Sovereignty, Cyberspace, and the Emergence of Internet Bubbles

Eldar Haber, PhD; and Lev Topor, PhD

Abstract*:* The cyber domain emerged as a perfect platform for international struggle over power and influence. International powers are actively engaged in cyber proxy warfare due to the relatively low risk of escalation, various enforcement challenges, and the vagueness of international law within this realm. These indirect conflicts might lead some global powers to close or restrict their virtual borders to avoid or reduce the plausibility of cyber proxy warfare or unwanted foreign influence in general. The formation of such restricted networks, articulated in this article as "internet bubbles," is already shaping within the realm of actors like Russia, China, North Korea, and Iran. The authors argue that liberal democracies like the United States might be at a severe disadvantage to fight against cyber proxy warfare due to legal and constitutional barriers. But at the same time, the emergence of platform governance and self-regulation might be proven as a new force within these proxy wars and reshape its boundaries.
Keywords: international security, cybersecurity, internet, proxy warfare, sovereignty

Introduction

> *From Stettin in the Baltic to Trieste in the Adriatic an iron curtain has descended across the Continent*.
>
> ~ Winston Churchill

Winston Churchill's quote refers to the Soviet Iron Curtain—the nonphysical boundaries dividing Europe at the end of World War II.[1] Today, countries worldwide are forming digital iron curtains

Dr. Eldar Haber is an associate professor at the Faculty of Law, University of Haifa, Israel. Dr. Lev Topor is a visiting ISGAP scholar at the Woolf Institute, Cambridge, UK, and a senior research fellow at the Center for Cyber Law and Policy (CCLP), University of Haifa, Israel.

Journal of Advanced Military Studies vol. 14, no. 1
Spring 2023
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20231401006

within their efforts to preserve sovereignty and control public opinion. Russia, China, North Korea, and Iran, to name a few key examples, control and restrict their cyber domains to prevent foreign intervention. In contrast, liberal democracies like the United States currently lack substantial legislative freedom to similarly control and restrict their cyber domains and are therefore becoming more susceptible to foreign interference of various types. This was demonstrated very recently with the conflict between Ukraine and Russia (2022–23)—the latter restricted domestic media to try and restrain opposition to this conflict while it also disseminated anti-Ukrainian and anti-Western propaganda to try and undermine Western support for Ukraine.

The main argument of this article is that some countries worldwide will attempt, and many times succeed, to form their own restricted internet networks—"internet bubbles"—for the purpose of avoiding undesired foreign influence and to better govern and control their domestic affairs.[2] The authors further argue that these internet bubbles position nondemocracies better than democracies to gain and preserve cyber sovereignty, considering the difficulty to attribute cyberattacks and propaganda.[3] However, these internet bubbles are not hermetically sealed, and the rise of platform and corporate governance might aid democracies to govern their virtual borders from foreign influence.

Examining the hypothesis begins with discussing the rise in cyber warfare and foreign interventions through cyber means. Notably, the internet was always subjected to hacking and manipulations by foreign agents, often conducted through its backbone.[4] But cyber warfare and other forms of foreign interventions became more common and prominent for many countries worldwide recently, directed mostly against the West and the United States, and might in turn threaten sovereignty. Cyberattacks were directed at the state not only directly but also through private parties, serving as a state's beneficiary proxy, as exemplified within the cyberattack by North Korea against Sony Pictures Entertainment in November 2014.[5] Further, it is only natural for a sovereign state to protect itself from malicious foreign interventions. Yet, authoritarian states also seek to limit foreign civil and cultural influences.

Methodologically, the authors examine the arguments, suggestions, and predictions with a traditional international relations approach and treat each international actor as a unitary actor seeking to gain complete sovereignty and independence. This argument is based on traditional theories of international relations, sovereignty, and proxy warfare, as well as a legal analysis of cyber proxy wars from both international and domestic law perspectives. Since it is an extreme and obvious case of undesired foreign influence, the focus of this article is on cyber proxy warfare.

This article examines and compares the three cyber domains of three global powers—the Russian, Chinese, and American domains—to predict how international actors will use cyber warfare against their adversaries, while keeping their own cyber domains safe. Finally, other modalities are suggested that can

replace the necessity of creating internet bubbles—a suggestion that is derived from the comparison of the American, Russian, and Chinese cases.

Interestingly, the February 2022 invasion of Russian forces into Ukraine and now the conflict between the parties has demonstrated that cyber warfare is limited. It is an important tool for times of peace and times of tensions and mainly for disseminating propaganda. However, in times of kinetic conflicts, the utility of cyber warfare is limited simply due to the fact that it takes kinetic means like infantry, tanks, jets, and other weapons to conquer land. The conflict between Ukraine and Russia has also demonstrated the argument about the strategic need of an internet bubble. That is, putting values like democracy, liberalism, and human rights aside, Russia has restricted its internet and media to deny any anti-governmental and pro-Western influences.

Sovereignty, Conflict, and Cyber Proxy Wars: Setting the General Framework

Nations generally desire to control their internal affairs. That is, they seek the ability to control their domestic affairs, control their population, as well as to control their ability to make foreign policy decisions like engagement in trade, war, or diplomatic relations in general.[6] In the context of this article, cyberspace is a platform upon which states can fulfill this desire of control, especially regarding their domestic affairs. Politicians and their constituents in the United States, the European Union (EU), Russia, and China have grown increasingly nervous about letting capital, goods, and people move freely across their borders and the threat of terrorism or even the COVID-19 pandemic only made this more prominent.[7] In the age of information and cyberspace, politicians and their constituents are also concerned about the type of information crossing into their digital borders.[8]

States are also willing to engage in conflicts over their sovereignty. In the twentieth and twenty-first centuries, major wars and conflicts have all been characterized by the involvement of foreign powers in the affairs of other actors or those of their allies and beneficiaries.[9] For the conceptual purpose of this article, conflict between states can emerge, among other ways, mainly in two ways: first, when actors disagree about their mutual international affairs. Second, when actors try to influence and intervene in the domestic political arena of other states.[10] In this regard, Fredric S. Pearson suggested that there are six key reasons for states' interventions in others' affairs: (1) they wish to acquire territory or domains; (2) to protect social groups; (3) to protect economic interests; (4) to protect military or diplomatic interests; (5) they intervene due to ideology; and, lastly, (6) to keep or adjust the regional balance of power.[11]

States may acquire control over matters through peaceful negotiations, military pressure, or any other use of power—soft, hard, smart, or sharp power.[12] In the context of this article, and the question of power and influence through cyberspace, the question of how one can measure sharp power such as disinformation or cyberattacks arises. This is rather complicated and has no definitive

answers yet, partially since many executions of power are made through proxies carrying out cyberattacks, blurring or hiding the involvement of an international actor in another's affairs, thus making the attribution of the hostilities even more difficult. Furthermore, the actual victim can be considered a state proxy itself, as one might treat Sony Pictures Entertainment as such within the abovementioned cyberattack against it in 2014. Moreover, even when a victim state can point at the perpetrator state or actor, traditional military or economical retaliation is often more difficult to justify than when dealing with kinetic actions, and the attribution problem often renders deterrence slow, blunt, and ineffective.[13] Furthermore, following Karl W. Deutsch and Andrew Mumford's theme, when states consider ideology, interests, and risks, they tend to opt for the use of proxies.[14]

