SSOAR

Open Access Repository
www.ssoar.info

Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet?

Masoumifar, Ali M.

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Masoumifar, A. M. (2022). Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet? *Journal of Cyberspace Studies*, *6*(1), 1-20. https://doi.org/10.22059/jcss.2022.327215.1064

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY-ND Lizenz (Namensnennung-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by-nd/4.0/deed.de

Terms of use:
This document is made available under a CC BY-ND Licence (Attribution-NoDerivatives). For more Information see:
https://creativecommons.org/licenses/by-nd/4.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

Original Article

Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet?

Ali M. Masoumifar

(Received 14 July 2021; accepted 28 December 2021)

Abstract

The internet is at a crossroads today. Whence once viewed as a borderless domain, today it is spoken of in alarmist terms that warn against its demise in the context of growing government censorship programs and powerful commercial interests. This essay reviews the literature on cyberspace and sovereignty, showing the emergence of pro-sovereigntist perspectives and predictions of cyberspace Balkanization in recent decades. It further links the conceptual debate over cyber-sovereignty to real-world geopolitical conflicts and struggles over the future of Internet governance, showing how different conceptions of cyberspace are functions of the geopolitical interests of different powers. Drawing on recent literature on cyber espionage, this essay provides a review of the defensive and offensive practices of state powers in and through cyberspace to argue that while impulses towards re-territorialization of cyberspace are undeniable, such attempts are ultimately frustrated by operations aiming to use common protocols for external security and internal surveillance. Such practices illustrate a more nuanced depiction of sovereignty in cyberspace that goes beyond the borderless versus Balkanized dichotomy.

Keywords: cyber-sovereignty, internet diplomacy, internet governance, political economy, territoriality.

Ali M. Masoumifar; MSc, The London School of Economics and Political Science (LSE), London, England | Email: ali.masoumifar@gmail.com

This is an open access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (CC BY NC), which permits distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

Introduction

In recent years data has increasingly developed social and political dimensions because of its potential to rearrange relationships between governments and individuals. Data and politics have now become intimately attached: data is not only shaping the social fabric of our societies but our very political systems (Hamanaka, 2020), democracies (Anderson & Rainie, 2020), and international affairs (Sanger et al., 2020). Early commentary on the emergence of the Internet presumed that it would significantly challenge the power of states and pose a specific threat to the capacity of states to exert control in authoritarian contexts (Johnson & Post, 1996). However, more recently the discourse has shifted to emphasize the opposite: that in fact, data contains the potential to increase the capacity of states to project power both within and without political borders (Farmanfarmaian & Mens, 2021; Zeng, 2016). Communications literature has established the empowering role of social media on the user and his transformed status from the passive consumer in the age of traditional mass media to his socio-politically influential position today (Sabbar & Matheson, 2019). While we now clearly see how digital connectivity and social media have empowered citizens to engage in civil action within societies (Maghbool, 2020), views about the effect they will ultimately have on the sovereign authority of states are much further from consensus.

Recent geopolitical tensions and calls for cyberspace sovereignty have made many wonder whether the Internet as we know it is in danger of breaking apart (Hill, 2012; Malcomson, 2016; Mueller, 2017; Silverberg, 2019). Some believe that governance on the Internet is a "post-state" issue and can ultimately only be addressed through a multi-stakeholder model of global Internet governance based on a global commons conceptualization (Mueller, 2020). Supporters of this view argue that the advent of the Internet challenges fundamental presumptions of territorial sovereignty as a stable basis for international organization and posit that applying any concept of sovereignty to governance on cyberspace is inappropriate to the domain.

Over the past few decades, however, a growing number of academics and journalist have questioned the legitimacy of the extra-territorial conception of the Internet and argued that government censorship programs, concerns over cybersecurity, influential commercial interests, and a host of dynamic changes in the ecosystem of the Internet are pulling the World Wide Web down to the entanglement of states, laws, and cultures and breaking up the global network into various separate "Internets" (or Splinternet). A process that has been described as the Balkanization of the Internet (Sagawa, 1997). They believe that this trajectory of increasing ambitions for territorialization is threatening the globally unified web and

the economic prosperity and innovation that the Internet has nurtured in the past three decades (Demchak, 2016; Demchak & Dombrowski, 2011; Hill, 2012; Malcomson, 2016; Meinrath, 2013; Mueller, 2017). This debate on cyberspace echo's a broader discursive tension between proponents of localization and globalization (Sabbar & Dalvand, 2018).

This article argues that while the attempts aimed at the re-territorialization of the Internet are undeniable, the mechanism by which the relationship between state control and the Internet's global compatibility is regulated closely responds to the interests of states to exercise mutual self-restraint. Extraterritorial projections of power in cyberspace are increasing in both quantity and sophistication. However, even the most autocratic states often connected to efforts to stimulate Internet sovereignty today depend on the openness of cyberspace. States are practicing power exertions beyond their political borders to obtain data about their surroundings: to forecast, examine, protect themselves from threats; to form the strategic landscape to their advantage; to advance their interests through the flow of information, capital, and goods and services. They are also using the affordances of new networked ICTs to broaden the reach of military systems. The collective, possibly unintended, network effect of such wide-ranging applications of power within and through cyberspace is to thwart singular strategies directed at territorial insularity. In other words, the faculty of states to apply power internally and abroad relies on the material potentials afforded by cyberspace, and that structural openness frustrates attempts to build impassable borders.

