***Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, Abingdon, UK: Routledge, 2019, pp. 81-99.**

CHAPTER 5

Mutual Entanglement and Complex Sovereignty in Cyberspace

Ronald J. Deibert and Louis W. Pauly

Contributor information:

Ronald J. Deibert is Professor of Political Science and Director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy.

Louis W. Pauly is the J. Stefan Dupré Distinguished Professor of Political Economy in the Department of Political Science at the University of Toronto. He is cross-appointed to the Munk School of Global Affairs and Public Policy.

Abstract (150 words):

Although state authorities around the world are trying to counter and deflect digital attacks from abroad, they are also projecting their own power externally through open electronic networks. The systemic outcome today is well-described as mutual entanglement. Mounting evidence suggests that efforts to bring digital networks back under territorial control are undercut by operations designed to use those networks for domestic surveillance and external security. In the end, re-territorialization strategies in cyberspace are self-limiting. The mutual entanglement characteristic of cyberspace today profoundly complicates state strategies aimed at either anarchical fragmentation or unquestioned hegemony (where rules are set by a dominant power).

Keywords (5): Internet; cyberspace; digital networks; OpenNet Initiative; cyber-security

When the Internet first emerged, many predicted that it would present a major challenge to the power of states in general and to the effective control of authoritarian states in particular (Johnson and Post 1996). More recent commentary has emphasized the opposite: that the Internet expands and intensifies the capacities of states within and across conventional territorial boundaries. While we now see clearly how social media and other digital technologies have empowered non-state actors in civil society, the verdict is quite mixed as to their ultimate impact on the sovereign authority of the state.[1]

Domestic-level information controls are today reinforced by norms promoted by states like China and Russia that try to shift governance away from multi-stakeholder or pluralist models toward more state-centric approaches. Even liberal democratic countries have lately been moving in the direction of territorially-defined policies of cyberspace governance through laws aimed at data localization and through the establishment of "cyber commands". While efforts to re-territorialize cyberspace are undeniable, the extent to which states depend on mutual restraint to project power in and through cyberspace has been obscured. Extraterritorial projections of state power in this sphere are expanding, deepening, and becoming more elaborate. The most extensive of these projections come from the United States, but even the most autocratic regimes associated with efforts to promote "Internet sovereignty" today rely on the openness of cyberspace.

States are exercising extraterritorial power to acquire data about the world around them: to anticipate, analyze, and interdict threats; to shape the strategic environment to their advantage; to promote their interests via the movement of goods and services, information, and capital. They are also using new communication technologies to broaden military command and control systems. The combined if not fully intended "network effect" of such extensive projections of power in and through cyberspace is to frustrate individual strategies aimed at territorial insulation. This effect today is well-described as mutual entanglement (Nye 2017). The capacity of states to project power domestically and extraterritorially rests on the material opportunities opened up by cyberspace itself, and that openness thwarts efforts to build impenetrable border controls. As states aim to shape cyberspace to their strategic advantage, their governance domains both expand and contract. Specific policies are continually being reconfigured in a dynamic if not necessarily symmetrical context of interaction. The legitimacy of those policies may be contested, but they rest on an apparently adequate degree of acquiescence internally and externally.

Drawing from recent research into state espionage and targeted digital attacks, as well as evidence now in the public domain from the Edward Snowden disclosures that cannot be ignored, this chapter provides an overview of extraterritorial projections of state power in and through cyberspace, from the United States to cases involving highly opaque autocratic regimes. This evidence suggests that efforts to bring digital networks back under territorial control are undercut by operations designed to use those networks for domestic surveillance and external security. In the end, re-territorialization strategies in cyberspace are self-limiting. The chapter concludes by sketching implications for sovereign authority in a dynamic system. The mutual entanglement characteristic of cyberspace today profoundly complicates state strategies aimed at either anarchical fragmentation (where no one sets governing rules) or unquestioned hegemony (where rules are set by a dominant power) (Ruggie 1993; Deudney 2007).

The Territorialization Impulse in Cyberspace

The OpenNet Initiative (ONI) – a university-based research project using a mixed methods approach to documenting Internet censorship – has conceptualized state power over cyberspace

within territorial boundaries in "generational" terms (Deibert 2015; Deibert and Rohozinski 2008). First generation controls refer to defensive Internet censorship systems erected at national borders, with governments restricting their citizens' access to online resources, the Great Firewall of China being the archetypal example. Internet filtering typically involves special software or hardware placed at key network chokepoints that inspect requests for web content, blocking those that are restricted from reaching their destinations. ONI tested for national-level Internet filtering in more than 70 countries and found evidence in more than 45 (Deibert et al. 2008; 2010; 2012). The number is likely expanding quickly, since many countries have begun censoring content involving the sexual exploitation of children, hate speech, and terrorist threats.

Second generation controls refer to government measures to control cyberspace domestically through laws, policies, and other sorts of Internet policing, often undertaken with the cooperation, coercion, or co-optation of private companies. Examples include content removal requests, compelled access to customer data, and the application of defamation or libel laws to Internet content. Sometimes second-generation controls are applied secretly, making documentation challenging for researchers. Occasionally we see glimpses of these controls through the window of private sector transparency reports, such as those published by Google, Microsoft, or Twitter. The remarkable Vodafone Law Enforcement Disclosure Report, for example, extensively documented country-by-country requests for customer data (Vodafone 2014). Researchers have also employed reverse engineering methods to uncover hidden surveillance or censorship functions built inside popular applications, such as the surveillance embedded inside the Chinese version of Skype (Dalek et al. 2015; Knockel, McKune and Senft 2016; Knockel, Senft and Deibert 2016; Villeneuve 2008). It is accurate to say that second-generation controls have become more complex, penetrating deeper into civil societies and filtering communications through a thicket of rules, laws, and practices.

Third generation controls refer to the use by states of more "offensive" methods, such as targeted surveillance, digital espionage, and disinformation campaigns. If first generation controls sought to bolster borders, and second generation controls deepened the internal reach of state agencies, third generation controls are projected outwards. Although varying in resources and capabilities, many governments' armed forces and intelligence agencies have developed aggressive external operations. Growing demand for offensive capabilities has produced a rapidly expanding market for computer network attack and surveillance products and services developed by private companies. These firms range from Cold War giants like Raytheon and Northrop Grumman to more obscure "niche" entities, like Italy's Hacking Team, the UK's Gamma Group, or the Israeli "cyber warfare" company, the NSO Group (Harris 2014). The overall industry is growing at an annual rate of 24% per year and will likely exceed USD $600bn in annual revenue by 2023 (Stiennon 2016).

