International Cyberpolitics

Benjamin R. Banta

Subject: Foreign Policy, International Relations Theory, Security Studies
Online Publication Date: Sep 2020 DOI: 10.1093/acrefore/9780190846626.013.553

Summary and Keywords

The earliest scholarly writing on “cyberpolitics” focused mainly on the domestic sphere, but it became clear by the mid-2000s that the Internet-generated “cyberspace” was also having massive effects on the broader dynamics and patterns of international politics. A great deal of the early research on this phenomenon focused on the way cyberspace might empower nonstate actors of all varieties. In many respects that has been the case, but states have increasingly asserted their “cyberpower” in a variety of ways. Some scholars even predict a coming territorialization of what was initially viewed as a technology that fundamentally resisted the dictates of sovereign borders. Such disparate possibilities speak to the ambiguity surrounding the intersection of the international system and the political affordances generated by the Internet and related technologies. Does cyberpolitics challenge the international system as we know it—perhaps altering the very nature of war, sovereignty, and the state itself—or will it merely be subsumed within some structurally mandated logic of state-centric self-help?

As might be expected, research that speaks to such foundational questions is quite sprawling. It is also still somewhat inchoate because the object of study is complex and highly malleable. The cyber-“domain” involves a physical substrate ostensibly subject to a territorially demarcated international system, but Internet-enabled activities have expanded rapidly and unpredictably over the past few decades because it also involves a virtual superstructure designed to be a network of networks, and so fundamentally at odds with centralized control. As such, some argue that because cyberspace has so enmeshed itself into all aspects of society, international politics and cyberspace should be seen as coevolving systems, and concomitantly that fields such as International Relations (IR) must update their theoretical and methodological tools. Such contentions indicate that an understanding of extra-domestic cyberpolitics has not so much involved progressively developing insights as differing perspectives compete to explain reality, but rather the growing recognition that we are only now catching up to a rapidly changing reality.

As part of that recognition, much of the cutting-edge International Studies (IS) work on cyberpolitics is aimed at researching how the central actor in global politics, the state, is increasingly a cyberpolitical actor. This has meant the abandonment of strong assertions about the way cyberspace would exist separate from the “real world” of state interaction, or that it would force the alteration of especially hierarchical forms of state power. In-

stead, burgeoning literatures examine the myriad ways states seek to resist and control cyberpolitical activity by others, deploy their own cyberpolitical power, and even shape the very cyberspace in which all of this can occur. This focus on “international cyberpolitics” thus involves tracking a complex and growing milieu of practices, all while reflecting on the possibly fundamental changes being forced upon the international system. All of this points to the likelihood that the study of international politics will increasingly also be the study of international cyberpolitics.

Keywords: cyberpolitics, International Relations, cyberspace, sovereignty, foreign policy, Internet, governance

The Meeting of International and Cyber Spaces

The Internet, and the global cyberspace it enables, has gone from a niche issue for analysts of international politics in the early 2000s to so ubiquitous and influential that even by 2011 Nye (2011, p. xviii) could speak of ours as a “cyberage.”[1] Most early discussion of what this article calls cyberpolitics—political activity taking place within, enabled by, or concerned with the management of cyberspace—adopted a domestic frame. Even so, there were prominent early debates on the international implications of the Internet that dealt with core focuses of traditionally state-centric IR. For instance, even as early as the 1990s scholars debated whether it was possible to imagine a “cyberwar,” what it might look like, and how states should prepare for it (Arquilla & Ronfeldt, 1993; Libicki, 2007; Rattray, 2001). Scholars also questioned whether the state could effectively maintain its territorially defined sovereign prerogatives over and in light of seemingly extraterritorial cyberspace activity (Johnson & Post, 1996; Lessig, 1999). From here, as the Internet expanded into every facet of social life, so too did research into a fantastically broad set of international and global cyberpolitical phenomena. This article, partly for length considerations, but largely because of the general thrust of global cyberpolitical happenings since at least the early 2010s, is a review of state-centric cyberpolitical interaction, or simply “international cyberpolitics.”

Initially piggybacking off a technologist-led literature that mostly exalted the ways the Internet might effect a flowering of communication, knowledge, and reason (the crest of this early wave can be found in Benkler, 2006; Jarvis, 2011; Mainwaring, 2011; Shirkey, 2010; Sunstein, 2006), the literature on extra-domestic cyberpolitics covers disparate and broad ground. Much of the thrust of early work in this area assumed the object of study required a refocusing away from the relatively parsimonious state-centricity of traditional IR and toward a much broader set of subjects. This is due to the contention that cyberspace generally enables “power diffusion” away from states (Nye, 2011, p. 114). The Internet so radically decreased the cost of communication that the masses could participate in “virtually infinite” information flows, thus empowering transnational actors and diminishing the gap between the powerful and the weak (Nye, 2011, p. 115).

Shifting an entire field’s focus is of course difficult. Even by the end of the 2000s, Manjikian (2010, pp. 381–382) could write that “despite the Internet’s undeniable presence in

contemporary international society, international analysts have devoted remarkably little ink to pondering its evolution, its meaning, or its significance." This seeming lag is perhaps partly due to the complexity and rapid mutability of the technology. Indeed, most experts recognize that in just over a few decades the Internet went through a number of evolutionary phases: a massive global expansion enabled by its privatization and the development of the World Wide Web, its application to mobile devices, the development of social media, and the ongoing process of every imaginable object becoming digitally connected (also known as the Internet of Things) (DeNardis & Raymond, 2017; Naughton, 2016).

As these phases proceeded, some began to push back against early cyber-utopians. They pointed to the ways the Internet could be used to spread intolerance and ignorance, entrench authoritarianism, and even induce purportedly rights-respecting democratic states to surveil and propagandize (MacKinnon, 2012; Morozov, 2011; Pariser, 2011). Likewise, the diffusion-focus of IS cyberpolitics literatures began to give way to scholarship that observed, theorized, and predicted the increased subsumption of cyberpolitics by the state (Drezner, 2004, 2010; Lewis, 2010). At this point, though, these interventions often made the mistake of at least implicitly conceiving cyberspace as merely some sort of new domain for interaction within international politics—one like air or sea that at most involved distinctive properties and challenges. Cyberspace is fundamentally different from those strategic domains, though, in that being made by humans, its "parameters are changeable," and so activity is not "limited to changing the rules of the game but . . . the game board itself" (Ebert & Maurer, 2013, p. 1056).