This article's argument is developed in four steps. First, a literature review is presented which provides an overview of discussions on cyberspace and sovereignty since the 1990s, pointing to the emergence of pro-sovereigntist arguments and predictions of a retreat to Cyber Westphalia and Internet Balkanization. The section that follows will clarify how states exert power over cyberspace in order to clarify the grounds on which a closer investigation into the legitimacy of claims reviewed in the first section will be developed. The third section looks at the role of the United States in the transformation of cyberspace and critically evaluates US advocacy of an open Internet. Finally, the fourth section looks at the paradox between the rhetoric and the practice of states that advocate for cyber sovereignty.

Literature Review

Cyberspace as a Post-state Realm. The internet was initially believed to be a borderless realm and its network architecture seen as opposed to state sovereignty and territoriality, promising an exceptional realm free from

the constraints of the legacies of soil and state (Wall, 1997). In the early days of scholarly work on cyber-sovereignty, the conversation revolved around a shared understanding that cyberspace presented a challenge to the application of traditional forms of state power and sovereignty (Hardy, 1993; Johnson & Post, 1996). In addition to cyberspace, terms such as the information superhighway were used that to communicate a lack of borders in this domain. In this view, it was argued that with the advent of the internet there would no longer be any divides that would hinder access to information (Ohmae, 1991).

These authors questioned the feasibility and legitimacy of the application of laws based on geographic boundaries to cyberspace (Barlow, 2019; Johnson & Post, 1996). Though met with some pushback by conservative legal scholars at the time that labeled such claims as "internet exceptionalism" and "cyber anarchy" (Goldsmith, 1998), this vision of exceptionalism set the tone for cyber-sovereignty discourse for a decade. The creation of the Internet Corporation for Assigned Names and Numbers (ICANN), a non-state transnational regulatory body, echoed this vision (Klein, 2002). The US government embraced a multi-stakeholder and bottom-up governance mechanism and deemed the regulatory frameworks established for telecommunications as inappropriate for the domain of cyberspace (Froomkin, 2000). Consequently, an independent cyberspace developed governed by transnational institutions ran by non-state actors.

Advocates of Sovereignty and the Cyber Westphalia Thesis. In the following decades, the libertarian optimism of early commentary on cyberspace gave its place to a vision of cyber sovereignty whereby it was argued that there should be a natural extension of national sovereignty onto the network environment. Responding to concerns over cybersecurity, the inherent conflict of multi-stakeholder internet governance with the notion of sovereignty as a foundational principle of international organization, the need for order on cyberspace, and enhanced national control over communications, scholars and state actors started to advocate for the need to territorialize cyberspace.

In the early 2000s, states began to take notice of the inherent conflict between the internet's multi-stakeholder governance regime and national sovereignty as a basic principle of international organization. At the United Nations' World Summit on the Information Society (WSIS) between 2002 and 2005, strong objections to ICANN's decision-making authority as a private entity and the special influence of the United States over ICANN from many states clashed with transnational civil activists' demands of multi-stakeholder global governance (Mueller, 2010). Countries such as Iran, China, and Belarus began efforts to control information flows across

borders through Internet filtering (Chadwick & Howard, 2010). With the increasing social significance of cyberspace, military rivalries began to be extended over to the domain. Scholarship documenting how states are engaged in exterritorial projections of state power through cyberspace began to emerge (Czosseck & Geers, 2009).

In response to perceived threats of attacks in cyberspace, scholars associated with security and military studies began advocating for the establishment of cyberspace borders, over which states can exercise monitoring and control, warning that a failure to extend sovereign control over cyberspace would have damaging repercussions for security (Franzese, 2009; Lewis, 2009). Some scholars argued that a new age of cybered Westphalia is emerging (Demchak & Dombrowski, 2011). The term "cyber-Westphalia" refers to the reverting of cyberspace to a Westphalian model whereby order is maintained based on mutually recognized territories subject to the supreme authority of states. Such scholarship that advocates for the establishment of sovereignty on cyberspace is critical of libertarian ideals of Internet freedom and views a global governance model of cyberspace as idealized, security-blind notions born out of a Western mentality's hubris (Demchak, 2016). The underlying logic behind much of the Westphalian or pro-sovereignty arguments is the argument that since every piece of the physical infrastructure of the net is placed within some sovereign territory, control over that physical infrastructure would serve as the basis for an arrangement whereby states are both enabled and constrained in their exercise of sovereignty over various activities in cyberspace (Betz, 2017; Heinegg, 2012).

Predictions of Internet Fragmentation (Rise of the Splinternet). With the growing tendencies of states to view the Internet as an extension of national territory and a space to be regulated and shaped by state authority, coupled with the rise of legal and technical instruments used to implement practices of Internet shutdowns, and Internet filtering, predictions of the Internet being in danger of balkanization (Mueller, 2017) gained traction in academic literature ranging from the works of authors in the field of Internet governance to international relations (Hill, 2012; Kuner et al., 2015; Meinrath, 2013).

Such scholarship defines cyberspace as a space of interaction that relies on the foundation of the joint use of compatible data transfer protocols, computer languages, and message formats collectively referred to as Internet standards (Hill, 2012; Mueller, 2020). As such this view privileges the non-proprietary software of Internet Protocol at layer three and UDP or TCP at layer four over the physical components of the network architecture in defining what constitutes cyberspace as we know it. Consequently, they

argue that if national sovereignty gains more importance for states than global compatibility and if frustrations with the current way standards are being designed by the Internet Engineering Task Force (IETF) mount to a sufficient level, the uniform technical standards that are the basis of the Internet could be put aside in favor of distinct national standards for data communication protocols, operating systems, and applications and lead to the disintegration of the Internet (Hill, 2012).

