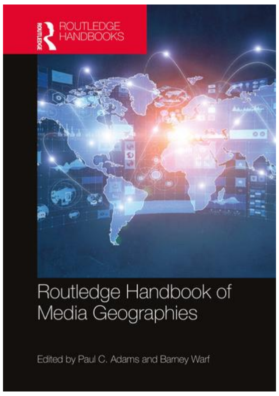

Routledge Handbook of Media Geographies

Paul C. Adams, Barney Warf

Internet censorship

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9781003039068-2
Barney Warf
Published online on: 28 Oct 2021

2 INTERNET CENSORSHIP

Shaping the world's access to cyberspace

Barney Warf

In mid-2021, more than 5.1 billion people used the internet, making it a tool of communications, entertainment and other applications accessed by roughly 65 percent of the world's population (www.internetworldstats.com/stats.htm). For countless numbers of people, cyberspace has become indispensable for entertainment, communications, shopping, bill payments and other uses. Increasingly the boundaries between the real and virtual worlds are evaporating.

Numerous geographers have written about the nature and growth of cyberspace, its uneven social and spatial diffusion, and its multiple impacts, ranging from cybercommunities to digital divides to electronic commerce (Warf 2012; Kellerman 2016). This literature offers a valuable means for spatializing the internet, rooting it in the concrete social and material circumstances that vary across the world, which serves to demolish utopian notions that it is somehow placeless or leads to a "flat earth."

One of the most insidious notions that swirls around cyberspace is that it is an inherently and inevitably emancipatory tool, and thus always serves to undermine authoritarian governments. Ronald Reagan once asserted that "The Goliath of totalitarianism will be brought down by the David of the microchip" (quoted in Kalathil & Boas 2003, 1), and the chair of Citicorp, Walter Wriston (1997, 174), argued that "the virus of freedom… is spread by electronic networks to the four corners of the earth." At times this notion is wedded to libertarian interpretations in which the global community of netizens is seen as a self-governing community in which the state has become largely irrelevant (Goldsmith & Wu 2006). Such views conveniently overlook how the internet can be used against people as well as for them.

In contrast, more realistic assessments take seriously the ability of governments to limit access to the internet, regulate what people can see, and how they wield power against cyberdissidents (Diebert et al. 2008; Diebert 2009; Morozov 2011). Most of the world's governments regulate internet access and contents to one degree or another, although the nature and extent vary widely. Indeed, opposition to censorship and political activism is typically confined to small groups of educated individuals, often diasporas, and has relatively little impact among the masses of their respective states (Kalathil & Boas 2003).

While the geographic literature has delved into issues of geosurveillance and governmentality, it has been largely silent about how governments erect obstacles to internet access as a form of political control (but see Warf 2010). Warf (2009a; 2009b) addressed the geographies of internet censorship in Latin America and the states that comprised the former

DOI: 10.4324/9781003039068-3

Soviet Union, and Warf and Vincent (2007) addressed the marked government restrictions found in the Arab world.

This chapter explores internet censorship in several steps. It opens with an overview of the dimensions of censorship and the various forms that it can take. Second, it offers a broad overview of the geography of global internet censorship. The third part highlights some of the world's most egregious offenders in this regard, while the conclusion summarizes major themes.

Dimensions of internet censorship

Internet accessibility reflects, among other things, incomes, the cost of access, the prevalence of computers (at home, work, and libraries), literacy rates, gender roles, and how willing governments are to allow their populations to utilize cyberspace. Repressive governments typically fear the potential of the internet to allow people to circumvent their monopoly over information. Several geographers have drawn upon Foucauldian conceptions of power to analyze geosurveillance, invasions of privacy and digital panopticons (Dobson & Fisher 2007). These works illustrate that clearly the internet can be made to work against people as well as for them. Rather than being inherently emancipatory in nature, the internet can sustain dominant authorities and be used to track and harass political opponents of the state.

Governments have varying motivations for internet censorship, including: the political repression of dissidents, suppression of civil rights groups, and the prevention of exposure of corruption or publication of comments insulting to the state (e.g. in China, Iran, Myanmar); religious controls to silence ideas deemed heretical or sacrilegious (as found in many Muslim countries); or cultural restrictions that exist as part of the oppression of ethnic minorities (e.g. refusal to allow government websites in certain languages) or sexual minorities. Often internet censorship is done on the ostensible grounds of protecting public morality from pornography or gambling. Preventing terrorism is another favorite rationale, often backed by vague notions of national security.

