African and Middle Eastern nations. These leaders argue that the values of the United Nations, in this instance, are not universal values but rather Western values that are not in keeping with their own nations’ historical and religious sensibilities. The United Nations has seen contentious policy debates on issues ranging from whether it is appropriate for states to draft child soldiers into conflict, whether children should be allowed to marry, and whether children have the same rights as adults or a more limited set of rights, with the final authority belonging to their families.

Other critics have argued that in the final analysis, bodies like the World Trade Organization and the United Nations are relatively weak bodies with no
real authority to enforce the standards and rules that they are attempting to set. The chaotic environment of the international system, such critics feel, mitigates against the ability of global governance to ultimately work.9

**Issues in Internet Governance**

We can see echoes of these same debates in the pages that follow, as we consider what it means to establish international governance in cyberspace. In this chapter, we consider some key ideas from international relations theory—like state sovereignty—which analysts use to understand and describe the role of states within the global system today. Throughout this chapter, you will be asked to think about how well or poorly concepts like sovereignty and territorial integrity can be “borrowed” and applied to thinking about interstate issues in cyberspace. Here, we can refer back to the uniqueness debate in asking whether it makes sense to think of cyberterritory as an extension of physical territory (in which case we can take traditional international relations concepts and graft or map them onto cyberspace) or whether we should think about cyberterritory as something so fundamentally different from physical territory that such theories do not apply.

Some critics suggest that the environment itself is far too chaotic and that the interests that currently exist in cyberspace are too different and too disparate for them to be effectively incorporated into a formal institutional body that would rule and guide the internet. Moreover, some critics, notably Russia, have argued that any organization that might be created to regulate cyberspace will not be apolitical.10 Here Russia claims that in the past, the United States participated in the United Nations when it suited its interests to do so, often utilizing the United Nations as a vehicle for carrying out US foreign policy interests under the guise of internationalism. In some instances Russia has accused the United States of hypocrisy, in arguing that the United States has sometimes adopted policies formally while informally seeking to violate them—in, for example, officially supporting the notion that states are sovereign in their domestic affairs while simultaneously intervening in others’ sovereign affairs on the grounds of preventing human rights violations or humanitarian disasters. In the same way, Russia argues, any international organization that is created to regulate the internet is more likely to embody the values of the United States, which created the internet, than it is to represent an international consensus about the role and meaning of the internet—if, indeed, such an agreement even exists.

As we will see in this chapter, each of these issues—whether an organization is genuinely international or merely a cover for the agenda of a few powerful states that use the organization for their purposes, the degree to which the creation of international organizations represents a threat to national and territorial sovereignty, and whether there are genuinely global values that an international organization should uphold and defend—has been debated within the context of cyberspace as well.

Also, we can ask whether there has indeed been convergence or evolution of shared norms among states regarding issues like the proper use of the internet, the
values that the internet should be governed by, and the rules that should govern activities online. If such shared norms have not evolved, we can also ask whether they can be created by the players currently working to shape cyberspace, including states, international organizations, technical groups, and global corporations like Facebook and Twitter.

The Global Governance View

As we saw in Chapter 1, in the heady initial days of the internet’s birth or creation, technology specialists like John Perry Barlow claimed that traditional international relations ideas like state sovereignty, citizenship, and even states were irrelevant in cyberspace. In this view, citizens were instead netizens with no particular loyalty to a state. Barlow envisioned cyberspace as a place where the major actors would not be states but where instead the internet would be regulated by loose confederations of volunteers, many with technical expertise, who would administer the internet. That is, they believed that nonstate actors like the Internet Society, and volunteers such as those who manage the root directories of the internet, would be able to perform the work of keeping the internet running on a technical level.

This open information viewpoint was based on specific values, including the benefits of transparency, openness, and freedom of information. Advocates of this view believed that cyberspace should not be carved up into territorial domains and that so-called digital sovereignty was neither possible nor desirable. Furthermore, they thought that it was possible for all of those involved in building cyberspace—technology specialists, corporations, nongovernmental organizations, and states—to work together to create a secure cyberspace without imposing ideas like sovereignty or territorial control or ownership on the space.

Today’s internet, such analysts argue, is being built from the bottom up by a broad coalition that includes nonstate actors like the International Telecommunications Union and the Internet Society, corporations like Facebook and Twitter, and international organizations like the United Nations Intergovernmental Group of Experts. As a result, these analysts believe that the best vehicle for building a stable and orderly internet for the future is to create institutions of global governance through a multistakeholder process in which states would be one of many actors involved in building institutions, policies, and norms for the internet.

In this view, global governance requires a system in which authority is granted to actors beyond the state, including to regional and international bodies. Also, it requires the ability to make and administer policies on a suprastate level and the distribution of governing resources among a diverse number of actors. Global governance advocates, then, see the evolution of multistakeholder global governance in cyberspace as a logical outgrowth of the internet’s unique history and organization. They also present the development of global governance and the waning of state power as the outcome of an inevitable process—or an evolution of the environment—and suggest that there is little that states or particular leaders can do to alter or change the shift toward this new form of organization and policy making.
THE CYBER SOVEREIGNTY POSITION

However, many states—including those that are the most cyber powerful—disagree with this orientation toward global governance and do not feel that the best way to evolve or create a stable, peaceful internet is through a multi-stakeholder approach. Instead, these actors argue that states should remain the dominant unit of organization within cyberspace and that states should act as the guarantors of a stable internet. This position can be titled the cyber sovereignty position in contrast to the global governance position.

Many analysts credit the United States with “inventing” the cyber sovereignty position, and they trace the idea back to the 1996 decision to form a US Commission on Critical Infrastructure Protection. The United States was also the first nation to draft a National Strategy to Secure Cyberspace under President Bush in 2001 as well as to create a cybersecurity branch within the Department of Homeland Security. The US Department of Defense also played a key role in creating the cyber sovereignty paradigm. Arguing from a realist perspective, the US Department of Defense established the understanding that states could claim sovereignty in cyberspace—that is, that states had a claim to territory in cyberspace as well the claim that states should get to be the final authority regarding actions and activities that occurred in “their” cyberspace. In this view, then, cyberspace was not merely international, ungoverned waters but instead could be broken into Russian cyberspace, American cyberspace, and Chinese cyberspace. Indeed, in 2010, Russia first defined the notion of a military cyber command, which it then began establishing. That same year, the United Kingdom defined a cyberattack against its critical infrastructure as a Tier One Threat.