This withdrawal would constitute a severing of the Internet at its core. In addition to this technical disintegration, this body of research warns that the implementation of the idea of sovereignty over cyberspace would fragment the services offered on the Internet, undercutting the permissionless innovation (Thierer, 2016), competition, and free trade that has been a positive consequence of the use of open Internet standards up to this point (Mueller, 2020). Proponents of the balkanization prediction argue that such fragmentation would transform the future of the Internet from a global commons to a fractured network that is limited by political boundaries (Malcomson, 2016).

Predictions of balkanization are nothing new. Although the focus of the discourse has shifted, anxieties around fragmentation and the end of the "free and open" Internet could be traced back to as early as the nighties. In earlier iterations, the reluctance of service providers to peer with each other was the drive behind the concern (Frieden, 1998; Sagawa, 1997). In later years, the focus adopted a geopolitical tone and argued that the practices of states that are considered adversaries of the United States, such as Russia and China, are responsible for the fragmentation of the Internet (Earle & Madek, 2002; Kuner et al., 2015).

However, the Internet was never completely cohesive and radically free. It has always been separate networks that are connected to one another through links. Filtering has always been embedded within the architecture at the network level of the Internet for security and efficiency reasons. It has always been governed by strict controls over data requests (Mueller, 2020). The vision of the free flow of information has always been somewhat of a myth. The following section will clarify how states exert power over cyberspace as a logically necessary step in any attempt to analyze how such practices could affect the global compatibility of the Internet.

State Power on Cyberspace

In his review of the methods employed by states, in particular authoritarian regimes, to shape the strategic landscape of cyberspace to their advantage, Ronald Deibert (2015) has theorized state power over cyberspace within

the borders of political territories in generational terms. He argues that information controls have evolved over three generations.

The first-generation controls have a defensive nature. These controls attempt to create cyber-barriers that could limit the access of citizens subject to the authority of the state to information originating in other jurisdictions. A typical example of such controls is the Great Firewall of China (Griffiths, 2019). In this method, keywords and URLs are filtered to control what computer users within a territory can get access to on the Internet (Deibert, 2015). Though China's firewall is an exceptionally sophisticated form of such systems, first-generational controls and some form of Internet filtering are commonly observed even in democratic countries (Ibid). We can expect that such controls will be expanding as more and more countries begin to censor content online in response to concerns over child pornography, hate speech, and terrorist threats (Akdeniz, 2001; Bowman & Bowman, 2016; Meserve & Pemstein, 2020). Generally, first-generation controls are crude and cases of vast errors and inconsistencies are not in short supply (Dalek et al., 2012; Haselton, 2014).

Second-generation controls are limitations implemented on the free flow of information through domestic regulations and policies often exerted states vicariously through Internet companies. They seek to deepen the reach of the state internally. For Deibert this form of control is most closely associated with limitations placed on privately-owned networks and companies through coercion and policing that is done in authoritarian countries often with the purpose of surveillance and censorship or the application of laws regarding defamation, libel, terrorism, and treason on questionable grounds to Internet content as a means to control the cyber-landscape (Deibert, 2015). Examples of this include Turkey's cybercrime law that will allow the state to extend surveillance and censor websites without court approval, or incidents in Egypt, Ethiopia, and Saudi Arabia where bloggers were arrested for the content they published online (Ibid).

More sophisticated versions of this form of control are hidden functions of surveillance and censorship placed in popular applications such as those embedded within Baidu (Knockel et al., 2016). Another example is Russia's requirement that telecommunication companies active in the country must comply with SORM, a surveillance system that sends copies of all communication to security authorities (Deibert, 2015).

One could argue that data localization initiatives motivated by privacy concerns such as Europe's General Data Protection Regulation (GDPR) could also be counted as an instance of second-generation information controls as they seek to govern when and where data can be transferred into other jurisdictions by means of domestic laws and regulation and thus

extending some degree of information control onto society, particularly as the strain of implementation is placed on private enterprise to placate the state's demands in this regard. In addition to being a response to the privacy concerns of citizens, these data localization trends insisting on tighter restrictions for the transnational processing of certain types of data can also be seen as a response to revelations such as the Edward Snowden disclosures that showed the technical possibility of extensive surveillance networks. As such, initiatives such as GDPR can be seen as a second-generational response to third-generation control exerted by foreign government.

Third-generational controls are of an offensive nature and the most relevant form of power projection for the purposes of this essay. These controls include targeted espionage, surveillance, and other hidden government interferences in cyberspace that are directed outwards. An example of this is Chinese cyberespionage campaigns against pro-democracy and independence movements outside of China as evidence by a four-year comparative study that investigated this phenomenon at the Citizen Lab at the University of Toronto (Deibert, 2015). Another example is what is referred to as the Great Cannon, a Chinese tool that is capable of redirecting the webpage requests of users outside of China to respond with a denial-of-service attack or malware (Marczak et al., 2015b; Pellegrino et al., 2015). Many other countries are now seeking to utilize such capabilities for similar external operations and this growing demand has created a market for ready-made espionage tools offered by private businesses such as the Gamma Group in the United Kingdom and Hacking Team in Italy are responding to this demand (Marquis-Boire et al., 2013).