Governments may limit the *scope* (or range of topics) permitted on the internet and engage in different degrees of intervention, ranging from permitting information to flow utterly unfettered (e.g. Scandinavian states) to essentially prohibiting access to the internet altogether (e.g. North Korea) (Warf 2015). States with highly centralized power structures tend to be the worst internet censors, particularly those run by a single political party (e.g. China, North Korea). Often their policies earn them great enmity not only domestically but internationally as well, and severe censorship can discourage tourism, foreign investment and innovation (Villeneuve 2006).

Internet censorship centers on control over access, functionality and contents (Eriksson & Giacomello 2009). A broad range of methods may be deployed: discriminatory ISP licenses, content filtering based on keywords, redirection of users to proxy servers, rerouting packets destined for a specific IP address to a blacklist, website blocking of a list of IP addresses, tapping and surveillance, chat room monitoring, discriminatory or prohibitive pricing policies, hardware and software manipulation, hacking into opposition websites and spreading viruses, denial-of-service (DOS) attacks that overload servers or network connections using "bot herders," temporary just-in-time blocking at moments when political information is critical, such as elections, and harassment of bloggers (e.g. via libel laws or invoking national security). Content filtering often relies on algorithms that identify target words or phrases, and can adapt as a new lexicon emerges over time. Filtering may occur at the levels of the individual service provider, the domain name, a particular IP address or a specific URL. Most forms of censorship are difficult to detect technically: users may not even know that censorship is in effect. Sometimes governments use foreign (usually American) software for this purpose. For example, the governments of Iran, Yemen, the UAE and Sudan use Secure Computing's SmartFilter, a program produced in the US (Lee 2001; Villeneuve 2006). Once formal censorship begins, there is the inevitable temptation to expand the list of prohibited topics and websites, or what Villeneuve (2006) calls "mission creep."

By far the most common and insidious form of censorship is self-censorship. Users in countries with authoritarian regimes typically know the boundaries of politically acceptable use and rarely cross them. Most are understandably intimidated by the threat of arrest or harassment, or less commonly, fines, for visiting prohibited websites. From the perspective of government authorities, self-censorship is more efficient and effective than brute force. Since the vast majority of internet usage is not for political purposes, only a minority of users are affected in this way.

The degree and type of internet censorship obviously varies widely and reflects how democratic and open to criticism different political systems are. In Scandinavia, censorship is non-existent. In North Korea, internet access is illegal except for a small cadre of Communist Party elites and hackers trained in cyberwarfare (Warf 2015). In between these extremes lies a vast array of states with modest to moderate forms of censorship. These variations reflect the complex geographies of democracy, civil society and governance systems, as well as resistance to authoritarianism in the defense of freedom of speech.

Viewed this way, internet censorship is a contested terrain of social relations. Opposition to censorship often involves a diverse array of social movements, political parties, activists, hackers, bloggers, journalists, labor unions, human rights groups, religious figures, women's rights campaigns and others. Resistance may be successful at times, such as when cyber-activists use anonymizing proxy servers in other countries that encrypt users' data and cloak their identities. Because cyberspace and physical space have become inseparable, the internet simultaneously reflects and in turn shapes the contours of politics. Moreover, this arena is constantly changing in size and scope, reflecting, among other things, rising penetration rates and growing computer literacy, fluctuations in government policies, and variations in popular sentiment. Internet censors and their subjects play a cat-and-mouse game that results in path-dependent, contingent and unpredictable results.

The empirics of global internet censorship

Reporters Without Borders, an NGO headquartered in Paris and one of the world's preeminent judges of censorship, ranks governments across the planet in terms of the severity of their internet censorship (Quirk 2006). Their index of internet censorship is generated from surveys of 50 questions sent to legal experts, reporters and scholars in each country. Thus, countries in northern Europe, the US and Canada, Australia and New Zealand, and Japan exhibit minimal or no censorship (scores less than 10). Conversely, a rogue's list of the world's worst offenders, including China, Vietnam, Myanmar, Iran and Turkmenistan, exhibit the planet's most severe and extensive restrictions (scores greater than 80). Table 2.1 summarizes the distribution of the world's population and internet users according to the level of severity of censorship. Thus, only 13% of the world's people, but a third of internet users, live in countries with minimal censorship; conversely, roughly one-quarter of the world's people and internet users live under governments that engage in very heavy censorship (the vast bulk of whom are located in China).