Accordingly, most work on extra-domestic cyberpolitics eventually began to work from the baseline of a coevolving "cyber-IR system" (Choucri & Clark, 2018; McCarthy, 2018). As part of this more nuanced frame, a few basic and crucial considerations have coalesced. First, as cyberspace expands it must be acknowledged that it is not "a separate and parallel system to the traditional world but rather . . . a deeply embedded aspect of that familiar world" (Choucri & Clark, 2018, p. 125). The idea of distinct "virtual" and "real" worlds is simply misleading. Second, as McCarthy (2015, p. 67) insightfully points out, cyberpolitics involves a high degree of "institutional power," defined by Barnett and Duvall (2005, p. 43) as the "control actors exercise over each other through diffuse relations of interaction." The Internet's very design gives form to its "episodic *power to*"—the social media organizing or cyberattacks or commercial opportunities where cyberpower is most evident—and this design is shaped in fundamental ways by states and their interactions, giving them in essence "the power to create power" (McCarthy, 2015, p. 68). Third, though, this then acts back upon states, a dynamic that will no doubt be shaped in path-dependent ways by the fact that even after over a decade of concerted state efforts to more directly shape cyberspace it is still an "arena dominated by private, not sovereign, order" (Choucri & Clark, 2018, p. 124). As Choucri and Clark (2018, p. 249) contend, in one of the more comprehensive and technologically sophisticated studies of international cyberpolitics, "the cyber domain is perhaps 'ultra-anarchic' given its distributed management that seemed to bypass the state system and its authority almost entirely." This may be changing; some offer a contrasting argument that the Internet is quite amenable to hi-

erarchical power structures (Carr, 2015; Raymond & DeNardis, 2015). Nevertheless, with these baseline insights taken together, it is clear that cyberspace is central to international politics.

Optimistically, this combination of an "ultra-anarchic" global phenomenon and state influence may mean that "the expansion of cyberspace and cyber participation may generate a demand for governance structures and processes that transcend territorial sovereignty" (Choucri & Clark, 2018, p. 151). Some, though, reflecting the continued debate over how much hierarchical potential cyberspace contains, contend it may also involve a fracturing of cyberspace along international lines. To capture the practices involved in this range of outcomes, this review proceeds in three sections. These sections move from state resistance against and efforts to control what many see as the radical openness of cyberspace, to the ways states leverage that openness in their foreign affairs, and finally to the increasingly heated interactions over how cyberspace should be governed. This spectrum is meant to loosely correspond to the shifting gaze of researchers, following as they were major developments in international cyberpolitics since the turn of the 21st century. Analysts first largely concentrated on the ways authoritarian states especially were resisting or seeking to control Internet activity, then began noticing how states of all kinds were finding its supposedly counterhegemonic affordances useful for securing power, and, going forward, many are recognizing the biggest questions relate to just how fundamentally international politics will intrude where earlier utopians asserted there could be no "sovereignty where we gather" (Barlow, 1996). States have intruded, though of course the extent of their influence is probably no more fated than that early utopian vision.

The International Cyberpolitics of Denial and Control

The title of this section is drawn from the most comprehensive early examinations of evolving state efforts to resist the radically open Internet of the 1990s and early 2000s. In a series of reports, which followed upon earlier prescient works that theorized how the state would or at least could heavily influence cyberpolitics (e.g., Wu & Goldsmith, 2006), Ronald Deibert (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, 2010, 2011) and his colleagues demonstrated how authoritarian states especially were not only maintaining stability in spite of the Internet, but learning to wield cyberpolitics to increase their power. This involved combining access denial and filtering of information with use of "offensive" online measures—surveillance, propaganda, and more "subtle" registration and licensing measures—in order to persist and even flourish in a cyberpolitical era (Deibert et al., 2011, pp. 10–11). Such efforts have meant that while the Internet is still held to be a particularly powerful vector for the spread of ideas, awareness of human rights, and bottom-up movements for progressive change, states have developed tools, many cyberpolitical in nature, to mitigate its revolutionary potential.[2]

Though in some sense these denial and control efforts are a domestic story, they are also very much a matter of international cyberpolitics. First and most obviously, domestic control over the Internet often means control over information and applications generated outside the particular state in question. As such, even when, in the early 2000s, analysts were mainly framing the Internet as a domestic human rights issue, that very discourse necessarily "put authoritarian regimes under scrutiny and created the perception that the internet's transnational connectivity threatened such regimes" (Fidler, 2014, p. 10). And so even if something like early Chinese filtering efforts were most directly about preventing organized domestic campaigns against the Communist Party, doing so was also related to and would generate further pressure from states committed to promoting freedom of speech and association.

The international component of this aspect of cyberpolitics further came into focus with the 2013 revelations by U.S. defense contractor Edward Snowden. His release of classified material showed that the National Security Agency (NSA) was using the Internet to support an incredibly extensive, and often illegal, domestic and foreign surveillance program, that numerous corporations and U.S. allies were cooperating with this program, and that the Pentagon was busy deploying and further developing myriad offensive cyber operations. This at the very least produced the perception that U.S. support for Internet openness was disingenuous, and rather than about rights or knowledge or commerce it was merely a means of securing power (Fidler, 2015). It also revealed the extent to which even democratic regimes sought to control the Internet. The NSA program may have been largely an example of leveraging cyberspace toward some foreign policy goal, which is covered in the next section, but as Bauman et al. (2014, p. 136) put it, these "new procedures for intelligence operations, data-gathering, mobilizing suspicions, and identifying potential threats . . . pose dangers to established liberties and rights that are analogous to regimes we prefer to imagine as swept away in revolutions, democratizations, modernizations." And rather than cause a reckoning, the revelations seemed only to intensify ongoing trends like the exploitation of "big data" and the "growing power and influence of the state," while throwing a "wild card" into the fight over whether the Internet would fulfill its promise as a kind of "global commons" (Deibert, 2015, pp. 9, 15). Finally, the Snowden revelations meant authoritarian regimes found it easier to respond to outside criticism of their control efforts, and could justify them internally by referencing the way an open Internet was a vehicle for outside threats and interference.

In general, this contributed to states as varied as Brazil, Holland, Germany, Iran, and China "thickening their digital borders" (Bauman et al., 2014, p. 130). The latter went furthest, moving beyond their sophisticated filtering system, known as the Great Firewall, to promoting the notion of "Internet sovereignty" (Fang, 2018; Zeng, Stevens, & Chen, 2017), which asserts "the authority of national-level regulators over web content and providers" (Qiang, 2019, p. 54). Under this doctrine, Chinese authorities went from control over the flow of information on the Internet to broader control of society by utilizing the Internet to surveil and manipulate. These more proactive measures included paying pro-government online commentators, requiring that Internet users register with their real names, and imposing legal penalties for the spread of "rumors" online (Jiang, 2016).