The conceptual soil on which the conflict is now fought, in this respect, is cyberspace itself. Cyberspace allows states a rather high degree of anonymity and detachment from their actions. The difficult forensic process of attributing an attack to a specific perpetrator makes the internet an ideal tool for waging a proxy war.[15] While states are legally responsible for activities undertaken through their proxies, holding them responsible will depend on proof (i.e., the attribution of the proxy's actions to its patron). However, some actions—such as spreading disinformation and online propaganda—are currently not even considered illegal on the international level and states use this to influence other international actors and even to resist traditional hard power such as the case of Russian disinformation against the North Atlantic Treaty Organization (NATO) in the Baltic region.[16]

States strive to control their affairs, including the type and nature of information their citizens consume. Even liberal democracies seek to restrict influence on public opinion if this influence is malicious. The extreme case of such influence is cyber proxy warfare like foreign mis/disinformation campaigns and for this reason this article demonstrates this argument with examples of cyber proxy wars. Following the discussion of sovereignty, conflict, and traditional proxy wars, the authors define the term *cyber proxy wars* to further elaborate the argument. Combining and extending the definitions of proxy wars by Deutsch and Mumford, cyber proxy wars could be defined as international conflicts between two foreign powers fought on or using the cyber domain, disguised as actions taken by unrelated international actors or entities, made in an attempt to influence an actor's strategic outcomes; for instance, where both the attacker and the victim can be a proxy.[17] In the age of information and technology, cyberspace—through cyber warfare—serves as the perfect arena to avoid direct conflict while trying to obtain Pearson's six goals for intervention. In general, cyber warfare can be defined as using cyber weapons as well as the domain itself in order to execute strategies and policies that undermine and influence other international actors. These acts can be executed by all forms of international actors.[18] The characteristics and associated benefits of cyber tactics make them very attractive for use by states and even terror groups alike.[19]

The Formation of the Russian and Chinese Internet Bubbles

In this section, the authors focus on Russia and China since their internet bubbles are still relatively premature, although they are constantly growing, and in contrast to the North Korean *Kwangmyong* internet bubble, are still not entirely hermetic. The North Korean internet bubble is almost hermetically sealed off, and all information and communications, in and out of the country, are controlled by Kim Jong-un and his government.[20] The article also addresses the actual structure of cyberspace and argues that all layers of cyberspace can be restricted—physical, logical (data routing), information, and users. These layers affect many things such as regulation and the relations and interactions between all users, states and people alike.[21] In practice, as exemplified by the Russian and Chinese examples, restricting physical and logical layers can lead to a more restricted internet bubble while controlling information and users in cyberspace can lead to a more subtle internet bubble. That is, for instance, the fact that North Korea is physically and virtually disconnected from the global grid makes the North Korean internet very restricted, more so than Russian legislation against foreign information.

Unfortunately, while writing this article, one of the largest international conflicts since World War II between sovereign nations erupted between Ukraine and Russia. Although Moscow sought to have its grip on what it perceived as its "backyard" already in 2013–14 and even before, the current 2022–23 conflict—or war—between Ukraine and Russia demonstrates the argument about the strategic need for internet bubbles but also demonstrates the limited magnitude of cyber warfare.[22] In fact, Russia acts in two spheres of information and one of warfare. First, Russia seeks to restrict and control its domestic affairs, through control of media and information, to oppose any domestic criticism regarding the invasion of Ukraine.[23] Second, it disseminates anti-Ukrainian and anti-Western propaganda globally to undermine international support for Ukraine.[24] Third, Russia puts more effort in kinetic warfare than in cyber warfare simply due to the fact that its aims are kinetic—Moscow wants to conquer land and one does not conquer land just with cyber means but coupled with kinetic means like weapons, tanks, and infantry (that is, cyberattacks are secondary to the main effort).[25]

The Russian Internet Bubble

Russia has the potential to pose the largest threat to the United States, the European Union, and other democracies in general.[26] Its influence over global affairs is probably not lesser than its predecessor, the Soviet Union, as Moscow influences almost every major actor, in every region of the globe, and, as was uncovered in 2016, on its main adversary, the United States.[27] The Russian Federal Council has in fact emphasized the increasing importance of cyber warfare and use of cyber-related actions to accommodate and complement other types of acts in the international relations arena.[28]

Russia does not only utilize cyberspace to exert its influence on a global scale but also to protect itself from foreign cyber influence. Russia is working to create its own protective shield, a Russian internet bubble. Moscow's December 2019 successful attempt to unplug itself from the internet was just another step toward total domestic control of its domestic cyber domain—*RuNet*.[29] The Russian exclave Kaliningrad was connected to Russia via the Kaliningrad Cable, owned by Rostelecom, in 2021, further expanding its capabilities of internal communication.[30] Moscow had begun the process in early 2000s when it established control over television and the press—an act that allowed it to gain more control over information consumed by its citizens.[31] Moscow then turned to address cyberspace, and the developing Russian internet bubble is meant to deal with the technological and psychological aspects of the internet and its use by Russian citizens. For example, the Yarovaya Law, Russia's "sovereign internet" law, the Russian mass communications surveillance system (SORM), and the law making Russian applications mandatory on smartphones are all examples of the legal regulation of the technological aspects of the internet—namely and mostly the logic layer, which Russia seeks to gain control of.[32] The psychological aspect of the Russian cyber domain is controlled through the "fake news" law, the law concerning disrespect, and a recent law regarding foreign agents' activities.[33] The efforts on the part of the technological aspect are aimed to regulate outside sources, while those on the part of the psychological aspect are aimed to discourage Russian citizens from criticizing the authorities and cooperating with outside forces.[34]

In the context of the Russian "special military operation" in Ukraine, the abovementioned restriction of domestic information and media and the influence campaigns on foreign audiences allow Russia to implement sharp power. While leaks, anonymous communications, and rogue media allow Russian citizens a glance at the outside world, mass media is generally protected against unwanted information about the conflict in Ukraine and thus antigovernmental sentiments are limited.[35]

The Chinese Internet Bubble

China is another key global adversary of the United States and is much closer in diplomatic and military relations to Russia than to the United States, a fact that downgrades the United States from the global premier to some extent.[36] At home, China has successfully gained almost complete control of its internet since the early twenty-first century, restricting social media such as Facebook, Twitter, and even Tinder; blog platforms such as WordPress; some email providers; and even search engines such as Google. As an alternative, China allows for domestic social media platforms and other service providers to operate like WeChat, Weibo, Tencent, Baidu, and many others.[37] China also restricts access to messaging applications such as Telegram, Signal, and WhatsApp. Furthermore, platforms such as YouTube, Netflix, the *New York Times*, the BBC, and even Wikipedia are all restricted in China.[38] As previously mentioned, China's

internet is also currently locked behind the "Great Firewall"—a national project aimed at monitoring and censoring available online content through various means and methods—which can be conceptually compared to the Soviet Iron Curtain.[39]

China's foreign policy and cyber activities are aimed to protect the Chinese Communist Party (CCP) and to ensure domestic stability, territorial integrity, modernization, and economic growth; or, in other words, to ensure Chinese sovereignty and national security.[40] In December 2016, China has released its first *National Security Strategy*, which states that there can be no national security without cybersecurity and further reaffirms that "cyberspace sovereignty is an important part of state sovereignty." China's cybersecurity law, which acts as the baseline of its cyber regulation, came into effect in June 2017, alongside many other additional laws and policies that were enacted to ensure complete regulation of the internet—to ensure the CCP's "cyber sovereignty."[41]