And as far back as 1999, the United States began asking when a cyber operation might be said to violate another state’s sovereignty. That is, when might a state be able to make a claim to an international body, like the United Nations or the International Criminal Court, because a cyberattack had violated state sovereignty? By 2014, the United States in particular had begun enforcing its claims to sovereignty over its internet. That year, the US Department of Justice indicted five Chinese soldiers for hacking and espionage against US companies.

States Enforcing State Sovereignty in Cyberspace

Cyber sovereignty proponents thus believe that the internet is not merely an abstract idea but one based on physical geography or topography. The internet cannot run without crucial components such as undersea cables and cable operators, search engines, and social network sites. Each of these elements has strategic significance for a state because it represents a bottleneck through which information flows and a place where it could be monitored, stolen, attacked, or blocked. Indeed, in recent years, many states have acted to shut down their citizens’ access to the internet through what has become known as an internet kill switch. Repressive
nations have shut down or cut off citizen access to the internet to prevent domestic demonstrations or as a way of prohibiting the free exchange of information in the run-up to an election. In 2015, Congo’s government shut down citizen access to the internet as a response to demonstrations calling for the imposition of term limits that would have prevented Congolese President Denis Sasou N’Guesso from running for another term in office. Turkey’s government introduced legislation in 2016 allowing authorities to suspend citizen internet access in situations that presented a threat to the public order. India has implemented regional internet cutoffs in response to minority activism and social unrest, and Egypt cut off internet access during the 2011 Egyptian Revolution. Most recently, Zimbabwe has engaged in internet cutoffs as a response to social demonstrations. Moreover, even democratic nations like the United Kingdom and the United States have entertained the possibility that all states should have the ability to shut down the internet to protect critical infrastructure from threats or prevent a virus from spreading online. Here, the ability of a state to control citizen access to the internet seems to bolster states’ claims that they do indeed “own” their national cyberspace—although, in some instances, international organizations like telecommunications providers have succeeded in overriding these controls.

Most recently, Russia’s parliament has begun considering a law that would require Russian internet providers to ensure the independence of the Russian internet. By 2020, Russia hopes to route 95 percent of its internet traffic locally rather than having it pass through the international network. Russia will conduct its first test of the ability of its internet to function internally through disconnecting from the international network in 2019. Here, Russia’s leadership has referred to digital sovereignty, arguing that each state has the right to determine what its state interests are in cyberspace along with the ability to structure its cyberspace in a way that best reflects and achieves those interests. Here, Russia’s leadership argues that just like a state can control which goods and services can transit through its territory through the use of trade agreements, economic legislation, and export regimes, the Russian state should be able to control what sorts of content and ideas can transit through its information space. They also argue that just like you go through customs and are monitored when you enter a foreign country, the Russian government should be able to look at and control all communications that transit in and out of Russia.

And in 2015, China enacted its own China Cybersecurity Law, which provided the legal basis of China’s claim to comprehensive control of its domestic cyberspace. This same law also noted that China would engage in active cyberdefense to defend its cyberspace.

**Cyber Sovereignty in Military Doctrine**

The notion that a state owns and controls its cyberspace also appears in the military doctrines of many countries. Here, states, beginning with the United States, argued that states had the right to control and administer cyberspace as a “domain.” In military doctrine and strategy, the state recognizes five domains
of warfare: land, air, space, maritime, and cyber. International legal rulings have
created an understanding that a state has the right to control its territory (land
domain) as well as the airspace above it (the air domain) and that others cannot
transit through it without asking permission. It also controls its territorial waters
(maritime domain), although it does not control any part of outer space (space
domain). Thus, satellites can travel freely in orbit.

The US Department of Defense thus contends that an unauthorized intrusion
into a state’s computer systems would constitute a violation of their cyber domain
and thus a violation of state sovereignty. Also, if an act led to the effects being felt
in a state, that state could also claim its sovereignty had been violated.

The US Department of Defense defines the cyber domain as

a global domain within the information environment consisting of the
interdependent networks of information technology infrastructures
and resident data, including the Internet, telecommunications net-
works, computer systems, and embedded processors and controllers.14

From this perspective, an actor could be said to have violated a state’s sov-
ereignty in the cyber domain through carrying out a physical (or kinetic) attack
on hardware like a cable that carries data to and from a state, or it might include
an activity like someone hacking into a computer that belongs to the Penta-
gon. It might also include an attack on a state’s critical infrastructure, defined by
the Department of Homeland Security as those sectors whose assets, systems,
and networks, whether physical or virtual, are considered so vital to the United
States that their incapacitation or destruction would have a debilitating effect
on security, national economic security, national public health or safety, or any
combination thereof.

Norms and Laws in Cyberspace

That is, adherents of the cyber sovereignty position believe that the norms
governing state behavior in the real world of physical territory can also be exported
and applied to the world of cyberterritory. If we apply these understandings to
addressing conflicts in cyberspace, then an actor could be said to be violating a
state’s sovereignty were it to attack targets that are physically within a state’s bor-
ders or owned by a state. In this view, then, a state could claim to have been invaded
or attacked if another country or actor attacked targets such as its critical domestic
infrastructure—even if these targets are private companies (like your telephone
company) rather than state-run or state-owned enterprises.15 In 2016, NATO rec-
ognized cyberspace as a military domain, following the lead of the United States.
In subsequent years, it has issued documents such as the Tallinn Manual, which puts
forth the understanding that international law applies to cyberspace.

However, there is still a debate about whether cyber norms merely codify
an existing consensus or whether they more accurately reflect the preferences of
strong states. Thomas argues that norms can and do reflect both a state’s foreign
policy interests and the distribution of power. He writes that “a strong state can thus help to structure the international system in ways that are favorable to it through acting to impose certain norms and lend them legitimacy.”

A Consensus regarding Global Cyber Norms?

Today, many leading global powers, including the United States, China, and Russia, would all like to be the state that gets to define global norms regarding cyberspace, its values, and what constitutes sovereignty. And today these states do not agree on what these values are or on the extent to which global norms for structuring cyberspace and interactions within that space are truly international. Here, the United States argues that cyberspace is indeed territory that states can defend, claim, and own. However, at the same time, the US position is that states do not, therefore, have the right or the ability to do anything that they want within the confines of “their” cyberspace. Here, the United States has historically identified “universal” values such as the right to assemble and the right to freedom of speech as existing within cyberspace, regardless of who claims to own that cyberspace. Thus, US policy makers believe that states have limited sovereignty in relation to what takes place in “their cyberspace.”