China also began concerted efforts to use big data and artificial intelligence (AI) technologies to predict where unrest might occur, and employed a “Social Credit System” that scores citizens’ financial *and* personal activities to “determine the results of applications for personal loans, jobs, visas, and more” (Qiang, 2019, p. 59). Further highlighting the international dynamics to this process, Qiang (2019, pp. 61–63; Demchak, 2019) warned that this “China model” of “digital totalitarianism” was being exported as Chinese tech companies that enable it spread abroad, and as Western companies like Facebook and Google succumb to it in order to remain in or re-enter the Chinese market.

The temptations that cyber-related technologies generate to control, surveil, and manipulate society are, of course, not limited to China, or even authoritarian regimes in general; it seems the Snowden revelations did little to dampen these activities even in the United States. To this Fidler (2014, p. 16; McCarthy, 2015, p. 159) suggests that there may be a “convergence of authoritarian leaders and U.S. officials on viewing the internet and cyberspace predominantly through the lens of power politics.” To be sure, the template for control measures is different in democratic states, and instead of a largely top-down approach there are a patchwork of public and private entities employing methods that, whether for security or profit, loosely intersect to generate “an irresistible proxy for authoritarian control” (Deibert, 2019, p. 35). From the business models of the largest social media companies, which essentially rely on the mass surveillance of their users, to the “imperfect legal safeguards” that regulate the government agencies that utilize this data, to the “complete U-turn” that companies like Google and Apple have made with respect to participating in Chinese censorship, Deibert (2019, pp. 34–35) sees a “bleak picture and a troubling forecast for the future of liberal-democratic practices.”

From an IR perspective, this potential convergence might be the most interesting aspect of the various state efforts to adapt to cyberspace. How far will it go? Will it move in any particular direction? Viewed from a certain vantage, for authoritarian regimes these control mechanisms also represent increased de facto levels of responsiveness to their publics. The Chinese government, for instance, is keen to use Internet surveillance to locate and deal with some instances of corruption, if only to stave off unacceptable levels of discontent among the populace (Gunitsky, 2015, p. 47). At the same time, for democratic publics the capture and leveraging of the data that Internet activity generates represents a subtle yet undeniable source for illiberal state and corporate control over their lives. What’s more, the scales may tip due precisely to the standard balance of power dynamics most readily studied by IR analysts. As Feldstein (2019, p. 41) points out, China “is driving the proliferation of AI technology to authoritarian and illiberal regimes, an approach that has become a key component of Chinese geopolitical strategy.” It will be of vital interest to research this process going forward, especially given the way cyberpolitical activity is increasingly central to state foreign policies.

International Cyberpower-Projection

Just as cyberspace affects how states relate to their populaces, it also alters and opens new avenues for state foreign policies. States must, of course, now concern themselves with the globally expansive growth and dynamism of cyberspace, whereby developments at any location of this global network can potentially change aspects of it anywhere else (Deibert & Rohozinski, 2011, p. 23). Indeed, there is an ongoing demographic shift of Internet users into the developing world, replete with regimes and cultures that do not fit the libertarian ethos of the Internet's early enthusiasts (Deibert & Rohozinski, 2011, pp. 25–28). There is also the massive global growth in cybercrime, a cybersecurity industry to meet it, and a plethora of corporate actors more willing than ever to push their agendas onto cyberspace (Deibert & Rohozinski, 2011, pp. 28–34). And as hinted at, even state mechanisms for controlling the Internet's domestic effects can generate interstate struggle. Fidler (2014, pp. 8–10) describes this as a "third image pushback," in which "*realpolitik* might increasingly characterize cyberspace as part of international relations." To combat criticism of their efforts to control Internet access and activity, authoritarian regimes "attempted to shift the focus to international system issues, such as sovereignty, non-intervention, and the exercise of political and military power by dominant states, particularly the United States" (Fidler, 2014, p. 10). This was largely successful, and meant greater awareness of the cyber-induced alterations in traditional foreign policy endeavors, as well as some novel assertions of international cyberpower.

Nye (2011, p. 123) defines cyberpower as both "a set of resources that relate to the creation, control, and communication of electronic and computer-based information—infrastructure, networks, software, human skills . . . [—and,] behaviorally, . . . the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain." Nye's early prediction (2011, p. 114) was that state abilities to leverage cyberpower would leave them still "the dominant actor on the world stage," but that they would "find the stage far more crowded and difficult to control." Some went further, reasoning that with organizations like WikiLeaks able to distribute state and corporate secrets given them by self-proclaimed whistle-blowers, democratic states especially would be forced to adopt "radical transparency" in their foreign policy, lest they crash against "a new wave and new culture of popular awareness and emancipation" (Pieterse, 2012, p. 1919). Some even lauded the transparency that would be brought to bear on one of the state's defining tasks, war-making, now that the progenitors of information about war went beyond the "hands of a very small minority of highly specialised and materially powerful actors" (Kaempf, 2013, p. 595). State resilience in combating these affordances is, though, quite apparent. Many of WikiLeaks' major activities, for instance, were effectively at the behest of the Russian government's efforts to assist in the election of Donald Trump to the U.S. presidency. There is also the state's ability to utilize these same affordances for their own ends.

The topline cyberpower concern for state foreign policies centers on the traditional core focuses for IR, war and international security. In a massive and still growing cyber-conflict literature—one that is beyond the scope of this review—the general observation is

that the use of highly damaging cyberweapons by states is largely subject to the same kinds of rivalries and restraints as uses of traditional military force, but that cyberpower does greatly expand the ways states can harm one another short of war (Valeriano & Maness, 2015). This is due not only to the means it makes available that do clearly fall below the threshold of an "armed attack," but also the great deal of ambiguity cyber-operations can entail. It is often unclear just who is attacking, how damaging an attack is, and how to calibrate a proportionate response. Initially, many argued these dynamics would favor the offense and induce highly destructive attacks (Arquilla, 2009; cf. Rid, 2013). Not only has that not been the case, but as Lindsay (2017, p. 494) argues, it is *increasingly* unlikely because "participation in the institution [of cyberspace] is the condition for the possibility of conflict within it," and so all-out cyberwar would likely entail the destruction or severe degradation of the "battlefield" for all sides. As such, as more activity moves online, and with it increased competition over cybersecurity, the kinds of "cheating at the margins" that cyberattacks usually represent will become "more devious, but less damaging" (Lindsay, 2017, pp. 494–495).[3]

Some still carry the banner of early alarmists, but do so by contending that cyberspace is so resilient that states can afford to take a more offensive posture (Rovner & Moore, 2017; cf. Healey, 2019). However, this proposition may chafe against growing recognition that the ambiguity surrounding cyberattacks, usually referred to as the "attribution problem," is less dire than previously thought (Brantly, 2016; Gartzke & Lindsay, 2015). Going forward, then, the biggest questions may not be about how revolutionary this new "virtual weapon" will be for warfare (Kello, 2017), but the degree to which it will generally alter the ways that states think about and practice core security concepts like deterrence (Nye, 2017; Wilner, 2020), coercion (Borghard & Lonergan, 2017), espionage (Bossetta, 2018), the offense-defense balance (Slayton, 2017), and the security dilemma (Libicki, 2016), as well as legal and ethical issues surrounding the nature of and proper response to differing kinds of cyber-attacks (Delerue, 2020; Haataja, 2019; Lee, 2014; Orend, 2014).

