Imposing and Evading Cyber Borders: The Sovereignty Dilemma

Alessandro Guarino and Emilio Iasiello

The world's perception of cyberspace has evolved from the libertarian promises of the 1990s to the current situation, where nation-states seek to reestablish their sovereignty. This paper explores the history of our conceptions of cyberspace, from the enthusiastic utopias culminating in the so-called "declaration of independence of cyberspace" to the technological underpinnings and the legislative steps being taken by today's governments to assert more control. It will address efforts in the West and East to resolve diverse, multi-faceted, and ongoing challenges that range from supporting open cyberspace to being able to heavily monitor the threat activities and the various state and non-state actors operating in cyberspace. The paper will highlight the technical and regulatory difficulties in establishing borders in cyberspace, as well as the corresponding policy consequences, and reveal how actors are evading borders by using various techniques such as cryptography and data havens, to name a few. The main takeaway is that the balkanization of cyberspace is not only a reality, but also a course that may be too difficult to reverse, and raises the question of how do open societies balance sovereignty with individual freedoms in cyberspace? A proposal is offered, drawing from examples in which the sovereignty of nation-states is limited and in which borders are not a factor, such as the international body of law regulating global commons.

Alessandro Guarino is the principal consultant of StudioAG, an Italian information security and cybersecurity consultancy firm. Emilio Iasiello is a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, as well as the private sector.

Keywords: cybersecurity, internet governance, international relations, cyberwarfare, cyber conflict, China, privacy

Introduction

The worldwide diffusion of a unique digital information-carrying infrastructure over the last decade of the twentieth century has deeply changed every facet of life and society, from social interactions to the global economy. Availability of internet access is—at least in developed nations—considered almost a "given" right. Cyberspace, however, is not a natural phenomenon, but a historical and political one, and as such, is subject to influence by social and political entities. Among political entities, nation-states are of paramount importance. The US government has been instrumental in the development of the internet since its inception, beginning as a research project of the Department of Defense Agency for Advanced Projects (DARPA). The international community, as well as several supranational organizations, are also interested in the internet's regulation and use. Recently, for very solid political and strategic reasons, NATO declared cyberspace an autonomous warfare domain, endorsing a position not universally shared among scholars. Since the internet's opening to commercial entities in the 1990s, private sector actors, ranging from network operators to service providers, have achieved a prominent position in the regulation debate itself—a borderless cyberspace that offers advantages to internet companies, but that would invariably put them into conflict with sovereign states. On the other side of the spectrum, individual citizens (e.g., operators, content providers, citizens, experts, journalists, or simply users) would form their own perception of what cyberspace is now and how (and if) it should be governed and regulated.

History

The conceptions of cyberspace cannot be properly understood without a solid understanding of its historical background. It should not sound strange studying a "history" that is only decades old; rather, the rapid rate of change and developments in the cyber realm makes looking back not only possible, but necessary to begin the debate on solid grounds.

The sudden and widespread diffusion of the internet was the result of a series of converging political and technical factors. It is likely that none of the actors involved predicted exactly what would happen and how

disruptive an innovation the internet was going to be. In a short period, the internet transitioned from being a mostly academic and military network, connecting tens of sites and usable only via command line interfaces, to a world-wide resource accessed by millions of people using a point-and-click interface—the web browser.

Voice telecommunications in the 1970s and 1980s were a world apart from the data networking world, involving computer-to-computer data exchange and communications. Telecommunications companies (Telcos) operating in this market enjoyed monopolistic or quasi-monopolistic dominant positions in their markets and the stable cash-flow that went with them. In the United States, however, with its tradition of anti-trust legislation dating to the nineteenth century, an ongoing process of deregulation and competition took place that included breaking existing monopolies and companies, with AT&T being a prominent example. The direct effect of this process was a push for innovation in the infrastructure. In addition to the liberalization of the telecommunication market, which enabled the United States to expand, to some extent, to the rest of the developed world, the other important policy was the decision by the US Federal Communications Commission to reclassify "data processing"—machine-to-machine digital communications—as a "value-added" enhanced service in contrast to the basic voice services.[1] The consequence was the creation of an unregulated and open market for digital services, even beyond trade barriers.[2] At the time, information services made up a tiny fraction of telecommunication companies' revenues, allowing this market to remain non-regulated. This was probably seen as a small price to pay compared to voice-services. Those policies paved the way for a global digital information network of networks.

