POROUS TERRITORIES: THE INTERNET BEYOND BORDERLESS VERSUS BALKANIZED

LUKE MUNN
Western Sydney University (Australia)
luke.munn@gmail.com

Abstract: If the internet was once viewed as a borderless realm, critics now warn it is in danger of being "balkanized", splintering into nationalized fragments. Certainly nation-states increasingly see the Internet as "their" internet, a national space to be regulated and actively shaped. The first half of this article charts the technologies that appear to place this vision within reach: data localization, internet shutdowns, and internet filtering. These moves promise to exert sovereign control, to make the internet an extension of national territory. Yet by drawing on two recent events in China, this article argues that these territories are messy and their borders are permeable. Pro-government activists jump across the firewall in order to attack individuals and organizations who threaten the stability and security of their motherland. Simultaneously, individuals scale the firewall in order to question the party line and express solidarity with democratic movements, undermining the political and technical boundaries established by their nation. Internet architectures create a condition where territorialization is constantly being both amplified and undermined by "extra-territorial" activities. These practices demonstrate the everyday porosity of internet territories, providing a messier portrait that goes beyond the dichotomy of borderless vs balkanized.

Keywords: territory, fragmentation, balkanization, internet, China.

When nations speak of the internet today, they no longer use the language of the virtual, but of soil. At the dawn of the internet, cyberspace was framed as a new realm decoupled from the state. This digital sphere stretched across the globe, making it essentially ungovernable. Yet over the last twenty years, this view has steadily been eroded, replaced instead by a vision of the internet as an extension of national territory. An array of technologies have arisen, both infrastructural and legal, that aim to align a nation's digital domain with its geopolitical domain, to marry its network with its physical bounda-

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

ries and political interests – in short, to create a domestic internet in the shape of the state. What, then, is the "shape" of the contemporary internet? How do these forces impose territoriality on a system supposedly global and ungovernable? And how does the architecture of the internet enable or frustrate these efforts at bordering? These are the questions this article explores.

Methodologically, I draw upon a wide array of literature, ranging from internet governance to technology journalism, Asian studies, and activist narratives, synthesizing this material into a portrait of contemporary internet conditions, with a special emphasis on China due to its role as one of the most strident champions of cyber sovereignty. The first half of the article charts this trajectory from borderless to "balkanized", showing how the global and single internet has increasingly been challenged in multiple ways by nation-states who see it as an extension of their sovereign territories. However the second half of the article draws on two recent events on the Chinese internet to suggest that such territories are always messy and composed of permeable borders. This porosity challenges the simple dichotomy of borderless or balkanized, providing a more nuanced understanding of how state intervention shapes the spatiality of the internet.

FROM BORDERLESS TO BALKANIZED

The internet was originally imagined to be a borderless realm. As the internet was adopted into more mainstream use in the mid-nineties, it was accompanied by the language of cyberspace. Cyberspace, it was argued, constituted a new realm in itself. On a technical level, network architectures – a flexible mesh that could reroute traffic at any time through any node – seemed diametrically opposed to the nation-state and its hard-edged boundaries. Yet this architecture also led easily into a compelling political claim of being free from the legacies of state and soil. The development of this "exciting new domain" promised a global or international space that was

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

"potentially free of conventional politics, social order and social regulation" (Wall 1997: 208).

For many, this borderless world would not and could not be governed. John Perry Barlow's "Cyberspace Manifesto" provides the quintessential representation of this view. "Governments of the Industrial World", he wrote (Barlow 1996), "cyberspace does not lie within your borders […]. Your legal concepts of property, expression, identity, movement, and context do not apply to us […]. Ours is a world that is both everywhere and nowhere". While Barlow's views certainly emerged from a more radical strain of politics, his view of the internet as ungovernable was taken up by far more mainstream politicians. In 2000, U.S. President Bill Clinton noted that Chinese authorities were already trying to crack down on the internet. "Good luck", quipped Clinton (2000), "that's sort of like trying to nail Jello to the wall". The internet epitomized the free circulation of free speech. Any effort to impose a national set of values on this domain, to force it into a national mold, would only end in failure.

Along with cyberspace, terms like the information superhighway also posited a borderlessness, even if framed in different terms. In this vision of the internet, the divides that once hindered access to knowledge – whether financial, geopolitical, or both – would be dissolved. In the words of Tim May (1999): "national borders aren't even speed bumps on the information superhighway". Through digitization, organization, and connection, the internet would take the storehouse of the world's information, once the domain of exclusive libraries and elite countries, and make it available for all. This information superhighway would allow data to flow wherever it was needed, rendering the boundaries of the nation-state increasingly superfluous. The new borderless world was characterized by globalized flows of information, argued Ohmae (2005: 20) "it is absurd to believe that lines drawn on maps can have any impact on its movements". In providing a universal and global resource, the internet would accelerate the education and prosperity of all.

Two decades later, those visions have been increasingly eroded to the point of seeming somewhat naive. Stepping into

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

their place is a vision of cyber sovereignty, "a natural extension of national sovereignty in the network environment" (Wang 2014). In this vision, the singular Internet should gradually be transformed into "our" internet, a national territory where norms should be defined, threats should be defended against, and borders should be enforced[1]. "Behind the mists and magic of the Internet lies an older and stronger order", asserted Tim Wu and Jack Goldsmith (2006: ix), an order based on national laws and sovereign governance – a territorial order. Over twenty years, an array of techniques have been developed that assist states in imposing this order on the supposedly global and ungovernable internet. The next few sections briefly survey a number of these measures, showing how they make possible the notion of the internet as a national territory. While territorialization was always desirable, these techniques now seem to make it feasible or even inevitable.

Territorialization through Localization

At one time, the internet was considered a boundless realm where data circulated freely. The immaterial rhetoric of early cyberspace discussed above will not be rehearsed here again. But even the far more recent language of "the cloud" posited an airy domain where data freely circulated, a space decoupled from the constraining politics of sovereignty and soil. For cloud companies, if data was certainly stored somewhere, that "where" was effectively "wherever". Forced to construct new domestic data centers to house data for the GovCloud initiative, Amazon Web Services complained about the requirement, arguing that "physical location has no bearing" (Ottenheimer 2018). For cloud companies and their vision of a distributed, decentralized web, situated data was an anathema.