Closely related are the new cyber-enhanced modes of what is often referred to as "information warfare." In its updated form, this perennial feature of state relations moves well beyond periods of even "cold" war and involves the general presence of "computational propaganda and disinformation during critical moments of public life" (Bradshaw & Howard, 2018, p. 23). Perhaps the most high-profile instance of this was the Russian campaign to use cyberspace to hack, propagandize, and sow discord in the 2016 U.S. election. With, then, the election of Trump and the concomitant illiberalism and dysfunction it entailed, Ziegler (2018, p. 517; see also Levinger, 2018) found that this and similar efforts in Europe "helped achieve Putin's primary goal—restoring the balance of power upended with the collapse of the Soviet Union, and positioning Russia once again as a key play in great power politics." Of course, just how much the cyberpolitical accounts for this is still very much up for debate. Lanoszka (2019), using an analysis of Russian efforts to shape international opinion of their 2014 aggression against Ukraine, and in particular to "deter unfavourable policy responses" among Baltic states, finds that disinformation campaigns run up against the uncertainty and pressures of international anarchy, the strength of the

preexisting ideological commitments of its targets, and the countermeasures that targets find available to them. What's more, there is the more legitimate practice of public diplomacy, where digital communications technologies are said to be shifting it away from being "adversarial, unidirectional, instrumental, and impersonal," as enabled by mediums like television and radio, and toward a more "relational orientation" that seeks out "genuine cooperation and collaboration" (Zaharna, Arsenault, Fisher, 2014, pp. 1–5). Unfortunately, such high-minded prospects also compete with less progressive but no less novel developments such as the destabilizing practice of "diplomacy-by-tweet" favored especially by Trump (Drezner, 2019, p. 287).

On the economic front, and possibly speaking most directly to Nye's notion of the "crowding" of international politics by nonstate actors, some foresaw large Internet companies —"digital giants" like Amazon or Google (McChesney, 2013, p. 130)—as foundationally challenging the ability of states to assert their power abroad. For instance, one early prediction was that the degree of global commerce enabled by cyberspace would present such difficulties for the core state function of taxation that states would have to "internationalize" their authority beyond territorial boundaries (Paris, 2003, p. 177). That has not come to pass; states have rather attempted to simply extend their jurisdiction by way of creative changes to their own domestic tax laws, while international coordination has been largely frustrated (Cockfield, Hellerstein, & Lamensch, 2020). Likewise, with respect to state foreign interests generally, the largest "giants" have developed business models that allow at the very least for an ad hoc symbiosis between their interests and those of the states they feel they need to work with at any particular moment.

By utilizing the Internet's very user-generated activity to gather immense amounts of personal data, the most powerful Internet companies are able to keep users engaged as long as possible and more directly target them with advertisements. From there, these giants can leverage the Internet's inherent network effects—where the greater number of users actually increases the performance of an application—to monopolize their particular sectors of the online world (Drezner, 2019, p. 297; Mosco, 2017). Powerful states have learned to utilize both dynamics, with big data enabling myriad new avenues for foreign surveillance and espionage, and the immense market share of some companies offering a useful leverage point in broader state competition. The previously mentioned Snowden revelations put a fine point on how far the former practice could be taken. A prominent example of the latter was China's effort to more explicitly fuse these public/private dynamics by fostering development projects and information-technology companies like Huawei, which offers highly competitive mobile and Internet infrastructure that some believe will "set the foundation for . . . a nascent global surveillance architecture" (Riikonen, 2019, p. 124). China likely views this as merely an advance on longstanding U.S. practice. As early as 2010 the U.S. State Department was famously using Google's refusal to continue censoring searches in China, and its threat to pull out of its market because Beijing was stealing Google's source code and hacking into Gmail accounts, to chastise China and "ask for new norms on the Internet" (Nye, 2011, pp. 140–142).

The purposes and methods sought by these political-economic interventions differ slightly, but the general thrust is much the same: utilizing the economic might of even supposedly private Internet companies to secure and gain power relative to other states. As Power and Jablonski (2015, p. 206) conclude in their provocative book on what they claim is the "real cyber war"—the war over who controls and shapes the Internet—"activists and academics alike need to be much more cautious in their use and defense of Internet-freedom discourse," as the very progenitors of that discourse—namely the United States and the digital giants—effectively colluded in utilizing the openness the Internet promises to develop the largest surveillance apparatus the world has ever seen. It is that war over the shape of the cyberspace to come that is now addressed.

Global Cyber-Governance

Early pronouncements that the Internet constituted its own sovereign space were partly a reflection of the fact that it was and to some degree still is largely governed by a mélange of nonstate entities. For instance, two of the earliest and most prominent, the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN), still interact with governmental and nongovernmental actors—from corporations to human rights nongovernmental organizations (NGOs)—to maintain the basic shape and operability of the global Internet. The former came out of U.S.–funded meetings of computer scientists and network engineers in the mid-1980s, and in 1993 became a voluntary association that works foremost on the protocols that determine how data travels online. The latter, an American nonprofit, manages the domain name system that plays "a critical role in maintaining universal connectivity" (Mueller, 2018, p. 2). Given the crucial role such entities play, the model for Internet governance is usually defined as "multi-stakeholder," an arrangement where "two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules" (Raymond & DeNardis, 2015, p. 573). This model is often assumed to be a function of the need to maintain openness and optimization given the technological complexity involved.

However, and hinted at by the origins of the previous examples, some scholars have pushed back on this benign image of multi-stakeholderism, noting how in key ways it is used cynically and often maintained by and for the benefit of the United States and its allies (Carr, 2015, 2016; Price, 2018; Raymond & DeNardis, 2015). This is certainly the view of the two countries, Russia and China, who have most sought to shift Internet governance toward a multilateral framework, wherein states would have formalized dominance over the shape of the Internet going forward (Lantis & Bloomberg, 2018; Nocetti, 2015).