Across all three generations, cyber security has risen to the top of policy agendas, driven by repeated instances of large scale data breaches, vulnerabilities to critical infrastructure, competitive issues, and domestic political concerns (Deibert and Rohozinski 2010). To the three generations of controls, moreover, might be added a fourth: the efforts of some states to

negotiate governance agreements at regional and international levels. Over the last several years, for example, a coalition of like-minded countries led by China and Russia, using the rhetoric of "Internet sovereignty" and leveraging the opportunity presented by the Snowden disclosures, has sought to move governance practices away from what they perceive as its current US-dominated system to one centered around the United Nations and organizations like the International Telecommunications Union (Deibert and Crete-Nishihata 2012).

Predictions of Internet "fragmentation" and a retreat toward "Cyber Westphalia" have become prominent (Demchak and Dombrowski 2011; Dombrowski 2016). Different sources have specifically been identified: filtering and blocking websites, social networks or other resources offering undesired contents; attacks on such networks and resources; digital protectionism blocking users' access to and use of key platforms and tools for electronic commerce; centralizing and terminating international interconnections; attacks on national networks and key assets; local data processing and/or retention requirements; architectural or routing changes to keep data flows within a territory; prohibitions on the transborder movement of certain categories of data; strategies to construct nationally bounded "Internet segments"; and international frameworks to legitimize restrictive practices (Drake, Cerf and Kleinwächter 2016).

Of these, the so-called "data localization" trend accelerated by specific reactions to the Edward Snowden disclosures is worth special emphasis. Those disclosures revealed intensive electronic intelligence-gathering by the U.S. National Security Agency (NSA) and its close allies. In reaction, many others began insisting on the holding of local data inside national jurisdictions and tightly restricting transborder processing for certain classes of data. Whether such restrictions can actually prevent effective surveillance or, in the case of official investigations, reduce reliance on cumbersome mutual legal assistance treaties (MLAT), is questionable. They also raise obvious concerns that their true intent may be more domestic in nature.

In hindsight, given the externalities around Internet communications (now used by well over 3 billion people on a daily basis worldwide), the impulse behind expanding state control efforts was foreseeable. It now seems inevitable that states would be ever more focused on trying to shape information environments quickly becoming integral to all aspects of society, from the cultural to the economic and political. Among other things, high-profile terrorist acts certainly encouraged citizens to demand such efforts. As obvious as such an impulse may now seem, however, its implications should not be exaggerated. It constitutes only one dimension of a complex process involving the extraterritorial projection of power by other states in and through cyberspace itself. The next sections surveys recent research illustrative of that process and its consequences.

The United States and the Transformation of Cyberspace

The contemporary cyber-security policies and practices of the United States offer the clearest example of extraterritorial power projection. The American defense of a borderless, open

internet may simply be depicted as based entirely on liberal values and ideals, and conveniently contrasted with "territorializing" processes of states that oppose this agenda. The US posture is actually more complicated. Its "Internet freedom" agenda is arguably more a function of interests than values. It is in many ways a discursive or ideological support for the projection of US power in global cyberspace. In this respect, it is analogous to the US position on treating the oceans and outer space as a "commons". The free movement of information globally (just as with free navigation of navies and satellites, and to a lesser degree, aircraft) serves global hegemonic power, not because US policymakers believe in the ideal of the open commons (although some very well might) but because sustaining a position of dominance depends on the ability to move goods, services, information, and capabilities across cyberspace.

US power projection is also connected both to long-term interests and to a changing threat environment. The US now operates nearly 800 military bases in more than 70 countries and territories worldwide (Vine 2015). This extended footprint is woven together by a bristling infrastructure of digital communications, today including 131 government and 149 military satellites in orbit as well as another 273 US-owned commercial satellites (Union of Concerned Scientists 2016). The Pentagon alone operates around 7,000 unmanned aerial drones (Friends Committee on National Legislation 2015). Today a Hellfire missile strike from a US Predator drone is guided by earth-orbiting global positioning satellites (GPS) to within a few metres of its target. The missile is typically fired by an operator based in a hangar in the mainland US, working on computer screens onto which are projected high-resolution images beamed back instantly by advanced imaging sensors.

Such technological advances, of course, track the emergence of the United States as a global superpower. They were preceded by the development of the Internet itself and by earlier innovations in telecommunications, including undersea cables and digital computing systems now global in scope (Starosielski 2015). The United States, in fact, enjoys a distinct "home field advantage" with respect to much of the geopolitics of cyberspace. Most of the Tier 1 telecommunications companies that operate the backbone of the earth's communications systems are headquartered in the United States; the largest software, social media, device, and Internet service providers are still mostly American (Deibert 2012). As a result, many firms can be compelled or quietly enlisted into US government policing and intelligence efforts – a lesson not lost on other governments. One of the more interesting consequences of the Snowden disclosures, however, has been the rolling out of consumer level end-to-end encryption by US-based companies. The consequence is to deepen and extend global networks and frustrate policies aimed at strict data localization.

US intelligence agencies have long reached directly into networks physically based outside their territorial jurisdiction. Officials and their helpers can penetrate or exploit vulnerabilities at critical nodes in the global flow of communications through remote access to cables, servers, routers, wireless networks, and Internet Exchange Points (IXPs). In this regard, switches and other hardware shipped overseas are hardly invulnerable, and encryption standards through international standard setting bodies are malleable.

Consider just one very important NSA program, codenamed XKEYSCORE. XKEYSCORE provides a portal for analysts into the massive amounts of digital electronic communication data that are vacuumed up from access points around the world. The Snowden disclosures indicated that as of the late 2000s, XKEYSCORE-accessible communications data included not only emails, chats and web-browsing traffic, but also pictures, documents, voice calls, webcam photos, web searches, advertising analytics traffic, social media traffic, botnet traffic, logged keystrokes, computer network exploitation (CNE) targeting, intercepted username and password pairs, file uploads to online services, Skype sessions and more (Marquis-Boire, Greenwald, and Lee 2015). At that time, XKEYSCORE involved at least 700 servers in 150 field sites across a wide array of countries.

