Learning Objectives

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

1. Define key terms related to the liberal internationalism paradigm, including regime, norm, and public good.
2. Define digital superpower, and describe the role of the firm in cyberspace.
3. Compare and contrast the realist view of cyber power with the liberal internationalist view of global digital superpowers.
5. Describe challenges to the establishment of regimes in cyberspace.

In this chapter, we apply the liberal internationalist lens to consider the internet as a venue for global interactions. In contrast to the realist paradigm, liberal internationalists view the international system not as a battlefield but as a market. The battlefield metaphor emphasizes competition among the world’s players, whereas the market metaphor emphasizes the ways in which markets create order, predictability, and stability. The market analogy also emphasizes how firms (or states) are interdependent—with their ability to achieve goals occurring not only as a result of their actions but also as a result of actions taken by competitors or cooperating firms and as the result of activities that
they might participate in collectively. States can thus cooperate to share in
rewards as well as to share in the risks that might arise within a market system.

In this chapter, we also consider political economy critiques of this para-
digm for explaining the growth of the internet as a vehicle of commerce and
trade.

WHAT IS LIBERAL INTERNATIONALISM?

Liberal internationalists, in contrast to realists, believe that peace is possible
within the international system—even without an overarching authority. In this
view, states are not seen as threatened by the rise of another powerful nation
because power is not regarded as zero sum, where one state’s rise in power nec-
essarily threatens another’s position within the international system. Thus, lib-
eral internationalists are more optimistic than realists are about states’ ability to
resolve conflicts. In this paradigm, conflict is seen not as an inevitable product
of an anarchic international system characterized by competition among states.
Instead, it is seen as emerging due to shortage or scarcity; therefore, liberal inter-
nationalists believe, conflict can often be avoided through supporting the estab-
ishment of markets and bargaining agreements among states and other players.

Liberal internationalists draw upon the work of Immanuel Kant (1724–1804),
who espoused the notion of perpetual peace. This view regards the international
system as characterized by mutual interdependence among states; that is, one state’s
actions can affect everyone in the international system. This approach assumes
that due to the nature of complex interdependence both in real life and in the
cyber environment, a state cannot ultimately control the risks that it is subject to
independently but only through cooperation with other states. Therefore, liberal
internationalists believe, aware of their shared vulnerabilities, states will learn to
cooporate to solve specific problems.

And although realists argue that states always seek to increase their power (in
relation to their neighbors or the international system), liberal internationalists
point to situations in which states might concede some aspect of power or decision-
making authority (sovereignty) to engage in policy making or the achievement of
a goal in concert with other states. Here, we can consider problems like climate
change, which no state can solve on its own, because the environment is a col-
lective good, not belonging to one state, but rather shared among states with no
ability to exclude any state from this resource. All states share the rewards and the
risks associated with the provision of these collective goods. In working together,
these analysts believe, states will build trust in one another, enabling them to avoid
conflict in the future.

Liberal internationalists also emphasize ideas like free trade because the inter-
national financial system requires the cooperation of all states to function effec-
tively to create greater wealth for all states. Here, they assume that markets are the
most effective way to create order and that therefore firms or states should not try to impede the free flow of goods, information, and services that are hallmarks of that market system. One of the most significant impediments to a liberal internationalist order, then, is a state that decides to erect barriers that interfere with the actions of a market for ideas, goods, or services. A state may refuse to participate in a market system through withdrawing entirely from the market (i.e., adopting a posture of isolationism or seeking autarky) or may attempt to actively damage existing markets through erecting barriers like tariffs.

Liberal internationalists are also optimistic about the ability of capitalism itself as a set of practices and beliefs to change nations. Some analysts thus speak of convergence, noting that if states need to adopt some form of capitalism to compete in the international system successfully, then over time, states will start to resemble one another through their dependence upon market mechanisms, openness to foreign investment, and other markers of their commitment to capitalist ideology.

LIBERAL INTERNATIONALISM IN CYBERSPACE

How does thinking about the internet as a market, not a battlefield, change our perspective on state action within cyberspace? First, it lets us ask: How might states cooperate to create order within the seemingly chaotic environment of the internet? As we saw in Chapter 3, the realist lens led states to refer to “American cyberspace” or “Russian cyberspace”—rejecting the claim that states need to cooperate to secure the internet as a common good.

But in this chapter, we assume that the internet is a public good or shared international space. States, therefore, need to cooperate to preserve this shared space—because a public good is one that no one can be prevented from partaking in and also one that can be produced only collectively. Furthermore, one user’s enjoyment of the good does not diminish others’ enjoyment or use of it. We often use the term public good to refer to utilities provided by one’s city or local providers, such as water and sewage, or emergency services like the fire department. Free goods are those objects, like air, from which no users are excluded, and where again cooperation is necessary to preserve them.1

In his work, philosopher Luciano Floridi suggests viewing the infosphere in much the same way that we think about nature and our obligations as global citizens to preserve nature.2 He suggests that internet users—including states and corporations—should work to maintain the infosphere as a space where information can flow freely and unimpeded, without the “pollution” created through wasteful information practices like the creation of spam or the barriers created by filters and firewalls. The internet is thus presented as a public good or a utility.

Other analysts use the term digital economy. The digital economy is “all of those economic processes, transactions, interactions, and activities that are based on digital technologies.”3 The digital economy is thus conceptualized of as a collective
good that is both national and transnational with resources moving among states seamlessly. No state can regulate its digital economy alone, and each state is vulnerable to disruptions and risks appearing in the digital economy. The digital economy is vulnerable to risks associated with the overall international economy because it is seamlessly interwoven into so many aspects of global commerce today.

Some analysts distinguish between the digital economy and the internet economy. The digital economy is different from the internet economy in that the internet economy is based on internet connectivity, whereas the digital economy rests on the creation and maintenance of tools like e-banking, e-commerce, and e-trade.4

The Electronic Market Space

As we know, the engineers who developed the internet initially thought it should be as free of regulation and state interference as possible. Similarly, e-commerce structure designers (or architects) wanted the digital economy to be largely unregulated and free of state interference. They hoped that the digital economy would become a “pure market” that was self-regulating through the actions of market forces with little government interference in the areas of taxation and regulation.

Indeed, to a large degree, state regulatory mechanisms have been slow to develop in the digital economy due to the speed at which the digital economy expanded (outpacing the ability of states to regulate it). Moreover, the digital economy developed chaotically, and over time, private organizations, including industry organizations (like the banking industry) have stepped in to establish sector-specific governance structures and procedures.5 Global organizations have also stepped up to support these private sector efforts, including the World Trade Organization and the Organization for Economic Cooperation and Development (OECD).