Alongside high-level policies, several technical aspects contributed to the explosion of the internet to include the way data communication is managed on the internet. The network was based on packet-switching technology, allowing two nodes to exchange information without having to establish a fixed, or even predetermined path between them. The data is divided into small-size "packets" and transmitted separately, possibly even on different paths, and in a different order than the original one. The whole is rebuilt at the destination by the networking software. This is in sharp

1 Milton L. Mueller, *Network and States* (Cambridge: MIT Press, 2010).

2 Ibid.

contrast to the circuit-switched technology of the telephone networks, where a dedicated "circuit"—or path—is established each time a communication is initiated between two nodes. The packet-switching architecture allowed for decentralized management because the routing decisions about packets could be made at the local level without the need for detailed information on the network. This was coupled with the fact that the particular communication protocols used at the time—the TCP/IP suite—were standardized and public, an engineering design choice made decades before the rapid growth of the internet by allowing whole pre-existing networks to be added. In fact, until then, the word "internet" meant just that; the interconnection of two or more computer networks (later it acquired the capital "I" and became the Internet). Also among the technical contributions, the maturation of the free software movement facilitated the availability of several robust elements, which—also for economic reasons—contributed to the building of many internet companies and servers; GNU/Linux and the apache web server are two prominent examples. Not to be underestimated is also the introduction of the xDSL technologies, which brought relatively high bandwidth connections to the public.

The Tension of Governance

The debate on governance has polarized around two opposite views. On one hand, there is the view that— as an entity—cyberspace is completely separated from the "physical" world, where information flows freely and neither distance nor ordinary law is binding. The opposing view is that each nation is responsible for its sovereign piece of the global internet and is justified in implementing any legal mechanisms in place to ensure the security of online activities traversing its network space. To date, there is neither consensus nor compromise on these opposing factions, leaving the status quo for the time being; nevertheless, how the internet should be governed remains hotly contested.

According to the hypothesis that cyberspace stands apart from the physical world, nation states would not and could not regulate anything that happened on the internet, meaning that cyberspace is not subject to "ordinary" laws, sovereignty, or borders. This sentiment is articulated memorably by John Perry Barlow, who states, "Governments of the Industrial world, you weary giants […], I come from Cyberspace, the new home of Mind […], You have

no sovereignty where we gather."[3] Supporting this view, the technical traits of the internet are what gives the system its independence from the physical world and the sovereignty of nation states: decentralization (thanks to IP protocols) and the easily transportable nature of information. The infrastructure allows and favors the birth and growth of network organizations composed of peers and relationships completely independent of physical locations, jurisdictions, and borders. In these social constructs—be they civil society groups, special interest clubs, or social networks—the internal organization of the peers depends only on the information's flow. The basic tenet of what can be called "cyber libertarianism" is that there is no need for sovereign regulations and laws in cyberspace. Unfortunately, the power of networked organizations can also be used to establish criminal or terrorist groups who leverage the relative anonymity that cyberspace permits. The transnational nature of these groups enables members to function cohesively, despite operating from different geographical locations and jurisdictions.