Observers commonly note that such programs suggest only that the United States is an exceptional power. That ignores, however, the experience of all 'arms races' in history. US innovations in SIGINT practices are closely followed by its key allies. Second and third tier partners may be expected to emulate them, and eventually so too will competitors. The Snowden disclosures may have accelerated this process, providing a "blueprint" of elite SIGINT techniques and practices that others surely now strive to imitate.

It is important to recognize that U.S. power projection in and through cyberspace is already partially coordinated through a long-standing and deeply institutionalized alliance system, most commonly referred to as the "Five Eyes," a partnership among the SIGINT agencies of the United Kingdom, Canada, New Zealand, and Australia. While Anglo-American history and culture, certain common political institutions and governing practices, and the experience of the Second World War still underpin the alliance, geography also accounts for much of its continuing vitality (Katzenstein 2012). The five agencies extensively exchange intelligence that ensures seamless coverage over the vast majority of international signals and telecommunications traffic. The United Kingdom alone remains a major hub for global flows of information to and from Europe, the Middle East, Asia, and the United States. Undersea cables terminate on its southwestern and eastern shores, while other linkages, including longstanding financial networks, connect it to the rest of the world. Canada (historically focused on North America and the Arctic) and Australia and New Zealand (focused on Asia-Pacific) provide their own regional complements. In recent decades, prompted by terrorist threats, other security concerns, and common economic interests, the Five Eyes have intensified collaboration with concentric rings of other states, including Denmark, France, Netherlands, Norway and then Germany, Belgium, Italy, Spain, and Sweden. In terms of actual practices of deep intelligence-sharing sufficient to construct what international relations scholars call a "security community", it makes sense today to talk about a collaborative arrangement involving at least "Fourteen Eyes".

The Extraterritorial Projection of Autocratic Power

Intense concerns about Internet fragmentation today typically center on the policies of a growing number of authoritarian regimes. Early predictions that the Internet would contribute to the demise of these forms of political rule were clearly misplaced. Autocratic governments

have proven to be adept at building sweeping information control systems. Indeed, there are many characteristics of digital technologies – biometric databases, commercial spyware, and deep packet inspection systems – that can facilitate centralized rule. The publicity around the Snowden disclosures, moreover, may have accelerated moves to emulate controls pioneered by democratic states. In any event, there is no doubt that authoritarian government interference in Internet traffic – from content filtering to complete disruption of services – has become commonplace (Gunitsky 2015). Re-territorialization strategies, though, have to be viewed with skepticism.

China has commonly been seen as the progenitor for a new paradigm aimed at closing or tightly controlling cyberspace. It employs all three generations of information controls, from its Great Firewall blocking access to websites and services hosted outside of China's borders, to its extensive, legally mandated system of social media controls imposed on domestic Internet service companies and providers. Companies employ thousands of individuals whose jobs are to censor posts on popular social media and other communications platforms. Many engineer their systems with surveillance functionalities, and all locally based companies are required to share user data with state security services upon request. Internationally, China pushes an agenda to build a new Internet governance regime assigning priority to state sovereignty and 'non-interference'.

Nevertheless, China has not been able to hide its own extraterritorial reach. Its external operations are most evident in vast and well documented cyber espionage campaigns, which include both global targets and an extensive transnational network of command and control servers based outside of China's jurisdiction. The US security company Mandiant (n.d.), for example, traced one of many major China-based campaigns. Known as APT1 ("Advanced Persistent Threat 1") and involving 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries, it has been convincingly linked to a unit of the People's Liberation Army.

Apart from its extraterritorial projection of power through electronic espionage campaigns, China also has extensive transnational reach through its telecommunication and software industries. Huawei, the largest telecommunications equipment manufacturer in the world, has engineered routers that by accident or design allow unauthorized access (Blue 2012). Researchers have documented, through reverse engineering techniques, massive privacy and security vulnerabilities in several China-manufactured applications, including UC Browser, QQ Browser, and Baidu Browser. UC Browser is used by 500 million people, many outside of China. Baidu Browser's software development kit, essentially a suite of code, has been adopted in tens of thousands of other applications that themselves have been downloaded hundreds of millions of times outside of China, which means that the same data collected by Baidu Browser and sent back to Baidu's servers, for possible sharing with Chinese authorities, is sent in the same way. Although there is no publicly available evidence connecting these privacy and security vulnerabilities directly to Chinese state agencies, the mere collection of such fine-grained information, coupled with well-established data retention and sharing practices inside Chinese industries, means the effect is the same. Non-Chinese national users

of these applications know or should know that they are exposed to surveillance by Chinese authorities (VanderKlippe 2016). It is highly probable that China's state security organs are harvesting this information, much the same way the Five Eyes harvest information collected by western companies.

One of the more remarkable examples of China's extraterritorial projection of power in cyberspace is the "Great Cannon", a digital attack tool co-located in China's Great Firewall. It was discovered and documented by researchers at the University of Toronto's Citizen Lab in collaboration with computer scientists at UC Berkeley and Princeton University (Marczak, Weaver et al 2015). After reports emerged of denial-of-service attacks targeting the websites of overseas critics of the Chinese government, the researchers used several network measurement techniques to document this new attack tool. They named it the Great Cannon because it repurposes a random set of external requests for access to websites inside China and then deploys them as packets in attacks aimed at overseas websites. Functionally speaking, the Great Cannon effectively "shoots" such requests back and thereby overwhelms servers located outside of China that Chinese operators wish to silence. The very nature of the attack tool – operating at the international gateway where China's domestic networks connect with networks abroad – points to the complex ways in which territorial impulses and transnational flows of information are necessarily entangled in the contemporary practice of digital power projection.

At the same time that Chinese authorities seek vigorously to defend their Internet borders, they also are pragmatic about the need to accommodate transnational data flows, principally for economic reasons (Lindsay 2015a). The Great Firewall of China therefore remains porous by intention. To cite just one example, CloudFlare, a US-based cyber-security firm recently entered into a "virtual joint venture" with Chinese web-services firm Baidu to create a unified network that makes foreign websites more easily accessible in China and allows Chinese sites to run in destinations outside the country (Mozur 2015). While the agreement may seem orthogonal to the regime's interests in strictly defending its territorial boundaries, it is perfectly congruent with the pragmatic approach the country's elites actually take to encourage economic growth. Digital networks are seen as essential in that regard, but so too are countervailing efforts to restrict the exchange of ideas that run contrary to one-party rule or that touch on taboo topics, such as religious freedom, regional autonomy, democracy, and human rights.