Cooperating to Reduce Risks in Cyberspace

What risks does the global digital economy face? We can identify two types of risks: threats to the internet’s physical infrastructure (i.e., attacks on the physical pipelines carrying data and information) and threats in which the internet itself could be utilized as a vector. That is, the internet could be weaponized to carry viruses or materials that could harm their recipients—from corporations to individuals to states. Both attacks on the infrastructure of the internet itself, as well as attacks on secondary targets carried through the internet, could cause massive political, social, and economic disruptions to the global digital economy. Thus, states have cooperated to develop regulations and norms governing how states and nonstate actors react to, prepare for, and mitigate financial risks brought about by cyberthreats, including issues like identity theft or hacking into critical infrastructure in the banking industry.
But although we might expect states to band together to secure the functioning of the internet and to confront threats to the structure, such cooperation does not always occur for two reasons: First, many of the attacks in which the internet is used as a vector target not states but rather private actors (such as banks that work to protect their customers’ data from identity theft). Private corporations own and operate many critical networks, and they have built and administered the backbone of the telecommunications infrastructure. Thus, states often must work together with private sector actors who may not agree about the severity of the threat that they are facing or who may not be equally committed to responding to these threats.

In addition, although some of these vectored threats (like the threat of identity theft) are considered universally threatening, other types of threats may be understood differently in different cultures, and states may not all agree about the severity of these threats or the necessity of a global response. For example, nations today disagree about how severe a threat is posed to the global digital economy by practices like intellectual property theft or economic cyber espionage.

**Issue Areas in Cyberspace**

For this reason, it is not helpful to think of cyberspace risk as a whole. Instead, we can speak of issue areas, such as risks to the international financial system, risks to international shipping and transportation, or risks to the e-commerce sector. Depending on the issue area, different types of actors are involved in making policy, including nonstate actors with specialized expertise, like international legal or banking professionals. And policy makers face different constraints when making policy across different issue areas. In addition, cooperation may be of a more limited or a more long-term duration among states, depending on the specific issue area that states are trying to resolve.

If we think about states cooperating to pool their resources as mutual “insurance” against possible future losses, we see that this strategy may be more effective in some issue areas than others. That is, states will be more likely to cooperate to insure themselves against losses when there is a great deal of uncertainty about the risks states face as well as the possibility that the gains and losses will be distributed inequitably. Thus, states may be inclined to cooperate to regulate the distribution of losses in relation to threats to critical infrastructure or the stock market because the threats that states are facing are so new and novel that it will be difficult for states to predict what the likely outcome will be or how these losses will be distributed. Thus, states have thus far been willing to band together to engage in specific cooperative programs, such as ensuring that wire transfers between banks internationally are secure. In addition, it is likely that democratic states might come together to form an organization dedicated to protecting the integrity of national elections from foreign interference—given how new, novel, and unpredictable this threat is. States have also come together to create both bilateral and multilateral mutual legal assistance treaties (MLATs) for tackling issues like crime when jurisdictional issues are a significant obstacle or barrier to cooperation in gathering information about terrorism internationally.
Cyber Risks as Part of Security Risks

Just as cyber capabilities are entwined with other types of state capabilities, cyber risks are intertwined with other types of risk categories. Today, vectored attacks conducted through cyberspace often target a nation’s supervisory control and data acquisition (SCADA) systems. These systems, which are computerized and online, serve to administer the supply of many goods that households depend on, like water and electricity. In addition, military command and control systems—that carry information about military operations among military officials and between officials and the equipment that they use—are highly dependent upon the internet to carry this information. The global financial system depends on access to a resilient internet that carries information about transactions and responds to events in real time. Disruption or interference with global internet connectivity in any one sector thus affects the entire global political and economic system. Thus, using the language of issue areas, we can see that rather than speaking about cyber policy as a whole—or about cyber risk as a whole—it is useful to think about cyber policy and cyber risk in specific issue areas.

HOW DO STATES COOPERATE TO REGULATE CYBERSPACE?

Thus far, our discussion of state cooperation has been rather abstract. But how specifically do states form agreements, and what is the basis of these cooperation agreements? We can identify three specific mechanisms used by states to create collective agreements in a situation where they must cooperate to produce a shared good. First, regimes can allow states to cooperate. Next, states can utilize pooled sovereignty, in giving up a measure of individual autonomy, to cooperate with others in administering a good. Finally, states can create a stewardship model in which a third party administers the good.

Regimes

In addition to comparing cyberspace to a market, analysts often compare the risks that states face in cyberspace to global health risks. Today, no state can individually ensure its citizens’ health because germs can easily cross borders carried by people and goods (just as “viruses” can in cyberspace). Therefore, states have created both formal and informal regimes of cooperation to secure public health. Regimes are “sets of implicit or explicit principles, norms, rules and decision-making procedures in a given issue area” that states adopt collectively. For example, if a global pandemic is declared, states have agreed to work together to share information and to engage in necessary life-saving measures like shutting down borders and erecting quarantines.
Today, states have established regimes to regulate maritime commerce, international air travel, and the exporting and importing of natural resources like oil. A regime may be formally codified in a treaty, such as the Geneva Convention, which specifies how states are to treat prisoners during wars, or the Law of Armed Conflict, which defines the rules that states should respect during warfare. A regime might also be informal and more temporary in duration.

Liberal internationalists argue for the creation of cybersecurity regimes due to the high level of interdependence among states in many different sectors of cyberspace. Thus, liberal internationalists argue that there are market incentives for actors to work together to confront cybersecurity challenges as well as to share information.

ASEAN’s Cybersecurity Regime

ASEAN is a group of ten nations that cooperate in the areas of politics, economics, and now cybersecurity. ASEAN views cybersecurity as a collective good, believing that the ASEAN states are interdependent, with one’s fortunes and security depending on another’s fortunes and security. Thus, those states within ASEAN that are technology leaders—like Singapore—are not threatened by the attempts of less developed states (like Burma) to join the technological revolution. Instead, states like Singapore and China are helping developing states create technological hardware like an ASEAN broadband corridor and are also working to help them create resilient technological infrastructure, including in essential areas like banking and the financial sector, because a threat that enters through a poorly guarded portal in a developing country can quickly spread to a developed country in a shared information space like ASEAN. The more developed states are concerned about problems like miscommunication and misattribution, specifically the fear that one ASEAN state might launch a cyberattack, but that another state might be blamed.

The ASEAN nations are also creating a shared CERT, deepening their defense cooperation and working to secure the supply chain throughout the region. The ASEAN states are also working to draw up a common framework for the application of international law to disputes in cyberspace as well as to agree on shared values and norms governing state relations in cyberspace.