The second viewpoint concerns state sovereignty in cyberspace. This argument contends that not only should the technological components of the internet be subject to state authority, but also the information that originates, crosses through, or enters its sovereign digital space. The potential for creating and maintaining transnational social networks with ease, flexibility, and relative anonymity has been seen as a threat both to state sovereignty as well as national security itself. This perception has increased since the beginning of this century, given the ongoing confrontation with organized terrorist networks; terrorism in Europe and America, however, is not the only powerful motivation behind the sovereign position. The social movements that led to the "Color Revolutions" and "Arab Spring" are indicative of what can happen if information goes unchecked. Moreover, nation-states have demonstrated a natural tendency to maintain and extend the limits of their power; cyberspace—with its potential as a channel for communications and warfare—is a natural extension of state power. Indeed, the control of financial fluxes and even currency policy is a trait of sovereignty under attack. Opponents of sovereignty see it as a legitimizing vehicle for more authoritarian regimes to increase monitoring and control of their citizens.

3 John Perry Barlow, "A Declaration of the Independence of Cyberspace," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge: MIT Press, 2001).

Dissidents and political oppositionists have often been the target of strict internal monitoring, and the West's perceived existential threat of terrorism has been the raison d'être of the surveillance state. Semi-democratic or autocratic states do not even need that kind of justification for imposing borders.

The tension between the two viewpoints informed the whole debate about "internet governance" in the 1990s, and especially since the beginning of the twenty-first century. Formally, it led to two governance models: one in which cyberspace is perceived as another international regime to be regulated by inter-state treaties and organizations— the International Telecommunication Union (ITU) is a prominent example—and the other advocating a network governance model (multi-stakeholder is the preferred term in official EU parlance). A governance network, formed by both government and non-governmental actors, is widely held to be the most appropriate for the internet and is actually the way that cyberspace currently works.[4] The vision of cyberspace as a global common is attractive but misleading: the cyber domain is entirely artificial and no part of it exists outside of some sovereignty (even deep-sea cables fall under a whole body of regulations and treaties dating back to the nineteenth century).[5]

Underscoring this tension is the fact that the network governance model was already in place when states began to realize the potential of cyberspace and to reestablish traditional sovereignty. The Internet Corporation for Assigned Names and Numbers (ICANN) and the decentralized management of the Domain Name System (DNS) are striking examples. Decentralized governance made the internet incredibly successful at various levels, and it is hard to argue to the contrary.

State of the Art

Well into the twenty-first century, nation-states have been gaining control over cyberspace. This policy view is widespread outside Western countries where internet and cyberspace are perceived to be dominated by the "cyber hegemony" of the United States. Admonishing cyber hegemony may be a propaganda tool for China, but the United States and its close allies—especially

4 Mueller, *Network and States*, ch. 3, p. 31.

5 Alessandro Guarino, "Cyberspace Does Not Exist," *Strange Loops,* January 15, 2015, http://www.studioag.pro/en/2015/01/la-nuvola-non-esiste/.

their security agencies—have consistently held a quasi "neocolonial" attitude towards cyberspace. Patent examples include the development and deployment of cyber weapons: the effects of Stuxnet; the attack on the Belgian telecom company, Belgacom by British intelligence; the claim to worldwide validity of US laws and the disregarding of other jurisdictions; and the injunction requiring Microsoft to relinquish data stored in one of its data centers in Ireland. Viewed from this perspective, liberal democratic state practices do not appear different from those of less democratic countries. Moreover, sometimes they can be contradictory; for instance, attempts to create a "Digital Single Market" without borders inside the European Union go hand-in-hand with the creation and enforcement of external borders, in order to avoid perceived or real dumping practices by companies outside the European Union, e.g., tax evasion.