China's tech companies have no choice but to participate in this balancing act. The popular chat application, WeChat, provides a prominent case in point. With 806 million monthly active users, it is the most popular such application in China and the fourth largest in the world. Citizen Lab researchers undertook several controlled experiments using combinations of China, Canada, and U.S. registered phone numbers and accounts to test for Internet censorship on WeChat's platform (Ruan et al. 2016). They found substantial censorship on WeChat but split along several dimensions. There is keyword filtering for users registered with a mainland China phone number but not for those registering with an international number. However, once a China-based user has registered with a mainland China phone number, censorship tools follow them around — even if they switch to an international phone number, or work, travel,

or study abroad. In what appears to be a complete subversion of the Cyber Westphalia thesis, a company tethered to the Chinese state is projecting an Internet censorship regime far beyond China's sovereign jurisdiction.

Another vivid illustration of China's extraterritorial projection of power into cyberspace is its ambitious, though byzantine and secretive, national space program. Since it launched its first satellite in 1970, China now has 177 satellites in orbit, second only to the United States (568) and surpassing Russia (133). These satellites include those whose purpose is communications, navigation, civil defense, remote sensing and surveillance, as well as science, and environmental monitoring. China also has a manned space program and ambitions to land a man on the moon by 2023. One of the cornerstones of China's space program is commercial launching capabilities, much of which have implications for the future of cyberspace. Its Long March (Chang Zheng) family of rockets is responsible for 155 satellites currently in orbit, second only to the Ariane family operated by a European consortium of countries (which is responsible for 200). That the supposed archetype of Cyber Westphalia is also one of the world's leading purveyors of satellite-based global monitoring systems underscores the need for conceptual adjustment.

Iran is another country often cited as a prime mover in the fragmentation of the Internet, but its actual practices too are more complicated in nature. The country has one of the most extensive national Internet filtering systems, and its controls embody all three generations outlined earlier. In recent years, the country has created several new agencies to oversee information controls, including the Supreme Council of Cyberspace, the Cyber Army, the Committee Charged with Determining the Instances of Offensive Content, and the Cyber Defense Command. Iran has been developing plans and gradually rolling out technology for a national Intranet walled off from the global Internet, called the "Internet E-Paak" or "clean Internet". It routinely throttles bandwidth to slow down connections to virtual private networks and circumvention tools around major events, like elections (Citizen Lab and ASL19 2013; Small Media 2015). Iran has even collaborated with China, and Chinese companies, on its domestic information controls regime. China's ZTE reportedly sold Iranian telecommunications carriers sophisticated equipment capable of monitoring backbone level communications and intercepting emails, and SMS, telephone calls (Stecklow 2012).

Yet Iran also employs a fairly advanced cyber espionage capability that is used to target state adversaries and to gather information on dissidents and human rights campaigners in the global Iranian diaspora. One of the cyber espionage campaigns attributed to the Iranian government, called Newscaster (Ward 2014), exploited several Internet and social media services to target 'senior U.S. military and diplomatic personnel, congressional personnel, Washington-based journalists, American think tanks, defense contractors in the United States and Israel, as well as vocal supporters of Israel. Newscaster worked by creating fake social media accounts, linking to targets, and then sending spear-phishing emails containing documents embedded with malicious software, which were then used to harvest private email and log-in credentials. Citizen Lab researchers have documented a similar Iranian-based spear-phishing campaign to

trick users into giving up their credentials to Gmail accounts, even bypassing Google's two-factor authentication security measures (Scott-Railton and Kleemola 2015).

The actions of Iran in cyberspace are thus a continuation of what Iran has long been doing in more conventional terms. For example, as part of clandestine intelligence support for the Assad regime in Syria, Iran has likely assisted in the organization of targeted digital attacks on the opposition (Regalado, Villeneuve and Scott-Railton 2015). Alongside the flow of finances, weapons, and strategic intelligence to Hezbollah, Iranian intelligence may also have supplied eavesdropping and other information warfare technology leading up to and during the 2006 attacks on Israel (Cordesman, Sullivan, and Sullivan 2007; Wege 2012). After American and Israeli-organized Stuxnet targeting of its nuclear centrifuges, Iran may have repurposed the same malware to target the computers of Saudi Arabia's Aramco refineries (Zetter 2014). To depict Iran as a model of Cyber Westphalia thus obscures the extent to which it has its own elaborate outward-facing digital strategy.

Also like China, as much as Iran wants to limit and contain the free inward flow of information, it depends on transborder communications for a myriad of commercial exchanges (Howard, Agarwal and Hussain 2011). Consider the practical trade-offs confronting Iran in its efforts to throttle access to certain VPNs used to circumvent Iranian firewalls. Traditionally, such circumvention has come at a price: connections to banking and other financial services using the same encryption protocols have been disrupted, to the chagrin of Iranian businesses and elites. Researchers have therefore observed Iranian information controls becoming much more fine-grained and precise, targeting the specific protocols associated with popular VPNs while limiting collateral damage to https connections associated with financial exchanges. This evolution of information controls shows both a maturation of techniques but also clear evidence of the importance of both licit and illicit trans-border traffic to the Iranian economy. Actual Iranian practices suggest a nuanced balancing act, but a robust and deepening international engagement in cyberspace.

Russia presents a similar case. Under the reign of Vladimir Putin, the country has gradually reverted to authoritarian rule, part of which includes a tightening grip on information within Russian territory. A major impetus behind these controls was the 2011 anti-government protests, organized through social media, which took Russian authorities by surprise. In order to contain future demonstrations of this sort, Russian authorities pressured Internet companies to comply with Russian government policies. Today, Russia evinces all of the elements of 'Cyber Westphalia' -- sweeping data localization laws imposed on foreign Internet giants like Facebook, Google, Twitter, and LinkedIn, a broadening Internet censorship regime, arrests and intimidation of independent media and bloggers, and an architecture of wholesale mass surveillance undertaken by the installation of equipment at telecommunications companies, known as the SORM system (Soldatov and Borogan 2015). Russia and China, moreover, have cooperated on information controls: in April 2016, Russia hosted the first Russia-China cyber security forum to share strategies and best practices. The meeting included Lu Wei, head of China's State Internet Information Office and Fang Bixang, the man widely thought to be the "father" of China's Great Firewall.