Analysts described ASEAN as a territory that is characterized by bounded or limited sovereignty and a high degree of regional pooled sovereignty before the advent of their efforts in the field of cybersecurity. That is, ASEAN member states have had a track record of working together in loose associations ever since the organization was founded in 1967. Here analysts...
(Continued)

sometimes distinguish between positive integration and negative integration, where negative integration refers to states’ practices of lowering regulatory and legislative barriers to better work with their neighbors, whereas positive integration refers to states’ practices of working together to implement specific policies and carry out initiatives.

Here, Hund suggests that ASEAN has failed to move beyond negative integration toward positive integration in many fields, including economic and political initiatives.\(^\text{12}\) Thus, one might expect to see limited efforts in terms of regional integration for cybersecurity. It might be easier to achieve objectives like the reaction of an ASEAN broadband corridor while formulating a common policy, like the European Data Privacy Initiative, might be more difficult because that would require ASEAN signatories to agree on values such as what constitutes the proper amount of surveillance of citizens by the government. That second type of agreement would be more difficult to achieve, given that ASEAN includes both more democratic and more repressive regimes among its members.

Sources


Pooled Sovereignty

As noted earlier, states may cede some of their independent authority (or autonomy) to work together with others to solve global problems. Pooled sovereignty refers to situations in which states choose to give up autonomy to cooperate with neighboring states, particularly in cases where a resource (such as a natural resource) is shared among members in a region. States can give up some measure of state authority to craft bilateral or multilateral agreements, including changing national legislation within their states so that it conforms to a regional set of standards.\(^\text{13}\)

Here, sovereignty may be understood not as an absolute concept (a state is either wholly sovereign, or it is not), but rather, a state may engage in what is known as bounded sovereignty. States may have complete sovereignty over some practices within their states, whereas in other areas they may cede some degree of sovereignty to a regional or international body. And the pendulum may swing back and forth between situations in which states maintain a high degree of sovereignty or control in making treaties and agreements governing a resource and cases in
which states are more willing to cede authority to governmental or intergovernmental bodies.

This arc occurs because not all attempts at creating pooled sovereignty work, as the example of Britain’s decision to withdraw from the European Union (known as Brexit) indicates. Citizens within a state may resent the notion that their state is not entirely independent but that their lives instead depend on a bureaucracy located far away that does not always seem responsive to their situations. They may resent the commitment of their tax dollars to regional projects that do not develop them directly (e.g., citizens of wealthier Western European nations have objected to financing the economic development of countries in Eastern Europe that have joined the European Union more recently). Also, pooled regional sovereignty may develop slowly just as statehood often grows only over a period of a hundred years or more. Thus, pooled sovereignty in relation to internet governance might not emerge for another thirty or forty years.

**Stewardship**

In other instances, states have created national and international trusts whose job it is to make sure that historic and natural resources within a state or global system are preserved for the current generation and for the generations to come. In allowing a national or international trust to administer a resource, or to engage in stewardship of the resource, states again cede sovereignty to this trust or foundation. In considering who might engage in stewardship of the internet as a global resource that should be preserved for future generations, we can consider the role currently being played in internet governance by actors like the Internet Society, or the International Telecommunications Union, which can be seen as acting in the role of steward or trustee of the internet, speaking on its behalf, and acting to make sure that it is preserved for future generations.

**OPPOISING THE LIBERAL INTERNATIONALIST VIEW**

States can gain much from cooperating with other states to secure a resource like the international internet. But not all states are on board with the liberal internationalist view of the internet as a collective good. Today, some states do not accept the notion that the internet is, in fact, a collective good. Other states accept this contention but do not trust other players within the cyberspace arena enough to depend on them for the provision of their security as a collective good. Finally, some analysts argue that traditional theorizing about how states cooperate to produce collective goods is not relevant to thinking about the development of today’s internet because firms—not states—have come to play an outsized role in creating, administering, and growing this entity.
Is the Internet a Collective Good?

Not all analysts agree that the internet and internet security are collective goods. The United States has always played an outsized role in its creation, its growth, and its protection and safety. Therefore, some analysts suggest that the United States will always serve as a primary guarantor of internet stability, with other states playing supporting roles. And they argue that although resources on the internet are shared, they are not shared equally. More powerful states benefit more from internet connectivity, and therefore, they argue, these states should play a greater role in securing the internet and paying the costs of doing so. (That is, in the language of realism, the United States will always serve as a hegemon.)

Other states don’t believe that the internet has to be international at all. They feel that the best way to preserve a nation’s cybersecurity is through adopting a policy of autarky or isolation—seeking to, for example, protect critical infrastructure by lessening dependence on cyberspace and reducing connectivity. Both Russian and Chinese cyberspace policies increasingly emphasize reliance upon local ISPs and hardware engineers and the localization of data within their sovereign borders. In 2018, Russia released its program for creating “the digital economy of the Russian Federation.” Russia plans to spend approximately $53 million in building up key sectors of its digital economy, including sectors devoted to search capabilities, e-commerce, content, social media, and devices and interfaces. In this realist view, then, a state’s digital economy is an essential component of its overall state power—both in terms of cyber power and traditional power capabilities. There is no global digital economy but only individual state economies that are components of state power.

CRYPTOCURRENCY AND THE INTERNATIONAL ECONOMY

If you follow the news regularly, chances are that you have heard of something called Bitcoin. Most likely you have heard that some individuals have become Bitcoin millionaires as the result of smart investing. But what is Bitcoin—and cryptocurrency—and why does it matter in international relations?

First, we begin with some definitions. Then, we explore the relationships among traditional currencies, cryptocurrencies, and the state. Finally, we consider the ethical, military, and political implications of the advent of cryptocurrencies in national and international economies.

Defining Our Terms

What is a cryptocurrency? A cryptocurrency is first a digital or virtual currency. That is, in contrast to national and regional currencies like the US dollar or
the Euro, cryptocurrency does not appear as paper money and is not printed in a conventional sense. Instead, individuals can use their computers to "mine" cryptocurrencies, like Bitcoin, through solving advanced mathematical problems for which they are paid sums of currency.

Here, one should note that although Bitcoin is the most well-known of existing cryptocurrencies, it is not the only one. Any currency scheme that relies on decentralized ledger technology, encryption, and mining is referred to as cryptocurrency. Different cryptocurrencies have different features, and users may find one type of cryptocurrency more useful than another, depending on the functions they are planning on carrying out using the currency. For example, Monero’s Privacy coin is useful for those who wish to conduct transactions with a high degree of anonymity because the coin hides the addresses of both the senders and receivers as well as the total transaction value.18

A defining feature of cryptocurrency is its reliance on cryptography for security. Cryptocurrencies thus rely upon encryption to safely carry digitized financial information between participants in a financial transaction.