Imposing Borders

State policies and actions aimed at establishing and enforcing borders in cyberspace can meaningfully be classified by considering two variables. The first variable considers whether an action is "overt" or "covert." The use of the term "covert" here is somewhat loose, comprising in a strict sense the meaning of both "covert" and "clandestine"; where the first terms implies concealing the source, the second does not. The second intersecting variable considers whether policies are technical in nature or not; that is, legislative or political. The policy of overt non-technical state efforts is an attempt to bring internet governance back under state control, directly or through inter-governmental organizations. Other overt actions are those deriving from the physical nature of cyberspace. All network devices (servers, routers, cable backbones, satellite stations) are located in the sovereign territory of a nation-state and are subject to its laws, or well-developed international law in the case of transoceanic submarine cables. While it is difficult to monitor and control data flow, laws and regulations can be created and enforced on the physical side of the "cloud." Overt political actions can also enable overt technical actions, by supplying them with legal justification (at least for the country in question). China's so-called "Great Firewall" is a clear example. Policy decisions created a whole arsenal of technical measures bent on reestablishing China's sovereignty over its "national" portion of cyberspace. These range from deep packet inspection and packet filtering

of the perimeter routers, to the blocking and blacklisting of websites, to the manipulation of the DNS inside China, as well as many others. Simply, control is easy at the physical level, but more difficult at a slightly higher level, such as with the TCP/IP protocol and routing. Contrary to a physical cable, packet-switching technology makes it hard to control its path (e.g., which national territories it crosses). The covert side of an ideal matrix classification comprises the technical level where states race to militarize global networks in an effort to gain the virtual "high ground" in order to steal information in the classic style of espionage and to be prepared for a futuristic "cyberwar." Readiness also means being able to defend the critical networks of a nation against intrusions. Examples of covert, non-technical measures are the monitoring of content on social networks and elsewhere online by intelligence and security agencies. Generally, covert policy decisions of the interested government enable the control of the information flow by internal security agencies. Another relevant example of covert, non-technical means is the "moral suasion" exerted by governments on private Internet Service Providers (ISPs) and other network operators in order to ensure their collaboration in controlling the information flow (for instance by installing government-operated interception equipment on their premises).[6]

Evading Borders

States have several motivations for wanting cyberspace to either remain unobstructed and unhindered, or to restrict it with more control, oversight, and monitoring. States may naturally seek to evade borders whether seeking to promote commerce, communication, steal secrets, or disrupt systems. The legal environment, or lack thereof, is one key way for states to maintain the status quo.

Countries currently are working to define acceptable behavior in cyberspace. For example, the recent 2015 G-20 meeting resulted in senior-level representatives pledging not to engage in cyber economic espionage in support of their respective commercial interests.[7] Yet despite promising platitudes, cyber espionage remains an attractive means of engaging in information theft and in the surveillance of friends and foes alike. The

6 James Bamford, *The Puzzle Palace* (New York: Penguin, 1982), pp. 302–305.

7 Emilio Iasiello, "G20 - No Commercial Hacking by Anyone," *Dead Drop,* January14, 2016, http://deaddrop.threatpool.com/g20-no-commercial-hacking-by-anyone/.

ultimate result from this pact may be that states will need to obfuscate more carefully their activities, rather than cease them altogether. As governments seek to bolster economic ties with one another using cyber as a facilitating agent, the very cyber boundaries that countries like China and Russia want to solidify become increasingly difficult to distinguish. This leaves states in the unenviable position of trying to defend their respective shares of the internet while trying to increase their political and economic ties with global partners.

Technologies Facilitate Border Evasion

There is no accepted global definition of cyberspace. The US Department of Defense defines cyberspace as a "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures."[8] Russia prefers to use the term "information space" instead of cyberspace. The term "information space" is broader and more inclusive than the American term, which focuses on the network architecture and processes that occur in the digital domain. In contrast, Russia identifies information space as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself."[9] Similarly, China views the information space holistically. The Chinese definition of it is as follows: "The main function of the information space is for people to acquire and process data . . . a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases and information, forming a 'landscape' huge, interconnected, with different ethnic and racial characteristics of the interaction, which is a three-dimensional space."[10] Despite their differences, all three definitions refer to the networked aspects of the cyber domain, which is completely

8 US Department of Defense, *Joint Terminology for Cyberspace Operations -Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, and the Directors of the Joint Staff Directorates* (November 2010).