As in the cases of China and Iran, however, Russia's information controls are not limited by its territorial boundaries. Russia's approach to cyberspace is instead highly elaborated. It is a key part of a larger geopolitical strategy that includes industrial scale cyber espionage and targeted digital attacks, sophisticated propaganda and disinformation campaigns through state-controlled media organs, and the extension of Russian equipment, technology and know-how to former client states, particularly in the countries of the former Soviet Union. For example, many members of the Commonwealth of Independent States have in place a SORM-compliant system of mass surveillance, the technical equipment for which is shared by Russian security services. Russian manufactured telecommunications routers are deployed throughout Asia and may contain hidden surveillance functions engineered by design to allow Russian interception. CIS countries also coordinate their cyber security strategies through regional forums like the Shanghai Cooperation Organization, the SCO, which also includes China, Iran, and Pakistan. The SCO have developed collective approaches to repelling social media inspired protests, which are typically framed by the rubric 'counter-terrorism'.

Russia is widely considered to be a tier-one cyber espionage power connected to many international cyber espionage campaigns. It is assumed, moreover, that Russian SIGINT makes use of the talented organized criminal groups that have long flourished in Russia and whose skills are connected to thriving science, technology, engineering and mathematics programs. The use of organized crime for offensive cyber operations is a convenient way to reap the benefits of such attacks while providing a cloak of plausible deniability, as evidenced in Estonia in 2007 and Georgia in 2008 (Deibert, Rohozinski and Crete-Nishihata 2012).

What we do know about Russian SIGINT campaigns is indicative of extraordinary skill at leveraging a multitude of mostly free Internet services to reach far across global cyberspace to gather information. Consider the so-called "Turla Group" Russian cyber espionage campaign, which affected many high-value targets in dozens of countries worldwide, and which uses earth-orbiting satellite uplinks as command and control servers (Tanase 2015). Another sophisticated Russian cyber espionage campaign (FireEye 2015), referred to in the security industry as APT29, uses a digital mélange (Lennon 2015) of Internet tools, like Twitter, Github, as well as file sharing and cloud computing services, to distribute its command-and-control infrastructure and help obfuscate the identity of those ultimately responsible. Military incursions into Crimea and Ukraine in 2014 and 2015 more directly illustrated an ability to maneuver through cyberspace at will, monitor activities, and mount targeted but isolated malware attacks meant to confuse, weaken, and compromise Ukrainian adversaries. At the same time, Russia had little incentive to disrupt Ukrainian telecommunications systems entirely. Even the December 2015 attack on Ukraine's power grid, which caused a massive power outage and which was attributed to Russian-based hackers, was limited in scope and scale.

One of the distinct traits of Russian cyber espionage are its "influence operations", which have a long history connecting back to the Soviet period. They are digital variations of Cold War propaganda, disinformation, and other espionage campaigns. For example, Russia makes extensive use of social media to discredit and sow discord among adversaries, including the

use of paid "trolls" who post messages favourable to the Putin regime, or harass those who are in opposition. Its long-standing use of "Kompromat" – "compromising material" - is commonly used as a technique to discredit political opponents with embarrassing information typically acquired clandestinely and then published. This was taken to a new level with intrusions into the email networks of prominent Democratic Party officials in 2016. Information acquired by Russian-backed cyber-criminal organizations was then provided to WikiLeaks and other social media, ostensibly to discredit Presidential-candidate Hillary Clinton. While Russia promotes territorially-based information controls in the international sphere, and routinely censors and monitors the Internet and social media within Russian territory, these and other well-publicized influence operations demonstrate that it also actively engages social media and other digital assets abroad in pursuit of its strategic objectives.

Perhaps the countries one would expect to be the least likely to project power extraterritorially would be lower-tier authoritarian, mixed or hybrid regimes and countries, like those in the Gulf, sub-Saharan Africa, the Middle East and North Africa, Asia, Latin America, and the former Soviet Union. Countries like Saudi Arabia, UAE, Bahrain, Sudan, Ethiopia, Egypt, Syria, Vietnam, Thailand, Singapore, Pakistan, Myanmar, Venezuela, Uzbekistan, Tajikistan, Kyrgyzstan, and Kazakhstan might arguably be expected to be principal proponents of a coming Cyber Westphalia. All of these countries have in fact moved aggressively to control domestic information space through technical and regulatory means, and in every case have in place Internet censorship systems to block access to information that crosses their territorial borders. They are also considered principal supporters of Russian and Chinese-backed international initiatives on "Internet sovereignty", and many of them have introduced data localization regulations. But the actual governance practices of a widening range of autocratic countries of the global South are not confined inside their territorial boundaries. Diaspora communities living in the industrialized north use telecommunications networks to send billions of dollars of remittances to back to their originating countries. These diaspora networks also organize politically in ways that may challenge autocratic regimes. Holes in digital firewalls are exploited to advance human rights campaigns and support independent media outlets. At the same time, autocrats themselves continue to depend on open extraterritorial communication channels to bolster their rule or prepare for the future by way of offshore banking havens and real estate investments. While their strategic aspirations may not match those of the United States, such activities require the external projection of digital power.

Finally, authoritarian countries constitute a growing and profitable client base for a vast and rapidly expanding cyber-security industry, which can help control information within territorial boundaries and assist in efforts to investigate and neutralize threats abroad. Thanks to the commercial spyware industry, for example, some of the world's least connected and most impoverished countries, which lack domestic science, technology, and mathematics capacities, are nonetheless able to purchase their own sophisticated "NSA"-like capabilities. Off-the-shelf digital tools are readily available from companies headquartered in the west. Citizen Lab researchers have mapped the proliferation of such commercial spyware services to dozens of authoritarian regimes in all regions of the global South. Espionage operations undertaken using

these services typically target diaspora networks. They can be routed through multiple state jurisdictions to obfuscate their origins. Even US-based cloud-computing infrastructure is now routinely employed in the espionage operations of intelligence agencies based in the global South (Marczak et al 2014; Marczak, Scott-Railton et al 2015; Marczak, Scott-Railton and McKune 2015).