As a national strategy, China addresses mainly the economic, political, and military spheres of cyberspace. As Amy Chang noted in 2014, there are six main issues promoted by the CCP: (1) economic development through cyber industrial espionage on other countries, including the United States; (2) pro-Communist propaganda and control over domestic information, as discussed; (3) utilization of offensive cyber operations to express discontent with acts of foreign powers; (4) development of military cyber capabilities both of infrastructure and of personnel; (5) maintaining intelligence and continuous reconnaissance of the cyber capabilities of China's adversaries; and (6) promotion and justification of domestic surveillance.[42] These six issues are executed by China's global footprint in the technological domain, especially as the Sino-American trade competition intensifies. Chinese companies like Huawei are perceived by the West as a challenge because China has found a way to penetrate the West not just with propaganda but with hardware and software as well. Yet this, of course, is a topic for another full article.[43]

China's strict control of its domestic internet and its general cyber sovereignty means that by now China effectively has an internet bubble. In comparison, Chinese internet regulation is stricter than its Russian counterpart, and in fact, it applies to all four layers of cyberspace: the Chinese government controls the physical layer through the regulation of routers, switches, servers, and other hardware in general. It commands the logic layer through its control of Domain Name Systems (DNSs), Internet Protocols (IPs), software, and websites. Power over the information layer is achieved through state censorship, and as a result, China also controls the user layer as the state manipulates and shapes users' experiences.[44] However, it should be noted that the restrictions imposed on the user layer and in part the information layer as well are not bulletproof as Chinese citizens and foreigners often employ workarounds, such as virtual private networks (VPNs) to bypass web restrictions.[45]

American Internet Regulation and Deproliferation: Responses to Foreign Insurgency

Cyber proxy wars are more challenging than kinetic ones from the legal and sovereignty aspects. They also negatively affect liberal democracies such as the United States more so than non or less-democratic states and might even threaten democracy. This is due, partially at least, to legal constraints and barriers for forming internet bubbles that serve to mitigate the dangers and harms of cyber proxy wars. The authors argue that the power to control parts of the internet, and the lack thereof, might eventually challenge the proper functioning of some governance forms, perhaps especially those whose legal regimes highly value and protect free speech. To further articulate the differences between cyber and kinetic proxy wars, one must first understand how some legal regimes might contest cyber proxy wars differently than kinetic ones. To do so, this article examines the two potential legal methods whereby cyber proxy wars are likely to be handled: international law and domestic law.[46]

The first realm that might affect cyber proxy wars is the international sphere, and more specifically international public law.[47] If international law prohibits proxy wars—then, prima facie, they should not be conducted. In reality, however, international law likely fails to regulate the conduct of states regarding proxy wars in general and cyber proxy wars in particular. Aside from political or otherwise economic barriers for such conduct regulation, the international sphere might prove trickier than one might presume, especially regarding cyber operations, which lack effective regulation within the realm of international law, as the article will discuss further.[48]

In the kinetic world, it is evident that states have almost full sovereignty over what occurs within their physical boundaries and can thus exercise various rights in response to certain hostile foreign acts, such as the right to self-defense.[49] The question of whether and how a state could respond to a nonphysical exercise of foreign powers within its own domain, be it the physical or cyber one, does not enjoy great legal certainty at this time. The answer would greatly depend on the characterization of the act and perhaps the harm that it caused, but also on a formal acknowledgment of state sovereignty in its cyber domain and its legal boundaries.[50]

Theoretically, the general legal status of cyber proxy wars could be inferred from that of regular proxy wars—those that existed prior to the emergence of the cybernetic ones. Proxy wars were formally acknowledged within the realm of international law since the 1980s.[51] While the legal framework around proxy wars consists of a patchwork of international treaties and customary law, it does establish legal obligations binding states to act responsibly in their use of proxies.[52] These rules and obligations establish, for example, a constraint on the use of force and the responsibility of a sponsor state for "internationally wrongful acts" committed by its sponsored proxy.[53] Conversely, the enforcement of such legal obligations is scant at best and thus lacks substantial teeth.[54]

To understand the extent to which cyber proxy wars could be regulated through international law, one might suggest setting a framework for interpreting cyber proxy wars under the existing legal framework, in equivalence to physical proxy wars. As previously suggested, building on Deutsch and Mumford's definitions of kinetic proxy wars, one might define cyber proxy wars as international conflicts between foreign powers, disguised as acts carried out by unrelated international actors in an attempt to influence an actor's strategic outcomes, using or fought on the cyber domain.[55]

Actions carried out as part of cyber proxy war campaigns might implicate and breach, inter alia, the existing international norms of nonintervention, as well as those prohibiting the "threat or use of force" and "armed attack" against a foreign state, similar to how kinetic actions by states and proxies could breach the same norms. If one further considers viewing cyber acts as acts of war, then, at least theoretically, they must first meet the requirements of *jus ad bellum* and then the law of armed conflict and international humanitarian laws. [56]

Nevertheless, cyber proxy wars are even more challenging to regulate than their kinetic predecessors. First, as previously mentioned, the problem of attribution is greatly enhanced in the cyber realm, adding difficulties to prove or even know which state was behind an attack. But aside from these challenges, applying the traditional legal framework of the international laws of war to cyber operations raises many difficulties regarding fulfilling traditional definitions and requirements originally meant to be applied to, and fulfilled by, the kinetic, physical world of war and its elements. Put simply, since international law only determines which physical actions would justify physical responses, the major challenge would be determining when a cyber action would amount to and equal such an action as to justify and make legitimate a response.[57]

This challenge served as one of the main reasons for the writing of the *Tallinn Manual*—a nonbinding expert's opinion on how international law should interpret and apply to cyber activities with respect to the law of war.[58] The manual addresses the issue of applying these norms to cyber operations and offers an interpretation of when a cyber conduct would breach each of them.[59] In international law, it is only when an action amounts to an "armed attack" that the right of self-defense may be invoked, allowing the injured state to respond to the hostilities.[60] Since states generally seek to retain sovereignty within their own cyberspace, they thus generally also enjoy the inherent right to act in self-defense in the face of an armed attack.[61]

According to the manual, one must examine whether the act in question constitutes either an intervention, a threat or use of force, or an armed attack; all depending on the purpose of the act, the target, and its impact. A state may therefore exercise its right to self-defense only when it is the target of a cyber operation that rises to the level of a kinetic armed attack.[62] Not every act conducted as part of a cyber proxy war will fall under the manual's or international law's requirements, as they will not constitute an "armed attack" and will therefore not qualify as an actionable act.[63] Even if the international law of war

were to unequivocally apply to cyber proxy wars, it would only allow for a very narrow and limited opportunity to respond, even if difficulties like attribution were overcome. With time, states might sign bilateral agreements in cyberwarfare, modeled on the Cold War-era arms control treaties.[64] But for now, such agreements do not exist, and international law currently lacks legally binding or sufficiently enforceable norms.

As the article previously established that the formation of internet bubbles will greatly affect cyber proxy wars, the authors further argue that domestic laws will greatly shape these bubbles and their creation. As laid down, cyberspace consists of several different layers, each of them facilitating the next.[65] The state could generally govern any layer of the internet in its effort to create an internet bubble: it could control the physical infrastructure; control the logic or information layer; or directly regulate end users, much like in the example of Russia's *RuNet*.

Regarding cyber proxy wars, however, the regulation of end-users might not advance the state's objective to a great extent since these users might not be under a state's jurisdiction. They might, for instance, be foreign agents residing outside of it, and pursuing them would prove highly difficult, expensive, or generally ineffective. The state might therefore be left focusing its efforts mainly on the first three layers. Control of the first three layers—the infrastructure, logic, and information layers—is gained mostly through control of those who operate and maintain them: the online intermediaries (i.e., internet service providers [ISPs] who maintain the different infrastructure and online platforms).