Russia and China, in contrast, describe that the norm of state sovereignty in cyberspace as more absolute. A state that owns its territory, they argue, also has a right to protect its citizens from sometimes immoral and corrupt foreign influences, even if that means imposing what outside observers might label as surveillance or censorship. Here, both China and Russia reject the claim that individuals who use the internet are somehow, therefore “global citizens.” Instead, as Cho and Chung note, people have IP addresses that are attached to physical locations as well as e-mail addresses that may contain geographic prefixes. They access the internet through ISPs that are registered in a particular state and access platforms that are also registered to physical addresses.

As a result, states utilizing the full (rather than limited) cyber sovereignty perspective claim full legal jurisdiction over their citizens and their activities as well as the activities of ISPs and related providers that act within their geographical space. In both Russia and China, this claim justifies establishing digital identification systems that would allow the state to track all of a citizen's online activity and to aggregate all of the data streams produced by an individual.17 Such data streams can then be used in making decisions about whether an individual should be permitted to borrow money for a purchase like a house or to have access to state or private-sector jobs that might require them to have a large amount of responsibility or access to classified materials. That is, they can predict whether someone would be a credit risk or a security risk.

Furthermore, the full cyber sovereignty position justifies states’ claims to own their citizens’ data and communications. These claims may include the right to store data within the geographic confines of their state or to access the data of others stored within their country. In this view, states can also exercise control over how their citizens behave in cyberspace. This may mean removing the option of
anonymous browsing or participating in the internet in favor of a system where citizens may be required to register as internet users using only their real names.

The Future of Cyber Sovereignty

Proponents of the cyber sovereignty view, then, believe that states will eventually evolve an understanding that has been described as Cyber Westphalia, based upon the 1648 Treaty of Westphalia, signed in Europe at the end of the Thirty Years War. The Treaty of Westphalia is seen as a hallmark because it represented the first time that states were able to create a new political order from the top down on the basis of mutual recognition by states of each other’s sovereign control over their territories. Similarly, Demchak and Dombrowski argue that an interstate system is evolving in cyberspace. In this Cyber Westphalia system, they believe that states will be recognized as the predominant actors in the environment and that states will recognize each other’s autonomy or ability to build, administer, and control their cyberspace. Within this environment, then, states will be able to identify when another country or actor has carried out a territorial incursion into their cyberspace, and they will be able to respond accordingly, just as they would if a foreign army invaded their real territory. As these analysts write, “The frontier era of the global cyberspace ‘substrate’ that increasingly underpins the world’s critical socio-economic systems is thus nearly over. A further transition towards what will eventually be the cybered interstate system is now taking place.”

Here, analysts point to the decision by the United Nations in 2001 to create the Group of Governmental Experts (GGE) for cybersecurity as the beginning of the cyber Westphalia model. They argue that the equating of cyberspace with cybersecurity made it inevitable that states would take a leading role in securing and building cyberspace. They also point to a 2013 activity report by the GGE working under the United Nations Office for Disarmament Affairs (UNODA), which stated that states should have jurisdiction over the information communications technologies infrastructure within their territories. The publication in 2013 of the Tallinn Manual on the International Law Applicable to Cyber Warfare is also seen as a critical development in the growth of cyber Westphalia because Chapter 1, Paragraph 1, of that document specifies that “a state may exercise control over cyberinfrastructure and activities within its sovereign territory.”

Realism and Cyber Westphalia

In this view, if international organizations (including international technical organizations like ICANN) play a role at all in global governance of cyberspace, they exist primarily as manifestations and extensions of a particular state’s power. Also, in this view, because so many technology-based international organizations either arose in the United States or are funded by the United States, such entities exist primarily as extensions of American state power in the global system rather than as separate actors.
In this realist view, then, cyber sovereignty is a critical component of a state’s cyber power and its overall power. In this view, a state needs to control its own “cyberterritory” to be considered a cyber power. A nation that depends on another power—like a stronger state or an international organization—to defend its critical infrastructure from attacks is considered to be a weak cyber power. Moreover, in this view, a state that ceded any amount of sovereign authority to an international organization to create cybersecurity as a collective good would be viewed as displaying weakness. Cyber Westphalia advocates then view cybersecurity as an individual good that states create for themselves rather than a collective good that countries create together in cyberspace.

**Cyber Sovereignty: The Isolationist Variant**

In the most extreme cyber sovereignty view, then, a state might aim for autarky or a situation in which it is utterly dependent upon its resources and did not depend on any other nation for its existence politically or economically. A fully autarkic state would thus aim to have its internet operate from its own indigenously supplied search engines, news sources, and social media platforms. The state could therefore effectively have complete control over the resources that its citizens could access and how news and other information would be presented to them and used by them. In many instances, this may mean that a state does not aim to eventually have a 100 percent internet penetration rate among its citizens where all have internet access; instead, it may confine internet access to a smaller or self-selected group of individuals.

An autarkic model, thus, rejects the claim that there are universal values that either reside in the internet itself (such as a desire for openness and transparency) or that all citizens should have a claim to by virtue of their global internet citizenship. Instead, the state claims the right to administer its cyberspace and to shape and create that cyberspace in line with its ideas and values derived from its own culture and not from the internet itself. Today, we can point to North Korea as the most restrictive information environment because its “internet” does not actually connect to the international community’s systems. Also, we can see how both Russia and China are moving toward situations in which citizens would utilize their own state’s search engines, auction sites, and social media rather than relying on those created by international platforms like Twitter or Facebook.

Cyber sovereignty advocates also reject the claims that there are specific human rights that all citizens throughout the world have by virtue of their humanity, which can be grafted onto the regulatory regimes, norms, and values associated with the internet. That is, a state that claims cyber sovereignty may reject the United Nations’ claim that internet access is a human right that needs to be extended to all citizens. It may also deny the claim that allowing citizens access to a free and open, unregulated internet is a state’s responsibility. Instead, countries claim their right to engage in censorship, filtering, and monitoring of their citizens because they control and administer the territory of their internet.
In evaluating the growth of cyber sovereignty, then, critics have warned about a growing Balkanization of the internet, suggesting that in the future, we may not have merely one international internet but, rather, a system in which there are multiple different internets: a Russian internet that reflects Russian values and interests, an American internet, and a Chinese internet, for example. The problem with Balkanization, however, is that groups of people no longer come into contact with one another in an international space where all ideas are welcome. Instead, people may encounter an echo chamber where they interact only with others who share similar values. Scholar Cass Sunstein has warned that this increasing tendency for users to wall themselves off into their internets where like-minded individuals surround them is likely to lead to people developing more polarized or extreme views than they might in a place where all opinions and ideas were welcomed and considered.24