The push for multilateral control was first explicitly voiced in a number international conferences in the early 2010s. This timing very much reflects Fidler's "third image push-back," and indeed the entire issue of governing or regulating the Internet has become securitized (Cavelty, 2013; Wagner, 2019), with the issue of cybersecurity[4] placed as both

the primary obstacle and motivator to "the ultimate goal of shaping an international consensus for the digital age" (Slack, 2016, p. 69).[4] The stakes, it seems, could not be higher. As one of the foremost scholars of Internet governance contends, the "ongoing battle over multistakeholder vs. multilateral governance was—and is—really a battle about sovereignty," the foundational norm of the international system (Mueller, 2018, p. 1). Sovereignty, of course, is usually thought to entail a defined geographic territory within which states have a monopoly over legitimate violence, and also suffer no higher authority externally—making it seemingly antithetical to a global and open cyberspace. As such, some question whether cyberspace will have its own "Westphalian" moment—a reference to the 17th-century treaty often marked as first enshrining modern notions of sovereignty—involving the "territorialization" of the Internet (Demchak & Dombrowski, 2013).

To some this sovereigntist framework oversimplifies the complexity and wide-ranging implications of Internet governance (Mueller, 2019). In the first place, all of the developments previously discussed are fodder for the ongoing struggle. Supporters of the multistakeholder model fear a multilateral framework will allow authoritarian states to further legitimize their control mechanisms, multilateralists view the multi-stakeholder model as a Trojan horse for Western intrusions upon their sovereignty, and the increasing militarization of cyberspace more generally reflects the sense in which all states are viewing their foreign policies through a cyberspace lens—and thus, whether through formal mechanisms or not, are more interested in shaping its contours. Any movement toward strict sovereigntist multilateral control will be far from simple or predictable. To this Lambach (2019, p. 2) contends much of the debate operates with an outdated notion of the connection between sovereignty and territory, which is then problematically juxtaposed to an idealized vision of the "network character of the Internet." A "more promising approach," he contends, is to concentrate on the ways states exercise control more generally in cyberspace—surveillance and influence over private cyberspace actors, for instance, as a form of governance—all while recognizing that the supposedly "flat" network actually entails nodes and processes of varying degrees of importance (Lambach, 2019, pp. 4–8). Likewise, Raymond (2016, p. 129; DeNardis, 2014) persuasively argues we must move beyond considering merely the "Internet governance regime concerned with core technical functions," and recognize "a nascent global cyber-regime complex . . . [where] organizations with primary interests and responsibilities removed from the Internet and cyberspace are beginning to make decisions and to enact rules that can have significant unintended consequences for the stability and interoperability of the cyber domain."

This broader vision reflects a conceptual shift. Earlier concentration on the multi-stakeholder model, and on particular organizations dealing with technical aspects of Internet operability, defined "governance as deliberate, targeted regulation," while those widening the scope of the governance debate saw governance as, at least in this realm, increasingly a de facto result of "heterogeneous, more or less interdependent processes and practices" (Hofman, Katzenbach, & Gollatz, 2017, p. 1409). If it can be recognized that the issue of governance is at its core motivated by concern for the shape of cyberspace going forward, it is clear that mere concentration on technical bodies and international

meetings will be unlikely to capture enough of the picture of the international forces at work. For even setting aside the potential increased role of state actors, “emergent orders are manifold in digital contexts,” meaning that “much of the Internet’s ordering takes place unintentionally” (Hofman, Katzenbach, & Gollatz, 2017, p. 1412; Van Eeten & Mueller, 2013). Given this complex environment for governance, Mueller (2017) argues that the network effects mentioned earlier serve to maintain cyberspace as a place with the same global “language” of Internet protocols, and so rather than a future where cyberspace becomes territorially “fragmented,” a better conceptual frame would be that of “alignment.” States are adapting a global Internet to fit their localized legal and political structures, but its global characteristic will be maintained.

This mosaic reality is reflected in a growing number of voices theorizing a way forward that mainly involves building upon the current “regime complex,” conceived as a loosely connected set of separate regimes, each with their own more or less hierarchically organized norms (Nye, 2014). Rather than attempting to construct a comprehensive international legal remedy for cyber-governance, most actors seem keen to concentrate on the more amorphous realm of norm construction (Finnemore & Hollis, 2016, pp. 437–438). Some do argue, pointing to efforts like the ongoing NATO-sponsored *Tallinn Manual* process (Schmitt, 2017), that it is possible to imagine like-minded groups of states using *existing* international law to come to agreement on crucial cyberspace norms, with this eventually leading to broader international consensus (Saran, 2016; Slack, 2016). But as those proposing a cyber-Westphalia warn, because of the complexity and uncertainty of the technology, we are likely in for a “nonlinear, dangerous, and lengthy” period of transition (Demchak & Dombrowski, 2013, p. 33). Overlapping and ever-changing norms may be an unwieldy necessity. For instance, on probably the most central regime of the entire complex, cybersecurity, Raymond’s creative proposal is for states to treat all “negative effects on the stability or global interoperability of cyberspace” as unintended, and invite cooperation from all in resolving problems (2016, p. 134). This “responsibility to troubleshoot” would hopefully then cultivate “a norm that all relevant actors must participate in good faith in efforts to resolve threats to the stability and interoperability of cyberspace,” thus not only warding against escalation but also exposing bad actors who failed to participate (Raymond, 2016, p. 135). Needless to say, the development of such a norm will be quite precarious, and will no doubt benefit from IS work on the “strategic social construction of norms” in cyberspace like that provided by Finnemore and Hollis (2016, pp. 462–477), who detail the complex processes that must operate for norms to be effective and offer advice on framing and context, the trade-offs necessary in choosing who and what a norm covers, and the tools best able to promote adoption. Mueller (2017; cf. Drezner, 2019) is hopeful that what comes out of such processes may result in the rise of a new global polity, one that, if not superseding the state, will at least be tasked with managing the cyberpolitical node of international politics.

Some, of course, are less optimistic. Are these merely “minimalist” proposals, largely aimed at avoiding worst-case scenarios? Is there a danger that “voluntary non-binding norms, rules and principles” effectively leave powerful actors in control of the “operating environment,” and thus the “emphasis on sub-optimal solutions supports the reckless cy-

berspace operations of the most powerful and the most eager governments" (Kerttunen & Tikk, 2019, p. 39; Mosco, 2017)? One way of dealing with this overreach/under-reach dilemma is to go back to first principles, an exercise conducted in a special "roundtable" in the venerable *Ethics & International Affairs*. Hollis and Mauer (2018) challenged the various authors to envision how cyberspace should be governed depending on various "prime directives," specifically those grounded in human rights, economics, or security. Deibert's "human-centric" approach (2018, p. 416; cf. Mueller & Badiei, 2019) emphasizes individual rights to privacy online, and so, for instance, would require that cybersecurity not involve special "back-doors" for state security agencies. Weitzner's proposal for constructing a cyberspace that does the most possible to generate economic prosperity (2018, p. 437) emphasizes measures for securing what he calls the Internet's "technology policy foundations—free expression, intermediary liability limitation, protection against unfettered government surveillance, open technical and operating standards, consumer privacy, and net neutrality"—against big data analytics, monopolistic platforms, and technologically sophisticated authoritarian regimes. Most provocative—and perhaps also most instructive—is imagining a cyberspace reshaped to primarily serve as a national security tool. Hollis and Ohlin (2018) argue this would entail much more robust and formal state control over the Internet, the extension to the cyber-domain of the rules that have guided warfare for centuries, and significant curtailment of the economic and political freedom of companies and individual online users. As they point out, depending on how much this dampens the insecurity cyberspace may entail going forward, such developments might "actually end up causing less harm . . . in interstate conflicts," and represent on balance a "positive outcome" for an admittedly much more regulated citizenry (Hollis & Ohlin, 2018, p. 453).