Cryptocurrencies also commonly rely on blockchain technology to track and settle financial transactions. Blockchain refers to a system whereby a record or ledger of financial transfers is kept, and it relies on distributed ledger technology (DLT). In a DLT system, the computers that are transferring funds interact directly with one another, transferring funds and checking to make sure that sufficient funds are held by a participant to pay for a transaction occurring. (That is, they engage in peer-to-peer networking, rather than carrying out their activities through a central node to which all computers would be connected.) Each participant in a transaction keeps its own records of the transactions that occur, and computers also interface with one another to update records of transactions. Thus, rather than there being one centralized record of transactions (as there might be in a conventional bank), there are instead multiple, identical records of transactions that occur, held on multiple sites.

As Frankenfield writes, "A defining feature of a cryptocurrency, and arguably its biggest allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation."19

That is, cryptocurrencies allow for a decentralization of economic power. Because cryptocurrencies are “self-governing,” they remove the role that has historically been played by states and central banks. Radical proponents of the use of cryptocurrency thus argue that it may represent a way out of the capitalist-based world order that has formed the basis of our political system.20

(Continued)
The Role of the Central Bank

To understand the implications of cryptocurrency, one needs to understand how traditional banks work and how states make fiscal policy. Historically, states have controlled how much currency is issued and what interest rates are charged to borrowers. In the United States, a government agency, the US Federal Reserve (the Fed) makes these decisions. The Fed is governed by a board of governors of the Federal Reserve Board. There are twelve governors who are appointed by the president.

The Federal Reserve Board (created in 1908) allows the country to control its currency’s value on the world market and to act to stem issues like inflation (simply defined here as too much money chasing too few goods). A central bank can adopt a tighter or a looser fiscal policy to encourage consumers and businesses to engage in saving or spending. A central bank also acts an insurer; it can step in to cover emergency situations like a shortfall in currency, out-of-control inflation, or a bank that fails due to making bad loans.

In addition, the value of government-issued assets resides in the fact that they are tied to a state’s gold reserves in some instances as well as to a state’s tax revenue streams and the value of government-owned assets. That is, people trust that their money will retain its value because they trust the country that issued it, and when people don’t trust their nation’s currency (due to destabilizing events like a civil war or a coup), then they are likely to move their assets elsewhere, including abroad or into alternate currencies.

Finally, in the United States—and in most nations—founding documents like the Constitution give the country the exclusive right to create money. In the US Constitution, Article 1, Section 8(5) grants the power to coin money and to regulate its value specifically to the federal government. The Constitution also forbids the use of “unauthorized instruments,” although this statute has historically been interpreted to mean that individuals should not create counterfeit money rather than being applied to cryptocurrency and other forms of virtual payment. In China, the Law on People’s Bank of China designates this organization as having the sole authority to issue and manage currency and its circulation. Individuals and corporations are forbidden to issue or print tokens or tickets that could replace China’s official currency, the renminbi.

“A New Type of Asset”

In 2018, Lael Brainard, a member of the US Federal Reserve board of governors, described cryptocurrency as a “new type of asset.” But what is the significance
of these assets and how can its emergence in the previous decade affect today’s international economy?

Today, analysts are divided about the threats and opportunities that the advent of digital or cryptocurrencies represents. Brainard points out that the new currency is not a liability of any individual or institution. Thus, he notes, “There is no trusted institution standing behind it.”

Because cryptocurrencies do not have a defined relationship with a particular state or state-backed institution, they are therefore currently not legal tender and thus could not be utilized for certain types of financial transactions. They are also considered to be virtual currencies because they do not exist in physical means and owners do not physically own anything; rather, their claim to own the assets is validated through the blockchain.23

In addition, traditional financial transactions are cleared by a bank that makes sure that there is enough money in the check writer’s account, for example, to allow the recipient to cash a check that has been written. In contrast, this clearing function takes place independently between computers using cryptocurrencies, with no central figure, like a bank, exercising control over these financial transactions.

And when traditional currencies are used, the state works to track financial activities by individuals and corporations. Particularly in the period since 9/11, US and international banks have developed systems for flagging suspicious transactions (such as regular recurring large cash transactions between nations associated with terrorist activity) and sharing this information with the proper authorities. Individuals and corporations must furnish proof of their identities before engaging in activities such as taking out a loan or establishing a bank account, and information is shared with the relevant authorities. Thus, the state is able to exercise its state power through extracting the relevant taxes from financial actors as well as ensuring that the proper rules and procedures for engaging in financial transactions are followed. In contrast, cryptocurrencies are considered to be borderless, international currencies—and there is not a strong state mechanism in any state for regulating international financial transfers conducted using cryptocurrency.

Cryptocurrencies thus present new challenges in areas as diverse as payments policy, supervision and regulation, financial stability, monetary policy, and the provision of financial services.24

Despite these concerns, however, in 2018, the global cryptocurrency market was valued at greater than $795 billion. A significant amount of the world’s economy is thus being conducted in cryptocurrency.25

(Continued)
Identified Problems with Cryptocurrency

Analysts have identified several issues with the new cryptocurrencies, which are significant for international relations.

First, like paper money, the value of Bitcoin is not fixed but can fluctuate. In a conventional financial system, an event like inflation might cause a dollar, for example, to be worth less in the sense that it buys less because prices are higher—even though its denomination is the same. In the same way, Bitcoin’s value may fluctuate, depending on demand for it as a good. Its value stems from its use as a means of purchasing other things and carrying out other financial transactions.

The value of cryptocurrency is related to its use, its scarcity, and its perceived value. Currently, only a finite amount of currency exists, making it rare and valuable. Indeed, in 2018, Bitcoin was the highest-valued currency in the entire world. In some ways, then, cryptocurrency has similar characteristics to shares of stock rather than currency. One is said to “hold” a specific cryptocurrency, and doing so confers privileges upon the holder, allowing him or her to have a voice in the activities that occur within a currency community. In this way, someone who holds a specific cryptocurrency is similar to a shareholder in a stock corporation.

In addition, policy makers are concerned about the anonymous nature of cryptocurrency transactions. The DLT system creates ledgers that do not contain information about the currency owners’ identity, although they do contain a chain of custody showing which assets have been transferred between which addresses, the amounts, and when. Because of this anonymity, as well as the fact that the currency system operates outside of state fiscal policy, the state cannot track illegal economic transactions. Cryptocurrencies are thus widely used on the dark web, where someone might, for example, pay for drugs or human trafficking with Bitcoin. And criminal groups might use Bitcoin to violate laws, whereas rogue states could use cryptocurrency to violate sanctions imposed by the international community. Cryptocurrencies can be used for money laundering and in ransomware attacks as well as physical kidnappings.