9 Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English" (Tallinn: Fifth International Conference on Cyber Conflict, 2013).

10 Emilio Iasiello, "Are Cyber Weapons Effective Military Tools?" *Military and Strategic Affairs* 7, no. 1 (March 2015): 27–28.

human-made. Such a complex environment is bound to include human error, among other vulnerabilities. Those who helped design this network over subsequent decades focused on the technical challenges of moving information quickly and reliably and did not anticipate that the internet's own users would ultimately use the network to attack one another.

While attack and exploitation efforts do not have to be advanced to be successful, the more proficient actors have demonstrated the ability to script unique tools and exploits against vulnerabilities and maintain persistence and invisibility in their operations. The following are various technical techniques through which actors evade the notional cyber borders of a nation-state:

Encryption: Actors leverage encryption to mask the data that they harvest and exfiltrate. In some instances, they hide it in innocent-looking files (steganography). Other tactics involve compression (reducing the size of files without removing information); chunking (breaking down data into smaller parts so that it better blends into normal traffic); and obfuscation (converting characters to hex code so that data can avoid detection). By encrypting the data, actors make it difficult for the exploited organizations to know what kind of information was stolen, thereby hindering post-breach investigative and recovery response as well as attribution efforts.

Onion Routing: Although there is some debate whether the Onion Router (Tor) is completely anonymous, it remains a popular way through which actors conduct their operations. The strength of Tor rests in the fact that it is theoretically impossible to know which computer requested the traffic, as a computer may have either initiated the connection or may just be acting as a relay to another Tor node. The Tor client picks a random path through Tor nodes to its ultimate destination. In this regard, Tor is a popular tool for users to bypass restrictions and censorship controls in a given country, as much as it is for hostile actors. An incident in 2014 demonstrated that the Tor network was leveraged for exploitation activity: a rogue Tor node was used to launch cyber espionage attacks on European governments.

Pluggable Transports: Pluggable transports disguise Tor traffic to look like traffic from other common services such as HTTPS or Skype, and to look like benign traffic by transforming the Tor traffic flow between the client and the bridge.

Virtual Private Networks (VPNs) and Proxies: VPNs and proxies shield users by encrypting all activity to and from a computer. As long as the

computer remains connected to a VPN, the network operators will not have access to traffic (e.g., sites visited). Similarly, proxies are used as intermediaries between the client and the server, eliminating the need for direct communication between the two parties. They provide some level of enhanced security in protecting the identity of a browsing computer.

The Tribulations of Cyber Diplomacy

The diplomatic environment for cyberspace continues to be a work in progress, a situation that favors hostile activity. The impasse in critical areas has left the legal environment in limbo; states continue to evade borders without any international legal repercussions and struggle to find consensus on definitions and key legal issues—such as cyber warfare and security terminology—while avoiding nation-state responsibilities. The same extends to cyber sovereignty. China, among others, continues to promote its cyber sovereignty as an extension of its natural sovereignty, a right afforded to them under the UN charter. The United States, as well as its allies to some extent, believes that the internet—as an interconnected global platform—should remain open. It must be noted that while this is an official US position, different views and cyber strategies exist within the US government itself, sometimes at odds with each other.

Internet governance is another major area of contention. At present, no single organization influences how the internet expands, which technologies are used, or what rules govern the global network. China and Russia would prefer an international government organization—such as the ITU (part of the UN system)—to oversee and manage all internet activities. In April 2016, India aligned with this position. The debate is important as both sides continue to try to find allies to put their positions at the forefront. The United States—at least officially—prefers a multi-stakeholder approach that includes not just governments, but also the private sector, academia, civil society, and the technical community.[11]

A third legal area that remains in flux concerns the definition of information weapons. In 2011, China and Russia proposed banning the use of all information weapons and related technologies in their initial code of conduct proposal to the UN General Assembly. The subsequent 2015 revision removed the