Thus, the creation of internet bubbles relies heavily on how online intermediaries are regulated by the state—or how much the government can control and command them. This is where the Chinese-Russian and American approaches greatly differ, walking down diverging paths. The American legal system generally abstains from imposing any form of direct or indirect liability on online intermediaries. Under the American liability regime—it would be highly difficult, if not almost impossible, to mandate or control an American internet bubble for almost any reason, let alone to combat cyber proxy wars. One of the main reasons that the United States might be in a severe disadvantage in defending against cyber proxy wars, or properly responding to them, is that its legal regime makes it highly difficult to form internet bubbles. The U.S. approach largely relies on the market to self-regulate, based partially on Adam Smith's monumental notion of the "invisible hand."[66]

This approach is currently articulated under the Communication Decency Act (CDA). While this 1996 act was originally aimed at curbing online pornography, large parts of it were deemed an unconstitutional infringement on free speech by the U.S. Supreme Court and thus struck down, all but keeping one highly influential section—known as section 230.[67] Under the current prevalent interpretation of section 230, the CDA grants broad immunity for online intermediaries, and they generally are not liable for third-party content they host.[68] This exemption from liability generally grants broad immunity to any

ISP, regardless of the legality or legitimacy of the content hosted, while ISPs are also entitled to remove offensive or otherwise objectionable content from their platforms when acting in "good faith." [69]

It is thus challenging from an American perspective to regulate ISPs, and thereby the content that is present in online platforms, as long as such content is considered protected speech under the current Supreme Court's libertarian stance on the First Amendment, and as long as section 230 remains intact. Such regulation might impede free speech, guaranteed by the First Amendment, which is considered a highly important human right for various reasons, but perhaps mostly plays an important role in protecting democracy.[70] In other words, the U.S. approach would generally abstain from obliging ISPs to act as censors, not because all content must remain online at any cost, but because the government should not, and legally speaking cannot compel intermediaries to make such judgments, at least for the time being.[71]

However, many argue that it is both possible and desirable to amend section 230 and that, at the very least, some internet intermediaries should bear legal liability in some instances.[72] The United States had, in fact, experienced some recent changes in its view regarding intermediary liability when former president Donald J. Trump claimed he intends to create a so-called "internet kill-switch" for national security purposes.[73] In the context of the COVID-19 pandemic, Twitter had begun tagging some of the tweets made by Trump as factually false, while adding informational links to news articles.[74] In response, Trump signed an executive order that allowed the Federal Communications Commission to craft rules that will govern internet intermediaries under section 230.[75] Even with this new order, and after the Capitol riot on 6 January 2021, Twitter had permanently banned Trump's account over the "risk of further incitement of violence," and Trump's attempt to file a lawsuit against them for doing so eventually failed.[76] But more importantly, such regulation did not last long, as U.S. president Joseph R. Biden decided to revoke Trump's executive order that targeted section 230.[77]

Still, section 230 is not a constant. Reshaping or even revoking section 230's safeguards to intermediaries might enjoy bipartisan support, at least at this time, as reflected in the view of President Biden, among other U.S. senators, and there are few proposed bills that aim to do so.[78] Other bills might also directly tackle foreign disinformation on social media, adding some exceptions to section 230.[79] Currently, however, more than 25 years after its enactment, section 230 remains intact, and other legislative attempts to limit its scope failed for now.

There are many facets to choosing a liability model, and it greatly depends on the legal jurisdiction in question. It is not our purpose here to discuss which liability model is more optimal in general (if such normative evaluation could even be objective), or to show how choosing one model would impact human rights and liberties differently than another.[80] Rather, this article aims to exemplify how the American liability regime comes into play within the context of

cyber proxy wars, and to further shed light on the potential future path that those susceptible to such wars might take (or are already taking)—if they keep their current legal approach to intermediaries.[81]

Even if section 230 changes over time, it is difficult to see how the United States would directly create an internet bubble, as such a move stands in stark contrast to the American notion of free speech. Any form of regulation that will attempt to create a U.S. internet bubble by infringing upon free speech, through any means of controlling one or more of the different layers, will very likely be constitutionally challenged, and thus subjected to strict scrutiny—the highest and almost impossible threshold that the state must pass to prove the lawfulness of such regulation.[82] Of course, if the president declares a "war or threat of war" or even "a state of public peril," then they might be able to exercise various authorities such as taking control over "wire communications" under a 1934 act—including the internet.[83] Therefore, at least in its territory, the U.S. president might be able to control the internet without even adhering to Congress.[84] With that being said, it is highly unlikely that this authority will be easily exercised, especially not in the context of proxy wars, cybernetic or not.

There could be some other forms of regulating intermediaries that could potentially also affect cyber proxy wars. One example could be using advertisement rules or other forms of mandatory disclosures regarding those who purchase online ads.[85] Following the 2016 U.S. election interference, some states had in fact passed election laws that obligate ISPs to disclose information about the identity of those who purchased political ads.[86] But, aside from potential practical difficulties, like that of acts of concealment by an actor within a proxy war, laws of this nature (if challenged in court) will not likely be deemed constitutional as they are considered compelled speech, which could also infringe upon the First Amendment.[87] Moreover, in the context of this article, such disclosure laws will only tackle potential cyber proxy wars from a very limited aspect—serving a narrow solution to a much wider challenge.

Means to Preserve Sovereignty in Cyberspace

The United States might make use of other potential means, which do not include the creation of an internet bubble per se, in its effort to preserve sovereignty and resist cyber proxy warfare. One means is to actively restrict transactions between U.S. entities and parent Russian or Chinese companies, essentially banning their use in the United States. Former president Trump had attempted to do so with ByteDance and Tencent (the parent companies of TikTok and WeChat, respectively).[88] The problem here is that such means are highly limited as it only targets a fraction of intermediaries and is less relevant for U.S. companies as long as section 230 remains intact.

A more plausible means is that of the market self-regulating. Under this argument, it is upon private actors—like ISPs—to regulate the kind of harmful conduct involved in cyber proxy war campaigns. In other words, the American approach, which created the governmental barrier of noninterference within

an invisible hand perspective, might also drive the market to respond to cyber proxy wars, and thus, even without forming an internet bubble, mitigate at least some of the risks to the United States from them.

The question of whether this approach advances the rationales of free speech or not could be debatable, but it is beyond the scope of this article.[89] Here, in this context, the authors merely strive to show how these constitutional barriers and the legal regime in the United States could be used as a tool by other jurisdictions within these cyber proxy wars. The problem with market self-regulation are its numerous potential failures. It is perceived as unlikely that for-profit companies will self-regulate their platforms, even despite ongoing cyber proxy wars, unless such self-regulation proves economically beneficial for them.

The market, however, could be nudged to combat these wars, at least to some extent. The government or other policy makers could, for instance, warn companies that they *might* be regulated if they do not act in a self-regulatory manner, which will, at the very least, reduce the scope of these proxy wars and their perceived damages and negative effects. Consider the congressional response to the Facebook-Cambridge Analytica data breach—an example of how one might use ISPs to influence politics (and advance their own agenda)—that could demonstrate how Congress might pressure or nudge online intermediaries to act without the need for direct legislation or regulation.[90]

Furthermore, these online platforms often aid the government under what is termed as public-private partnerships (PPPs)—collaborations between governments and online intermediaries in managing online behavior.[91] The authors have witnessed such PPPs in American history and more closely within some of the secret surveillance programs that Edward Snowden revealed in 2013.[92] If properly incentivized to "voluntarily" assist the government, online intermediaries might assume a role as a cyber proxy for governance responses to cyber proxy wars.[93] In the post-Snowden era, Congress further granted authorization for ISPs to monitor their information systems, operate defensive measures, and share "cyber threat indicators" or "defensive measures" for a cybersecurity purpose.[94]

But all in all, the United States might just attempt to respond to cyber proxy wars by utilizing other means at hand, which might prove simply more feasible. It might deploy its political, economic, or otherwise kinetic strength to directly or indirectly combat those who operate against it within the cyber domain.[95] The limits of such means, however, lie within those sovereign powers who are less reliant or dependent on American political or economic support. While the United States, on the other hand, might find itself heavily reliant on foreign powers who may already have an internet bubble in place and therefore places it in a severe disadvantage in fighting the cyber proxy wars.