Conclusion

State agencies around the world are energetically attempting to re-establish territorial control over the Internet. At the same time, they are increasingly engaged directly or indirectly in extraterritorial projections of power in and through cyberspace. Their mutual entanglement both expands and constrains their own strategic options. The effective sovereignty of states defined in terms of uncontested territorial control in this domain has always been an illusion. The contested openness of cyberspace today, however, exposes the extent to which offensive and defensive policies have in fact constituted a new and very highly interdependent systemic architecture. Anarchy does not describe its political underpinnings, and neither does a straightforward notion of hierarchy. The interaction of dominant intelligence-sharing arrangements of rapidly expanding scope, challenges from autocratic governments simultaneously threatened and empowered by digital openness, and the rapid technological deepening of transnational networks permissive of the nearly instantaneous transmission of data—all render authoritative rule by states ever more complex in principle and in practice.

American hegemony in cyberspace was once manifested by governmental agencies and American-led firms and non-state actors. The observable fact today is that even core interests of the United States cannot be secured without the active collaboration of a growing community of allies and a degree of acquiescence and self-restraint by challengers. The currently surging extraterritorial exercise of both official and corporate digital power, moreover, entangles the United States and other public authorities around the world even as it transforms and reshapes cyberspace itself.

For every “Internet blackout” or “national Intranet” researchers identify, they also find the regimes behind them exploiting transnational communications systems and using common protocols to infiltrate adversaries, gather intelligence, and influence and shape events outside their territories. Together, these kinds of activities have a combined network effect, continuously re-embedding political authorities in distributed and fast-changing digital webs. Extraterritorial projections of state power contribute to a mutual entanglement that has collectively channelled and localized conflict, while restraining temptations to engage in all-out electronic warfare (Lindsay 2017). States continue to depend on and benefit from global networks, and even the most autocratic of them confront compelling incentives not to disable or destroy them (Mueller 2010). Despite all the attention recently paid to issues of digital attacks, disinformation campaigns, and money laundering, researchers have uncovered no suggestion of an emerging global consensus that would be required to secure impenetrable boundaries in cyberspace. The absence of such evidence, moreover, does not appear simply to be attributable to the momentary material interests of dominant social and political elites. The

openness of cyberspace is endogenous to all dimensions of national security policy, the traditional core feature of territorial states.

Watch what actual state agencies do, not what they say. A paradox is revealed. Persistent competitive pressures incentivize attempts to manipulate telecommunications networks internally and externally, but taking those global networks down is widely understood to be self-destructive and self-defeating. Territorially-anchored states depend on trans-border networks to defend themselves and to project their power abroad. The more states become entangled in those networks, the less likely they are to degrade or destroy them, and the more likely they are to join overtly or tacitly in common cause if a rogue non-state actor seriously threatens them.

The broader implications of mutual entanglement in cyberspace bear on the changing character of global political authority itself. National, intergovernmental, and transnational forces together determine the contours of the very space within and through which states now act. Even dominant states must live with the structural denial of locality in this critical domain. The essential quality of cyberspace binds them. Indeed, the kinds of evidence outlined in this chapter suggests that cyberspace is having a transformative impact on the territorial state as conventionally conceived. In the end, global networks cannot be effectively and legitimately governed at the national level. A process of unbundling political authority and recasting it is underway. That process reflects the dynamic interplay of frustrated impulses toward re-territorialization and the imperatives of projecting power extraterritorially. A high degree of global policy ambiguity may therefore be expected for the foreseeable future, since multiple and overlapping claims over rights and responsibilities in cyberspace look set to remain in contention. The external projection of power in and through cyberspace, nevertheless, disturbs systemic order and forces observers to contemplate the entangling effects of functional and political spill-overs (Braman 2013; Daskal 2015; Mueller 2017).

Mark Zacher long ago underlined the transformation underway within and among states in a system that inclined toward openness and encouraged deeper and more intrusive ‘violations’ of Westphalian sovereignty: ‘cobwebs of agreement have grown, and states have become more aware of the importance of both order and openness for national prosperity’ (Zacher and Sutton 1996, 232-3). Of course, the leaders of states have always adhered formally to conventional norms of sovereignty, but they have also often deviated when necessary or convenient (Krasner 2009). Mutual entanglement in cyberspace suggests both mounting constraints on such tactical political calculations as well as stark disappointment for libertarian hopes of Internet freedom. The transformative complexities of sovereign authority when a still territorially anchored political system meets an increasingly global social and economic system are observable in cyberspace (Rosenau 2003; Grande and Pauly, 2005; Buzan and Lawson 2015; Zürn 2018).

At the global level, it is not difficult to discern the outlines of emergent “digital security communities”. More implicit but also becoming discernible are workable understandings among strategic competitors. Despite very different perspectives on the meaning or applicability of the rule of law and the supposed sanctity of the principle of non-interference in

internal affairs, China and the United States, for example,, have begun discussions on acceptable behaviour in cyberspace. They are doing so bilaterally as well as multilaterally through the United Nations and other forums (United Nations 2015; G20 Research Group 2015). The two countries even agreed in September 2015 on a limited set of restraining principles concerning industrial espionage, the theft of intellectual property, the targeting of critical infrastructure, and the need to cooperate on investigations of electronic crimes (The White House 2015; Harold, Libicki and Cevallos 2016). Despite continuing concerns about compliance, other countries are moving in the same direction as they contemplate expanding Chinese investment across a range of economic sectors. Future on-line activities, and the cooperation of like-minded authorities on either side of the autocracy divide, will determine whether new principles and policies become effective and broadly accepted as legitimate.

The risks of catastrophic miscalculations or accidents in cyberspace remain. But uncertainty at this point does not suggest disorderly fragmentation along territorial lines. Through their trans-territorial interaction, the governments of states will likely continue to live with paradox. They look set to continue moving toward new forms of authority to govern the Internet—contested but acceptable enough to permit a dynamic system to persist. States still matter, but mutual entanglement in cyberspace reinforces the idea of complex sovereignty and mocks dreams of retreat to a simpler past.