The Downside of Cyber Sovereignty

However, what are the pros and cons of a cyber sovereignty model of internet governance? In her work, Cavelty notes that there is indeed something compelling about breaking up the internet along national lines. It appears to offer states a large measure of control—in that they can establish their internets, protect their citizens from harmful outside influences (including real threats like cyberterrorism or perceived threats like “spiritual pollution” by Western ideas), and better carry out cybersecurity and protection of critical infrastructure. However, she and others warn that establishing the precedent that states alone are responsible for structuring “their cyberspace” may also mean creating a recipe for autocratic control and abuse of human rights.25

And technology scholar Berman argues that states have a unique power in the cyber arena to not merely forbid activities that are not socially sanctioned but rather to create an online environment or architecture (through the use of code) in which the ability to exercise choice and engage in anti-state activity, for example, does not exist. He argues that, for example, it is preferable to have a law against speeding that citizens must decide to follow than it is to have a state that produces cars that are incapable of speeding. Granting states unlimited ability to shape their national internet architecture, he argues, is giving them unprecedented regulatory power and robbing citizens of the ability to choose how they behave in cyberspace.26

Most worrying to those who are advocates of the multistakeholder model is that digital sovereignty appears to give states the right to engage in almost unlimited surveillance of their citizens’ online activities. States would be free to declare certain types of online behaviors illegal, often based on national norms and values. States would be able to wall off their citizens from the whole international internet, allowing them instead access only to those parts that are seen to be in keeping with the state’s values and policy priorities. In this model, then, citizens who live in a repressive society would not experience a markedly different environment in cyberspace. Instead, all of the same repressive structures, like press censorship
and surveillance, that occur in the real world would merely be reproduced in that
nation’s cyberspace.

In this state-led model of internet regulation, then, other players, like ISPs
or content hosting platforms, are subordinated by the state to state interests with
only limited autonomy to act on their own. In some cases, ISPs and online service
providers may be state owned directly. In other instances, they have been “respon-
sibilized,” or been enlisted as guardians of public morality, national security, and
individual privacy.27 We will return to this question in our discussion of online
privacy under the digital sovereignty model.

RUSSIA’S CYBER REALIST VIEW
OF CYBERSPACE

In considering the cyber sovereignty view of internet governance, it is useful
to consider how Russia’s leadership has articulated this view because they are a
leading proponent of this view. In the Russian view, as in the American military
view, cyberspace is seen as anarchic. It is an arena of conflict. Also, in keeping
with the realist position, Russian military planners believe that the most crucial
goal in creating a national cyber strategy should be the preservation of the state
or the assurance of state survival. This lens, then, assumes that other countries
are not potential partners for cooperation but are rather potential enemies whose
motes are to challenge Russian survival both in cyberspace and in real space.

In the Russian view, then, the Russian segment of the internet (known as
RU-Net for the prefix .ru which accompanies all Russian internet addresses) is
considered an extension of existing territory in the Russian information space,
and RU-Net is viewed as a platform for the Russian state. The Russian cyber
sovereignty view then believes that each state can and should administer its own
information space—in terms of providing security of its hardware, software, and
information quality in addition to content and information flows. In this view, then,
the ideal situation may be one in which Russia’s internet is mostly inwardly ori-
ted, based on the Russian language and dependent on Russian language plat-
forms (like the Russian equivalent of Facebook, V Kontakte).

Here, the Russian view echoes the older Soviet Communist language about
the danger of “capitalist encirclement.” At the height of the Soviet empire, the
leadership had a somewhat paranoid view, believing that the United States, in par-
ticular, wanted to support satellite states and engage in proxy wars around the
world to encircle the Soviet Union with states hostile to the communist belief
system and way of life. Today, Russia feels threatened by the growth of NATO and
the European Union (EU), with the offering of membership or provisional mem-
bership to Eastern European nations that were previously part of the Soviet Bloc.
An article published in 2018 by Sergei Shoigu, Russia’s minister of defense, also
suggests that Russia reads the establishment of cyber operations centers in Europe
as a sign of “intense military preparations” by Europe against their neighbors to
the East, including Russia. In this same article, Shoigu evinces concern about the establishment of CERTs throughout European states that are modeled upon the US CERT and voices suspicion regarding US motives in assisting in establishing a European Center for Excellence in Countering Hybrid Threats opened jointly by the EU and NATO in Helsinki in 2018. In this way, Russia’s fears about participation in the internet—which it sees as Western in origin, orientation, and values—is related to its fear of territorial encirclement in the real world. In the Russian mind, having its citizens participate in a free and open internet that includes having unrestrained contact with Western citizens and Western ideas thus represents a sort of virtual capitalist encirclement.

As Ristolainen points out, Russia uses different terms to understand and describe cyberspace. Their view of “information security” is broader than the Western view of cybersecurity, which focuses on defending and protecting internet software and hardware. In contrast, in the Russian view, information security refers to defending and protecting internet software and hardware as well as protecting the information that people are exposed to as well—through keeping it free from falsehoods, extremist ideas, and ideas that may constitute a form of “spiritual pollution.” Here, Russia worries as well about the fact that the majority of information available on the internet is in English. Instead, the government wants to make sure that the Russian language is preserved by producing or assisting in the production of high-quality Russian language information for its citizens.

Not all analysts see these issues from the same viewpoint, however. James Lewis argues that the “information revolution” is more of a threat to state survival for authoritarian regimes. He writes:

Information technologies create an existential threat for authoritarian regimes that they are hard-pressed to manage. Authoritarian regimes, with their brittle relationship with their citizens, have reacted by trying to suppress this political effect by restricting access to information, providing counternarratives for both domestic and foreign consumption, and by creating ubiquitous surveillance regimes in a powerful effort to maintain control.

In this view, then, for authoritarian regimes in particular, there are few benefits to cooperation and few reasons to cooperate in cyberspace.

**Russian Suspicion of International Organizations**

Moreover, as noted, this digital sovereignty model also rests on suspicion of international bodies such as ICANN, which works internationally to administer and assign domain names. As we saw in Chapter 1, ICANN began as a nonprofit organization incorporated in the state of California in 1998. Initially, funding for this international body was provided by the US Department of Commerce through a contractual arrangement. However, ICANN signed an Affirmation of Commitments in 2009 with the United States, which formally ended this relationship.
Currently, ICANN is “formally independent” and administered through multi-stakeholder governance. ICANN has a board of directors that includes individuals from the technology community as well as supporting organizations including the Address Supporting Organization (ASO); the Country-Code Name Supporting Organization (CCNSO), which includes members of country-specific DNS providers; as well as the Generic Name Support Organization (GNSO), which includes individuals involved with the administration of domains like .com, or .biz. Also, there is a Government Advisory Committee (GAC), which provides a forum for states to weigh in on issues related to technical global internet governance.30

However, although ICANN thus provides a forum for state actors’ involvement in internet governance, the governments of both Russia and China have objected to participating in this forum. In explaining their objections to participating on a state basis in this forum, China’s government has stated that they resent the large role granted to private-sector organizations within ICANN. They have also objected to the fact that the United States still plays the most prominent role in the organization. China has even undertaken attempts to establish its Chinese version of ICANN, which would administer Chinese IP addresses.