Most of the world lives under governments that censor the internet. Using the Reporters Without Borders scores, only 2.9% of the planet, and only 4.7% of netizens, lives in countries

Table 2.1 Global population and internet users by severity of internet censorship, 2020

Internet RWB score	*Population (millions)*	*%*	*Users (millions)*	*%*
<10.0	26.8	0.3	25.9	0.6
10.0–19.9	204.2	2.6	186.8	4.1
20.0–29.9	1,270.6	16.3	1,008.5	22.2
30.0–39.9	1,350.6	17.4	759.7	16.7
40.0–49.9	2,691.3	34.6	1,298.6	28.5
50.0–59.9	410.1	5.3	221.2	4.9
60.0–69.9	139.1	1.8	108.8	2.4
70.0–79.9	1,555.2	20.0	930.7	20.5
>80.0	124.9	1.6	9.1	0.2
Total	7,772.7	100.0	4,549.2	100.0

Source: Calculated by author

[a] Reporters Without Borders

with zero or minimal government intervention. These include Scandinavian states, Canada and New Zealand. The majority of the world's people and internet users (68%) live under regimes with moderate levels of censorship (RWB scores 20–50), including Russia, most of the Arab world and parts of Africa. About one-fifth of the world, notably including China, lives under governments that practice extreme censorship.

These broad categories fail to reveal important geographical variations in censorship levels (Figure 2.1), which may be mapped using Reporters Without Borders scores. Most of the world's worst internet censors are located in Asia, including China, Turkmenistan, Vietnam and Iran. The majority are run by Communist Parties, including Cuba, the worst offender in the Western Hemisphere. Censorship is a common tool of totalitarian governments, which tolerate little dissent and fear unfettered lines of communication. The Middle East and Arab world do not fare well, nor does most of Africa. Most Latin American countries are moderate internet censors as well. In contrast, prosperous, stable democracies, including northern Europe, the US, Canada, Japan, Australia and New Zealand, exhibit very low levels of censorship, as does South Africa.

Egregious examples of censorship

While the types and severity of censorship vary widely across the globe, it is worth noting a few of the most extreme examples as a means of understanding the lengths to which governments can go to regulate internet access, the strategies they deploy, and their effects.

Chinese internet users, who numbered roughly 989 million people in mid-2021, face some of the world's greatest restrictions (Roberts 2018; Qiang 2019). The Chinese government has been blunt in its justification for censorship, asserting its necessity to maintain a "harmonious society." It deploys a vast array of measures commonly known as the "Great Firewall," which includes publicly employed internet monitors and citizen volunteers, and screens blogs and email messages for potential threats to the party's hegemony. International internet connections to China operate solely through a selected group of state-controlled backbone fiber networks. Access to common Web services, such as Google and Yahoo!, is heavily restricted (Paltemaa & Vuori 2009). The national government hires commentators,