Alongside technology providers, legal scholars also questioned how information could be seen as situated given the conditions of the internet. Grappling with new technologies, researchers argued that network connectivity fundamentally challenged longstanding paradigms such as territoriality. In an

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

article exploring jurisdiction and the cloud, Andrews and Newman (2013) suggested that "the territorial-based conception of states and nation-states may be quickly becoming archaic in an increasingly connected world". Similarly, in her paper titled *The Un-Territoriality of Data*, Jennifer Daskal (2015: 326) argued that, due to the ease and speed of data travel across borders, in essence, "data is everywhere and anywhere".

Such a view is increasingly at odds with the state-led push towards a territorial understanding of data. Cross-border laws seek to govern when and how data can be transferred into another jurisdiction. Information according to these frameworks is not swirling in some nebulous realm "out there", but is housed in data centers located inside the borders of the nation-state. As one scholar wrote (Duggal 2018), these cross-border laws challenge "countries to adapt pre-digital modes of national sovereignty and economic competition to a digital industry that thrives on borderless and seamless exchange of information". While the internet may be global, "their" internet has clear boundaries. Indeed, one of the core aspects of cross-border laws examined by legal scholars are their "territorial effect", the properties specifying what types of data are covered and under what conditions this data may be transferred outside the nation. Data itself has a geographical location, a place that lies inside or outside of the dotted line of the nation-state. From Malaysia to South Korea, the Philippines, and Japan, an array of Asian countries have passed or are currently considering cross-border legislation (Girot 2018).

As a result of this understanding, governments are placing companies under increased pressure to store and process this data in domestic data centers. China's cybersecurity law, a rough analog of Europe's General Data Protection Regulation, requires data by critical infrastructures to remain within their territory[2]. According to Article 37 of the law, "all personal information and other key data produced and gathered by CII operators (and now also network operators) must be stored in servers located in mainland China" (Koty 2017). In the United States, GovCloud promises cybersecurity by offering a data center infrastructure "operated by employees who are U.S. cit-

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

izens on U.S. soil" (Amazon 2020). The language of soil and citizenry, dismissed as outdated or irrelevant two decades ago, points to the resurgence of territoriality within an internet context.

A site, service, or platform is further coupled to the nation by the personal data that it leverages. This data is not generic nor abstract, but represents the highly intimate and highly valuable details of their citizens. This data may be used or misused, particularly if it escapes the jurisdiction of the government. As such, the protection of this data comes under the wing of the state and its remit to support the lives and livelihoods of these subjects. As one brief example of this tight attachment to the nation, consider Singapore. According to its Personal Data Protection Act, this cross-border rule applies to an organization or corporation "formed under the law of Singapore" or any resident "having an office or place of business in Singapore" (Chia 2018: 327). In Chander and Le's (2015) formulation, these localization strategies collectively construct a kind of "data nationalism". Cross-border legislation frames data as a tangible and sovereign resource, information that is both inside the nation and linked to a national subject.

Territorialization through Shutdowns

Alongside data localization, the increasing use of internet shutdowns represents a crude but powerful form of sovereignty. These intentional disruptions render the internet "inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information" (Access Now 2019). Certainly shutdowns have taken place in countries typically regarded as authoritarian: Chad, the Democratic Republic of Congo, Iraq, Kazakhstan, and Russia (Taye 2018: 2). However the world leader in shutdowns is a nation widely regarded as a democracy-India. Over 381 shutdowns have been logged by the Software Freedom Law Center (2020), which maintains a page that tracks shutdowns across the country. These statistics show that India not only shuts down its internet more than all other countries com-

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

bined, but is doing so more often, with the number of shutdowns ramping up over the last few years to become the "new normal" (Suresh 2019).

For India, the internet is not a public good that must remain constantly available, but a national infrastructure that can and should be switched on and off as necessary. As one specific case, the longest shutdown in the world has been imposed in Kashmir. On August 4 of 2019, parliament abrogated Article 370 of the constitution, splitting the administered territory and stripping it of former rights. Anticipating activism and civil unrest, a shutdown was instigated. Officials justified the shutdown as necessary to "keep the peace" in the region (Nazmi 2019). The shutdown continued for 176 days, with both landlines and mobile services being restricted. Finally on January 26 2020, the shutdown was partially lifted when access to second generation (2G) mobile services was restored. However, along with incredibly slow speeds, accessible services only include a highly selective whitelist: a "minuscule list of 300 websites, including banks, some news portals, educational institutions, utilities, travel and food delivery applications" (Al Jazeera News 2020).

Governments often fail to provide any sort of public explanation for enacting a shutdown. When reasons are given, these often revolve around preventing the harmful spread of information, defusing tension, and maintaining order. In 2018, the most common justifications were public safety, fake news or hate speech and related violence, and national security (Taye 2018). Of course, whether such shutdowns are effective in these aims is debatable. In a study on India's shutdowns, Rydzak (2019) found they encourage activists to substitute non-violence protest, which often require coordination via online communication, with more ad hoc violent interventions. However, regardless of its ability to quell civil unrest, the key point here is that the shutdown frames the internet as "our" internet. Rather than a universal resource extending across the globe, this internet becomes a domestic infrastructure, a territory that follows the footprint of the nation-state and ends at the border. Along with this geographical link to the nation, there is also a link via power. Shutdowns are a

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

concrete display of sovereign control, demonstrating a nation's ability to exert a crude but devastating force over their infrastructure by turning it off entirely. India frames the internet as a space that should be dictated by sovereign decisions.

Shutdowns establish a blueprint for national intervention. For Selva (2019), India's increasing use of this technique has led other nations to "discover the off switch", including Sudan, following a brutal government take down of democratic protest, and Benin and Malawi, coinciding with parliamentary and presidential elections. In Asia-Pacific specifically, Nauru, a tiny but significant island used for asylum detention and processing, announced a temporary shutdown in 2015. The nation imposed a ban on Facebook and other websites as a protection mechanism to "ensure that Nauruans are not left exposed and vulnerable to the actions of criminals, sexual perverts and cyber bullies"; the shutdown attended new laws imposing jail time for speech that was deemed to threaten national security (Olukotun 2015). More recently, Indonesia enforced a shutdown meant "to accelerate government effort to restore order" in West Papua, following angry and ongoing protests" (Firdaus 2019). These shutdowns demonstrate the state's sovereignty, flexing their authority over their internet.