In this Russian view, then, a state feels most secure in cyberspace when it exercises autonomy and agency over its cyberterritory, when it can control the information flows that enter and leave its territory and when it can defend its cyber infrastructure against threats both domestically and internationally. Cybersecurity is thus an individual good best pursued by a state acting on its own through a self-help system.

Russia has therefore acted consistently to introduce resolutions to the United Nations in the area of cybersecurity. Beginning in 1998, and annually every year after that until 2011, Russia has launched a resolution titled, “Developments in the Field of Information and Telecommunications in the Context of International Security.” This resolution, which has been described as controversial, set forth the idea that there should be an international code of conduct regarding cyberspace that all states should agree to. Specifically, states should agree not to interfere in the sovereign affairs of other nations concerning cyberspace. The resolution (which was backed by many states, many of them deeply repressive) stated that signatories would not “use their resources . . . to undermine the right of . . . independent control of information and communications technologies or to threaten the political, economic, and social security of other countries.”31

**Russia’s Alliances for Cybersecurity**

At the same time, Russia has worked to form its own regional and international alliances with states who share their suspicion of international governmental bodies and who remain equally committed to a vision of national internets administered in line with national values and priorities. In 2003, Russia acted to create a multinational organization called the Shanghai Cooperation Organization (SCO). The SCO is a bloc of nations, including China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan, who have worked to voice concerns and put
forth proposals of non-Western internet users. The SCO has advocated for these states’ rights to develop their national internets along national lines and has acted to oppose attempts to create an international vision of the internet’s mission and goals.

Here, the term multilateral governance (as distinguished from multistakeholder governance) is sometimes invoked to describe this situation where states, taking the lead, reach out to other countries to create specific agreements among themselves regarding procedures for addressing conflicts and disagreements in cyberspace. That is, the cyber sovereignty perspective is not inherently conflictual; instead, it is suspicious of the use of multistakeholder approaches as the overarching framework for structuring cyberspace as well as the claim that states need to be participating on an equal footing with other types of organizations, such as civil society organizations. We can point to the conclusion of an agreement between the United States and China in 2018 in the area of cyber conflict to show that cyber sovereignty approaches have merit and that they can play a useful role in helping create global order, even if only on a limited scale.

Also, states like China and Russia have participated in multistakeholder governance organizations like the World Information Society (which we address later in this chapter). However, within these organizations, they have advocated for a stronger, more hierarchical role for states in particular and specific recognition of the state’s interests in the conduct and structuring of cyberspace. Cuihong describes Chinese officials as seeing a complementarity between multilateral and multistakeholder approaches, with both being necessary.32

As this short analysis shows, then, Russia remains deeply suspicious of the motives of other nations in cyberspace. Cyber sovereignty is thus seen as the best mechanism for limiting the overall societal effects of internet connectivity, allowing states to benefit economically in global commerce, for example, while choosing not to participate in the growth of democratic institutions. This model also will enable countries to view the internet not as a global phenomenon that will inevitably connect them to others but rather as a tool that states can use and shape as they wish in line with their history and values.

**Should America Adopt a Cyber Sovereignty Approach?**

However, American analysts have also made a strong case for states adopting a cyber sovereignty viewpoint rather than a more cooperative model. In writing about cyber power, analyst Joe Nye describes how power transition theory can be applied to cyberspace. This theory suggests that conflict is most likely to break out in a situation in which power formations in the international system are changing. Power formations might change because a great power begins to lose its leading role, or they might change due to a rising hegemon, or a state that is increasing in power, thus threatening to destabilize the preexisting balance of power. Here, Nye worries about “power diffusion,” noting that although the United States has clearly been the hegemon in cyberspace for the past thirty years, other players are
beginning to catch up to it. Brezhnev et al. write that it is easier and cheaper for a middle power to become a great power in cyberspace than it is in conventional military conflicts. They write, “Cyberspace is an offense-dominated domain with low barriers to entry, one that diffuses power away from traditionally powerful states and towards historically marginalized actors.”

Here, analysts differ about what the US response to these rising hegemons (like China) should be. Some recommend that the United States should take strong measures to keep its leading edge, but they also worry that other rising powers might band together against the global cyber hegemon that is the United States. In such a situation, it might make more sense for the United States to cooperate than to attempt to go it alone.

What Is Global Governance?

Although many states appear to be committed to the reproduction of traditional forms of organization in cyberspace, a second model has also emerged in recent years. In her work, Halbert describes the emergence of global governance—characterized by the internationalization of policy making, the diffusion of authority beyond the state, the development of procedural norms on a level beyond that of the state, and the distribution of governing resources among an increasing range of actors. She describes this emergence as a “fundamental shift” in the way that international relations function.

We can trace the term internet governance back to 1996 in the United States, when scholars at the Harvard Information Infrastructure Project (which later became the Berkman Center) published two volumes on the subject. In this study, scholars asked if the internet was in fact “governable.” That is, they interrogated Barlow’s claim that the imposition of state control and the development of institutional bodies to administer the internet were impossible. Here, Barlow argued that cyberspace was too different from regular space and that it was inherently ungovernable due to the existence of networks of actors without a clear hierarchy.

Those who advocate for the creation of supranational (beyond the state) governance structures to administer the internet as an international space argue that Barlow was wrong in describing cyberspace as fundamentally unique. Instead, they say that broad coalitions of actors—to include private and public sector partners—have cooperated to make policies internationally in many highly specialized areas (like public health, nuclear weapons regulation, or cyberspace). For example, pharmaceutical manufacturers may have a seat at the table when a body like the World Health Organization is discussing how best to respond to the threat of a global pandemic or a crisis like AIDS. In each of these situations, many functions that we previously thought of as the exclusive province of states—such as the authoring of treaties or international legislation—are today undertaken by networks of actors working interdependently and sometimes autonomously from the state. Here, Liargopoulos notes that internet governance refers to a situation in which the borders or boundaries between countries and business interests in cyberspace are “fuzzy.”

However, as we will see in Chapter 7, on the role of the private sector in cyberspace

Copyright ©2021 by SAGE Publications, Inc. This work may not be reproduced or distributed in any form or by any means without express written permission of the publisher.
policy making, the notion of public-private partnerships is again not unique to cyberspace.