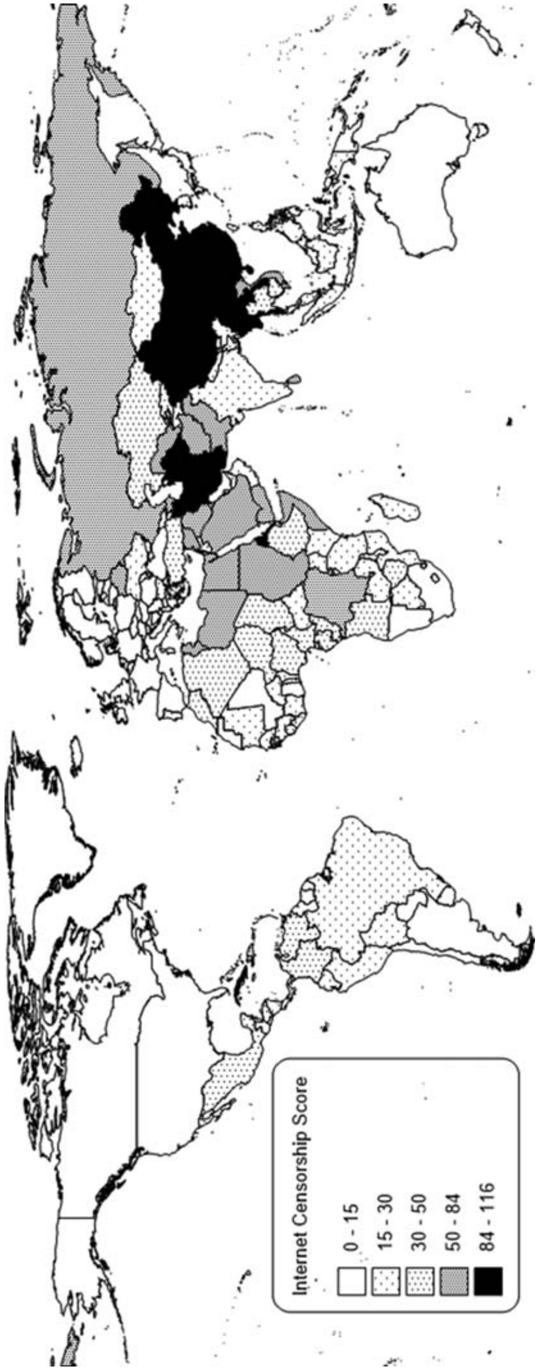

Figure 2.1 Map of internet censorship scores

commonly referred to by the derogatory term the "five-mao party," to monitor blogs and chat rooms, inserting comments that "spin" issues in a way favorable to the Chinese state. Internet service providers censor themselves (Zhang 2020) by monitoring monitor chat rooms, blogs, networking services, search engines and video sites for politically sensitive material in order to conform to government restrictions. Anonymizing websites that help users circumvent censorship are prohibited. Users who attempt to access blocked sites are confronted by Jingjing and Chacha, two cartoon police officers who inform them that they are being monitored. Instant messaging and mobile phone text messaging services are heavily filtered, including a program called QQ, which is automatically installed on users' computers to monitor communications. Blogs critical of the government are typically dismantled within days. Notably, American firms have assisted the Chinese state in this regard (Simonite 2019).

The Great Firewall system began in 2006 under an initiative known as "Golden Shield," a national surveillance network that China developed with the aid of US firms Nortel and Cisco Systems (Lake 2009; Griffiths 2019). It rapidly extended beyond the internet to include digital identification cards with microchips containing personal data that allow the state to recognize the faces and voices of its 1.4 billion inhabitants. Golden Shield has been exported to Cuba, Iran and Belarus. In many respects, China's state-led program of internet development serves as a model for authoritarian governments around the globe.

The Chinese government has periodically initiated shutdowns of data centers housing servers for websites and online bulletin boards, disrupting use for millions. Email services like Gmail and Hotmail are frequently jammed; before the 2008 Olympics, Facebook sites of critics were blocked. In 2007, the State Administration of Radio, Film and Television mandated that all video sharing sites must be state-owned. Police frequently patrol internet cafes, where users must supply personal information in order to log on, while website administrators are legally required to hire censors popularly known as "cleaning ladies" or "big mamas."

China has clashed with foreign parties over its censorship. The government long blocked access to the *New York Times* (Hachigian 2002). Google, the world's largest provider of free internet services, famously established a politically correct website, Google.cn, which censors itself to comply with restrictions demanded by the Chinese state, arguing that the provision of incomplete, censored information was better than none at all (Dann & Haddow 2008). In 2010, Google announced it would no longer cooperate with Chinese internet authorities and withdrew from China altogether. The Chinese government responded by promoting its home-grown search engines such as Baidu, Sohu and Sina.com, which present few such difficulties.