Territorialization through Filtering

If shutdowns are a forceful display of internet-as-national-territory, they are also crude. Filtering information is a more sophisticated intervention that seeks to construct an internet shaped in the image of the state. Filtering, blocking, or censoring information falls under the same umbrella, with techniques ranging from port blocking and keyword filtering to search engine alterations (Hamade 2008). The idea, as with any firewall, is that inspection of the packets passing through shows what information the user is requesting, whether a forbidden website or a controversial search term. Control at this "digital border" allows packets to be modified, diverted, or ignored altogether.

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

One of the most recent examples of filtering is the "Russian Internet Law" passed in May 2019, an act that "requires internet service providers to filter all traffic through special nodes under the control of Roskomnadzor, the Kremlin's internet censor" (Financial Times 2019). A Russian domain name service, combined with legislation that forces companies to store data domestically, could theoretically allow all internet traffic to remain in the country. Requests for "foreign" sites and services could be blocked or transformed into their national equivalents, ensuring that information always remained within the borders of the nation-state. As Epivanova (2020: 9) suggests, despite the rhetoric of cybersecurity, the aim of the amendment is not about defending Russia from outside attacks, "but rather a proactive step toward splitting its own national segment off from the infrastructure of the global internet in order to gain state sovereignty over it".

Of course the prime example in any discussion of filtering is China. Even as early as 1997 *Wired* was describing a set of technical and legislative mechanisms that it collectively dubbed the Great Firewall, now often shortened to GFW. By filtering out polluting material "aimed at undermining the unity and sovereignty of China", engineers sought to create their own distinct version of the internet, "a Net that has Chinese characteristics" (Barme, Ye 1997). Technically this was enacted by peering with the small number of gateways at the edges of the Chinese network. As data passed through those points, it was identified and altered. Some requests were granted and others refused, blocking those sites and services from users. Since its inception, this project has only become more sophisticated. Over the last twenty years, new functionality has gradually been integrated, resulting in a highly articulated and extensive degree of control. In the first stage, the GFW blocked domain names and IP addresses; in the second stage, it implemented keyword censorship; in the third stage, it began detecting VPNs (virtual private networks) and other circumvention tools; and in the fourth stage, these hardware and software mechanisms were supplemented by legislation that targeted anonymity and VPNs (Chandel et al. 2019).

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

Filtering information seeks to remove or block media that is considered objectionable according to both governmental legislation and societal norms. In this sense, filtering inherently frames the internet as an extension of national territory. To counter the dangerous and unfiltered information "out there", hardware or software mechanisms control the kind of information allowed "into" a country. The aim is to align the digital territory of China with its physical territory, to eliminate any kind of disparity when a subject moves between offline and online environments. For Xi Jinping (Economy 2018) "there is no distinction between the virtual world and the real world: both should reflect the same political values, ideals, and standards".

BALKANIZATION CRISIS?

What inspires this territorialization of the internet through shutdowns, localization, and filtering? Certainly one motivation is control. For states, these techniques aim to claw back a degree of authority over a domain seen as frustratingly slippery. When the internet becomes a tinder box that may ignite tensions – or more cynically, a site of counter-protest or embarrassment for the political establishment – then states want the ability to clamp down on these communications. Citing the India shutdowns discussed above, the state-aligned *People's Daily* of China asserted that such measures are a "necessary regulation" of the internet, a "reasonable choice of sovereign countries based on national interests, and a natural extension of national sovereignty in cyberspace" (Wang 2014). Whether through legislation or hardware, these moves seek to regulate "their" internet in the way they see fit.

Yet perhaps more justifiably, these measures also kick back against a "universal" vision of the internet long recognized as implicitly US-led. For some nations, the supposedly global internet appears more like American dominance enjoyed by a handful of technological giants: Google, Facebook, Apple, Amazon, and others. These corporations are aligned with the technolibertarian ideologies of Silicon Valley and the

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

broader Western values of consumerism and individualism. For Kalev Leetaru (2019), this cluster of companies represents a new generation of "cultural colonialism" in that they enforce a global set of norms set out by Silicon Valley; these "digital dictatorships transcend traditional national borders, enforcing their beliefs, narratives and rules on the world at large". For states with more authoritarian leanings, a shift from the global Internet to a national internet allows them to strip out these unwanted values and begin embedding their own ideals.

For critics, these moves put the internet in danger of balkanization. Urgent calls to avoid balkanization can increasingly be found in mainstream outlets, from technology blogs and civic organisations to political magazines. "We can't let the internet become Balkanized," pleaded Sascha Meinrath in an early and widely cited article (2013); such fragmentation would transform the future internet from a "global commons to a fractured patchwork severely limited by the political boundaries on a map". While these calls have become more frequent, their rhetoric has also been ramped up, with urgent language seeking to point out the enormous stakes. Fragmentation, we are told, signals nothing less than the death of the internet. "Governments have broken the world wide web" lamented Mark Scott (2017), "regional digital rule-making threatens to derail the economic, societal and political advances of the internet age".

Yet, examining the literature, the world has stood on the edge of the balkanization precipice for twenty years. Anxieties around fragmentation emerged as early as 1997 and have continued uninterrupted since then, with each scholar proclaiming the end of the "free and open" internet. Of course, the conversation has certainly shifted over time. Early concerns were mainly commercial and technical, focusing, for example, on internet service providers refusing to "peer" with each other (Sagawa 1997; Frieden 1998). Later concerns took on a markedly more geopolitical tinge, stressing how the once "global" web was being fragmented by anti-American enemies such as China and Russia (Earle, Madek 2002; Wu 2004; Werbach 2008; Kuner et al. 2015; Cattaruzza et al. 2016).