Attempts at Regulating Cryptocurrency Transactions by States

Is a competition taking place between conventional and cryptocurrencies? Can both exist side by side, or will cryptocurrency put existing banks and financial services providers out of business?

Political economists suggest that a showdown between the financial systems is inevitable. They worry about crypto-secession, as key actors withdraw from the existing international economic system. If enough actors secede in this way,
states, state-backed banks, and other financial entities lose the privileged position they have thus far enjoyed.27

As a result of states’ wishes to more tightly regulate these “anarchic” financial transactions, which seem to be occurring largely free of state interference, states have responded in two ways: States seek to more tightly regulate financial transactions involving cryptocurrencies. Next, states and international organizations may create their own cryptocurrencies, which would utilize DLT and the blockchain but which might still be the subject of fiscal and regulatory policy.

Many states have already passed rudimentary legislation recognizing cryptocurrency as a form of exchange, including Japan and Belarus. National banking authorities in both the United States and the UK now recognize a limited number of cryptocurrencies. The Federal Reserve Bank of St. Louis recognizes Bitcoin, Litecoin, Bitcoin Cash, and Ethereum. Daily prices on these currencies can now be obtained from the Federal Reserve Economic Database (FRED).28 And in September 2017, International Monetary Fund President Christine Lagarde asked international bankers to pay more attention to cryptocurrency. Her statement can be read as a recognition of cryptocurrency as a legitimate means of exchange.29 And the European Court of Justice ruled in 2015 that Bitcoin transactions should be exempt from value-added taxes (VAT).30

Facebook’s Own Cryptocurrency

Recently, social media giants like Google and Facebook have discussed developing their own cryptocurrencies. These cryptocurrencies differ from projects like Bitcoin because they are asset backed. (That is, they are tied to specific items of monetary value, such as shares of Facebook stock.) Thus, they might be viewed more as private currencies, issued by corporations, rather than states. However, they will rely upon DLT to keep records of assets.

Facebook is reportedly developing a stablecoin—a new type of cryptocurrency that is easier to settle transactions between parties and with less price volatility.31 Facebook employees would have the option of being paid in this currency. The new coin places a high emphasis on guaranteeing the privacy of individual’s financial transactions.32

Here, policy makers are concerned about corporations like Amazon and Facebook achieving the status of monopoly corporations as they acquire a leading market share in more and more industries from book sales (Amazon) to advertising sales (Facebook) to banking.33

(Continued)
Applying the Paradigms

Depending on one’s overall stance toward the international system—including how one defines power and influence within that system—an analyst might view the rise of cryptocurrencies differently.

Realism

Realists have four concerns in response to the rise of cryptocurrencies. They worry that the United States may lose its power within the international system if its central role as an arbiter of international fiscal policy is threatened by the rise and popularity of cryptocurrencies. Next, realists are concerned about the threats to international system stability presented as adversary nations harness the power of cryptocurrency for their own ends. Third, analysts are concerned about security risks as states move toward a “cashless society” in which individual citizens and corporations depend on cryptocurrency and other cashless mechanisms like e-wallets for the majority of financial transactions. Finally, nations may see the move toward an international currency as a threat to state power.14

If nations and citizens begin looking to cryptocurrencies as places to invest, and ways to preserve the value of their assets, or perhaps turn predominantly to cryptocurrencies rather than the US dollar as a medium of exchange, then the United States may lose its leading role in the world economy. It will be less able to dictate fiscal and political terms to other nations as a result of the rising role of cryptocurrency.15

Central Bank Digital Currencies

Due to concerns about digital currency volatility and states’ inability to regulate their issuance, many states are considering creating central bank digital currencies (CBDCs) that would function as national digital currencies. A CBDC would likely still be administered through a DLT through the blockchain. But this new currency would be a liability of a central bank. In this way, the state could also monitor and regulate the transfer mechanism of digital currencies. However, a CBDC would not have to provide the anonymity that is currently associated with other forms of cryptocurrency.16

Some analysts are concerned that such a digital currency would be a new target for criminal actors. In addition, the use of strong centralized digital currency might also drive traditional banks and traditional currencies out of business.
In addition, Hall writes of a "potential nightmare scenario" in which Russia’s economy moves toward a digital-only economy. He argues that the requirement that all financial transactions be conducted in a transparent manner in which a ledger is kept to track the movement of money could be a first step toward the construction of a vast and all-encompassing surveillance state. In such a scenario, a security threat—like a terrorist attack—could provide the pretext for allowing the state to take tighter control over the economy. In the future, DLT might even be paired with biometric identity technologies to tie people explicitly to all of their financial transactions over their lifetimes. Hall therefore concludes that “a DLT-based currency issued by the Russian Central Bank would allow the administration to wield a significant level of access to personal information in addition to economic control.”

The Problem with Cashless Economies

Finally, security analysts have voiced concerns about the fact that so many citizens are now dependent on cashless economic transaction mechanisms (like PayPal or Venmo) and upon the functioning of the technologies that underlie these mechanisms. Because electronic payment systems cannot function without a working communications infrastructure, functioning software and functioning electricity and servers, attacks (either physical, i.e., kinetic, or cyber enabled) on any one of these components could potentially lead to social chaos if individuals were unable to access funds to purchase groceries, for example. An attack that was able to erase financial transactions (either temporarily or permanently) could sow even more chaos if, for example, financial records were destroyed and people were unable to prove that they should be receiving social benefits or a pension.

In addition, if electronic payment systems and decentralized currencies become the norm in the future, it may be increasingly difficult for states to mount a response (including a military response) aimed at securing a state’s financial system if that financial system is increasingly decentralized and maintained by actors other than the state.

Liberal Internationalism

Liberal internationalists worry that relying on cryptocurrency might affect activities such as free trade or even massively disrupt the existing international economic system. Devries notes that “if cryptocurrencies became the global norm for transactions, long standing systems for trade would need to be completely reformed to deal with this type of competition.”

(Continued)
This new system could be more volatile than our current system. Here we can consider the increased demand in Britain for Bitcoin when investors became worried about how Britain’s withdrawal from the European Union (Brexit) in 2019 would affect their investments. Brainard suggests that investors might flee what they see as “sinking global markets” through instead turning to cryptocurrencies. In such a scenario, states would play a less significant role in protecting markets from volatility and even collapse. In addition, reliance on Bitcoin is likely to be particularly high in countries where the state is seen as not being sufficiently responsive in its fiscal policy to threats like inflation. For example, in a nation like Argentina, where high inflation is the norm, citizens used to keep their money in dollars but are now more likely to keep it in Bitcoin.