Still, even without resorting to kinetic wars, the United States might simply act aggressively within the cyber realm directly against its adversaries.[96] It might also begin to heavily regulate what enters its kinetic and digital borders to some extent. In the physical realm, the United States could respond to proxy wars by

banning specific imports.[97] In the digital realm, it might regulate end-users by banning specific apps or regulate the market by banning or otherwise restricting transactions between U.S. companies and foreign ones—relying on national security arguments. Such tactics had been taken regarding the Chinese-owned apps TikTok and WeChat.[98]

Eventually, without a significant shift in the American perception of online intermediaries' regulation, the solution to cyber proxy wars will probably lie elsewhere than with the formation of a U.S. internet bubble. The United States will likely continue to have an open internet, as opposed to an isolated bubble, albeit with independent market forces, as part of a notion of self-regulation, likely to intervene more to address harmful effects. Under corporate social responsibility or other incentives, we are likely to see platform governance on the rise, which could eventually include a direct response to cyber proxy wars. We have already begun to witness how some social media companies, like Facebook or Twitter, are forming their own oversight boards, intended to make principal decisions regarding content moderation.[99]

And truly, corporate governance is on the rise and might prove useful as a shield against foreign influence. Content moderation and the removal of accounts that are linked to domestic political influence is constantly occurring around the world, such as in Ukraine, Iran, Russia, to name but a few examples.[100] These platforms are already shaping the scope of national security in many countries.[101] On the other hand, there are still limits for such influence, especially when for-profit companies wish to stay in the market. To exemplify, when the Russian government was dissatisfied with Twitter's content removal procedures, it almost immediately slowed it down for users.[102] Thus, one of the problems with platform governance is that eventually these for-profit companies act to increase their revenues outside of the United States as well.

Only time will tell whether such an approach could work for the United States. Perhaps internet bubbles make a more direct and efficient way of handling cyber proxy wars. But they do come with costs in terms of human rights and liberties, and if ISPs do a rather decent job in combating these proxy wars—even if not as good as with a strict liability regime in place—then this trade-off might prove worthwhile. It would be unfortunate if nondemocratic states will eventually misuse democratic and liberal values against those same states who attempt to safeguard them.[103]

Finally, it is important to note that while the United States and Russia-China serve as opposing examples for domestic law regimes, other legal regimes could be placed along the spectrum between a liberal democracy and a nondemocracy.[104] Indeed, the greater fear and challenge might lie within those other legal jurisdictions that desire to implement a regulatory regime rather similar to that of the United States, but lack any meaningful other powers—be it political, economic, military, or otherwise—to challenge and engage with cyber proxy wars without adhering to direct legislation or intervention. Lacking strong constitutional safeguards such as those of the United States, countries may resort to

legislation and deeper intervention in cyber space, and internet bubbles might form in many countries as a defensive measure. This could, in turn, eventually negatively affect online free speech rather dramatically, and subsequently affect and perhaps even threaten democracy and liberalism itself. This concern grows more severe as we move further away from the United States' end of the political spectrum toward that of Russia, China, North Korea, and their likes.

Conclusion

The authors began their article with Churchill's note on the Soviet Iron Curtain, which existed to serve the Soviet regime and enable it to both control its domestic affairs and avoid extensive international influence. With the proliferation of the internet, along with a toothless international law system regarding cyberattacks, influence, and espionage, countries now seek to gain more control with a contemporary iron curtain of their own, thus gaining cyber sovereignty meant to avoid or resist foreign influence and intervention. Furthermore, cyber deterrence or retaliation is becoming almost impossible due to the practice of cyber proxy warfare—cyberspace is an evasive and anonymous proxy. Countries like Russia, China, Iran, and North Korea could resist foreign influence by creating their sovereign internet bubbles and gain power by influencing countries that lack such bubbles. These internet bubbles could cover all of the layers that make cyberspace what it is: Russia's *RuNet* experiment, China's sovereign internet, and North Korea's *Kwangmyong* intranet project all exemplify the bubbles created by the physical layer (aimed to protect hacking and eavesdropping), the logic layer (aimed to protect from computational manipulations), the information layer (aimed to protect from disinformation or malicious software), and the user layer (aimed to protect from manipulative users).

To some extent, liberal democracies such as the United States are in a severe disadvantage in this regard. That is, while Russia and China, lacking meaningful legal and constitutional restraints, are dealing with the deficiencies of the cyber domain and the lack of binding international law, the United States is left behind due to its democratic values and governance. Cases like the 2016 presidential elections intervention by Russia or COVID-19 disinformation might all serve as examples in which the United States failed to properly protect itself from foreign threats. In contrast, the conflict between Ukraine and Russia has demonstrated, at least as of this writing (May 2023) that restricting and regulating domestic internet and media are important strategic tools to undermine foreign propaganda and antigovernmental sentiments. Still, Moscow is not safe from its own domestic arena as internal rifts and power struggles intensify in Russia but many are not directly connected to Western propaganda. The practice of cyber proxy warfare might further allow foreign powers to attack their adversaries through targeting nonstate entities and institutions associated with them, as exemplified by the Sony Pictures case.

How can the United States and other similar democracies protect themselves and remain sovereign in the age of (dis)information and cyber warfare?

As the authors argue and predict throughout the article, if the United States will not eventually "catch up" with internet-related restrictions to stand strong against its global adversaries, it will be up to private intermediaries to self-regulate such threats. The United States is not likely to form a hermetic internet bubble, but if platform governance fails, it might strive to find other ways to influence ISPs or use other means to aid them in the fight over sovereignty and control. As the authors suggest, the practice of cyber proxy warfare has in fact influenced international orders and norms. Now, the only questions are how and whether they will succeed. Otherwise, perhaps even true liberal democracies will begin to form their own internet bubbles and the internet will transform into something different altogether.