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

Despite the hand-wringing of these critics, the internet was always already balkanized. The singular "Internet" implies a cohesive and overarching network that spans the globe. But the internet is better understood as a system of systems, a network of networks. "The entire Internet is a collection of long-distance links between discrete, locally connected networks", Jack Goldsmith (2019: 54) reminds us, while appearing "smooth and featureless, it is actually a group of islands with links between them". Each network is connected to the others through a complex array of cables, gateways, and interconnection nodes. The Internet is the result of these functioning links. Nothing reveals this illusion of unity more than interruptions of connectivity on a national or regional level. When shutdowns occur or cables are broken, this cohesive effect is also broken.

Even at a mundane level, the "free flow" of information has been a myth from the very beginning. Networks were never realms where anything goes, but instead imposed a strict set of controls over the data requests that were honored, the users and ports that were enabled, and the communications that could be circulated (Mueller 2019). For both security and efficiency reasons, filtering was integral, embedded at both the network layer and as a basic feature in network routers. Indeed, it was precisely this functionality that allowed network filtering at a company level to translate to a national or geopolitical level. "Nobody questions the authority and the right of a corporation to tightly manage and control and monitor the communication in and out of a company's network", documents James Griffiths in his history of the Great Firewall (2019: 75): "that tech had been built from the very beginning to serve the market of corporate customers. All China did was turn on those switches for the entire country".

Along with this technical fragmentation, each network also possesses a degree of autonomy emerging from its unique social, cultural, and historical development. This is why scholars can chronicle the emergence of the Chinese internet (Negro 2017; Griffiths 2019), the Cuban internet (Harris 2015), the attempt and failure to construct the Soviet internet (Peters 2017), and so on. As one scholar argued (Yang 2012: 49) just

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

as there is no singular television but rather "this television, our television," there is also no singular internet; instead, "the Chinese Internet is a cultural form much like American television or British television". While global standards and protocols certainly had to be adhered to, each of the networks is a "nationalized" internet in the sense that its construction required the labor of national engineers, documentation in the national language, and particular decisions made in the national interest.

These observations show how fragmentation has always been integral to the internet, both in technical architecture and historical development. But perhaps the most damaging aspect of "balkanization" as a specter is that it replaces a myth of the borderless internet with another myth of the tightly bordered internet. Based on an (idealized) Westphalian model, the world is carved up into "spatially exclusive units" without overlapping jurisdictions (Caporaso 2000: 7). In this vision, each nation's internet conforms perfectly to the dotted lines of their national boundaries. Each nation establishes gateways at the edges of this cyber zone, comprehensively ring-fencing the information and communications that take place inside it. Each nation takes "global" information and delineates it cleanly into domestic and foreign, national and international. The Internet becomes their internet, a space governed with lock-tight precision.

As discussed above, there is certainly a shift towards territorialization, with nations framing these networks as an extension of sovereign space. However, these territories are messy and their borders are permeable. The state dream of territorialization remains incomplete, and this is not due merely to technical inability, but because the nation derives its identity from entities outside itself. This view echoes glocalization, a concept introduced in recognition of the fact that "much of the promotion of locality is in fact done from above or outside"; even in the "more aggressive forms of contemporary nationalism", notes Robertson (2002: 26), "there is still a translocal factor at work". Territorialization is constantly being shaped by practices, narratives, and institutions taking place in the "extraterritorial" space surrounding its borders. To

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

demonstrate this dynamic in a more concrete way, I return to China – arguably the strongest example of cyber sovereignty – to examine how activities beyond the firewall are able to both intensify and undermine the internet as national space.

POROUS TERRITORIES

It is China above all who has led the way in asserting that the internet is an extension of a national territory and should be governed as such. For two decades, as chronicled above, the state has continuously developed more sophisticated measures of filtering, blocking, and controlling information in order to assert their sovereignty, slowly transforming a global Internet into a more distinctly Chinese internet. And yet this internet territory is not impermeable. The firewall can be bypassed through virtual private network (VPN) software and secure shell (SSH) software.

The quest to bypass filtering and escape "beyond the wall" often takes the form of an arms race, with the Chinese state attempting to recognize and defeat technologies, while technology providers constantly add new workarounds. The anonymous software Tor, for example, follows this pattern. Anderson (2012: 7) describes how Tor was once used throughout China, yet its core directory nodes were quickly recognized and shut down; however, in 2011 "bridge nodes" were introduced, allowing Chinese users to leverage the tool again; after these "bridge nodes" were similarly blocked in 2012 "obsproxy" was released, rendering the traffic between the Tor client and these nodes "innocent-looking" and thereby making the tool effective once more. As new tools come online, they poke holes in the firewall, allowing users access to the world beyond.

For Margaret Roberts (2018), the firewall is about deterrence rather than a lock tight solution; if porosity is possible, it incurs additional costs in terms of time and money. VPNs are paid services that still require a nominal level of technical expertise to setup and use. For many users, this puts them out of reach. Rather than an insurmountable barrier, the firewall is

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

better understood as an edifice of technical, financial, and legal hurdles. These hurdles are designed to make travel outside the territory costly, risky, or inconvenient. Pursuing information outside the domestic internet is not impossible, but it is undesirable. However, as the next two examples of porosity hope to show, transgressing these borders complicates simple distinctions such as inside/outside, censored/free, pro/anti government.

Diba is a popular subforum of the larger Baidu Tieba subforum. In some respects it is the Chinese equivalent to Reddit or 4chan, yet with a distinct user base of pro-government mainlanders. In recent years, the site has led to the creation of the Diba Central Army, often described by critics as a troll army. This cyber-nationalist community, with 20 million or more members, is known for its highly organised "battle missions" (Hailong 2019). Over the last few years, by sharing access and instructions for VPN technology, these young patriots have bypassed filtering in order to conduct a series of campaigns on Facebook, a platform blocked in China. These campaigns vary, ranging from flooding attacks that hope to take down platforms, to more playful memes and textual propaganda presenting a pro-China perspective.

In 2016, the group conducted one of its highest profile campaigns, now known as the Diba Expedition. Tsai Ing-wen had been elected president in Taiwan, a candidate that had long advocated independence for the island. In the eyes of Diba members, her views were an affront to Chinese sovereignty, and forum admins called for action. On January 20th, her page began filling up with nationalist memes and messages, most written in the simplified Chinese used by Mainlanders; 12 hours into the campaign, 40,000 comments had been posted (Dong 2016; see also Yang, Chen 2017; Lang, Chen 2019).