11 US Department of State Fact Sheet, "Internet Governance," August 2015, https://www.state.gov/documents/organization/255010.pdf.

term, as it implied the potential use of information as a subversive element for inciting civil instability as had occurred during the Arab Spring. The United States has traditionally been opposed to outlawing offensive cyber weapons. The leading Department of State representative for cyber issues does not believe that conventional military or diplomatic treaties can work in cyberspace, preferring the development of "norms" instead.[12] This is at odds with the results of ongoing research by legal scholars at the invitation of the NATO Cooperative Cyber Defense Center of Excellence.[13]

Even among "friendly" nations, finding common legal ground is difficult to achieve. Fundamental differences in the legal underpinnings of privacy between the United States and the European Union led to the repealing of the "Safe Harbor" agreement on data transfer between the two sides. The new "Privacy Shield" framework appears on shaky legal ground as well.

Political Environments

Political environments also contribute to states' evasion of borders. Whether they consciously avoid establishing legislation in their own countries or choose selective enforcement of the law, some governments create a permissive environment that allows for commercial, criminal, disruptive, and other nefarious activities to pass through their spaces. These political environments are not exclusively the purview of specific types of regimes and political systems; rather they depend largely on the interests of the governments that allow them to continue.

Russia's political environment, for example, has shown tolerance to cyber criminals, as well as nationalistic hackers. According to Reporters Without Borders, Russia maintains a robust surveillance apparatus known as SORM. SORM-1 focused on intercepting telephone communications; SORM-2 focused on data transmitted via the internet, and SORM-3 can intercept any form of communication and includes long-term storage. Censorship is

12 Kenneth Corbin, "State Department Argues Against Cyber Arms Treaty," *CIO*, May 26, 2016, http://www.cio.com/article/3075442/government/state-department-argues-against-cyber-arms-treaty.html.

13 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

also routinely enforced.[14] When it comes to cybercrime, Russia's prolific cybercriminals seems to follow two basic rules: 1) Russians do not hack Russians; and 2) If Russian intelligence asks for help, they comply. Russian hackers have gained attention since their 2007 DDoS attacks against Estonia and their 2008 involvement in the Georgia conflict. During these incidents, nationalistic hackers engaged in cyberattacks in defense of Russian culture and nationalism, with some of the attacks originating in or traversing through Russian internet space. More recently, similar activity has occurred in Ukraine where a conflict rages between Ukraine and Russian separatists, and online attacks are frequent.

Unlike Russia, the United States' political environment does not implicitly condone or support the activities of nationalistic actors hacking on behalf of US interests. However, the fact that an American patriotic hacker known as "The Jester" conducts attacks against terrorists and other hacktivists without being investigated and arrested by law enforcement certainly suggests that he has approval to do so. Even more so, the political environment of the United States is one where the highest levels of government condone questionable global surveillance activity, which collects incredible amounts of data not only internationally, but also domestically without citizen knowledge or approval. In this context, the US government evades its own borders, using its robust technical surveillance capability to capture and store information against adversarial nations, friendly nations, as well as its own citizens.

Legal Jurisdiction

While transnational cybercrime affects all countries in the world, many governments still do not have adequate, if any, cybercrime legislation to support criminal investigation and prosecution. Even in those that do, such legislation has not yet proven to deter such activities; for example, the United States has some of the stricter cybercrime laws in the world and an increasingly competent law enforcement element, yet it remains among the leaders in cybercrime activity.

International law enforcement collaboration is spotty at best, a reality that constantly forces law enforcement officials to play catch up with advanced

14 "Russia: Control from the Top Down – FSB (The Federal Security Service of the Russian Federation)," *Reporters Without Borders*, March 11, 2014, https://12mars.rsf.org/2014-en/2014/03/11/russia-repression-from-the-top-down/.

cybercriminal actors. There is no internationally accepted cybercrime legislation, although the Council of Europe Convention on Cyber Crime—the first international treaty seeking to address internet crime—has made great strides in getting governments on board. There are times, however, when cooperation between states is limited or when jurisdictional problems hinder the progress of investigations. The fact remains that not all law enforcement entities are as advanced as their colleagues, and in some cases, one entity may simply refuse to help another.