A fourth generation of control can be added to the three proposed by Deibert: an effort to influence the narrative of Internet governance at the regional and international level (Deibert & Pauly, 2019). This form of power is one achieved through diplomatic means where groups of likeminded nations attempt to negotiate governance agreement in a struggle for determining the future of Internet governance.

In this struggle NATO and the US push for a multi-stakeholder model (Carr, 2015) while Russia and China are advocating for a greater role for national governments (Nocetti, 2015). In the aftermath of the Estonia attacks (Herzog, 2011) NATO formed the Cooperative Cyber Defense Center of Excellence (CCDOE) in Tallinn, Estonia (Mueller, 2020). Experts of international law where employed to convene a group with an agenda to extend the laws of armed conflict to the domain of cyberspace. The results of this endeavor were expressed through the Tallin Manual (Schmidt, 2012; Schmitt, 2013). The motive was to produce fitting mechanisms to respond

to cyberattacks initiated by adversary yet weaker states by military means. Both China and Russia rejected the Tallin Manual and opposed what they viewed as the militarization of cyberspace (Huang & Mačák, 2017).

While they are disputing such interpretations on the application of international law, both Russia and China are pursuing their own international policy initiatives on cyber-governance from an approach that gives privilege to sovereign states as the primary governing entities. As a counterpart to the multi-stakeholder UN Internet Governance Forum, China has initiated the World Internet Conference in Wuzhen (Xinbao, 2017). Russia has taken measures in the same direction. Russia views the multi-stakeholder governance model as a US-led hegemonic framework. During proceeding to revise the International Telecommunication Union's (ITU) International Telecommunication Regulations, Russia suggested that naming and numbering coordination should be taken over from ICANN and the responsibility should be entrusted to the ITU (Nocetti, 2015).

US Interest and Cyberspace as a Commons

Though the American defense of an open Internet, a multi-stakeholder model of governance, and the conceptualization of cyberspace as a global commons could simply be viewed as a reflection of Western social norms and the ideals and values of liberalism (Hill, 2012) this agenda is arguably much more a function of US interests than values. One can better understand this point by reviewing the history of the transformation of telecommunication and information regulation from a sovereignty-based approach during the Post, Telephone, and Telegraph (PTT) monopolies of the nineteenth century to a decentralized model in the age of the Internet. PTT monopolies were owned by the state and controlled the infrastructure of electronic communications within a country (Noam, 1992).

One wonders: under what circumstances was the Internet allowed to bypass existing regulations so easily? The process began in the mid-1970s and continued through the 1990s. At the time, the United States was dominant in both telecommunication and information and was the starting point for the emergence of the new order (Mueller, 2020). The United States created separate regulatory categories for computer information services so as to free them from the telecommunication monopolies. In addition, the US wanted to enable multinational companies to create private networks and support American companies in entering foreign markets, so it promoted interconnection and competition in telecommunication infrastructures as well. At that time information services were a very small fraction of value compared to voice telephone services and therefore other governments accepted this. With the emergence of the Internet as a new public medium in

the mid-1990s, the United States welcomed and celebrated the way it evaded old controls and led to the leadership of American firms (Mueller, 2020).

The American position on cyberspace is similar to its position on treating outer space and the oceans as a common in that it provides discursive support for the projection of US power in global cyberspace. The free movement of information supports the maintenance of hegemonic power as sustaining dominance depends on the ability to move capabilities, goods, information, and services across cyberspace. The United States has a certain advantage in regard to much of the geopolitics of cyberspace. Most of the leading telecommunication firms that operate the physical infrastructure of the Internet are headquartered in the United States. The software companies, social media companies, and even Internet service providers with the largest market shares are still predominantly American (Deibert & Pauly, 2019). As a result, the American government has more scope to utilize second and third generational controls to exert power over cyberspace as these firms could be enlisted in US intelligence efforts.

The reach of US intelligence agencies into networks physically based outside their territorial jurisdiction by exploiting vulnerabilities through remote access to servers, cables, wireless networks, routers, and Internet Exchange Points (IXPs) has long been established (Lee et al., 2015). Just one example is XKEYSCORE, a system that has been described as the NSA's Google (Ibid) and allows NSA analysts access to vast amounts of private digital communications that are gathered from different access points around the world (Ibid). One could argue that this is not necessarily an exceptional position exclusively held by the United States. As with all arms races, allies are expected to emulate (Deibert & Pauly, 2019). Such projections of extraterritorial power are already partly coordinated through a long-standing alliance referred to as the "Four Eyes" (Pfluke, 2019), a partnership between the intelligence agencies of the United States, United Kingdom, New Zealand, and Australia. These agencies regularly swap intelligence that provide a consist coverage of a significant share of the world's international signals and telecommunications traffic.

Cyber Westphalia and the Practices of Pro-sovereigntist States

Predictions of Internet fragmentation usually revolve around the practices of a select group of authoritarian states where government interference in Internet traffic whether through Internet filtering or complete shutdown has become common (Mueller, 2017). Early predictions that the Internet would limit the ability of states to implement autocratic control (Johnson & Post, 1996) have clearly been proven wrong. Autocratic states have proven to be capable of erecting sophisticated information control systems. In fact,

many of the affordances of the networked world of digital innovation such as biometric databases actually hold tremendous potential to facilitate central control. However, strategies aimed at the re-territorialization of cyberspace ought to be viewed with skepticism.