Endnotes

1. Winston Churchill, address at Westminster College, Fulton, Missouri, 5 March 1946.
2. The term *internet bubbles* was coined by the authors in the context of cyber sovereignty. The term mostly exists in the context of the internet bubble of the 1990s, a.k.a. the dot-com bubble. It can also refer to a generation that grew up in a digital bubble and social media.
3. Richard J. Harknett and Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71, https://doi.org/10.1162/ISEC_c_00290; and Laura Rosenberger, "Making Cyberspace Safe for Democracy—The New Landscape of Information Competition," *Foreign Affairs*, no. 99 (May/June 2020): 146–59.
4. The Internet Backbone is an infrastructure of mainly fiber optic cables that connects multiple nodes and effectively connect various networks worldwide. See Nazli Choucri and David D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma* (Cambridge, MA: MIT Press, 2018), 33–65, 101–22.
5. Kristina Daugirdas and Julian Davis Mortenson, "United States Responds to Alleged North Korean Cyber Attack on Sony Pictures Entertainment," *American Journal of International Law* 109, no. 2 (2015): 419.
6. Andreas Osiander, "Sovereignty, International Relations, and the Westphalian Myth," *International Organization* 55, no. 2 (2001), 251–87; Gene M. Lyons and Michael Mastanduno, eds., *Beyond Westphalia?: State Sovereignty and International Intervention* (Baltimore, MD: Johns Hopkins University Press, 1995); and Robert O. Keohane and Joseph S. Nye Jr., "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (1998): 81–94.
7. Rawi Abdelal and Adam Segal, "Has Globalization Passed Its Peak?," *Foreign Affairs* (2007): 103–14; and Josh Salisbury, "Omicron: More Countries Restrict Foreign Travellers over New Variant Fears," *Evening Standard*, 30 November 2021.
8. Alexander Lanoszka, "Disinformation in International Politics," *European Journal of International Security* 4, no. 2 (2019): 227–48, https://doi.org/10.1017/eis.2019.6.
9. Aysegul Aydin, *Foreign Powers and Intervention in Armed Conflicts* (Stanford, CA: Stanford University Press, 2012), 1–5.
10. Osiander, "Sovereignty, International Relations, and the Westphalian Myth."
11. Frederic S. Pearson, "Foreign Military Interventions and Domestic Disputes," *International Studies Quarterly* 18, no. 2 (1974): 259–90.
12. Joseph S. Nye Jr., "Soft Power," *Foreign Policy*, no. 80 (1990): 153–71, https://doi.org/10.2307/1148580; Joseph S. Nye Jr., "Get Smart: Combining Hard and Soft Power," *Foreign Affairs* 88, no. 4 (July/August 2009): 160–63; Ernest J. Wilson III, "Hard Power, Soft Power, Smart Power," *Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 110–24, https://doi.org/10.1177/0002716207312618; Ra-

chelle Faust, " 'Sharp Power': Rising Authoritarian Influence," National Endowment for Democracy, 5 December 2017; and Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Foreign Affairs*, 16 November 2017.

13. Harknett and Nye, "Deterrence and Dissuasion in Cyberspace," 44–71.
14. Karl W. Deutsch, "External Involvement in Internal War," in *Internal War: Problems and Approaches*, ed. Harry Eckstein (New York: Free Press of Glencoe, 1964); Andrew Mumford, *Proxy Warfare* (Cambridge, UK: Polity Press, 2013), 1–29; and Andrew Mumford, "Proxy Warfare and the Future of Conflict," *RUSI Journal* 158, no. 2 (2013): 40–46, https://doi.org/10.1080/03071847.2013.787733.
15. Harknett and Nye, "Deterrence and Dissuasion in Cyberspace"; Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution," *Fletcher Security Review*, no. 1 (2014): 53–72; and Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2017).
16. Tim Maurer, " 'Proxies' and Cyberspace," *Journal of Conflict and Security Law* 21, no. 3 (2016): 383–403, https://doi.org/10.1093/jcsl/krw015; Pnina Shuker and Lev Topor, "Russian Influence Campaigns Against NATO in the Baltic Region: Spread of Chaos and Divide et Impera," in *The Russian Federation in Global Knowledge Warfare*, ed. Holger Mölder et al. (Cham, Switzerland: Springer, 2021), 295–314, https://doi.org/10.1007/978-3-030-73955-3_15.
17. Deutsch, "External Involvement in Internal War"; Mumford, *Proxy Warfare*, 1–29; Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, UK: Cambridge University Press, 2018), 3–28; and Andreas Krieg and Jean-Marc Rickli, "Surrogate Warfare: The Art of War in the 21st Century?," *Defence Studies* 18, no. 2 (2018), 113–30, https://doi.org/10.1080/14702436.2018.1429218.
18. Jason Andress and Steven Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Amsterdam, Netherlands: Syngress, 2013), 1–14.
19. Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington, DC: Brookings Institute Press, 2019), 1–8.
20. There is, however, an available domestic intranet, known as *Kwangmyong*, which allows access to domestic websites and emails, but these are controlled by the government. "North Korea: Connection Denied: Restrictions on Mobile Phones and Outside Information in North Korea," Amnesty International, 9 March 2016; "North Korea: Tightened Controls on Communications with the Outside World Leave Families Devastated," Amnesty International, 7 March 2016; and Cheng Chen, Kyungmin Ko, and Ji-Yong Lee, "North Korea's Internet Strategy and Its Political Implications," *Pacific Review* 23, no. 5 (2010): 649–70, https://doi.org/10.1080/09512748.2010.522249.
21. Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, CT: Yale University Press, 2006), 23; Choucri Nazli and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma" (ECIR Working Paper No. 2012-3, MIT Political Science Department, 6 November 2012); and Nazli and Clark, *International Relations in the Cyber Age*, 33–65, 101–22.
22. Jonathan Masters, "Ukraine: Conflict at the Crossroads of Europe and Russia," Council on Foreign Relations, 14 February 2023; and Jon Bateman, Nick Beecroft, and Gavin Wilde, "What the Russian Invasion Reveals About the Future of Cyber Warfare," Carnegie Endowment, 19 December 2022.
23. Anton Troianovski and Valeriya Safronova, "Russia Takes Censorship to New Extremes, Stifling War Coverage," *New York Times*, 4 March 2022.
24. Tetyana Klug and Rachel Baig, "Fact Check: Russia's Disinformation Campaign Targets NATO," DW, 13 February 2023.
25. Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endowment, 16 December 2022.
26. Stephen Blank, "Threats to and from Russia: An Assessment," *Journal of Slavic Military Studies* 21, no. 3 (2008): 491–526, https://doi.org/10.1080/13518040802313746;

and Andrea Shalal, "U.S. Air Force Leader Sees Russia as 'Biggest Threat'," Reuters, 9 July 2015.

27. *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper* (Washington, DC: Department of Defense, May 2019).
28. Совет Федерации, "Концепция Стратегии Кибербезопасности Российской Федерации" [Russian] (The Concept of the Cyber Security Strategy of the Russian Federation); and Michael Connell and Sara Vogler, "Russia's Approach to Cyber Warfare," CNA, March 2017.
29. Russia's successful attempt to unplug from the global internet was an effort to test an internal (or domestic) internet that would allow internal communication without being connected to external information flow and without relying on external services. This was done by unplugging Russia from submarine fiber optic cables that connect Russia to the global internet. See Jane Wakefield, "Russia 'Successfully Tests' Its Unplugged Internet," BBC, 24 December 2019.
30. "Cable Compendium: A Guide to the Week's Submarine and Terrestrial Developments," CommsUpdate, 19 February 2021.
31. Daria Litvinova, "Human Wrongs: How State-Backed Media Helped the Kremlin Weaponise Social Conservatism" (Reuters Institute Fellowship Paper, Oxford, UK, University of Oxford, July 2018); and Jill Dougherty, "How the Media Became One of Putin's Most Powerful Weapons," *Atlantic*, 21 April 2015.
32. The Yarovaya Laws (Russian: Закон Яровой) are a set of bills (374-FZ, 375-FZ) passed in 2016 that amend preexisting counterterrorism laws and deal with the regulation and monitoring of cyberspace. The bills compel the telecommunication industry to allow Russian authorities access to their data by providing them the encryption and decryption keys necessary to decode and monitor online data. For the bill amending counterterrorism measurements, see: Законопроект № 1039149-6 [Russian]. The Russian Sovereign Internet Law provides Moscow the capacity to turn off connections within Russia or with the worldwide web entirely in case of an emergency. See Isabelle Khurshudyan, "The Kremlin Is Notorious for Global Meddling Online. But Controlling Cyberspace at Home Has Been Trickier," *Washington Post*, 26 January 2020. SORM—System for Operative Investigative Activities is Russia's mass communications surveillance. Russian law gives Russia's security service, the FSB, the authority to collect, analyze, and store all data that was transmitted or received on Russian networks. See James A. Lewis, "Reference Note on Russian Communications Surveillance," Center for Strategic and International Studies, 18 April 2014; and Anton Zverev and Gabrielle Tétrault-Farber, "Putin Signs Law Making Russian Apps Mandatory on Smartphones, Computers," Reuters, 2 December 2019.
33. On 18 March 2019, Vladimir Putin signed two laws passed by the Russian Federal Assembly aimed at countering the creation and dissemination of fake news. The laws establish fines for knowingly spreading fake news and procedures for internet service providers to block access to websites disseminating fake news. The laws are the Federal Law on Amending Article 15-3 of the Federal Law on Information, Information Technologies and Protection of Information (№ 31-ФЗ) and the Federal Law on Amending the Code of Administrative Violations (№ 27-ФЗ). Mark Bennetts, "Russia Passes Law to Jail People for 15 Days for 'Disrespecting' Government," *Guardian*, 6 March 2019. The Russian Foreign Agent Law applies to individuals who distribute online information and receive funds from foreign sources. Individuals who distribute foreign media can also be labeled as foreign agents. Russian citizens and foreign visitors can be labeled as foreign agents. Интерфакс, "Путин подписал закон о физлицах-иноагентах," 2 декабря 2019.
34. Lev Topor and Alexander Tabachnik, "Russian Cyber Information Warfare," *Journal of Advanced Military Studies* 12, no. 1 (Spring 2021): 112–27, https://doi.org/10.21140/mcuj.20211201005.
35. Rob Picheta, " 'It's All a Lie': Russians Are Trapped in Putin's Parallel Universe. But Some Want Out," CNN, 27 February 2023.
36. Samuel Charap, John Drennan, and Pierre Noël, "Russia and China: A New Model of