Currently, only the Convention on Cyber Crime appears positioned to help address border evasion issues from a collaborative perspective, rather than by relying on case-by-case, state-by-state bilateral legal agreements. Signatories under the Convention agree to adopt laws outlawing specific types of cybercrime and to take appropriate legal action as required to ensure law enforcement cooperation. As of March 2016, forty-eight states have ratified the convention, while a further six states had signed the convention but not ratified it. China and Russia are noticeably absent on this list.

China: A Case Study

Beijing first introduced its views on internet sovereignty in a 2010 White Paper entitled "The Internet in China."[15] The intimation was clear: Beijing sought to establish as clear lines of sovereignty in cyberspace as there were for land, sea, and air. Building on this at the 2015 World Internet Conference hosted in Wuzhen, senior Chinese government and business officials, as well as government officials from Kazakhstan, Kyrgyzstan, Pakistan, and Russia, met to discuss internet issues. In his opening remarks at the conference, President Xi Jinping highlighted the need for governments to respect the rights of individual countries in developing a cyber governing path for its own citizens.[16] This plays an important role supporting China's security concerns, which focus on keeping the Communist Party in power, protecting China's territorial interests, and preserving internal stability. In a time when

15 Shannon Tiezzi, "China's Sovereign Internet," *Diplomat*, June 24, 2014, thediplomat.com/2014/06/chinas-sovereign-internet/.

16 "China Allows No Compromise on Cyberspace Sovereignty," *China Daily*, December 17, 2015, http://www.chinadaily.com.cn/world/2015wic/2015-12/17/content_22735756.htm.

the internet connects all facets of society, China sees cyber sovereignty as a critical component to national sovereignty.[17]

Beijing views cyber sovereignty not only as a way of further securing its interests, but also as an important means of countering "cyber hegemonic" activities that seek to undermine the country's national security. Chinese authors have written about US attempts to control the global internet, a fear reinforced by Snowden's revelations in 2013 of global surveillance. The "absolute freedom" of cyberspace as championed by the United States is viewed as beneficial to it and its national security, while it creates insecurity for the rest of the world.

To promote cyber sovereignty, China has been leveraging the UN Charter as justification to extend the principle of sovereign equality to cyberspace. This achieves two important objectives for Beijing: it demonstrates China's intent on using existing applicable international law to support its proposal, and it shows China's desire to raise such issues to a government level and in an international forum. Leveraging the legal angle lends legitimacy to China's proposal. Using the United Nations as a venue demonstrates China's commitment to multilateral action. In December 2015, China successfully fought to include the word "multilateral" in a document created by the United Nations that would direct the policies of the internet in the future. The importance of this addition was to show that governments—and not civil groups or organizations—should be the ones responsible for framing the rules. While this is non-binding for member states, it does provide the necessary counterbalance to previously established and accepted guidance.

China is not moving forward alone, but is promoting cyber sovereignty in various international forums, such as the Brazil, Russia, India, China, and South Africa (BRICS) Consortium, the Shanghai Cooperative Organization, and the UN Group of Governmental Experts, to name a few.

Notably, Beijing has engaged in strengthening the protection of its core national security interests through a series of laws and draft legislation. Examples of this trend include:

17 "Why Does Cyber Sovereignty Matter?" *China Daily*, December 16, 2015, http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm.