Cryptocurrencies themselves are volatile because of the speed at which transactions occur; they don’t need to be cleared through a central financial institution, which slows down transaction speeds. Governments might therefore be tempted to embrace cryptocurrencies because it would be mean that governments could quickly shift money in response to a national disaster, for example. However, states might also find it harder to intervene in a situation where cryptocurrencies markets are threatening to fail due to the speed at which transactions occur.

In addition, different nations might adopt different cryptocurrencies, in this way creating new types of trading blocs. For this reason, some analysts argue that states within the international system should come together cooperatively to establish rules—or even a global regime—aimed at regulating how states will treat cryptocurrencies. That is, whereas realists envision a system in which each state might issue its own cryptocurrency, with the strength of competing cryptocurrencies thus serving as a proxy for state power, liberal internationalists see a system in which states might cooperate to bolster the value and utility of a single or diverse set of cryptocurrencies that would be accepted by all states.⁴⁰

In this way, the debate about global financial governance is closely related to the debate about global internet governance (described in Chapter 6). Some states may have a realist, national sovereignty view in which each state might attempt to issue and administer its own national cryptocurrency, acting in a competitive manner. But other actors may instead advocate for a multistakeholder approach toward the global governance of international economic matters, including the issuing, administering, and support for cryptocurrency. In a multistakeholder
approach, actors as diverse as global banks, national treasuries, and international technology actors, like Facebook, might work together to create and steer the regulation of cryptocurrencies.  

Constructivism

Finally, a constructivist approach allows us to consider the language being used to describe cryptocurrencies at the moment as well as to think about the ideas that underlie debates about cryptocurrencies.

Here, we can consider the ways in which states have acted to either legitimize or delegitimize these newly emerging institutions and cryptocurrencies like Bitcoin themselves as well as the ways in which leaders and citizens have spoken about the issue of trust in these institutions and these currencies. How governments speak of cryptocurrency will affect these issues: Do they themselves regard it as part of their official banking sector or as something else—like an anarchic space where illegal transactions occur?

Language can also be used to paint cryptocurrency either as a niche market or as part of a larger, more mainstream shift within the international economic system. Here, the use of words like “risky” or “volatile” in particular by state officials could affect user perceptions of the currency.

Using language, states might attempt to “capture” the cryptocurrency market through painting it as existing either within or outside traditional economic relations. Cryptocurrency markets can thus be described either as an adjunct or complementary sector for traditional markets or as a competitor to these markets.

China’s Constructivist Approach to Regulating Cryptocurrencies

As the world’s largest economy, China has the potential to be a major actor in the field of cryptocurrency. In addition, China’s citizens are already heavily dependent on cashless means of transferring money, utilizing electronic wallets for many of their day-to-day economic transactions. In addition, a majority of the activity involved in mining cryptocurrency has historically taken place in China because the power and resources necessary to carry out this activity are relatively cheap relative to other sites worldwide.

Therefore, in theory, one would expect China to be highly supportive of the development of cryptocurrencies as part of this cashless economy. However, (Continued)
China has adopted a cautious approach to allowing cryptocurrencies within its borders. There are several reasons for this:

First, China has proven to be the epicenter of cryptocurrency speculation. Several scandals have broken out in China in which investors and purchasers claim that they were defrauded. In 2013, Global Bond Limited, a trading platform for Bitcoin in China, suddenly shut down. The company is said to have vanished with $5 million worth of Bitcoin. And the lack of clear legal guidelines governing cryptocurrency transactions made this case nearly impossible to prosecute. (Indeed, China’s law enforcement personnel were “confused about what exactly was stolen.”) In some ways, cryptocurrency speculation appears to operate as a Ponzi or pyramid scheme, in which the initial investors are able to enrich themselves and then exit the system, leaving the next generation of “investors” to pay the price of the fraudulent scheme.

As a result of these concerns, China has enacted progressively stricter legislation spelling out the limits of what citizens may and may not do with cryptocurrency. In 2013, China passed legislation declaring that cryptocurrency could not be used as payment for goods or services, although it could be used as a vehicle for investment, and in 2017, China banned the exchange of funds between cryptocurrency and conventional economic means. In addition, China has designated initial coin offerings (ICOs) as “unauthorized illegal public financing.” It has also forbidden official state or private banks from engaging in financial activities involving cryptocurrency. The existence of a volatile currency that encourages speculation has been painted as simply too risky for a nation whose economic progress is still a relatively new phenomenon. The question has thus been whether it is worth jeopardizing China’s economic miracle to participate in the international cryptocurrency market.

Sources

The Free Rider Problem in Cyberspace

Some states don’t trust their neighbors to help secure cyberspace because of the problem of free riding. A free rider is an entity (like a state or individual) who reaps the benefits of a collective good (like clean air, clean water, or a stable internet) without actually paying into the costs of creating that collective good. Because the good established is public, no one can be excluded from its enjoyment, even if they have not paid into its creation.

In thinking about cybersecurity, some analysts argue that when one state decides not to engage in protocols aimed at guaranteeing cybersecurity, it does not merely “steal” a collective good that it did not have a hand in creating; rather, it actively undermines efforts to produce that collective good. Thinking back to the analogy of public health, we can consider how a state refusing to cooperate with international public health rules and regulations endangers everyone. Similarly, when one state decides not to act to preserve cybersecurity, this renders the whole system less stable and safe, and in this way, the costs of not acting to preserve cybersecurity are passed on to others.45 Today, particularly in developing countries, nations may not have optimal levels of cybersecurity provisions. State and commercial entities may run outdated software that is not updated periodically. Pirated or illegal copies of software may also be used. As a result, these nations risk creating cybersecurity vulnerabilities that will then be passed on to other parts of the global internet.46

The 2016 Attack on the Central Bank of Bangladesh

When we think of a bank robbery, we might picture a masked man with guns ordering customers to lie on the floor of a bank as they make off with paper bags full of cash. However, the largest bank robbery in the world occurred in February 2016, and it was a virtual bank robbery.

Throughout the world, customers—from individuals to multinational corporations—rely on SWIFT codes to instruct their banks how to route their money to make a payment. SWIFT refers to the Society for the Worldwide Interbank Financial Telecommunication, a cooperative of nearly 3,000 organizations that work together to maintain a messaging system used to move funds internationally. The organization, founded in 1973, is headquartered in Belgium. Data resides in Belgium and the United States.47

Schwartz describes the risks associated with relying on SWIFT codes, noting that “any attack . . . is a concern because attackers could literally transfer money from a victim’s account into their own.”48 (Not all analysts agree, however, about the flaws in the SWIFT transaction system. Others feel that the SWIFT system is safer than other electronic payment systems because it...
is a closed system whereby payments travel within a predefined space with a recipient at either end who must identify him- or herself.)