However, what specifically is governance? We can define governance as a form of deliberate steering aimed at rule making. That is, governance refers to a process by which an order is created rather than merely evolving spontaneously or from the bottom up. Governance is also described as “intentional interventions directed towards solving public policy problems and enhancing the common good.” Whereas opponents of global internet governance describe it as a mechanism whereby a supranational organization might impose control over subordinate units, including states, Hofmann et al. focus on governance as a mechanism of coordination. In their view, governance occurs when groups of people come together, often through highly interconnected networks of people or things.

GLOBAL GOVERNANCE IN CYBERSPACE

In this perspective, then, the term governance can be applied to describe the work done by a body like ICANN but also to define mechanisms by which ISPs might share information about emerging threats among themselves as well as the ways in which users in the technical community might come together to share and regulate the use of a technology like open source code. Governance also occurs when organizations and content platforms share information and techniques for monitoring user behaviors—including norms regarding when users should be banned for, for example, using hate speech. Finally, Singer and Friedman argue that governance in cyberspace often aims at creating systems for interoperability among different types of systems internationally. Here, they point to the work of groups like the Internet Engineering Task Force (IETF), which is an international body that works to set voluntary standards, as well as the US National Institute of Standards and Technology (NIS), which sets standards for internet architecture. They also describe the work of the Internet Architecture Board (IAB). Both the IETF and IAB are subgroups that grew out of the Internet Society, an international group formed in 1992 that oversees most of the technical standards processes.

Here, Hoffman et al. suggest that governance is a process rather than a product or an institution. They argue that governance often involves not merely recognizing a situation in which all parties agree but instead may include de-conflicting a position in which multiple different entities disagree strongly or sources of authority to which participants might refer in resolving a dispute. Governance thus becomes a way of unraveling and sorting out these contradictions through, for example, establishing a hierarchy of existing rules and procedures that might apply to a situation that arises in the international system. In the global environment of the internet, in particular, we can identify many conditions in which there may be multiple actors claiming legal jurisdiction over an issue whose claims would need to be considered, sorted out, and coordinated.
For example, we can point to the Budapest Convention on Cybercrime, signed in 2001 by members of the Council of Europe. This agreement established mechanisms for capacity building, allowing all members to strengthen their ability to track, react to, and punish incidents of cybercrime online—through sharing resources and information or data between EU members through a central clearing house. Before the establishment of the Budapest Convention, a French policing agency would encounter difficulty in, for example, responding to a situation in which French citizens had been the victims of identity theft by a group operating elsewhere in Europe. Before the Budapest Convention, they would have been required to formally request information and assistance from the second nation’s police forces, and the procedure might be bureaucratic and lead to a slow response. The agreement put in place in 2001, however, allows states to respond quickly and efficiently to instances of suspected cybercrime through the creation of a mechanism for data sharing and cooperation.

Also, governance processes may focus on harmonizing regulations, including evolving commonly held definitions of key legal, political, or technical vocabulary. Thus, multistakeholder governance becomes a useful process for resolving issues like what constitutes an act of force in cyberspace and whether or not the Law of Armed Conflict (LOAC) applies in cyberspace. More recently, international bodies like the World Summit on the Information Society (WSIS) have examined questions like this: How do we understand election meddling and information warfare as well as psychological operations? What are the responsibilities of nonstate actors, including platforms like Twitter and Facebook, in supporting values like upholding the integrity of electoral systems? Who should regulate these activities, and how might actors be penalized who violate these accords?

As noted, governance is meant to be a cooperative process in which solutions are not imposed (as happens in a regulatory process) but instead are sought out on the basis of mutual interests. Governance is understood here not as something that emerges or evolves but rather as a process that can be “steered.” All of the actors involved act in a bottom-up fashion, feeding ideas up to a central authority that can then act to formalize these agreements. Here, Hofmann et al. suggest that this definition resembles Krasner’s definition of a regime, a vehicle for coordination in a specific subject area within international relations—that excludes contracts and policies. The description itself, therefore, fits within a liberal internationalist paradigm, suggesting that states and other actors will cooperate to produce global internet governance as a sort of collective good, which would be shared by all actors to enrich them all.

Moreover, in the governance paradigm, the state is understood to be just one among many actors involved in this cooperative process. It does not have a privileged role, nor does it occupy the top tier of some hierarchy. That is, whereas the traditional model of the international system assumed that states and international organizations were “rule makers” and other actors were “rule takers,” this distinction does not hold in multistakeholder governance in the cyber environment. Instead, in considering international questions like how best to defend freedom of information and freedom of the press online or how best to secure free electoral
discussions in cyberspace, private actors including social media platforms often appear to be leading the way in making policy.

Multistakeholder Governance in Cyberspace

In applying the term multistakeholder governance, then, we refer specifically to the fact that administering and de-conflicting international issues in cyberspace today often involves a process that includes the participation of a broad coalition of actors—from states to civil society organizations, to education organizations, to business to technical specialists.41 As Take suggests, there are three possible international forms of governance that might emerge in cyberspace: those enacted by intergovernmental institutions; transnational forms of governance (which include networks among international, national, and non-state actors); and private forms of governance (networks consisting only of nonstate actors). 42 As he notes, in each case, the organization created is a cross-border arrangement that doesn’t have formal authority or central enforcement power. Thus, as he notes, such mechanisms depend on the voluntary cooperation of participants.

But what causes participants to want to comply with the organization and to regard it as legitimate? That is, what are the conditions that the organization must meet for all players to buy into its existence and leading role?

Multistakeholder governance advocates often point to 2003 as the starting point for this way of governing the internet. They look to the first United Nations-backed World Summit on the Information Society (WSIS), which functions as a coordinating organization allowing states and other actors to work together to finance and carry out regional projects such as the creation of internet infrastructure. This group also works to increase access to the internet for citizens internationally, focusing mainly on those in developing countries. At this meeting, the WSIS formulated the Geneva Declaration of Principles. This document states that

international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, and civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the internet, taking into account multilingualism.43

WSIS has been praised for its incorporation of experts from telecommunication and information technology sectors as well as those from civil society and epistemic communities. 44

Tensions regarding internet governance came to a head in 2012 at the so-called Dubai Summit of the World Summit on the Information Society. At this meeting, many states signed an agreement that would give many internet governance functions over to the supervision of the United Nations. The United States, however, opposed this measure and passed a congressional statement voicing its opposition to either national sovereignty or international organization vision of internet governance.45
Objections to Multistakeholder Governance

In his work, Take notes that not all multistakeholder governance arrangements are regarded as legitimate, nor are the rules, norms, and values that these organizations identify as being common to all necessarily accepted by all members. He identifies several threats to the legitimacy of multistakeholder arrangements. In some instances, both participants and outside observers may conclude that the party that is making rules and establishing understandings is not representative of everyone who should be included in these deliberations. They might also raise questions of equity in, for example, asking if all of the stakeholders have been able to participate freely and equally—without undue boundaries to their participation erected (such as high dues or fees for participation). Critics of multistakeholder governance in cyberspace have raised concerns about the exclusion of representatives from developing nations that sometimes cannot afford to send a representative to conferences, such as the summits of the World Information Society. Other critics have criticized US-based groups like Google for playing an outsized role in deliberations at the expense of other smaller civil society groups and members.