The "success" of the Diba Expedition has since inspired more campaigns in recent years. These efforts have particularly ramped up in the wake of the Hong Kong anti-extradition protests aiming to preserve autonomy from China. "China Is Sending Keyboard Warriors Over the Firewall" observed one story (Teixeira 2020), these battalions "reported pro-Hong Kong Instagram accounts; flooded comments sections with

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

Chinese flag emojis; and disseminated patriotic memes". By poking holes in the digital border, pro-Chinese groups are able to harass individuals and organizations deemed counter to the values of the motherland.

Diba and its missions trouble the clean dichotomy of territorial versus extraterritorial. On the one hand, these are Mainlanders who are based within the geographical footprint of China. Whether operating out of a cybercafe in Shenzhen or from a bedroom in Wuhan, their activities of surfing, posting, and clicking take place on national soil. In this sense, they fall within the jurisdiction of the state, the area governed by Chinese law. This spatial link to the territory is further strengthened by the legal status of these individuals. These are Chinese citizens, subjects that retain a close connection to the state and its associated territory. Yet on the other hand, there is clearly an extraterritorial element to these activities. The targets of Diba's attacks have lived in countries ranging from Taiwan to Australia and New Zealand. The Facebook or Instagram servers that store and process their posts may be located in Singapore, in Ireland, or in the United States (Bell 2020). Moreover, many of these platforms are owned and operated by American companies. Together, these aspects work to blur hard-edged distinctions between domestic and foreign, national and international, territorial and extraterritorial. Global activism is performed by hordes of loyal citizens who never leave the country.

Beyond the location and citizenship of their participants, the politics of the campaigns themselves demonstrate the ambivalency between the territorial and the extraterritorial. Government policy is that those wishing to carry out "cross-border networking" must apply for official approval and may only use state-sanctioned providers; those who have failed to comply in the past have been fined (Sixth Tone 2019). Jumping over the firewall and accessing blocked platforms through VPNs, then, clearly runs counter to the party-line. But if this unauthorized cross-border activity goes against state guidelines, these campaigns aim to reinforce China and its values. The trolling, doxxing, and spamming carried out by Diba on "extraterritorial" targets and servers are ultimately about bolstering the na-

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

tion. The result is a strange tension that other scholars have described as "patriotism without state blessing" (Han 2019). As Yang et al. (2017: 7) notes, these campaigns are contradictory, "simultaneously violating China's sociotechnical laws and norms while promoting a pro-PRC political ideology". Diba burrows through the border, venturing out into politically and legally grey space-yet does so only in order to uphold Chinese authority.

In terms of the nation, this activism takes place externally, but is felt most clearly internally. Diba selects targets and organizes campaigns against those it believes have offended the nation. Whether based in Hong Kong, Taiwan, or elsewhere, the actions of these individuals or institutions have threatened the identity and authority of the country. While Diba's actions may seek to delegitimize Western narratives and damage foreign individuals, they do so in order to reinforce the norms, values, and worldviews of those inhabiting Chinese territory. When asked about the reaction of Taiwanese to their expedition, one Diba participant admitted that they "did not convince anyone"; the only winner of the campaign was "the Chinese nation" whose "feelings have deepened" (Feng Shang 2016). The transformation, then, is primarily in the participants themselves. Their activity intensifies their personal connection to the nation, their loyalties to its interests and honor. At the same time, these practices strengthen alliances with those deemed to be part of it, establishing the "deep, horizontal comradeship" (Anderson 2016: 33) so vital for reproducing the imagined community of the nation.

Other researchers of Chinese internet nationalism have echoed this observation. The aim of these campaigns, argues Fang Kecheng (Chen 2019), is not actually "about winning hearts and minds overseas, but being applauded in mainland China". Despite the politically grey nature of these campaigns, applause has come directly from media closely aligned with Beijing. In a recent prime-time news segment, state-broader CCTV praised Diba and a related fan-girl community as "forces that love China", an open endorsement that was immediately recognized by the participants themselves (Shen 2019). While patriotic activism conducts negative online at-

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

tacks against others, it also functions positively in these sense of reconstructing the "motherland" and demonstrating allegiance to it.

Yet alongside jingoistic attacks, VPNs have also allowed individuals to venture out of China's internet territory in order to express opinions counter to Beijing. In fact, these two phenomena have coincided at particular moments. Diba's massive anti-Taiwan campaign of 2016 discussed earlier taught many to use virtual private networks. Yet users not only carried out their instructions on Facebook, they also ventured further afield onto platforms with contrary voices like Twitter; as a result, one well-known dissenter received 490 new followers on the same day as the nationalist attacks (Lam 2016).

If not outright anti-government, these Mainlanders have a more critical or at least skeptical position to the Chinese state. The phenomenon of these agnostic individuals jumping the firewall has been noted more recently during Hong Kong's anti-extradition movement. One of the major platforms used by Hong Kong activists has been Telegram. As an encrypted messaging app operated by a non-Chinese entity, Telegram is blocked within China. Indeed earlier in the same year, the app blamed China for a powerful Denial of Service attack that attempted to take it offline entirely (Porter 2019). Nevertheless, in late 2019, Hong began observing more messages from Chinese users appearing in their Telegram groups. These messages ranged in tone, from tentative to more strident in their critiques of the state. Yet whether expressing their support for peaceful protests or questioning the official state-backed narrative, they were all written in the simplified Chinese script used on the Mainland.

By jumping across the firewall and out of China's digital territory, these individuals also move out of China's political, cultural, and social territory. If these individuals are located in the Mainland, the online environments they venture into are far-removed from Beijing and its normalizing force. One user, scared of sharing his views with others, found a group of friends online who shared his political persuasions. "Everyday they'd scale the Great Firewall to gather news on HK. Everyday they'd share and discuss the news within the WeChat

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

group" (Mainland Voices 2020). Here the state-media depiction of the protests – violent riots instigated by radical or freeloaders – is not the only narrative. Here party lines may be challenged and official doctrines discussed. "With them coming across the Firewall, we are trying to respond and interact more. We hope to change them" stated one activist (VanderKlippe 2019). Activists in Hong Kong attempt to dialogue with these mainlanders, explaining the five demands of the movement, for example, and defending their viewpoints.