The Chinese state has also arrested and detained internet users and activists who ventured into politically sensitive websites. The state pursues the intimidation strategy popularly known as "killing the chicken to scare the monkeys" (Harwit & Clark 2001). China has incarcerated cyberdissidents and bloggers, and waged intensive campaigns against activists for democracy in Hong Kong, Tibetan independence, Taiwanese separatism, those who investigate the Tiananmen Square massacre, and the religious-political group Falun Gong. However, given the polymorphous nature of the web, such restrictions are inevitably met with resistance. By accessing foreign proxy servers, a few intrepid Chinese netizens engage in *fanqiang*, or "scaling the wall" (Stone & Barboza 2010). Using programmers in the US, Falun Gong has developed censorship-circumventing software called Freegate, which it has offered to dissidents elsewhere, particularly in Iran (Lake 2009). The Chinese state and its opponents are thus engaged in a cat-and-mouse game common across the globe. As one Chinese blogger put it, "It is like a water flow—if you block one direction, it flows to other directions, or overflows" (quoted in James 2009).

Vietnam is another serious internet censor. Only one service provider, Vietnam Data Communications, is licensed for international connections, and it is a subsidiary of the government telecommunications monopoly. Domestic content providers must obtain special licenses from the Ministry of the Interior and lease connections from the state-owned Vietnam Post and Telecommunications Corporation. Like China, the Vietnamese government uses firewalls and encourages self-censorship. Government censors routinely search email for keywords. The government has also imprisoned advocates for internet freedom (International Censorship Explorer 2006). Owners of cybercafés who permit searches of internet sites considered to be "offensive to Vietnamese culture" face stiff fines. Vietnamese bloggers have been routinely harassed and imprisoned. However, recently, in an attempt to curry favor with foreign investors, Vietnam has begun to ease its censorship (Sicurelli 2017).

Likewise, Myanmar operates a highly restrictive censorship regime (Ochwat 2020; Sinpeng 2020). The government uses software purchased from the US company Fortinet to block access to selected websites. At times it has shut down the internet altogether to silence protestors. The state has also tolerated, if not promoted, incendiary attacks on Facebook against the Muslim Rohingya minority (Caryl 2015).

Iran runs a brutal regime that closely monitors internet traffic through its Ministry of Information and Communication Technology (Michaelsen 2018; Yalcintas & Alizadeh 2020). The state uses software purchased from Nokia and Siemens to engage in deep packet inspection of web traffic. The state has blocked access to millions of websites, ostensibly on the grounds of combatting pornography and limiting immoral behavior or that deemed insulting to Islam, reasons that are commonly found throughout the Muslim world. It has arrested numerous bloggers. However, using software developed by Falun Gong, dissidents have found ways to circumvent state controls.

In the Arab world, where censorship of different types has long been practiced, the fascistic regime of Saudi Arabia stands as a particularly offensive case (Pan & Siegel 2020). It has created formidable firewalls to regulate flows of information and banned access to millions of webpages. All internet service providers with international connections must go through the government-owned King Abdul Aziz City for Science and Technology, which uses Smart-Filter software developed by the US company Secure Computing. The government has imprisoned and tortured activists and blocked sites associated with Shia rights and the Muslim Brotherhood (Pan & Siegel 2020).

Vladmir Putin's Russia is another heavy-handed censor of the internet (Ognyanova 2015; Maréchal 2017; Soldatov 2017). Putin long regarded the internet as an avenue for the promotion of American interests inside his country, and upheld censorship as a path toward "information sovereignty" (Nocetti 2015). The state's internet surveillance law, the System for Operational-Investigative Activities, allows security services unfettered physical access to ISPs. The government also promotes websites that offer views supportive of its policies and fosters networks of nationalist bloggers.

Belarus, whose government Reporters Without Borders called one of the world's "bitterest enemies of the Internet," likewise rules the net with an iron fist (European Federation of Journalists 2018). In 2010, President Alexander Lukashenka officially imposed censorship to combat "anarchy on the internet," a move the European Union called, in a classic bit of understatement, a "step in the wrong direction." All service providers are required to connect through Belpak, a subsidiary of the state-controlled ISP Beltelecom. The government occasionally stations troops at cybercafés, where users must register their names, and launches denial-of-service attacks against opposition party websites. Newspapers critical of the state have had their websites blocked by the Ministry of Information.