China is often cited as the quintessential example of states that are advocating for the emergence of the new paradigm of tighter controls and the closure of cyberspace. China implements all three generations of information controls. From the great firewall of China (Griffiths, 2019) that aims to bolster borders around its territories, to the rules and regulations inside China that subject domestic Internet service companies to strict legally-mandated controls (Tai & Fu, 2020). Diplomatically, China has consistently pushed for an agenda to promote a structure of Internet governance that is gives privilege to the principles of sovereignty and non-interference (Xinbao, 2017).

In spite of this, China is engaged in its own practices of the extraterritorial projection of power through cyberspace. The country is engaged in various cyber-espionage campaigns (Lindsay et al., 2015; Magnus, 2011). Apart from espionage campaigns, it also enjoys transnational reach through its software and telecommunication industries. Routers produced by Huawei, a Chinese firm that is currently the largest telecommunications equipment manufacturer, have been found to have backdoors that allow unauthorized access (Doffman, 2019; Neate, 2019). Researchers have documented that many of the applications produced by china have built-in surveillance capabilities (Deibert, 2015). One of such software is the Baidu browser (Knockel et al., 2016). The Baidu browsers software development tool has been used in creating numerous applications that have been downloaded millions of times outside of China (Knockel et al., 2016).

In much the same way that the Snowden revelations exposed how information was being collected from Western companies, the well-established data retention and data sharing practices in Chinese industries could facilitate the collection of data from users and which could then be possibly shared with Chinese state agencies from Baidu's servers exposing users to surveillance by Chinese authorities. Another example of how the globally compatible Internet is harvested to support Chinese extraterritorial projection of power is the so called "Great Cannon" (Marczak, 2015b). This attack tool essentially repurposes a random set of requests for webpages inside China as packets in attacks against website based outside of China. This tool functions at the point where China's networks connect to networks abroad. This is a very good illustration of how transnational flows of information are a necessary component of contemporary forms of digital power projection.

Though Chinese authorities might want to defend their Internet borders, they also pragmatically facilitate the transnational flow of information primarily to encourage economic growth. Transnational partnership such as the one formed between Baidu and CloudFare to create a unified network that would more easily make external websites available to Chinese users might seem counterintuitive to the one dimensional aim of promoting a closed-off Chinese Internet but are perfectly aligned to a broader strategy to promote economic growth (Mozur, 2015). China is attempting to strike a balancing strategy that aims to both harvest the utility of unified digital networks and to countervail the threat of exchanges that could be damaging to the Chinese status quo, such as criticism of one-party rule or pro-separatist ideology (Deibert & Pauly, 2019) and Chinese technology companies are participating in this balancing act.

One study has found that phone numbers registered outside of China are also subject to censorship on WeChat's platform (Ruan et al. 2016). Such extraterritorial projections of power are a serious challenge to the Cyber Westphalia thesis. When countries that are advocates of cyber sovereignty have interests to be engaged in practices of digitally-enabled projection of power outside their jurisdiction, the idea that with the rise of the bargaining power of such nations we are going to witness a trend of cyberspace effectively retreating to a Westphalian model becomes much less credible.

China is not an exceptional case in this sense. We can see a similar digital dilemma (Howard et al., 2011) in other states often regarded as advocates of Cyber Westphalia and pioneering movers in the fragmentation of the Internet. Russia is another example. Under the administration of Vladimir Putin, the country has gradually tightened its controls of information within the Russian territories, major incentive for which was the 2011 anti-government protests in Russia. Today, Russia employs all dimensions of the Cyber Westphalia thesis; data localization laws imposed on foreign platform corporations such as Google and Facebook, a comprehensive internet censorship regime, intimidation and incarceration of independent journalists and bloggers, and mass surveillance apparatus at the architectural level through the installation equipment at telecommunications companies, known as the SORM system (Soldatov & Borogan, 2015).

Much like China, Russia's approach to information controls is not limited to its borders but a part of a larger more elaborate geopolitical strategy that involves state scale cyber espionage, sophisticated propaganda, and disinformation programs, and the promotion of the

implementation of Russian technology in former client states. An instance of the latter is the implementation of the SORM system, a compliance system of mass surveillance, in many members of the Commonwealth of Independent States (CIS) (Lupion, 2021; Soldatov & Borogan, 2013). Russia's "influence operations", wherein Russia utilizes social media to promote discord among adversaries, is another example of the outward facing dimensions of this strategy (Allen & Moore, 2018; Iasiello, 2017). While Russia employs information controls within its territories and promotes a territorially-based cyberspace governance model in the international sphere, to understand Russia's practices as a typical case of Cyber Westphalia is to ignore the extent to which it relies on a globally compatible Internet for its own outward facing digital strategy as well as the balancing act it employs to reap the advantages of international engagement in cyberspace.

Low-tier authoritarian countries that are principal supporters of the Chinese and Russian initiative of cyber-sovereignty are also similarly engaged in a more complex form of sovereignty on cyberspace. Countries such as Saudi Arabia, the UAE, Bahrain, Sudan, and Venezuela are all engaged in information controls domestically and many of them have initiated data localization regulations (Deibert & Pauly, 2019). Yet the practices of governments in the Global South are not limited to the borders of their political jurisdictions either. Telecommunication networks are used by diaspora communities living abroad to send back remittance. The same diasporas organize politically in ways that may pose a challenge to autocratic rule at home. With the rapidly-expanding cyber-security industry (Marczak & Guarnieri, 2014) such states are able to purchase capabilities and digital tools without the need to grow domestic capabilities. This may already be in practice. Researchers have tracked espionage operations against diaspora communities to a number of authoritarian regimes in the Global South (Marczak et al., 2014; Marczak et al., 2015a).