Whether interacting with individuals in Hong Kong or Taiwan, or browsing platforms further afield, the vision of China encountered in these chats, tweets, and articles is radically different from that put forward on the "domestic" internet. "I've always known CCTV is selective with its reporting", stated one user after comparing state news of the protests against international news (Mainland Voices 2019), "now, I know that when it needs to, CCTV is more than happy to outright lie". This disjuncture may be jarring, causing individuals to call into question the metanarrative of the nation that was once assumed. While anecdotal, we may surmise that these individuals "come back" from these experiences with their concept of the nation fundamentally altered. If Diba's extraterritorial pursuits aimed to amplify the nation, these experiences undermine it – if only in the mind of a single person.

CONCLUSION

The internet was originally conceived as a borderless realm, a global cyberspace disconnected from the nation-state and its legacy concerns of sovereignty and soil. In technolibertarian rhetoric, the internet should not be governed; in more mainstream political channels, the internet could not be governed. The broad arc of internet governance over the last twenty years has attempted to do just that, with "cyber sovereignty" framing the internet as a natural extension of a nation's territory.

From data localization to filtering and internet shutdowns, an array of techniques have arisen that seem to put this

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

vision within the grasp of the nation-state. In one sense, these moves promise to deliver a degree of control over an arena once seen as uncontrollable. Yet these moves also push against the Western and specifically American values that have predominated the ostensibly global internet. States hope to take the singular Internet and mold it into "their" domestic internet, a territory aligned with the norms, values, and regulations of the nation.

For critics, these moves represent a dangerous tendency towards "balkanization", where the internet is splintered into incompatible islands. However, examining both the technical architecture and the historical development of national networks demonstrates that such fragmentation has always been an integral aspect of the internet. Balkanization replaces the myth of the borderless with a newer myth of the tightly bordered. In this imaginary, the internet is fractured into nationalized versions that mirror their boundaries. Each internet is an autonomous island, governed meticulously, that carefully distinguishes between the interior and exterior of their territory.

Instead, drawing on two recent events from China, I argued that territories are messy and borders display a porosity. China's Great Firewall can be crossed using virtual private networks, or VPNs. Using these technologies, the massive troll-army of Diba jump the firewall in order to attack individuals and institutions that they declare have offended the nation. In venturing outside the domestic internet and onto platforms like Facebook and Twitter, these campaigns overtly disobey the sociotechnical borders established by the state. And yet these "extraterritorial" activities seek primarily to reinforce the authority of the Party and bolster the concept of the nation for its inhabitants.

In the second example, I noted how Hong Kong activists have observed more mainlanders "coming across" the firewall in order to interact. Whether showing support for democratic movements of questioning state media, these forays out of the nation's digital territory allow individuals to encounter an alternate set of political and social norms. These experiences may leave individuals more critical or skeptical of the nation and its claims. In both circumstances, the territory is shaped

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

by activities outside it; the identity and stability of the nation is derived from its surroundings. The porosity of territory presents a counter image to the simplistic dichotomy of borderless vs balkanized, offering a more nuanced view of state attempts at internet nationalization.

While China has provided the primary example in this article, this is a broader global phenomenon that can be witnessed across a wide variety of countries. Future research could productively investigate similar plans in Russia or Iran, for instance, authoritarian regimes that have followed China's lead on cyber-sovereignty. Yet equally researchers might consider a nation like the United States and its various moves to establish a digital jurisdiction with sufficiently "American" norms, values, and capabilities. Over the next decade, the dream of a global Internet will fade even further into the distant past. In its place will rise the compelling vision of the internet as an extension of sovereign territory. This framing will bring further moves to ring-fence it, to manage its content and police its borders. And yet the scenarios discussed above show how these visions are both constructed and complicated by everyday technopolitical practices. Far from being clean-edged and hermetic, territoriality is a messy phenomenon defined in part from its porosity.

ACKNOWLEDGMENTS

The article emerged from the funded research project "Data Centres and the Governance of Labour and Territory, Australian Research Council Discovery Project" (DP160103307).

NOTES

[1] Internet is capitalized in this article where it particularly refers to this vision of a singular, cohesive global system.

[2] While the General Data Protection Regulation (GDPR) is an important legal precedent, it has also been the dominant focus of much research, spawning countless articles on data localization, privacy and personal data, and the nationalization of the

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

internet. The contribution here moves away from these Western-centric narratives and instead pays more attention to Asia and China more specifically.

REFERENCES

Al Jazeera News (2020), *Limited Internet Restored in Kashmir, No Access to Social Media,* 26 Jan. 2020, https://www.aljazeera.com/news/2020/01/limited-internet-restored-kashmir-access-social-media-200125132533497.html.

Amazon Web Services (2020), *AWS GovCloud (US)*, https://aws.amazon.com/govcloud-us.

B. Anderson (2016), *Imagined Communities* (London: Verso).

D. Anderson (2012), *Splinternet: Behind the Great Firewall of China*, in "Queue", 10, 11, pp. 40-49.

D.C. Andrews, J.M. Newman (2013), *Personal Jurisdiction and Choice of Law in the Cloud*, in "SSRN Electronic Journal".

G. Barme, Y. Sang (1997), *The Great Firewall of China*, in "Wired", https://www.wired.com/1997/06/china-3.

E. Bell (2020), *Facebook Data Center Locations, News, Photos, and Maps*, in "Baxtel", https://baxtel.com/data-centers/facebook.

J.A. Caporaso (2000), *Changes in the Westphalian Order: Territory, Public Authority, and Sovereignty*, in "International Studies Review", 2, 2, pp. 1-28.

A. Cattaruzza et al. (2016), *Sovereignty in Cyberspace: Balkanization or Democratization*, in "2016 International Conference on Cyber Conflict (CyCon U.S.)", pp. 1-9.