Conclusion

This review operated from the general thesis that the study of international politics will, by necessity, increasingly become the study of international cyberpolitics. In probing that thesis, it was organized around state efforts to resist and control the global cyberspace phenomenon, utilize it in their foreign policy, and shape cyberspace to serve their interests. All three of those aspects of international cyberpolitics are rich with activity and import, so much so that, as Wagner (2019, p. 64) puts it, there is an ongoing "cyberfication" of states' security and foreign policy institutions. Far from a temporary development, then, the challenge now seems to be theorizing a future where cyberpolitics becomes only further entrenched as a core element of international relations (DeNardis, 2020).

Most theorists, even those operating from realist premises and proposing the notion of a cyber-Westphalia, seem to share a baseline agreement with Choucri and Clark's notion of co-evolving systems (2018), which suggests what occurs in and through cyberspace is of equal weight to more traditional international practices. That insight, though, means little if we cannot theorize and analyze in adequate detail the practices and processes by which that coevolution is unfolding. Toward that, helpful are theorizations like Deibert and Pauly's description of the "complex sovereignty" being generated by this co-evolution

(2019), where they introduce the dynamic of "mutual entanglement." This concept describes a dialectical process whereby sovereign prerogatives are realized both by taking advantage of opportunities to enclose or at least shape Internet activity "inside" a territorially based state, *and* by utilizing some degree of Internet openness to observe and effect happenings on the "outside." Which means, as they put it, that 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" (Deibert & Pauly, 2019, p. 82). The cyberpolitical practices reviewed here, then, are generating "a new and very highly interdependent systemic architecture":

> Anarchy does not describe its political underpinnings, and neither does a straightforward notion of hierarchy . . . [It instead involves] continuously re-embedding political authorities in distributed and fast-changing digital webs. . . . 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 . . . [and] is having a transformative impact on the territorial state as conventionally conceived. . . .
>
> (Deibert & Pauly, 2019, pp. 93–94)

If even a fraction of that vision is true, it will also likely have profound implications for how we analyze our subject. Indeed, even Demchak and Dombrowski (2013, p. 32) claim we must "move beyond the framing of mainstream political science, international relations, and security studies scholarship." Demchak (2017, pp. 150–152) calls for a "new explanation of the world" that can account for a "more authoritarian global order," and guide Western democracies toward a cyber-alliance that is "adaptively secured and securable over the longer term, [and] which also, in the near term, defends each joint partner along with itself." Some, like McCarthy (2018, p. 10), go even deeper, arguing that to be attuned to both the socially constructed and constructing nature of Internet technology we must operate somewhere under the broad post-positivist philosophical and methodological umbrella. This, of course, is a quite sweeping claim, especially given that McCarthy (2018, p. 14) also argues "all of global politics is necessarily socio-technical." Others, either by example or explicitly, emphasize the degree to which scholars will have to develop transdisciplinary ties and expertise (Bigo, Isin, & Ruppert, 2019), especially in the technical fields themselves (Steed, 2019).

As this illustrates, cyberpolitics is also internal to research in IR and other disciplines within IS. Just as scholars have branched out to investigate how international politics is practiced online, is affected by the Internet, and is part of the continuing technological evolution of cyberspace, so too have they begun to question whether and how this revolutionary technology should change the way researchers approach their task (Carpenter & Drezner, 2010; Shephard, 2016). To date there is no coherent construction of or debate over the disciplinary and methodological implications of international cyberpolitics. But if, as Der Derian (2003, p. 452) argued some time ago, the growth of cyberpolitics requires

"new modes of comprehension and instruction"—because the technology evolves so unpredictably, because it brings new levels of rapidity to politics, and because to truly understand how this works requires some degree of technological expertise—determining just what those are may be crucial to the future salience of the knowledge produced about international politics.

References

Arquilla, J. (2009, July 26). **Click, click . . . counting down to Cyber 9/11**. *SFGate*.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141–165.

Barlow, J. P. (1996). **A declaration of the independence of cyberspace**.

Barnett, M., & Duvall, R. (2005). Power in international politics. *International Organization*, *59*(1), 39–75.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press.

Bigo, D., Isin, E., & Ruppert, E. (Eds.). (2019). *Data politics: Worlds, subjects, rights*. Abingdon, UK: Routledge.

Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, *26*(3), 452–481.

Bossetta, M. (2018). The weaponization of social media: Spear phishing and cyberattacks on democracy. *Journal of International Affairs*, *Special Issue*, *71*(1.5), 97–106.

Bradshaw, S., & Howard, P. N. (2018). The global organization of social media disinformation campaigns. *Journal of International Affairs*, *Special Issue*, *71*(1.5), 23–31.

Brantley, A. F. (2016). *The decision to attack: Military and intelligence cyber decision-making*. Athens, GA: University of Georgia Press.

Carpenter, C., & Drezner, D. W. (2010). International Relations 2.0: The implications of new media for an old profession. *International Studies Perspectives*, *11*(3), 255–272.

Carr, M. (2015). Power plays in global internet governance. *Millennium: Journal of International Studies*, *43*(2), 640–659.

Carr, M. (2016). *US power and the Internet in International Relations: The irony of the Information Age*. London, UK: Palgrave Macmillan.

Cavelty, M. D. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Choucri, N., & Clark, D. D. (2018). *International Relations in the Cyber Age: The co-evolution dilemma*. Cambridge, MA: The MIT Press.

Cockfield, A., Hellerstein, W., & Lamensch, M. (2020). *Taxing global digital commerce*. Alphen aan den Rijn, The Netherlands: Kluwer Law International BV.

Deibert, R. J. (2015). The geopolitics of cyberspace after Snowden. *Current History*, *114*(768), 9–15.

Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. *Ethics & International Affairs*, *32*(4), 411–424.

Deibert, R. J. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy*, *30*(1), 25–39.

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

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2011). *Access contested: Security, identity, and resistance in Asian cyberspace*. Cambridge, MA: MIT Press.