Great-Power Relations," *Survival* 59, no. 1 (2017): 25–42, https://doi.org/10.1080/00396338.2017.1282670; and Michael Mastanduno, "Partner Politics: Russia, China, and the Challenge of Extending US Hegemony after the Cold War," *Security Studies* 28, no. 3 (2019): 479–504, https://doi.org/10.1080/09636412.2019.1604984.

37. Nina Hachigian, "China's Cyber-Strategy," *Foreign Affairs* 80, no. 2 (March/April 2001): 118–33; and William T. Dowell, "The Internet, Censorship, and China," *Georgetown Journal of International Affairs* 7, no. 2 (2006): 111–19.
38. According to the privacy-oriented site vpnMentor, China blocks more than 8,000 websites: Ariel Hochstadt, "The Complete List of Blocked Websites in China & How to Access Them," vpnMentor, 16 June 2020.
39. Niels N. Schia and Lars Gjesvik. "China's Cyber Sovereignty," Norwegian Institute of International Affairs, Policy Brief no. 2, 17 March 2017.
40. Amy Chang, *Warring State: China's Cybersecurity Strategy* (Washington, DC: Center for a New American Security, 2014).
41. "China Announces Cybersecurity Strategy," State Council, People's Republic of China, 27 December 2016; Jyh-An Lee, "Hacking Into China's Cybersecurity Law," *Wake Forest Law Review* 53, no. 1 (2018): 57; and Paul Rosenzweig, "China's National Cybersecurity Strategy," *Lawfare* (blog), 27 December 2016. For a detailed review of Chinese internet regulation, see Samm Sacks and Manyi K. Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," Center for Strategic & International Studies, 2 August 2018.
42. Chang, "Warring State."
43. Gregory J. Moore, "Huawei, Cyber-sovereignty and Liberal Norms: China's Challenge to the West/Democracies," *Journal of Chinese Political Science*, no. 28 (2022): 1–17, https://doi.org/10.1007/s11366-022-09814-2.
44. Sacks and Li, "How Chinese Cybersecurity Standards Impact Doing Business in China."
45. VPN is a virtual private network; it extends a private network on top of a public network and enables users to use the web as if they were connected to the internet from a different location.
46. Mark A. Lemley, "Rationalizing Internet Safe Harbors," *Journal on Telecommunication & High Technology Law* 6, no. 1 (2007): 115–16; and Michael L. Rustad and Thomas H. Koenig, "Rebooting Cybertort Law," *Washington Law Review* 80, no. 2 (2005): 392.
47. Malcolm N. Shaw, *International Law*, 5th ed. (Cambridge, UK: Cambridge University Press, 2012), chaps. 1–2.
48. Harknett and Nye, "Deterrence and Dissuasion in Cyberspace," 47.
49. The right of self-defense is an inherent one under customary international law, as well as under the UN Charter. See United Nations, *Charter of the United Nations* (1945), art. 2(4), 51; and Shaw, *International Law*, 1,024–32.
50. An "armed attack" would include "the sending by or on behalf of a state of armed bands or groups which carry out acts of armed force of such gravity as to amount to an actual armed attack." The involvement of the state would be considered in order to hold it liable and legitimate an act of self-defense against it. See Shaw, *International Law*, 1,026–28. The consequences of a cyber act and its surrounding circumstances will determine whether it had crossed the "use of force" threshold. See Schmitt, *Tallinn Manual 2.0*, 328–56.
51. Robert Heinsch, "Conflict Classification in Ukraine: The Return of the 'Proxy War'?," *International Law Studies*, no. 91 (2015): 340.
52. Brittany Benowitz and Tommy Ross, "Time to Get a Handle on America's Conduct of Proxy Warfare," *Lawfare* (blog), 9 April 2020; and *The Legal Framework Regulating Proxy Warfare* (Chicago, IL: American Bar Association, 2019).
53. *The Legal Framework Regulating Proxy Warfare*; and International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (New York: United Nations, 2001), art. 8.
54. International Law Commission, *Draft Articles on Responsibility of States for Internation-*

ally Wrongful Acts. See also Harknett and Nye, "Deterrence and Dissuasion in Cyberspace," 44–71.

55. Deutsch, "External Involvement in Internal War"; and Mumford, *Proxy Warfare*.
56. General Assembly, United Nations, *Resolution 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations* (24 October 1970); Clare Sullivan, "The 2014 Sony Hack and the Role of International Law," *Journal of National Security Law & Policy*, no. 8 (2016): 455–59; United Nations, *Charter of the United Nations*, art. 2(4), 51; and Sullivan, "The Sony Hack," 455 and onward. These would include, inter alia, just cause, proportionality, right intention and authority, last resort, and reasonable chance of success. See Anthony Pfaff, "Proxy War Ethics," *Journal of National Security Law and Policy*, no. 9 (2017): 308.
57. Sullivan, "The Sony Hack," 455 and onwards; and Schmitt, *Tallinn Manual 2.0*, 1–2.
58. Schmitt, *Tallinn Manual 2.0*, 1–2. See rule 69 that states that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."
59. Schmitt, *Tallinn Manual 2.0*, 1–2, rules 66 (Prohibition of Intervention), 68–70 (Prohibition of the Use of Force), and 71 (Self-Defence Against Armed Attack).
60. United Nations, *Charter of the United Nations*, art. 2(4), 51; and Sullivan, "The Sony Hack," 455n128 and onward.
61. Drew Marvel, "Protecting the States from Electoral Invasions," *William & Mary Bill of Rights Journal* 28, no. 1 (October 2019): 216.
62. Schmitt, *Tallinn Manual 2.0*, rule 71.
63. Marvel, "Protecting the States," 220; and Sullivan, "The Sony Hack."
64. Anton Troianovski and David E. Sanger, "Putin Wants a Truce in Cyberspace—While Denying Russian Interference," *New York Times*, 25 September 2020.
65. These layers comprise of the physical, logic, information, and end-user. See Benkler, *The Wealth of Networks*.
66. See Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (1776; repr., Amsterdam, Netherlands: MetaLibri, 2007).
67. See Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
68. Communications Decency Act, 47 U.S.C. § 230 (2006).
69. For more on section 230, see Danielle K. Citron and Benjamin Wittes, "The Internet Will Not Break: Denying Bad Samaritans Sec. 230 Immunity," *Fordham Law Review* 86, no. 2 (November 2017): 401–24.
70. Jack M. Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society," *New York University Law Review* 79, no. 1 (2004): 34. The First Amendment currently protects speech, even if such speech is false. See United States v. Alvarez, 132 S. Ct. 2537, 2539, 2544 (2012).
71. Corey Omer, "Intermediary Liability for Harmful Speech: Lessons from Abroad," *Harvard Journal of Law & Technology* 28, no. 1 (Fall 2014): 315.
72. Cass R. Sunstein, "The First Amendment in Cyberspace," *Yale Law Journal*, no. 104 (1995); and Rebecca Tushnet, "Power Without Responsibility: Intermediaries and the First Amendment," *George Washington Law Review*, no. 76 (2008).
73. Sean Lawson, "The Law that Could Allow Trump to Shut Down the US Internet," *Forbes*, 2 December 2016.
74. "Twitter Tags Trump Tweet with Fact-Checking Warning," BBC, 27 May 2020.
75. John T. Bennet, "Trump Signs Controversial Executive Order that Could Allow Federal Officials to Target Twitter, Facebook and Google," *Independent*, 28 May 2020.
76. Kate Conger and Mike Isaac, "Twitter Permanently Bans Trump Capping Online Revolt," *New York Times*, 8 January 2021; and Adi Robertson, "Judge Dismisses Donald Trump's Twitter Ban Lawsuit," *Verge*, 6 May 2022.
77. Kim Lyons, "Biden Revokes Trump Executive Order that Targeted Section 230," *Verge*, 15 May 2021.
78. Editorial Board, "Opinion: Joe Biden—Former Vice President of the United States,"