Another former Soviet republic, Turkmenistan, is also a severe internet censor; Reporters Without Borders lists it as an "internet enemy." For years private internet cafes were illegal, although the government monopoly Turkmen Telecom operated a handful of them, with troops stationed at the front (Eurasianet 2007; Reporters Without Borders 2009). The state-owned monopoly, Turkmentelecom, keeps a list of blacklisted internet undesirables, and regularly blocks their IP addresses. The state's use of deep packet inspection goes without saying.

In the Americas, Cuba stands out as the worst internet censor. For years, individual access to the internet was essentially prohibited (Kalathil & Boas 2003), and the state only grudgingly began to allow access starting in 2006. A limited infrastructure and high prices remain a serious access problem for many. The state has used Avila Link software to monitor users, which it may have obtained from China. It has also harassed dissidents, such as the famous blogger Yoani Sánchez.

Concluding thoughts

Early accounts of the internet celebrated its emancipatory potential, particularly the ways in which it allowed billions of people unfettered access to information and permitted them to bypass government monopolies. The reality has been much more sobering. Many governments have become adept at monitoring and controlling digital data flows (Mozorov 2011). Relatively few countries, and only a small minority of the world's netizens, permit unfettered access to the web. Most states control their residents' access to the internet and its contents. Restrictions can vary from invisible filters to the imprisonment of dissidents and bloggers. American and European companies have played tragic but important roles in this process: there is profit to be made in selling software to unsavory regimes (China plays this game too). And of course, self-censorship is likely the most pervasive form of internet regulation of all. The notion of the "dictator's dilemma," which posits that totalitarian states must choose between censorship and economic stagnation, is thus false; many authoritarian regimes can have it both ways.

These comments serve as a sobering reminder that new technologies rarely, if ever, live up to early utopian expectations. The class mistake is to herald such events as uniformly positive. Yet the reality of internet censorship testifies that it is a serious error to underestimate the flexibility of governments in regulating cyberspace. Many repressive regimes, such as China's, are impervious to international criticism on this account. Hopes for overcoming and reducing censorship, therefore, often lie in the networks of rhizomic resistance that invariably form when the state curtails freedoms of online expression. Dissident groups, Falun Gong, human rights activists, religious parties, expatriate communities and others have long played major roles in combating censorship.

References

Caryl, C. 2015. Burma gives a big thumbs-up to Facebook. *Foreign Policy Online* (November 13). https://foreignpolicy.com/2015/11/13/burma-gives-a-big-thumbs-up-tofacebook/.

Dann, D., and Haddow, N. 2008. Just doing business or doing just business? Google, Microsoft, Yahoo! and the business of censoring China's internet. *Journal of Business Ethics*, 79 (3), 219–234.

Deibert, R. 2009. The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In H. Andrew and P. Chadwick (eds.) *The Routledge handbook of internet politics*. pp. 212–226. London: Routledge.

Deibert, R., Palfrey, J., Rohozinski, R., and Zittrain, J. (eds.) 2008. *Access denied: The practice and policy of global internet filtering*. Cambridge, MA: MIT Press.

Dobson, J., and Fisher, P. 2007. The panopticon's changing geography. *Geographical Review*, 97 (3), 307–323.

Eriksson, J., and Giacomello, G. 2009. Who controls what, and under what conditions? *International Studies Review*, 11, 206–210.

Eurasianet.org. 2007. *In Turkmenistan, internet access comes with soldiers*. www.eurasianet.org/departments/insight/articles/eav030807.shtml.

European Federation of Journalists. 2018. *Belarus: More media censorship and control with new amendments of the Media Law*. https://europeanjournalists.org/blog/2018/06/24/belarus-more-media-censorship-and-control-with-new-amendments-of-the-media-law/.

Goldsmith, J., and Wu, T. 2006. *Who controls the internet? Illusion of a borderless world*. New York: Oxford University Press.

Griffiths, J. 2019. *The Great Firewall of China*. London: ZED.

Hachigian, N. 2001. China's cyber-strategy. *Foreign Affairs*, 80 (2), 118–133.

Harwit, E., and Clark, D. 2001. Shaping the internet in China: Evolution of political control over network infrastructure and political content. *Asian Survey*, 41 (3), 377–408.

James, R. 2009. A brief history of Chinese internet censorship. *Time* (March 18). www.time.com/time/world/article/0,8599,1885961,00.html.