Notes

---

[1] Portions of this chapter are derived from Ronald J. Deibert and Louis W. Pauly, "Cyber Westphalia and Beyond: Extraterritoriality and Mutual Entanglement in Cyberspace," paper prepared for the Annual Meeting of the International Studies Association, Baltimore, Maryland, February 2017, and Ronald J. Deibert and Louis W. Pauly, "Boundaries and Borders in Global Cyberspace," in *Borders, Boundaries, and the Future of Canadian Society*, The Third Annual SD Clark Symposium on the Future of Canadian Society Celebrating Canada's Sesquicentennial, 10 November 2017. For comments, we thank Daniel Deudney, Joseph Nye, Abe Newman, Jon Lindsay, Lennart Maschmeyer, Hans Klein, Milton Mueller, and the editors of this volume. We also gratefully acknowledge support provided by the Canada Research Chairs Program and the Social Sciences and Humanities Research Council of Canada.

References

Blue, Violet. 2012. "Hack In The Box." ZDNet, October 11; accessed at: http://www.zdnet.com/article/hack-in-the-box-researcher-reveals-ease-of-huawei-router-access/, May 13 2016.

Braman, Sandra. 2013. "The geopolitical vs. the network political." International Journal of Media and Cultural Politics 9(3): 277-296.

Buzan, Barry and George Lawson (2015). The Global Transformation, Cambridge: Cambridge University Press.

Citizen Lab. 2014. “Communities @Risk.” Citizen Lab, Report 48; accessed at: https://targetedthreats.net/index.html, May 13, 2016.

Citizen Lab and ASL19. 2013. “After the Green Movement.” OpenNet Initiative Special Report, March 11; accessed at: https://opennet.net/sites/opennet.net/files/iranreport.pdf, May 13 2016.

Cordesman, Anthony H., George Sullivan, and William D. Sullivan. 2007. “Lessons of the 2006 Israeli-Lebanon War.” Center for Strategic and International Studies, Significant Issues Series, 29(4); accessed at: https://csis.org/files/publication/120720_Cordesman_LessonsIsraeliHezbollah.pdf, May 13 2016.

Dalek, Jakub, et al., 2015. “A Chatty Squirrel: Privacy and Security Issues with UC Browser.” Citizen Lab, Research Brief 55, May 21; accessed at: https://citizenlab.org/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/, May 17 2016.

Daskal, Jennifer. 2015. “The Un-Territoriality of Data.” Yale Law Journal, 125(2): 326-398.

Deibert, Ronald. 2012. “Social Media, Inc.: The Global Politics of Big Data.” World Politics Review, June 19; accessed at: http://www.worldpoliticsreview.com/articles/12065/social-media-inc-the-global-politics-of-big- data, May 17 2016.

Deibert, Ronald. 2015. “Authoritarianism Goes Global.” Journal of Democracy 26(3): 64-78.

Deibert, Ronald. 2017. “Cyber Security.” In Routledge Handbook of Security Studies, edited by Myriam Dunn Cavelty and Thierry Balzacq, 172-182. Abingdon: Routledge.

Deibert, Ronald, and Masashi Crete-Nishihata. 2012. “Global Governance and the Spread of Cyberspace Controls.” Global Governance 18(3): 339-361.

Deibert, Ronald, et al., eds. 2008. Access Denied: The Practice and Policy of Internet Filtering. Cambridge, Massachusetts: MIT Press.

Deibert, Ronald, et al., eds. 2010. Access Controlled: Policies and Practices of Internet Filtering and Surveillance. Cambridge, Massachusetts: MIT Press.

Deibert, Ronald, et al., eds. 2012. Access Contested: Security, Resistance, and Identity in Asian Cyberspace, Cambridge, Massachusetts: MIT Press.

Deibert, Ronald, and Rafal Rohozinski. 2008. “Good for Liberty, Bad for Security? Internet Securitization and Global Civil Society,” in Access Denied, edited by Ronald Deibert, et al., 123-165. Cambridge, Massachusetts: MIT Press.

Deibert, Ronald and Rafal Rohozinski. 2010. “Risking Security: The Policies and Paradoxes of Cyberspace Security.” International Political Sociology 4(1):15-32.

Deibert, Ronald, Rafal Rohozinski, and Masashi Crete-Nishihata. 2012. “Cyclones in Cyberspace.” Security Dialogue 43(1): 3-24.

Demchak, Chris C., and Peter Dombrowski. 2011.“Rise of a Cybered Westphalian Age.” Strategic Studies Quarterly 5(1): 32-61.

Deudney, Dan. 2007. Bounding Power, Princeton: Princeton University Press.

Dombrowski, Peter. 2016. “China wants to Draw Borders in Cyberspace.” New Perspectives Quarterly 33(2): 38-42.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwächter. 2016. “Internet Fragmentation: An Overview.” World Economic Forum, Future of the Internet Initiative Whitepaper; accessed at: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, May 12 2016.

FireEye. 2015. “HAMMERTOSS.” FireEye Special Report; accessed at: https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf, May 13 2016.

Friends Committee on National Legislation. 2015. “Understanding Drones.” Friends Committee on National Legislation, accessed at: http://fcnl.org/issues/foreign_policy/understanding_drones/, May 13 2016.

G20 Research Group. 2015. G20 Leaders’ Communiqué’, G20 Research Group, November 16; accessed at: http://www.g20.utoronto.ca/2015/151116-communique.html, May 13 2016.

Harold, Scott Warren, Martin C. Libicki, and Astrid Stuth Cevallos. 2016. "Getting to Yes with China in Cyberspace." RAND Corporation, Research Report 1335; accessed at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR 1335.pdf, May 13 2016.

Grande, Edgar, and Pauly, Louis, eds. 2005. Complex Sovereignty. Toronto: University of Toronto Press.

Harris, Shane. 2014. @War: The Rise of the Military–Internet Complex. Boston, MA: Eamon Dolan/Houghton Mifflin Harcourt.

Howard, Philip N., Sheetal D. Agarwal, and Muzammil M. Hussain. 2011. "The Dictators' Digital Dilemma" Issues in Technology Innovation 13:1–11.

Johnson, David R., and David G. Post. 1996. "Law and Borders - The Rise of Law in Cyberspace." Stanford Law Review, 48(5):1367-1402.

Katzenstein, Peter J., ed. Anglo-America and Its Discontents. Abingdon UK: Routledge, 2012.

Knockel Jeffrey, Sarah McKune, and Adam Senft. 2016. "Baidu's and Don'ts." Citizen Lab, Research Brief 72, February 23; accessed at: https://citizenlab.org/2016/02/privacy-security-issues-baidu-browser/, May 17, 2016.