2016 Cyber Security Law: In November 2016, the Chinese government approved its "Cyber Security Law."[18] The law addresses the security of key internet and information systems, while it increases the government's powers to record and impede the dissemination of information deemed "illegal." Two key reoccurring themes are stressed: 1) the ability to monitor and control information; and 2) compliance of foreign enterprises with the rules set forth. Critics have cited this law as being a government attempt to tighten its control on civil society while making unreasonable demands on foreign businesses.[19]

2016 Overseas Non-Government Organization Management Law: All NGOs are required to get approval from a supervisory unit to operate in China. It further prohibits any Chinese organization from conducting activities on behalf of or with non-authorized NGOs. While the law is not specifically cyber related, it is safe to assume that NGOs properly registering with Chinese authorities would be required to comply with any acceptable technology use policies set forth by the Chinese government in other legislation.

2015 National Security Law: This law provides a framework for China's security considerations in the face of emerging threats. Overlapping security considerations demonstrates Beijing's perspective that national security is an inherently integrated process, creating "a national security path with Chinese characteristics."[20] Perhaps most notably, however, is that the law is not restrictive to China's borders, and it includes the polar beds, outer space, and cyberspace.

2015 Anti-Terror Law: Passed in December 2015, it compels technology companies to help decrypt information, giving Chinese authorities access to encrypted data. The law combines administrative, judicial, and military means to address Chinese anti-terrorism efforts, demonstrating a comprehensiveness that reflects Beijing's desire to integrate all facets of security under the

18 "China Passes New National Security Law Extending Control Over the Internet," *Guardian*, July 1, 2015, http://www.theguardian.com/world/2015/jul/01/china-national-security-law-internet-regulation-cyberspace-xi-jinping.

19 Bethany Allen-Ebrahimian, "The Chilling Effect of China's New Cybersecurity Regime," *Foreign Policy*, July 10, 2015, http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/.

20 "China Focus: China Defines Overall National Security Outlook in Draft Law," *Xinhuanet*, April 20, 2015, http://news.xinhuanet.com/english/2015-04/20/c_134166428.htm.

umbrella of its new national security law. This idea resonates with the recent push by US security agencies to weaken encryption systems to allow government access.[21]

While these efforts can be viewed as Beijing's attempt to gain greater resiliency in the face of external influences and to reduce potential economic and/or diplomatic liabilities imposed by the United States (e.g., cyber sanctions, economic sanctions, indictments, and so forth), such measures further reinforce China's position that governments have the right to manage their own internal cyber affairs. Indeed, many of these laws have been criticized for promoting economic self-interests and the tightening of controls, despite Beijing's insistence that they all are well in accordance with UN charter dictates.

Conclusions

The internet governance debate presently remains a contested issue among nation-states. As a result, the so-called "Balkanization" of cyberspace is already happening, spurred on by a combination of national security interests, perceived threats, and economic warfare in the Western world and by the desire of states to control and monitor public opinion and political discourse. Imposing borders, however, would ultimately lead to the loss of huge opportunities in terms of economic development, the free flow of information, and online freedoms. While it is true that the somewhat naive vision of cyberspace embodied in Barlow's "Declaration of Independence" was never actually realized, it is imperative now to find a balance between sovereignty and globalization, as well as between national security and freedom.

It is incumbent on liberal democracies and on the seemingly hegemonic United States to lead the effort in finding such a consensus. It is unrealistic to minimize governments' involvement in this process as much as it is to solely empower them to find resolutions that could lead to a loss of accountability. Therefore, a multilateral agreement—based upon the successful guidance set forth by the regulation of global commons models such as banning military activities in space, ensuring the freedom of navigation on the open seas, and prohibiting sovereign claims on Antarctica—could very well provide the

21 Joseph Lorenzo Hall, "Issue Brief: A Backdoor to Encryption for Government Surveillance," *CDT*, March 3, 2016, https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/.

Cyber, Intelligence, and Security | Volume 1 | No. 2 | June 2017

most viable solution. Building a long-term, networked governance in the context of which both nation-states and non-state parties can work together seems the only mutually beneficial way for governments to reap the benefits of cyberspace without endangering their respective security interests.