S. Chandel et al. (2019), *The Golden Shield Project of China: A Decade Later-An in-Depth Study of the Great Firewall*, in "2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)", pp. 111-19.

A. Chander, P.L. Uyen (2015), *Data Nationalism,* in "SSRN Scholarly Paper", https://papers.ssrn.com/abstract=2577947.

L. Chen (2019), *China Troll Army's Battle Expeditions Leap Great Firewall*, in "South China Morning Post", 7 August, https://www.scmp.com/news/china/society/article/3021798/china-troll-armys-battle-e x peditions-leap-great-firewall.

K. Chia (2018), *Singapore*, in C. Girot (ed.), *Regulation Of Cross-Border Transfers Of Personal Data In Asia* (Asian Business Law Institute), pp. 315-42.

B. Clinton (2000), *Clinton's Words on China: Trade Is the Smart Thing*, in "The New York Times", 9 March.

J. Daskal (2015), *The Un-Territoriality of Data*, in "The Yale Law Journal", 326, 125, pp. 326-399.

Y. Dong (2016), *Let the Cross-Strait Internet Trolling Commence*, in "Foreign Policy", 20 January, https://foreignpolicy.com/2016/01/20/china-taiwan-tsai-ing-wen-facebook-troll-election.

P. Duggal (2019), *Data Localization: A Review Of Proposed Data Localization Legislation In India, With Learnings For The United States* (Washington DC: Data Catalyst Institute).

B. Earle, G.A. Madek (2002), *International Cyberspace: From Borderless to Balkanized*, in "Georgia Journal of International and Comparative Law", 31, 2, pp. 225-64.

E.C. Economy (2018), *The Great Firewall of China: Xi Jinping's Internet Shutdown*, in "The Guardian", 29 June.

A. Epifanova (2020), *Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet* (German Council on Foreign Relations).

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

Y. Feng Shang (2016), *亲自参加两岸Facebook'表情包大战'是一种什么样的体验？|PingWest品玩*, http://www.pingwest.com/fighting-with-fun.

F. Firdaus (2019), *Indonesia Blocks Internet in West Papua as Protest Rages*, in "Al Jazeera", 23 Aug, https://www.aljazeera.com/news/2019/08/indonesia-blocks-internet-west-papua-protest-rages-190822022809234.html.

E. Fraser (2016), *Data Localisation and the Balkanisation of the Internet*, in "SCRIPTed: A Journal of Law, Technology and Society", 13, pp. 359-73.

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

C. Girot (ed.) (2018), *Regulation Of Cross-Border Transfers Of Personal Data In Asia* (Asian Business Law Institute).

J. Goldsmith (2019), *Sovereign Difference and Sovereign Deference on the Internet*, in "Yale Law Journal Forum", 128, pp. 818-826.

J. Goldsmith (2018), *The Failure of Internet Freedom*, https://knightcolumbia.org/content/failure-internet-freedom.

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

L. Hailong (2019), *From Cyber-Nationalism to Fandom Nationalism: The Case of Diba Expedition In China* (London: Routledge).

S.N. Hamade (2008), *Internet Filtering and Censorship*, in "Fifth International Conference on Information Technology: New Generations", pp. 1081-1086.

R. Han (2019), *Patriotism without State Blessing: Chinese Cyber Nationalists in a Predicament*, in "Handbook of Protest and Resistance in China", June https://www.elgaronline.com/view/edcoll/9781786433770/9781786433770.00036.xml.

J. Harris (2015), *Castro Hates the Internet, so Cubans Created Their Own*, in "Vox", 5 October, https://www.vox.com/2015/10/5/9434407/cuba-internet-explained-castro.

Hong Kong Internet Service Providers Association (2019), *Urgent Statement of HKISPA on Selective Blocking of Internet Services*, 28 August, https://www.hkispa.org.hk/139-urgent-statement-of-hkispa-on-selective-blocking-of-internet-services.html.

R. Kathuria et al. (2018), *The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India*, in "Indian Council for Research on International Economic Relations", April, https://think-asia.org/bitstream/handle/11540/8248/Anatomy_of_an_Internet_Blackout.pdf?sequence=1.

A. Koty (2017), *New Data Localization Rule in China's Cybersecurity Law to Impact HR*, in "China Briefing News", 17 May, https://www.china-briefing.com/news/chinas-cybersecurity-law-to-expand-data-localization-requirements.

C. Kuner et al. (2015), *Internet Balkanization Gathers Pace: Is Privacy the Real Driver?*, in "International Data Privacy Law", 5, 1, pp. 1-2.

F. La Rue (2011), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,* United Nations, 16 May, doi:10.1163/2210-7975_HRD-9970-2016149.

O. Lam (2016), *Chinese Netizens Climb Over the Great Firewall to Go After Advocates of Taiwanese Independence*, in "Global Voices Advocacy", 25 January, https://advox.globalvoices.org/2016/01/25/chinese-netizens-climb-over-the-great-firewall-to-go-after-advocates-of-taiwanese-independence.

T. Lan (2016), *National Sovereignty Applies to Cyberspace*, in "China Daily", 20 April, https://www.chinadaily.com.cn/opinion/2016-04/20/content_24681612.htm.

P. Lang, L. Chen (2019), *China's Internet Warriors Going to Battle over Hong Kong Protests*, in "South China Morning Post", 4 September, https://www.scmp.com/news/china/society/article/3024223/emergence-and-evolution-chinas-internet-warriors.

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

K. Leetaru (2019), *Is A Fragmented Internet Inevitable?*, in "Forbes", 13 April, https://www.forbes.com/sites/kalevleetaru/2019/04/13/is-a-fragmented-internet-inevitable/#74acd692223c.

Mainland Voices (2020), *Everyday They'd Scale the Great Firewall to Gather News on HK. Everyday They'd Share and Discuss the News within the WeChat Group. 4/7*, in "Twitter", 27 January, https://twitter.com/MainlandVoices/status/1221610356616912899.

Mainland Voices (2019), *In the Past, I've Always Known CCTV Is Selective with Its Reporting. Now, I Know That When It Needs to, CCTV Is More than Happy to Outright Lie. 8/11*, in "Twitter", 4 December, https://twitter.com/mainlandvoices/status/1202065192240087040.