Conclusion

States around the world are shaping their engagement with cyberspace in somewhat paradoxical directions. On the one hand the growing political will to territorialize cyberspace is undeniable. On the other hand, states depend on a globally compatible cyberspace in their practices of extraterritorial projection of power in and through cyberspace. For this reason, arguments that suggest the practices and positions of pro-sovereigntist states indicate a looming threat of the complete disintegration of the Internet seem unlikely. Similarly, state sovereignty

defined as supreme territorial control (Jackson, 1999) in the sphere of cyberspace is equally unrealistic.

The offensive and defensive policies of states create a context of interdependence. The hegemonic power of the United States over cyberspace built upon the foundation of the leverage gained through American-led firms, government agencies and non-state actors has given way to a new circumstance whereby even the interests of the United States cannot be secured without a degree of mutual self-restraint in US relationship with challengers. The exercise of digital power in cyberspace has an effect of increasing the entanglement of states within the digital webs and thus restrains temptations to initial full-scale digital warfare (Brantly, 2020; Deibert & Pauly, 2019).

Authoritative rule is more complex today as autocrats are both empowered and limited by digital openness. Behind almost every strict information control and Internet censorship program, are states that are simultaneously using common Internet protocols to gather intelligence, target adversaries, and attempt to shape the strategic environment around them. The network effect of such activities entangles political authorities in distributed global networks. No matter how adamant they might appear to be in their pro-sovereignty rhetoric, states continue to be confronted with compelling reasons against any serious attempt to destroy or disable global networks in the face of the benefits they stand to gain from them, upon which they have come to depend (Mueller, 2010).

The absence of compelling evidence that would suggest the emergence of a global consensus to erect solid borders in cyberspace is born out of the utility of cyberspace openness for national security policy as a core feature of all territorial states. Sovereign states depend on open global networks to defend themselves against threats and to project power abroad. The more they become engaged in these networks the less likely they are to degrade them. Moreover, the paradox of territoriality on cyberspace reveals a larger tension between territorially-based political systems confronted with increasingly global social and economic systems (Buzan & Lawson, 2016).

Cyberspace may be having a transformative influence on the very nature of political authority as conventionally conceived. This transformative influence reflects the dynamic interaction between unfulfilled impulses toward territorialization and the necessities of the extraterritorial projection of power. States are now more inclined towards violations of Westphalian sovereignty as they become more aware of the significance of both openness and control for national prosperity (Zacher & Sutton, 1996).

Ethical considerations

The author has completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc.

Data availability

The dataset generated and analyzed during the current study is available from the corresponding author on reasonable request.

References

Akdeniz, Y. (2001). "Governing Pornography & Child Pornography on the Internet: The UK Approach". *University of West Los Angeles Law Review, 32*: 247–275.

Allen, T.S. & Moore, A.J. (2018). "Victory without Casualties: Russia's Information Operations". *The US Army War College Quarterly: Parameters, 48*(1): 8.

Anderson, J. & Rainie, L. (2020). "Conerns about democracy in the digital age". *Pew Research Center: Internet, Science & Tech*, February 21. https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/

Barlow, J. (2019). "A Declaration of the Independence of Cyberspace". *Duke Law & Technology Review, 18*(1): 5–7.

Betz, D.J. (2017). Cyberspace and the State: Towards a Strategy for Cyber-Power. Routledge.

Bowman, W.M. & Bowman, J.D. (2016). "Censorship or self-control? Hate speech, the state and the voter in the Kenyan election of 2013". *The Journal of Modern African Studies, 54*(3): 495–531. https://doi.org/10.1017/S0022278X16000380

Brantly, A.F. (2020). "Entanglement in Cyberspace: Minding the Deterrence Gap". *Democracy and Security, 16*(3): 210–233. https://doi.org/10.1080/17419166.2020.1773807

Buzan, B. & Lawson, G. (2016). "Theory, History, and the Global Transformation". *International Theory, 8*: 502.

Carr, M. (2015). Power Plays in Global Internet Governance. *Millennium, 43*(2): 640–659. https://doi.org/10.1177/0305829814562655

Chadwick, A. & Howard, P.N. (2010). *Routledge Handbook of Internet Politics*. Taylor & Francis.

Czosseck, C. & Geers, K. (2009). *The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press.

Dalek, J.; Deibert, R.; Senft, A. & Wiseman, G. (2012). *Routing Gone Wild: Documenting upstream filtering in Oman via Indi*a. The Citizen Lab, July 12. https://citizenlab.ca/2012/07/routing-gone-wild/

Demchak, C.C. (2016). "Uncivil and Post-Western Cyber Westphalia: Changing interstate power relations of the cybered age". *The Cyber Defense Review, 1*(1): 49–74.

Demchak, C.C. & Dombrowski, P. (2011). "Rise of a Cybered Westphalian Age". *Strategic Studies Quarterly, 5*(1): 32–61.