Deibert, R. J., & Pauly, L. W. (2019). Mutual entanglement and complex sovereignty in cyberspace. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics: Worlds, subjects, rights* (pp. 81–99). Abingdon, UK: Routledge.

Deibert, R., & Rohozinski, R. (2011). Contesting cyberspace and the coming crisis of authority. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access contested: Security, identity, and resistance in Asian cyberspace* (pp. 21–41). Cambridge, MA: MIT Press.

Delerue, F. (2020). *Cyber operations and international law*. Cambridge, UK: Cambridge University Press.

Demchak, C. C. (2017). Defending democracies in cybered world. *Brown Journal of World Affairs*, *24*(1), 139–158.

Demchak, C. C. (2019). China: Determined to dominate cyberspace and AI. *Bulletin of the Atomic Scientists*, *75*(3), 99–104.

Demchak, C. C., & Dombrowski, P. (2013). Cyber Westphalia: Asserting state prerogatives in cyberspace. *Georgetown Journal of International Affairs*, 29–38.

DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press.

DeNardis, L. (2020). *The Internet in everything: Freedom and security in a world with no off switch*. New Haven, CT: Yale University Press.

DeNardis, L., & Raymond, M. (2017). The Internet of Things as a global policy frontier. *University of California, Davis Law Review*, *51*(2), 475–497.

Der Derian, J. (2003). The question of information technology in International Relations. *Millennium: Journal of International Studies*, *32*(3), 441–456.

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498

Drezner, D. W. (2010). Weighing the scales: The Internet's effect on state-society relations. *Brown Journal of World Affairs*, *16*(2), 31–44.

Drezner, D. W. (2019). Technological change and international relations. *International Relations*, *33*(2), 286–303.

Ebert, H., & Mauer, T. (2013). Contested cyberspace and rising powers. *Third World Quarterly*, *34*(6), 1054–1074.

Fang, B. (2018). *Cyberspace sovereignty: Reflections on building a community of common future in cyberspace*. Singapore: Science Press Beijing and Springer Nature Singapore.

Feldstein, S. (2019). The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy*, *30*(1), 40–52.

Fidler, D. P. (2014). Le cyberspace, c'est moi?: Authoritarian leaders, the Internet, and international politics. *Seton Hall Journal of Diplomacy and International Relations*, *1*(Fall–Winter), 7–22.

Fidler, D. P. (2015). U.S. foreign policy and the Snowden leaks. In D. P. Fidler (Ed.), *The Snowden reader* (pp. 52–69). Bloomington: Indiana University Press.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425–479.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, *13*(1), 42–54.

Haataja, S. (2019). *Cyber attacks and international law on the use of force: The turn to information ethics*. New York, NY: Routledge.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, *5*(1), 1–15.

Hick, S., Halpin, E., & Hoskins, E. (Eds.). (2000). *Human rights and the Internet*. New York, NY: St. Martin's Press.

Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*, *19*(9), 1406–1423.

Hollis, D. B., & Maurer, T. (2018). Introduction: Competing visions for cyberspace. *Ethics & International Affairs*, *32*(4), 407–410.

Hollis, D. B., & Ohlin, J. D. (2018). What if cyberspace were for fighting? *Ethics & International Affairs*, *32*(4), 441–456.

Jarvis, J. (2011). *Public parts: How sharing in the Digital Age improves the way we work and live*. New York, NY: Simon & Schuster.

Jiang, M. (2016). The coevolution of the Internet, (un)civil society, and authoritarianism in China. In J. deLisle, A. Goldstein, & G. Yang (Eds.), *The Internet, social media, and a changing China* (pp. 28–48). Philadelphia: University of Pennsylvania Press.

Johnson, D. R., & Post, D. (1996). Law and borders? The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367–1402.

Jørgensen, R. F. (Ed.). (2019). *Human rights in the age of platforms*. Cambridge, MA: The MIT Press.

Kaempf, S. (2013). The mediatisation of war in a transforming global media landscape. *Australian Journal of International Affairs*, *67*(5), 586–604.

Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.

Kerttunen, M., & Tikk, E. (2019). **The politics of stability: Cement and change in cyber affairs**. NUPI Report.

Lambach, D. (2019). The territorialization of cyberspace. *International Studies Review, viz022*, 1–25.

Lanoszka, A. (2019). Disinformation in international politics. *European Journal of International Security*, *4*(2), 227–248.

Lantis, J. S., & Bloomberg, D. J. (2018). Changing the code? Norm contestation and US antipreneurism in cyberspace. *International Relations*, *32*(2), 149–172.

Lee, S. P. (2014). The ethics of cyberattack. In L. Floridi & M. Taddeo (Eds.), *The ethics of information warfare* (pp. 105–122). New York, NY: Springer.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic Books.

Levinger, M. (2018). Master narratives of disinformation campaigns. *Journal of International Affairs*, *71*(1.5), 125–134.

Lewis, J. A. (2010). Sovereignty and the role of government in cyberspace. *Brown Journal of World Affairs*, *16*(2), 55–66.

Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge, UK: Cambridge University Press.

Libicki, M. C. (2016). Is there a cybersecurity dilemma? *The Cyber Defense Review*, *1*(1), 129–140.

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

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books.

Mainwaring, S. (2011). *We first: How brands and consumers use social media to build a better world*. New York, NY: Palgrave Macmillan.

Manjikian, M. M. (2010). From global village to virtual battlespace: The colonizing of the Internet and the extension of realpolitik. *International Studies Quarterly*, *54*(2), 381–401.

McCarthy, D. R. (2015). *Power, information technology, and International Relations Theory: The power and politics of US foreign policy and the Internet*. New York, NY: Palgrave Macmillan.

McCarthy, D. R. (2018). Introduction: Technology in world politics. In D. R. McCarthy (Ed.), *Technology and world politics: An introduction*. London, UK: Routledge.

McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the Internet against democracy*. New York, NY: The New Press.

Monshipouri, M., & Mokhtari, S. (2016). Conclusion: The quest for human rights in the digital age: How it has changed and the struggle ahead. In M. Monshipouri (Ed.), *Information politics, protests, and human rights in the Digital Age* (pp. 267–293). New York, NY: Cambridge University Press.

Morozov, E. (2011). *The Net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs.

Mosco, V. (2017). *Becoming digital: Toward a post-Internet society*. Bingley, UK: Emerald Group.

Mueller, M. (2017). *Will the Internet fragment?: Sovereignty, globalization and cyberspace*. Cambridge, UK: Polity Press.

Mueller, M. (2018). **Sovereignty and cyberspace: Institutions and Internet governance**. 5th annual Vincent and Elinor Ostrom memorial lecture.

Mueller, M. L. (2019). Against sovereignty in cyberspace. *International Studies Review*, *viz044*, 1–23.