However, the two most significant objections to global internet governance—the allegation that international organizations often serve the needs of wealthy actors better than they serve the needs of the disenfranchised and the assertion that at worst such organizations are “colonialist” in that they provide mere window dressing for a process in which wealthy nations impose their values and norms upon less powerful, poor nations—are not actually arguments unique to the cyber-space environment. Rather, both of these arguments can be traced back to earlier discussions within the United Nations about how issues of international development and income equities affect and are affected by global policy making overall. Allegations that developing nations mostly seek new global markets to buy Western information communications technologies, rather than genuinely seeking to empower those in the Global South, have been raised before concerning the extension of telephones and even telegraph service to the developing world. Moreover, the debate about whether those in developing nations need to share the international commitment to paying for information, rather than engaging in information theft or intellectual property theft, is again an older debate that has simply reemerged in the online environment.

Other critics have raised concerns related to transparency. That is, stakeholders may feel that they are merely being informed of all decisions made on behalf of the group but that a small inner group is not acting to make decisions without telling the group as a whole. Other concerns relate to accountability. Does the body possess clear rules and procedures regarding how group requirements will be applied and how those who fail to comply should be treated? Finally, critics have raised concerns about expertise. Here, they have voiced concerns that state representatives, in particular, may not possess the necessary knowledge to understand and administer rule making in this subject area or sector.

Those who support structuring the internet through a process of multilateral stakeholder governance tend to be reasonably optimistic about the prospects
that all actors will be able to identify shared interests (including the avoidance of shared risks) and move therefore to cooperate to achieve these interests. That is, this view assumes that there are shared principles, norms, rules, and decision-making procedures that exist and all actors can discover them through some coordinated process. Here we can consider the definition of internet governance put forth in 2005 by the Internet Governance Forum, a working group associated with the World Summit on the Information Society. This group wrote that “internet governance is the development and application by Governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the internet.”

In contrast, as we saw, advocates of cyber sovereignty tend to be much more pessimistic about the threats they see as emerging within the cyberspace environment, which they feel states are unlikely to avoid through cooperation. Critics of the multistakeholder governance model, therefore, understand this process as doomed to failure because it appears to be messy and chaotic as there are no clear rules as to who might lead this process or how.

Case Study: Online Privacy, Anonymity, and Global Governance

One way to think about the question of internet governance and universal norms is to consider the related issues of privacy and anonymity online. From the earliest dates of online activity, one of the draws of the medium for many individuals was the ability to participate in events like web browsing in an environment where one was anonymous. Indeed, early internet enthusiasts described anonymity as an unchangeable characteristic of the technology that they saw as built in by its designers. However, in recent years, many states have taken active steps to roll back this characteristic of anonymity, instead undertaking new legislative initiatives in the areas of surveillance and online privacy.

In some instances, states have implemented laws and procedures to limit their citizens’ ability to act anonymously. For example, in South Korea, in 2007, the government decided to require that users verify their identities online through submitting a resident registration number. (This would be similar to requiring US users to enter a social security number to access or create content online.) This registration requirement, however, made it difficult for non-Koreans (such as those of Korean descent who lived abroad) to access a great deal of material. In 2011, South Korea reversed this decision and no longer requires that users register with their real names.

In other instances, states have worked with ISPs, co-opting these organizations by asking them to perform activities that support state surveillance. For example, in China, bloggers and microbloggers must register their real names and personal information with their ISPs. Also, in the United States, the US Department of Homeland Security has required technology companies like Apple to provide so-called back doors to their technology, so that, for example, the government...
could bypass a suspected terrorist’s password security to access his devices to gather evidence.

States can also co-opt platforms like Twitter and Facebook, requiring that they furnish information about citizens’ online activities as well as offering state security organizations access to materials collected. For example, the US National Security Agency has utilized social network analysis to map terrorist networks. By analyzing terrorist use of tools like social media, counterterrorism analysts have been able to map linkages between key players in terrorist networks and establish who is the leader of a terrorist organization and how parts of the organization work together and with other organizations.49

Indeed, in the aftermath of terrorist events throughout the 2000s, including the September 11, 2001, attack in the United States and the July 7, 2005, London bombings in the United Kingdom, states have begun to cooperate internationally, creating both bilateral and multilateral regulations and mechanisms to govern how states should collect and share users’ social media and online data for counterterrorism and anti-crime policing purposes. For example, the 2004 EU Data Retention Directive (DRD) attempted to harmonize data retention regulations among EU member states in addition to making data available for sharing among countries.

However, from the beginning, different groups with different interests have clashed in considering how best to protect user privacy and civil rights while simultaneously creating safe cyberspace. Whereas those in the field of international cybersecurity worried about the growth of dangerous threats online, other analysts were concerned about what they saw as the massive and unbridled growth of global surveillance. These analysts began to ask what a global privacy regime that established norms and procedures for preserving citizen rights online might look like. (This approach, then, assumes that citizen privacy is a value or norm that all internet users internationally should value and seek to safeguard. It is viewed as a universal norm rather than a subject about which states can and should have different views.)

Cyber Sovereignty and the Problem of Jurisdiction

Thinking back to the digital sovereignty debate, the question that arises in considering whether citizens have a right to privacy and anonymity online is whether a state should actually have the ability to alter the terrain or working of the internet in this way to lessen citizen privacy or increase government surveillance capacities, even within its own online “territory.” In the instances described here—China requiring an ISP to furnish data regarding usernames and activities and the United States requiring Apple to provide a back door into their devices—the state has claimed to have legal jurisdiction over technological actions occurring within its physical space and within its online territory as well as over those corporations and individuals acting within that space. As a result, Western companies doing business in China have felt strong pressures from the Chinese government to comply
with Chinese rules regarding user registration—and Google has withdrawn from China due to disputes regarding whether China’s government should, for example, be allowed to access the web search results of its citizens. In response to claims that the state has harmed citizen rights through surveillance practices, countries will often claim that the risks posed to national security from online organizing in cyberspace of anti-state activities (from terrorism to democracy activism) are severe enough and that they are justified in taking such steps in seeking to control cyberspace.