Kalathil, S., and Boas, T. 2003. *Open networks, closed regimes: The impact of the internet on authoritarian rule*. Washington, DC: Carnegie Endowment for International Peace.

Kellerman, A. 2016. *Geographic interpretations of the internet*. Dordrecht: Springer.

Lake, E. 2009. Hacking the regime. *The New Republic* (September 3), www.tnr.com/article/politics/hacking-the-regime.

Lee, J. 2001. Companies compete to provide Saudi internet veil. *New York Times* (November 19), p. A1.

Maréchal, N. 2017. Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy. *Media and Communication*, 5 (1), 29–41.

Michaelsen, M. 2018. Transforming threats to power: The international politics of authoritarian internet control in Iran. *International Journal of Communication*, 12, 3856–3876.

Morozov, E. 2011. *The net delusion: The dark side of internet freedom*. New York: PublicAffairs.

Nocetti, J. 2015. Russia's' "dictatorship-of-the-law" approach to internet policy. *Internet Policy Review*, 4 (4), 1–19.

Ochwat, M. 2020. Myanmar media: Legacy and challenges. *The Age of Human Rights Journal*, 14, 245–271.

Ognyanova, K. 2015. In Putin's Russia, information has you: Media control and internet censorship in the Russian Federation. In M. M. Merviö (ed.) *Management and participation in the public sphere* (pp. 62–79). Hershey, PA: IGI Global.

Paltemaa, V., and Vuori, J. 2009. Regime transition and the Chinese politics of technology: From mass science to the controlled internet. *Asian Journal of Political Science*, 17 (1), 1–23.

Pan, J., and A. Siegel. 2020. How Saudi crackdowns fail to silence online dissent. *American Political Science Review*, 114 (1), 109–125.

Qiang, X. 2019. The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy*, 30 (1), 53–67.

Reporters Without Borders. 2009. *Internet enemies*. www.rsf.org/en-ennemi26106-Turkmenistan.html.

Roberts, M. 2018. *Censored: Distraction and diversion inside China's Great Firewall*. Princeton, NJ: Princeton University Press.

Sicurelli, D. 2017. The conditions for effectiveness of EU human rights promotion in non-democratic states: A case study of Vietnam. *Journal of European Integration*, 39 (6), 739–753.

Simonite, T. 2019. *US companies help censor the internet in China, too*. www.wired.com/story/us-companies-help-censor-internet-china/.

Sinpeng, A. 2020. Digital media, political authoritarianism, and internet controls in Southeast Asia. *Media, Culture & Society*, 42 (1), 25–39.

Soldatov, A. 2017. The taming of the internet. *Russian Social Science Review*, 58 (1), 39–59.

Stone, B., and Barboza, D. 2010. Scaling the digital wall in China. *New York Times* (January 16), p. B1.

Villeneuve, N. 2006. The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. *First Monday*, 11 (1–2). https://journals.uic.edu/ojs/index.php/fm/article/download/1307/1227. Warf, B. 2009a. Diverse spatialities of the Latin American and Caribbean internet. *Journal of Latin American Geography*, 8 (2), 125–146.

Warf, B. 2009b. The rapidly evolving geographies of the Eurasian internet. *Eurasian Geography and Economics*, 50 (5), 564–580.

Warf, B. 2010. Geographies of global internet censorship. *Geojournal*, 76 (1), 1–23.

Warf, B. 2012. *Global geographies of the internet*. Dordrecht: Springer.

Warf, B. 2015. The hermit kingdom in cyberspace: Unveiling the North Korean internet. *Information, Communication and Society*, 18 (1), 109–120.

Warf, B., and Vincent, P. 2007. Multiple geographies of the Arab internet. *Area*, 39, 83–96.

Wriston, W. 1997. Bits, bytes, and diplomacy. *Foreign Affairs*, 76 (5), 172–182.

Yalcintas, A., and Alizadeh, N. 2020. Digital protectionism and national planning in the age of the internet: The case of Iran. *Journal of Institutional Economics*, 16 (4), 519–536.

Zhang, C. 2020. Who bypasses the Great Firewall in China? *First Monday*, 24 (1). https://firstmonday.org/ojs/index.php/fm/article/download/10256/9409#author.