In February 2016, hackers gained unauthorized access into the Bangladesh Central Bank. They then sent thirty-five fraudulent orders, requesting that money be withdrawn from the bank and sent to addresses in the Philippines and Sri Lanka. The orders totaled nearly $1 billion! Even though there were numerous errors in the requesting documents, and even though there were several red flags raised by the intermediary and receiving organizations, nearly $80 million was transferred, and most of it will never be recovered.

This story illustrates a new type of risk in international monetary systems. It involves a great many players: the governments of Bangladesh, Sri Lanka, Belgium, the United States, and the Philippines; the US Federal Reserve Bank of New York; numerous law enforcement agencies; and nonstate actors like corporations, which often administer cybersecurity. Some analysts also believe that North Korean state-sponsored hackers participated in the heist and that some of the money ultimately wound up in North Korea.

In the aftermath of the theft, numerous investigations were carried out in Bangladesh, in the US Senate, and in the infected financial institutions. These investigations reached different conclusions about who was responsible for the errors. The New York Fed blamed Bangladesh, pointing to possible involvement by insiders within Bangladesh Bank who might have provided their credentials to hackers. In addition, the bank’s system had no firewall and had used secondhand equipment in building out its system. But Bangladesh blamed the SWIFT cooperative for carrying out the transactions even when there were mistakes in the orders and when no one responded to their queries. They are suing the US Federal Reserve for damages related to the incident. Meanwhile, the US Federal Bureau of Investigation believes that the North Korea-based Lazarus Group, a state-sponsored hacking collective, may have been involved. Some of the code used resembled that used in the 2014 Sony Pictures hack, which was attributed to North Korea. Indeed, a US National Security Agency official has stated that in this new financial world, “nation-states may be robbing banks.”

Also, we can see how international actors may have made mistakes in creating procedures due to insufficient cultural knowledge. In retrospect, we can see that even though the New York Fed queried the SWIFT orders due to certain improprieties in the way they were formatted, the director of Bangladesh Bank did not receive the queries. This was because his office computer had been infected with malware that caused his printer to malfunction. However, it’s also important to note that the hackers were aware that Bangladesh was an Islamic country that closed for business on Friday. In contrast, New York’s offices were closed on the American weekend, for Saturday and
Critiquing Liberal Internationalism

Throughout these chapters, we have described each international relations lens as a way of seeing the international system. Each lens highlights certain facets of the international system while downplaying the influence of other factors within that system. And each lens rests on different assumptions about the international system itself.

Those who reject the liberal internationalist view of the international system, including the liberal internationalist view of cyberspace, build their critique by querying some of the assumptions that liberal internationalists take for granted. In particular, those who are critical theorists have faulted the liberal internationalist lens for the ways in which it presents the “evolution” of the international economy as organic and natural and, in their minds, neglecting the role of agency and power politics. That is, throughout this chapter, we have assumed that there are natural shared interests that states become aware of (such as a need to provide maritime security for boats traveling in international waters), and as a result, they move to create agreements to guarantee these shared interests.

Critical theorists, in contrast, believe that the international arrangements for security, including economic security, which have evolved within the international system have not merely “grown” naturally. Instead, they argue that
some actors, including corporations, have consciously steered states toward adopting these cooperative arrangements that do not just benefit the international system but that also enrich corporations that are better able to conduct economic activities in a system with few tariffs, few borders, and less conflict. They argue that our present international system did not evolve organically or naturally and that its present shape is not inevitable, although liberal internationalists may present it as such.

The notion that businesses have always played a role in a state’s foreign policy and a state’s power—particularly its economic power—has, at least in a capitalist society, always depended on the fortunes of its businesses, including how they fare in the international sphere, is not a new idea. Indeed, state power is—in the liberal internationalist view—tied to its gross national product, which is a function of manufacturing and the production of goods and services within a state, as well as to the existence of a highly educated and trained workforce. Manufacturing, thus, depends on a state’s foreign policy to keep markets open internationally so that domestic companies have international markets to buy their goods as well as to access inputs into manufacturing that are not available domestically. Free trade is thus critical for the growth of state power. Historically, this relationship has sometimes been summed up in the shorthand phrase: “What’s good for General Motors is good for America.”

**Critiquing the Liberal Internationalist View of Cyberspace**

However, the relationship between businesses and the state in the area of cyber policy and cybersecurity is somewhat different from these historical relationships. This is because firms are creating the architecture or system that makes up e-commerce themselves, and states are thus in a weaker position in terms of attempting to regulate policies in this arena because firms have gotten there first and, in creating the architecture, begun to establish terms. Here, one can argue that technologies (including the technologies of e-commerce) are driving the train forward in developing new understandings for rules and regulations in the cyber arena, with states playing catchup and following behind firms as they seek to assert control over events occurring in this arena.

In one of the best critiques of the liberal internationalist view of the internet, analyst Micky Lee calls our attention to the fact that much of the early rhetoric about the internet, particularly in the United States, used the language of technological determinism. US policy makers and corporate leaders presented it as inevitable that the internet would represent democracy and that it would gradually extend throughout the world, carrying with it certain values. However, she argues that the internet’s growth was far from organic and inevitable. Rather, she suggests that we consider how corporations are complicit in creating the internet in its present form.

In Lee’s retelling of the history of the internet’s birth, she asks us to consider the power that corporations and technological corporations in particular
have in political life as well as the role that corporations have had in lobbying for and supporting government economic policies that supported the international expansion of the internet. She writes that “technology is developed within a political and economic context,” and “laws are drafted to consolidate the dominant groups.”

In particular, Lee argues that the extending of the internet into China and the creation of billions of internet-enabled citizens in China did not merely “happen.” Rather, she argues that corporations like Google in particular lobbied the Clinton administration to be allowed to do business with China despite its identified human rights violations. As a result, the Clinton administration aided and encouraged corporations to enter the Chinese market by approving the permanent normal trading status and by lobbying the World Trade Organization to admit China as a member.