Knockel Jeffrey, Adam Senft, and Ronald Deibert. 2016. "Wup! There it is." Citizen Lab, Research Brief 75, March 28, accessed at: https://citizenlab.org/2016/03/privacy-security-issues-qq-browser/, May 17 2016.

Krasner, Stephen. 1999. Sovereignty, Princeton: Princeton University Press.

Lennon, Mike. 2015. "Russian Hacker Tool Uses Legitimate Web Services to Hide Attacks: FireEye." SecurityWeek, July 29; accessed at: http://www.securityweek.com/russian-hacker-tool-uses-legitimate-web-services-hide-attacks- fireeye, May 13 2016.

Lindsay, Jon R. 2015. "The Impact of China on Cybersecurity: Fiction and Friction." International Security 39(3):7–47.

Lindsay, Jon R. 2017. "Restrained by design: The political economy of cybersecurity" Digital Policy, Regulation and Governance, 19(6): 493-514.

Mandiant (n.d.) APT1: Exposing One of China's Cyber Espionage Units. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Marczak, Bill, et al., 2014. "Mapping Hacking Team's Untraceable Spyware." Citizen Lab, Research Brief 33, February 17; accessed at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/, May 13 2016.

Marczak, Bill, John Scott-Railton, and Sarah McKune. 2015. "Hacking Team Reloaded?" Citizen Lab, Research Brief 50, March 9; accessed at: https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/, May 13 2016.

Marczak, Bill, John Scott-Railton et al. 2015. "Pay No Attention to the Server Behind the Proxy." Citizen Lab, Research Brief 65, October 15; accessed at: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/, May 13 2016.

Marczak, Bill, Nicholas Weaver, et al. 2015. "An Analysis of China's Great Cannon." 5th USENIX Workshop on Free and Open Communications on the Internet, Washington, D.C.

Marquis-Boire, Morgan, Glenn Greenwald, and Micah Lee. 2015. "XKEYSCORE."The Intercept, July 1; accessed at: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/, May 13, 2016.

Mozur, Paul. 2015. "Baidu and CloudFlare Boost Users Over China's Great Firewall." The New York Times, September 13; accessed at: http://www.nytimes.com/2015/09/14/business/partnership-boosts-users-over-chinas-great-fir ewall.html?_r=0, May 13 2016.

Müller-Maguhn, et al. 2014. "Treasure Map." Der Spiegel, September 14; accessed at: http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-de utsche-telekom-a-991503.html, May 13 2016.

Mueller, Milton L. 2010. Networks and States. Cambridge, MA: MIT Press.

Mueller, Milton 2017. Will the Internet Fragment? Cambridge, UK: Polity.

Nye, Joseph. 2016. "Deterrence and Dissuasion in Cyberspace," International Security, Winter, 41(3): 44-71.

Ruan Lotus, et al. 2016. "One App, Two Systems." Citizen Lab, November 30, 2016; accessed at: https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/, February 3, 2018.

Ruggie, John G.1993. "Territoriality and Beyond." International Organization, 47(1): 139-174.

Regalado, Daniel, Nart Villeneuve and John Scott-Railton. 2015. "Behind the Syrian Conflict's Digital Front Lines." FireEye Special Report, February 2015; accessed at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-t he-syria-conflict.pdf, May 13 2016.

Rosenau, James. 2003. Distant Proximities. Princeton: Princeton University Press.

Soldatov, Andrei, and Irina Borogan. 2015.The Red Web. New York: Public Affairs.

Scott-Railton, John, and Katie Kleemola. 2015. "London Calling: Two Factor Authentication Phishing From Iran." Citizen Lab, Research Brief 61, August 27; accessed at: https://citizenlab.org/2015/08/iran_two_factor_phishing/, May 17 2016.

Stecklow, Steve. 2012. “Chinese firm helps Iran spy on citizens.” Reuters, March 22; accessed at: http://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322, May 13 2016.

Small Media. 2015. “Iranian Internet Infrastructure and Policy Report.” Small Media; accessed at: https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb15.pdf, May 13 2016.

Starosielski, Nicole. 2015. The Undersea Network. Durham: Duke University Press.

Stiennon, Richard. 2016. “The Entire IT Security Landscape.” 25th RSA Conference San Francisco, CA, March 18; accessed at: https://www.youtube.com/watch?v=YYNM2VRmncE, May 13 2016.

Tanase, Stefan. 2015. “Satellite Turla.” Securelist, September 9; accessed at: https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sk y/, May 13 2016.

The White House. 2015. “President Xi Jinping’s Visit to the United States.” White House Press Release, September 25; accessed at: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-stat e-visit-united-states, May 13 2016.

Union of Concerned Scientists. 2016. “Union of Concerned Scientists Satellite Database.” February 25; accessed at: http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.VyykWxUrKgQ, May 13 2016.

United Nations. 2015. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations General Assembly A/70/174, July 22; accessed at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174, May 13 2016.

VanderKlippe, Nathan. 2016. “China collecting sensitive personal data through Android apps.” The Globe and Mail, February 24; accessed at: http://www.theglobeandmail.com/technology/tech-news/millions-of-android-apps-send-sensiti ve-data-to-china-u-of-t-report/article28865055/, May 13 2016.

Villeneuve, Nart. 2008. “Breaching Trust.” Information Warfare Monitor; October 1; accessed at: https://www.scribd.com/doc/13712715/Breaching-Trust-An-analysis-of-surveillance-and-secu rity-practices-on-China-s-TOM-Skype-platform, May 17 2016

Vine, David. 2015. Base Nation, New York: Henry Holt.

Vodafone. 2014. “Vodafone Law Enforcement Disclosure Report 2013/2014.” Accessed at: https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/priv acy_and_security/law_enforcement.html, May 12 2016.

Ward, Stephen. 2014. “An Iranian Threat Inside Social Media.” iSIGHT Partners, May 28; accessed at: https://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/, May 13 2016.

Wege, Carl. 2012. “Hizballah’s Counterintelligence Apparatus.” International Journal of Intelligence and Counter-Intelligence, 25(4): 771-785.

Zacher, Mark W., and Brent A. Sutton. 1996. Governing Global Networks, Cambridge: Cambridge University Press.

Zetter, Kim. 2014. Countdown to Zero Day. New York: Crown Publishers.

Zürn, Michael. 2018 A Theory of Global Governance. Oxford: Oxford University Press.