However, not all players in the internet governance debate agree with state claims in this regard. Particularly in the aftermath of the 2013 revelations by whistle-blower Edward Snowden regarding the extent of US National Security Agency surveillance of citizen activities in cyberspace, European states as well as international organizations like the United Nations have attempted to speak back to what they see as state or government overreach in cyberspace and the rampant growth of state-sanctioned surveillance.

Here, we can identify two related issues in the field of internet governance. First, we can point to the legal question of jurisdiction. Here, digital sovereignty advocates would state that a nation has the right to do what it likes within its cyberspace. However, as Schmitz points out, in a globalized world, there can be many overlapping claims and many different lenses through which we can view the problem of jurisdiction. Here, she asks us to consider the matter of whether Facebook, an American corporation, has the authority to require that users everywhere use their real names rather than a pseudonym when participating in the online platform. Facebook, the corporation, is a US multinational corporation headquartered in the United States. However, Facebook also has a European branch that was established in 2008 in Dublin, Ireland. In addition, Facebook has a German subsidiary, Facebook Germany GmbH, which sells advertising and other services to German companies trying to reach German Facebook users. However, all users sign a set of agreements when they establish a Facebook account that state that they understand that all disputes are to be resolved in California, United States, under Californian laws.

Schmitz writes that Facebook’s “real name policy” might be legal in the United States but that it is also in conflict with EU laws. She notes that the German Telemedia Act “requires tele media providers to allow for anonymous or pseudonymous use of services insofar as this is reasonable and technically feasible.” Here, Schmitz argues that because Facebook’s activities regarding privacy are covered under the European General Data Protection Directive, there is, therefore, a case to be made that European law should have precedence in resolving the dispute related to anonymity.

**Ethical Issues Related to Cyber Sovereignty**

In addition to the legal jurisdiction issues raised when considering problems of online privacy, anonymity, and surveillance, we can also point to ethical issues that arise—specifically in the field of human rights. Here, the American organization
Freedom House has suggested that states that take away their citizens’ rights to browse and participate anonymously online are depriving them of their universal human rights, including the right to freedom of speech.\textsuperscript{51} Freedom House claims that citizens’ rights to online privacy are not rights that their government can choose to confer or not confer upon them because they are universal human rights that all citizens everywhere have by virtue of their humanity. Therefore, they argue, states cannot deprive their citizens of such rights, even if they are sovereign states with legal authority over what happens in their territory.

CAN INTERNATIONAL NORMS REGARDING HUMAN RIGHTS BE GRAFTED ONTO CYBERSPACE?

Can existing treaties regarding human rights be extended to apply also to cyberspace rights? Some analysts believe that two international treaties—the 1966 United Nations International Covenant on Civil and Political Rights (ICCPR) and the 1998 European Convention on Human Rights (ECHR)—might be extended to incorporate human rights as they exist in cyberspace. Here, we can consider Article 17 of the ICCPR, which states, “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence nor to unlawful attacks on his honor and reputation,” as well as Article 8 of the ECHR, which states, “Everyone has the right to respect for his private and family life, his home and his correspondence,” and that “there shall be no interference by a public authority with this exercise of this right except such as is . . . necessary in a democratic society in the interests of national security.”\textsuperscript{52}

Reflecting these understandings, in October 2013 Brazil and Germany submitted a draft resolution titled “On the Right to Privacy in the Digital Age” to the third committee of the UN General Assembly. The resolution was adopted, including the line that “the same rights that people have offline must also be protected online, including the right to privacy.” Many analysts point to this resolution as the beginning of a conversation within the international community about whether international human rights norms apply to state behaviors in the areas of surveillance, interception, and data collection.

Here, privacy advocates suggest that states must come to an understanding globally about how to balance the interests of privacy and security and whether too much surveillance can ultimately pose a threat to democracy internationally.

CONCLUSION

As we conclude this chapter, one might pessimistically find that it will be impossible to resolve international issues related to the conduct of cyberspace. The
two positions described here—the global governance perspective and the cyber sovereignty perspective—do indeed rest on different assumptions about the likelihood and desirability of cooperation. They disagree regarding who should have the authority to make decisions in cyberspace (the state or some other entity or coalition of entities). They differ as well as to what cyberspace should look like in the future.

Here, again, however, it is useful to return to our starting point—and to consider that the mechanisms that exist to govern and prevent conflict in the real world did not arise overnight but instead were created in fits and starts over several hundred years. Therefore, as we consider this issue, it may be worthwhile to look forward and to ask what cyber governance might look like ten, fifty, or even a hundred years in the future.

In the next chapter, we consider explicitly the role of the private sector in establishing and controlling the internet environment as well as the challenges and opportunities that arise as the result of the leading role which such actors play.

QUESTIONS FOR DISCUSSION

1. In his work, Klimburg describes cyberspace as a four-layered pyramid with the pyramid standing on its head. He describes the first layer as “the bones of cyberspace”—the bones are the hardware of the physical layer, such as undersea cables. The second layer, which he describes as “the neurons and nervous system of cyberspace,” is “the coded behavior of the domain: the various computer protocols and software programs.” The second layer, which he compares to human muscle systems, is data—business documents, scientific inquiries, and all of the information that the internet houses. Finally, the largest layer is the social layer, which he describes as “the actual internet of people, the total sum of human actions and aspirations in cyberspace.”
   a. As you think about these four layers—hardware, software, data, and social media—which layers do you think should be regulated by a particular state as a matter of sovereignty, and which layers would need to be regulated internationally through either multilateralism or a multistakeholder approach?
   b. Also, how optimistic or pessimistic are you about the ability to define and create norms regarding state behavior in relation to each of these layers of the internet?

2. What constitutes a violation of sovereignty in cyberspace? What are the controversies regarding these principles?

a. What values do you see reflected in this document?
b. What assumptions did the writers make about the future evolution of the internet, about its origins, and about the values that the internet represents?
c. Imagine that you are a policy maker from Russia or China. How might you read this document? What parts would you agree or disagree with? How specifically might you respond to the writers of this document in arguing for cyber sovereignty?

**KEY TERMS**

- Architecture 147
- Digital identification system 144
- Digital sovereignty 142
- Internet kill switch 141
- Open information viewpoint 140
- Platform 148

**FOR FURTHER READING**