These companies, she argues, actually had a vested interest in doing business with international countries, even when these countries were not democratic and did not evince a commitment to democratic values. The major aim of these corporations was to extend the global reach of their businesses, which was at odds with the publicly stated goals of countries like the United States, to extend democracy to all. She argues that these corporations were actually interested in building a stable system of global internet commerce. They were not interested in the economic, moral, or ethical import of their decisions. Such firms, one can argue, are less concerned with preserving the internet as a global common and more concerned with creating a profitable market for their goods and services. Indeed, some analysts have suggested that in relation to the internet, state policy making has often been merely a formalization of the practices already adopted by firms and professional organizations. This is because firms have lobbied democratic states specifically, in this way tailoring the regulations that would later be used to regulate the corporations themselves.

**Digital Superpowers in the Global Economy**

The critique of liberal internationalism, therefore, also suggests that those corporations that became digital superpowers did not merely evolve to occupy this position. Rather, they consciously engaged in monopolistic practices, driving competitors out of the marketplace and securing advantages for themselves that would enable them to play a commanding role in building the internet architecture as it presently exists.

Economists Iansiti and Lakhani describe the digital economy as a collection of wheels or hubs, arguing that the best way to measure an entity’s digital power is through considering the size of the hub which it commands—or the number of other entities whose economic fortunes are tied to the primary entity. That is, the more connected an entity is, and the more dependent other entities are upon it, the more powerful an entity is. (Here, we can think of the firms that possess the largest market share of digital resources and users.) When they map out these connections, however, something unusual emerges. Their list of the
digital superpowers thus consists of a list not of states but instead of economic entities. They write:

The global economy is coalescing around a few digital superpowers. We see unmistakable evidence that a winner-take-all world is emerging in which a small number of “hub firms”—including Alibaba, Alphabet/Google, Amazon, Apple, Baidu, Facebook, Microsoft, and Tencent—occupy central positions. While creating real values for users, these companies are also capturing a disproportionate and expanding share of value, and that’s shaping our collective economic futures.54

In considering these new digital superpowers, we can distinguish between those platforms that host the infrastructure to carry out services like e-commerce (i.e., eBay and Amazon) as well as those platforms or hosts that grant users access to other types of goods and services (i.e., Facebook and YouTube) including content that users create themselves.

Here we can ask: Do these digital superpowers have the same “buy-in” that a state might have in terms of feeling compelled to maintain the international digital environment (or ecosystem) as a safe and stable place? Should content and

<table>
<thead>
<tr>
<th>State or Firm</th>
<th>Number of Citizens, Users, or Members</th>
<th>Annual Revenues (or GNP) in USD</th>
<th>Size of the Workforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>270 million</td>
<td>8.445 trillion</td>
<td>163 million55</td>
</tr>
<tr>
<td>Facebook</td>
<td>2.5 billion16</td>
<td>51 billion17</td>
<td>25,00058</td>
</tr>
<tr>
<td>Google</td>
<td>1.58 billion59</td>
<td>100 billion60</td>
<td>98,77161</td>
</tr>
<tr>
<td>Belgium</td>
<td>10 million</td>
<td>374 billion</td>
<td>5 million62</td>
</tr>
<tr>
<td>France</td>
<td>65 million</td>
<td>2.647 trillion</td>
<td>23 million61</td>
</tr>
<tr>
<td>Russia</td>
<td>143 million</td>
<td>1.538 trillion</td>
<td>75 million64</td>
</tr>
<tr>
<td>Alibaba</td>
<td>552 million65</td>
<td>39.3 billion66</td>
<td>101,95867</td>
</tr>
<tr>
<td>Baidu</td>
<td>800 million68</td>
<td>Unknown69</td>
<td>42,00070</td>
</tr>
<tr>
<td>Amazon</td>
<td>100 million prime members, 203 million regular users71</td>
<td>70 billion72</td>
<td>647,50071</td>
</tr>
</tbody>
</table>

Source: Statista

Figure 4.1 Digital Superpowers versus States

---
infrastructure platforms be forced to spend their resources on policing these structures to guard against cybercrime, child trafficking, or terrorism? Are these issues better confronted by states rather than private firms?

**Digital Superpowers as Reluctant Global Hegemons**

Many commercial interests claim that this role (as “guardian of the digital infosphere”) has been thrust upon them, and it is not a role that they have either desired or sought out, nor is it one that they want. Here, most citizens and policy makers believe that corporations should have an ethical or normative concern about the impact of their products as well as an interest for those in their communities. However, some critics have argued that corporations are not predominantly driven by ethics and that the carrying out of corporate social responsibility activities may be driven as much by public relations concerns or the desire for a tax incentive for charitable giving as it is by a corporation’s actual ethical goals. Thus, they argue it is insufficient for citizens and policy makers to expect corporations to police themselves and instead argue for regulations that might, for example, require companies (including internet platforms) to undertake and issue environmental impact statements or to consider matters such as whether a technology like artificial intelligence will decrease the availability of jobs for humans and how such a situation might be addressed. (We discuss this question further in our chapter on artificial intelligence.)

**CONCLUSION**

We have now considered two lenses of international relations as they relate to cybersecurity. As we saw in Chapter 3, realism helps us understand the sources of conflict among states through the assumption that cyberspace is an extension of the anarchic international system and that conflicts in cyberspace are an extension of territorial disputes that states have traditionally fought in real space. Realism helps us understand the formation of alliances like the Shanghai Cooperation Organization, how states can engage in balancing within cyberspace, and why a conflict spiral and cyber arms race may be inevitable.

In contrast, liberal internationalism helps us understand the phenomenon of technological, social, political, and economic interdependence among states and how cybersecurity can be recognized as a collective good that requires cooperation for its preservation. This lens illuminates how globalization has caused economic and financial systems to become more intertwined as well as how phenomena like global outsourcing have led to the breakdown of state barriers in favor of greater international trade.

Each of these lenses will be relevant as we continue to examine the debates about internet governance in Chapter 6.
Questions for Discussion

1. Compare and contrast the pros and cons associated with the use of cryptocurrencies, like Bitcoin, for individual investors, corporations, and state actors. Should states attempt to get on board with the rise of cryptocurrencies, or should they leave this sector of the economy to develop independently?

2. Do you regard the internet as a public good, like a utility? Or do you see it as a private good that should belong to each nation individually?

3. What are some collective problems that exist online that states might cooperate to regulate and overcome?

Key Terms

Blockchain 93  Peer-to-peer network 93
Cryptocurrency 92  Stablecoin 97
Cryptography 93  Supervisory control and data
Digital economy 85  acquisition (SCADA) 88
Digital superpower 107  SWIFT (Society for Worldwide
Distributed ledger technology (DLT) 93  Interbank Financial
Infosphere 85  Telecommunication) code 103
Legal tender 95  Virtual currency 92

For Further Reading


Students may also wish to watch the congressional hearings held in November 2018 on the matter of corporate social responsibility in internet governance found on YouTube.