Deibert, R. (2015). "Authoritarianism Goes Global: Cyberspace Under Siege". *Journal of Democracy, 26*(3): 64–78. https://doi.org/10.1353/jod.2015.0051

Deibert, R. J. & Pauly, L. W. (2019). *Mutual entanglement and complex sovereignty in cyberspace*, 81–99. Routledge. https://doi.org/10.4324/9781315167305-5

Doffman, Z. (2019). *Huawei Backdoors Found By Vodafone, Risking Unauthorized Access To Network*. Forbes. https://www.forbes.com/sites/zakdoffman/2019/04/30/huawei-backdoors-found-by-vodafone-risking-unauthorized-access-to-network/

Earle, B. & Madek, G.A. (2002). International Cyberspace: From Borderless to Balkanized. *Georgia Journal of International and Comparative Law, 31*(2): 225–264.

Farmanfarmaian, R. & Mens, J. (2021). In the Middle East, War Is Going Digital. *Foreign Policy*. https://foreignpolicy.com/2021/02/22/in-the-middle-east-war-is-going-digital/

Franzese, P.W. (2009). "Sovereignty in Cyberspace: Can It Exist Cyberlaw Edition". *Air Force Law Review, 64*(1): 1–42.

Frieden, R. (1998). "Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanization". *Virginia Journal of Law & Technology, 3*(2): 1–31.

Froomkin, A.M. (2000). "Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution Thirtieth Annual Administrative Law Issue Goverance of the Internet". *Duke Law Journal, 50*(1): 17–186.

Goldsmith, J.L. (1998). "The Internet and the Abiding Significance of Territorial Sovereignty". *Indiana Journal of Global Legal Studies, 5*(2): 475–491.

Griffiths, J. (2019). *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. Zed Books Ltd.

Hamanaka, S. (2020). "The role of digital media in the 2011 Egyptian revolution". *Democratization, 27*(5): 777–796. https://doi.org/10.1080/13510347.2020.1737676

Hardy, I.T. (1993). "The Proper Legal Regime for Cyberspace Symposium: Law in Cyberspace". *University of Pittsburgh Law Review, 55*(4): 993–1056.

Haselton, B. (2014). Blue Coat Errors: Sites Miscategorized as "Pornography." *The Citizen Lab*, March 10. https://citizenlab.ca/2014/03/blue-coat-errors-sites-miscategorized-pornography/

Heinegg, W.H. von. (2012). "Legal implications of territorial sovereignty in cyberspace". *2012 4th International Conference on Cyber Conflict (CYCON 2012)*: 1–13.

Herzog, S. (2011). "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses". *Journal of Strategic Security, 4*(2): 49–60.

Hill, J.F. (2012). "A Balkanized Internet?: The Uncertain Future of Global Internet Standards". *Georgetown Journal of International Affairs, 49*–58.

Howard, P.N.; Agarwal, S.D. & Hussain, M.M. (2011). *The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?* (SSRN Scholarly Paper ID 2568619). Social Science Research Network. https://doi.org/10.2139/ssrn.2568619

Huang, Z. & Mačák, K. (2017). "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches". *Chinese Journal of International Law, 16*(2): 271–310. https://doi.org/10.1093/chinesejil/jmx011

Iasiello, E.J. (2017). "Russia's improved information operations: From Georgia to Crimea". *The US Army War College Quarterly: Parameters, 47*(2): 7.

Jackson, R. (1999). "Sovereignty in World Politics: A Glance at the Conceptual and Historical Landscape". *Political Studies, 47*(3): 431–456. https://doi.org/10.1111/1467-9248.00211

Johnson, D.R. & Post, D. (1996). "Law and Borders: The Rise of Law in Cyberspace". *Stanford Law Review, 48*(5): 1367–1402. https://doi.org/10.2307/1229390

Klein, H. (2002). "ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy". *The Information Society, 18*(3): 193–207. https://doi.org/10.1080/01972240290074959

Knockel, J.; McKune, S. & Senft, A. (2016). *Baidu's and Don'ts: Privacy and Security Issues in Baidu Browser*. The Citizen Lab, February 23. https://citizenlab.ca/2016/02/privacy-security-issues-baidu-browser/

Kuner, C.; Cate, F. H.; Millard, C.; Svantesson, D. J. B. & Lynskey, O. (2015). "Internet Balkanization gathers pace: Is privacy the real driver?" *International Data Privacy Law, 5*(1): 1–2. https://doi.org/10.1093/idpl/ipu032

Lee, M.; Greenwald, G. & Marquis-BoireJuly, M. (2015). *A Look at the Inner Workings of NSA's XKEYSCORE. The Intercept*. https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/

Lewis, J.A. (2009). "Sovereignty and the Role of Government in Cyberspace The Internet and the State". *Brown Journal of World Affairs, 16*(2): 55–66.

Lindsay, J.R.; Cheung, T.M. & Reveron, D.S. (2015). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

Lupion, M. (2021). "The Sino-Russian Digital Cooperation and Its Implications for Central Asia". *Digital Silk Road in Central Asia: Present and Future, 55*.

Maghbool, A. (2020). "Black Lives Matter: From social media post to global movement". *BBC News*, July 9. https://www.bbc.com/news/world-us-canada-53273381

Magnus, H. (2011). "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence". *Journal of Strategic Security, 4*(2): 1–24.

Malcomson, S. (2016). *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web*. OR Books.

Marczak, B. & Guarnieri, C. (2014). Mapping Hacking Team's "Untraceable" Spyware. *The Citizen Lab*, February 17. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

Marczak, B.; Guarnieri, C.; Marquis-Boire, M. & Scott-Railton, J. (2014). *Hacking Team and the targeting of Ethiopian journalists*.