S. Meinrath (2013), *We Can't Let the Internet Become Balkanized*, in "Slate", http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html.

S. Moss (2019), *The Great Disconnect*, 6 December, https://www.datacenterdynamics.com/analysis/great-disconnect.

M. Mueller (2019), *Against Sovereignty in Cyberspace*, in "International Studies Review", pp. 1-23.

M. Mueller (2017), *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* (London: Polity Press).

S. Nazmi (2019), *Why India Is the World Leader of Internet Shutdowns*, in "BBC News", 19 Dece,ber, https://www.bbc.com/news/world-asia-india-50819905.

G. Negro (2017), *The Internet in China: From Infrastructure to a Nascent Civil Society* (London: Palgrave Macmillan).

K. Ohmae (1999), *The Borderless World: Power and Strategy in the Interlinked Economy* (New York: Harper Business).

D. Olukotun (2015), *Why Is a Tiny Island Nation Facing an Internet Shutdown?*, in "Access Now", 14 May, https://www.accessnow.org/why-is-a-tiny-island-nation-facing-an-internet-shutdown.

D. Ottenheimer (2018), *Amazon's About Face on GovCloud: "Physical Location Has No Bearing"*, in "Security Boulevard", 1 March, https://securityboulevard.com/2018/03/amazons-about-face-on-govcloud-physical-location-has-no-bearing.

B. Peters (2017), *How Not to Network a Nation: The Uneasy History of the Soviet Internet* (Cambridge: MIT Press).

J. Porter (2019), *Telegram Blames China for "Powerful DDoS Attack" during Hong Kong Protests*, in "The Verge", 13 June, https://www.theverge.com/2019/6/13/18677282/telegram-ddos-attack-china-hong-kong-protest-pavel-durov-state-actor-sized-cyberattack.

M.E. Roberts (2018), *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton: Princeton University Press).

R. Robertson (2002), *Glocalization: Time-Space and Homogeneity-Heterogeneity*, in M. Featherstone et al. (eds.), *Global Modernities* (London: Sage), pp. 25-44.

J. Rydzak (2019), *Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India*, in "SSRN Scholarly Paper", https://papers.ssrn.com/abstract=3330413.

P.I. Sagawa (1997), *The Balkanization of the Internet*, in "The McKinsey Quarterly", 1, pp. 126-139.

S. Sassen (2000), *Territory and Territoriality in the Global Economy*, in "International Sociology", 15, 2, pp. 372-393.

M. Scott (2017), *Goodbye Internet: How Regional Divides Upended the World Wide Web*, in "*POLITICO*", 15 December, https://www.politico.eu/article/internet-governance-facebook-google-splinternet-europe-net-neutrality-data-protection-privacy-united-states-u-s.

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org

M. Selva (2019), *Reaching for the off Switch: Internet Shutdowns Are Growing as Nations Seek to Control Public Access to Information*, in "Index on Censorship", 48, 3, pp. 19-22.

X. Shen (2019), *Nationalists Hopping the Great Firewall to Attack Hong Kong Protesters Praised by Chinese State Media*, in "Abacus", 20 August, https://www.abacusnews.com/digital-life/nationalists-hopping-great-firewall-attack-hong-kong-protesters-praised-chine se-state-media/article/3023377.

Sixth Tone (2019), *China's VPN Regulations Won't Affect Companies, Official Says*, in "Sixth Tone", 23 September, https://www.sixthtone.com/ht_news/1004591/China'sVPN RegulationsWon'tAffectCompaniesOfficial Says.

Software Freedom Law Centre (2020), *Internet Shutdowns in India*, https://internetshutdowns.in.

H. Suresh (2019), *93 Disruptions in 2019: Are Internet Shutdowns Becoming the New Normal in India?*, in "The News Minute", 17 December, https://www.thenewsminute.com/article/93-disruptions-2019-are-internet-shutdowns-becoming-new-normal-india-11 4273.

B. Taye (2018), *The State Of Internet Shutdowns Around The World: The 2018 #keepiton Report*, in "Access Now", https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf.

L. Teixeira (2019), *China Is Sending Keyboard Warriors Over the Firewall*, in "Foreign Policy", 26 August, https://foreignpolicy.com/2019/08/26/china-is-sending-keyboard-warriors-over-the-firewall.

N. VanderKlippe (2019), *In Encrypted Chats, Hong Kong Protesters Find Support from Mainland China*, in "The Globe and Mail", 22 August, https://www.theglobeandmail.com/world/article-in-encrypted-chats-hong-kong-protesters-find-support-fro m-mainland.

Y. Wang (2014), *人民日报权威论坛：网络主权，一个不容回避的议题--观点--人民网*, in "People's Daily", 23 June, http://opinion.people.com.cn/n/2014/0623/c1003-25183666.html.

K. Werbach (2008), *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, in "U.C. Davis Law Review", 42, 2, pp. 343-412.

T. Wu (2004), *The Balkanization of the Internet,* 17 August, https://www.lessig.org/2004/08/the-balkanization-of-the-inter.

G. Yang (2012), *A Chinese Internet? History, Practice, and Globalization*, in "Chinese Journal of Communication", 5, 1, Mar., pp. 49-54.

S. Yang et al. (2017), *Cross-Strait Frenemies: Chinese Netizens VPN in to Facebook Taiwan*, in "Proceedings of the ACM on Human-Computer Interaction", 1, CSCW, pp. 1-22.

S. Yang, P. Chen (eds.) (2017), *Diba Expedition to Facebook": A Preliminary Study of Massive Online Collective Action in China,* in "iConference 2017 Proceedings", pp. 904-907.

孙晓宇 (2019), *India's Internet Shutdown Shows Normal Practice for Sovereign Countries*, in "People's Daily Online", 17 December, http://global.chinadaily.com.cn/a/201912/17/WS5df8702ca310cf3e3557eb07.html.

ISSN 2283-7949
GLOCALISM: JOURNAL OF CULTURE, POLITICS AND INNOVATION
2020, 1, DOI: 10.12893/gjcpi.2020.1.3
Published online by "Globus et Locus" at https://glocalismjournal.org