New York Times, 17 January 2020; "Senate Panel Mulls Revoking Immunity, Citing COVID Scams Online," Reuters, 21 April 2021; and Oscar Gonzalez, "Bill Unveiled to Reduce Section 230 Protections for Social Media Companies," CNET, 5 February 2021.

79. Maggie Miller, "House Lawmakers Reintroduce Bipartisan Bill to Weed out Foreign Disinformation on Social Media," *Hill*, 22 January 2021.
80. Jonathan Zittrain, "A History of Online Gatekeeping," *Harvard Journal of Law & Technology*, no. 19 (2006).
81. For more on section 230, see Eric Goldman, "An Overview of the United States' Section 230 Internet Immunity," in *The Oxford Handbook of Online Intermediary Liability*, ed. Giancarlo Frosio (forthcoming).
82. Strict scrutiny requires demonstrating that the regulation is necessary to a compelling state interest; that it is narrowly tailored to achieve such purpose, and that the regulation uses the least restrictive means to achieve its purposes.
83. See 47 U.S.C. § 606(d) (1934).
84. Maura K. Perri, "Build the Fire-Wall: Potential Dangers to Internet Freedom under the Trump Administration," *Duquesne Law Review* 57, no. 1 (Winter 2019): 195.
85. Steven T. Dennis, "Senators Propose Social-Media Ad Rules after Months of Russia Probes," *Bloomberg*, 19 October 2017.
86. See, for instance, in Maryland: MD. Code Ann., Elec. Law § 13-405 (2020).
87. Eugene Volokh, "The Law of Compelled Speech," *Texas Law Review*, no. 95 (2018). Specifically, the Fourth Circuit recently held that Maryland law was unconstitutional on these grounds. For more on the debate of whether such move is constitutional under U.S. law, see "Notes: Two Models of the Right to Not Speak," *Harvard Law Review,* no. 113 (2020).
88. Adi Robertson, "The Big Legal Questions Behind Trump's TikTok and WeChat Bans," *Verge*, 10 August 2020.
89. Marcelo Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries," *Vanderbilt Journal of Entertainment and Technology Law* 18, no. 4 (Summer 2016).
90. Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *Guardian*, 17 March 2018; Jamie Condliffe, "How to Fix Social Media's Big Problems? Lawmakers Have Ideas," *New York Times*, 30 July 2018; and Lauren Feinr, "Senators Threaten to Regulate Encryption If Tech Companies Won't Do It Themselves," CNBC, 10 December 2019.
91. Niva Elkin-Koren and Eldar Haber, "Governance by Proxy: Cyber Challenges to Civil Liberties," *Brooklyn Law Review*, no. 82 (2017); Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (2016): 43–62; and Kristoffer K. Christensen and Karen L. Petersen, "Public–Private Partnerships on Cyber Security: A Practice of Loyalty," *International Affairs* 93, no. 6 (2017): 1435–52, https://doi.org/10.1093/ia/iix189.
92. Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps into User Data of Apple, Google, and Others," *Guardian*, 7 June 2013.
93. Elkin-Koren and Haber, "Governance by Proxy."
94. See Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2016).
95. Kate Conger, "Twitter Removes Chinese Disinformation Campaign," *New York Times*, 11 June 2020; Mark Scott, "Facebook Slaps Labels on Chinese and Russian State-Controlled Media Amid Anger over Donald Trump's Posts," *Politico*, 4 June 2020; and Ellen Nakashima, "Biden Administration Imposes Significant Economic Sanctions on Russia over Cyberspying, Efforts to Influence Presidential Election," *Washington Post*, 15 April 2021.
96. Zachary Evans, "Trump Gave CIA Authorization to Increase Aggressive Cyber Attacks: Report," *National Review*, 15 July 2020.

97. Ben Westcott, "New US Bill Could Ban Imported Chinese Goods from Xinjiang Amid Forced Labor Concerns," CNN: Politics, 12 March 2020.
98. After first contemplating a nationwide ban on their operation, the president opted instead for a future ban on two Chinese-owned apps, unless they are sold to American hands. See Nikki Carvajal and Caroline Kelly, "Trump Issues Orders Banning TikTok and WeChat from Operating in 45 Days If They Are Not Sold by Chinese Parent Companies," CNN, 7 August 2020; and John Koetsier, "TikTok to Be Banned in USA, Trump Announces," *Forbes*, 1 August 2020.
99. Kate Klonick, "Creating Global Governance for Online Speech: The Development of Facebook's Oversight Board," *Yale Law Journal*, no. 129 (2020); and Nick Clegg, "Welcoming the Oversight Board," Facebook, 6 May 2020.
100. Elizabeth Culliford, "Facebook Removes Ukraine Political 'Influence-for-Hire' Network," Reuters, 6 May 2021.
101. Cameron Jenkins, "Twitter Removes Hundreds of Accounts Tied to Iran, Russia," *Hill*, 24 February 2021; Culliford, "Facebook Removes Ukraine Political 'Influence-for-Hire' Network"; Igor Bonifacic, "Twitter Bans 100 Accounts Linked to Russian Troll Farms," engadget, 23 February 2021; and Elena Chachko, "National Security by Platform," *Stanford Technology Law Review* 25, no. 1 (2021).
102. Anton Troianovski and Andrew E. Kramer, "Russia Says It Is Slowing Access to Twitter," *New York Times*, 10 March 2021.
103. Some might even argue that democracy is deteriorating, both online and offline, thus it might be somewhat inevitable that states will intervene in internet regulation more closely. See Nathaniel Persily, "Can Democracy Survive the Internet?," *Journal of Democracy* 28, no. 2 (2017): 74–75.
104. Lingling Wei, "China Declared Its Russia Friendship Had 'No Limits.' It's Having Second Thoughts," *Wall Street Journal*, 3 March 2022.