Marczak, B.; Scott-Railton, J. & McKune, S. (2015a). Hacking team reloaded? US-based Ethiopian journalists again targeted with spyware. *Citizen Lab, 9*.

Marczak, B.; Weaver, N.; Dalek, J.; Ensafi, R.; Fifield, D.; McKune, S.; Rey, A.; Scott-Railton, J.; Deibert, R. & Paxson, V. (2015b). *An Analysis of China's "Great Cannon" , 5th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 15)*. https://www.usenix.org/conference/foci15/workshop-program/presentation/marczak

Marquis-Boire, M.; Marczak, B.; Guarnieri, C. & Scott-Railton, J. (2013). *For Their Eyes Only: The Commercialization of Digital Spying*. Citizen Lab.

Meinrath, S. (2013). We Can't Let the Internet Become Balkanized. *Slate*. October 14. http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html?via=gdpr-consent

Meserve, S.A. & Pemstein, D. (2020). "Terrorism and internet censorship". *Journal of Peace Research, 57*(6): 752–763. https://doi.org/10.1177/0022343320959369

Mozur, P. (2015). "Baidu and CloudFlare Boost Users Over China's Great Firewall". *The New York Times*, September 14. https://www.nytimes.com/2015/09/14/business/partnership-boosts-users-over-chinas-great-firewall.html

Mueller, M. (2017). *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. John Wiley & Sons.

Mueller, M.L. (2020). "Against Sovereignty in Cyberspace". International Studies Review, 22(4): 779–801. https://doi.org/10.1093/isr/viz044

Mueller, M.L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press.

Neate, R. (2019). Huawei says alleged router "backdoor" is standard network tool. *The Guardian*, April 30. http://www.theguardian.com/technology/2019/apr/30/alleged-huawei-router-backdoor-is-standard-networking-tool-says-firm

Noam, E. (1992). *Telecommunications in Europe*. Oxford University Press.

Nocetti, J. (2015). "Contest and conquest: Russia and global internet governance". *International Affairs (London), 91*(1): 111–130. https://doi.org/10.1111/1468-2346.12189

Ohmae, K. (1991). "The Borderless World: Power and Strategy in the Interlinked Economy". *Business Horizons, 34*(5): 73–75. https://doi.org/10.1016/0007-6813(91)90053-X

Pellegrino, G.; Rossow, C.; Ryba, F.J.; Schmidt, T.C. & Wählisch, M. (2015). Cashing Out the Great Cannon? *On Browser-Based DDoS Attacks and Economics*. 9th {USENIX} Workshop on Offensive Technologies ({WOOT} 15). https://www.usenix.org/conference/woot15/workshop-program/presentation/pellegrino

Pfluke, C. (2019). "A history of the Five Eyes Alliance: Possibility for reform and additions: A history of the Five Eyes Alliance: Possibility for reform and additions". *Comparative Strategy, 38*(4): 302–315. https://doi.org/10.1080/01495933.2019.1633186

Ruan, L.; Knockel, J. & Nishihata, M. (2016). One App, Two Systems: How WeChat uses one censorship policy in China and another internationally. *The Citizen Lab*, December 1. https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

Sabbar, S. & Dalvand, S. (2018). "Semiotic approach to globalization: Living in a world of glocal things". Journal of Cyberspace Studies, 2(1): 75–88.

Sabbar, S. & Matheson, D. (2019). "Mass media vs. the mass of media: A study on the human nodes in a social network and their chosen messages". *Journal of Cyberspace Studies, 3*(1): 23–42.

Sagawa, P.I. (1997). "The balkanization of the Internet". *The McKinsey Quarterly, 1*: 126–139.

Schmidt, A. (2012). "At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker". *Telecommunications Policy, 36*(6): 451–461. https://doi.org/10.1016/j.telpol.2012.02.001

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

Silverberg, D. (2019). How China-US rivalry is dividing the internet. *BBC News*, December 3. https://www.bbc.com/news/business-50570838

Soldatov, A. & Borogan, I. (2015). *The red web: The struggle between Russia's digital dictators and the new online revolutionaries*. Hachette UK.

Soldatov, A. & Borogan, I. (2013). "Russia's surveillance state". *World Policy Journal, 30*(3): 23–30.

Tai, Y. & Fu, K. (2020). "Specificity, Conflict, and Focal Point: A Systematic Investigation into Social Media Censorship in China". *Journal of Communication, 70*(6): 842–867. https://doi.org/10.1093/joc/jqaa032

Thierer, A. (2016). *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Mercatus Center at George Mason University.

Wall, D. (1997). "Policing the Virtual Community: The Internet, Cyberspace and Cyber-Crime". In P. Francis, P. Davies, & V. Jupp (Eds.), *Policing Futures: The Police, Law Enforcement and the Twenty-First Century (pp. 208–236)*. Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-25980-9_9

Xinbao, Z. (2017). "China's Strategy for International Cooperation on Cyberspace". *Chinese Journal of International Law (Boulder, Colo.), 16*(3): 377–386. https://doi.org/10.1093/chinesejil/jmx026

Zacher, M.W. & Sutton, B.A. (1996). *Governing Global Networks: International Regimes for Transportation and Communications.* Cambridge University Press.

Zeng, J. (2016). "China's date with big data: Will it strengthen or threaten authoritarian rule?". *International Affairs, 92*(6): 1443–1462. https://doi.org/10.1111/1468-2346.12750