Mueller, M. L., & Badiei, F. (2019). Requiem for a dream: On advancing human rights via Internet architecture. *Policy & Internet*, *11*(1), 61–83.

Naughton, J. (2016). The evolution of the Internet: From military experiment to general purpose technology. *Journal of Cyber Policy*, *1*(1), 5–28.

Nocetti, J. (2015). Contest and conquest: Russia and global Internet governance. *International Affairs*, *91*(1), 111–130.

Nye, J. S., Jr. (2011). *The future of power*. New York, NY: PublicAffairs.

Nye, J. S., Jr. (2014). ***The regime complex for managing global cyber activities***. Global Commission on Internet Governance, Paper 1. Centre for International Governance Innovation and the Royal Institute for International Affairs.

Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44–71.

Orend, B. (2014). Fog in the fifth dimension: The ethics of cyber-war. In L. Floridi & M. Taddeo (Eds.), *The ethics of information warfare* (pp. 3–23). New York, NY: Springer.

Paris, R. (2003). The globalization of taxation? Electronic commerce and the transformation of the state. *International Studies Quarterly*, *47*(2), 153–182.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. New York, NY: Penguin.

Pieterse, J. N. (2012). Leaking superpower: WikiLeaks and the contradictions of democracy. *Third World Quarterly*, *33*(10), 1909–1924.

Powers, S. M., & Jablonski, M. (2015). *The real cyber war: The political economy of Internet freedom*. Urbana: University of Illinois Press.

Price, M. (2018). The global politics of Internet governance: A case study in closure and technological design. In D. R. McCarthy (Ed.), *Technology and world politics: An introduction* (pp. 126–145). London, UK: Routledge.

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

Rattray, G. (2001). *Strategic warfare in cyberspace*. Cambridge, MA: MIT Press.

Raymond, M. (2016). Managing decentralized cyber governance: The responsibility to troubleshoot. *Strategic Studies Quarterly*, *10*(4), 123–149.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616.

Rid, T. (2013). *Cyberwar will not take place*. Oxford, UK: Oxford University Press.

Riikonen, A. (2019). Decide, disrupt, destroy. *Strategic Studies Quarterly*, *13*(4), 122–145.

Rovner, J., & Moore, T. (2017). Does the Internet need a hegemon? *Journal of Global Security Studies*, *2*(3), 184–203.

Saran, S. (2016). Striving for an international consensus on cyber security: Lessons from the 20th century. *Global Policy*, *7*(1), 93–95.

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. New York, NY: W. W. Norton.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge, UK: Cambridge University Press.

Shepherd, L. J. (2016). Authors and authenticity: Knowledge, representation and research in contemporary world politics. In C. Hamilton & L. J. Shepherd (Eds.), *Understanding popular culture and world politics in the Digital Age* (pp. 32–47). New York, NY: Routledge.

Shirkey, C. (2010). *Cognitive surplus: Creativity and generosity in a connected age*. New York, NY: Penguin.

Slack, C. (2016). Wired yet disconnected: The governance of international cyber relations. *Global Policy*, *7*(1), 69–78.

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, *41*(3), 72–109.

Steed, D. (2019). *The politics and technology of cyberspace*. New York, NY: Routledge.

Sunstein, C. (2006). *Infotopia: How many minds produce knowledge*. New York, NY: Oxford University Press.

Torres, P. (2019). The possibility and risks of artificial general intelligence. *Bulletin of the Atomic Scientists*, *75*(3), 105–108

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. New York, NY: Oxford University Press.

Van Eeten, M. J., & Mueller, M. (2013). Where is the governance in Internet governance? *New Media & Society*, *15*(5), 720–736.

Wagner, B. (2019). Constructed “cyber” realities and International Relations Theory. In J. P. Singh, M. Carr, & R. Marlin-Bennett (Eds.), *Science, technology, and art in International Relations* (pp. 60–70). New York, NY: Routledge.

Weitzner, D. J. (2018). Promoting economic prosperity in cyberspace. *Ethics & International Affairs*, *32*(4), 425–439.

Wilner, A. S. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*, *43*(2), 245–280.

Wu, T., & Goldsmith, J. (2006). *Who controls the Internet? Illusions of a borderless world*. New York, NY: Oxford University Press.

Zaharna, R. S., Arsenault, A., & Fisher, A. (Eds.). (2014). *Relational, networked and collaborative approaches to public diplomacy: The connective mindshift*. New York, NY: Routledge.

Zeng, J., Stevens, T., & Chen, Y. (2017). China’s solution to global cyber governance: Unpacking the domestic discourse of “Internet sovereignty.” *Politics & Policy*, *45*(3), 432–464.

Ziegler, C. E. (2018). International dimensions of electoral processes: Russia, the USA, and the 2016 elections. *International Politics*, *55*(5), 557–574.

Notes:

(1.) Cyberspace is here defined as “the billions of computers it connects, its management, and the experiences it enables” (Choucri & Clark, 2018, p. 3). As Mueller (2019, p. 10) notes, the sense that cyberspace is a unitary and global phenomenon may be basically true at present, but it need not be the case; the current “internet protocol family is not an essential part of the definition. If some other set of standards became globally adopted and enabled universal interoperability of computers, digital devices, and data in a virtual space, then they would create a global cyberspace too. Likewise, one could speak of multiple local or regional ‘cyberspaces’ if each of them relied on different and technically incompatible standards to create their own, isolated virtual spaces. But while theoretically possible, the idea of multiple cyberspaces is utterly counterfactual and irrelevant for IR. Cyberspace as we know it became a powerful factor in international relations because of society’s convergence on a single protocol family . . . which has created a globalized virtual space.”

(2.) There is a robust literature on the intersection of the human rights movement and cyberspace that largely concentrates on the flip side of this article’s focus, the emphasis being on how the Internet enables movements from below (e.g., Hick, Halpin, & Hoskins, 2000; Jørgensen, 2019). In a particularly insightful volume, Monshipouri and Mokhati (2016, p. 293) conclude that, partly because of the very denial and control mechanisms this section surveys, “for new technological tools to be used to effectively influence electoral politics, stage peaceful civil disobedience and protest, mobilize efforts for any other

democratic purposes, and offer a sense of promise, a variety of other conducive social and political circumstances must be in place.”

(3.) This is not to say some are not still sounding alarm bells, but the focus has shifted to future developments like artificial intelligence (AI) and its effects on cyber-conflict (Scharre, 2018; Torres, 2019).

(4.) Finnemore and Hollis (2016, p. 431) succinctly define cybersecurity as “the protection of information and communication technologies from unauthorized access or attempted access.”

Benjamin R. Banta

Department of Political Science, Rochester Institute of Technology