3 Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field

Milton L. Mueller and Farzaneh Badiei

This chapter tracks the emergence of "Internet governance" as a label, a field of research and academic study, and a real-world arena where stakeholders and interest groups clash and cooperate. We try to look at all three of them simultaneously—label, field of study, and set of practices and institutions—focusing on the interplay among them over time. We have chosen to begin our assessment of the field of Internet governance on the basis of when the term started to be consciously recognized as a phenomenon and labeled as such.

Some may argue that some form of Internet governance was occurring before this; they might, for example, begin with the US Department of Defense's ARPANET and would characterize hammering out some of the early design principles of internetworking as Internet governance. An even broader approach, developed by Sandra Braman in chapter 2, tries to situate Internet governance in the convergence of computing and communication technologies in the 1950s and 1960s and the globalization of communication networks in the 1970s and 1980s. And while it is true that the Internet entered a policy context shaped by these processes, it is also true that the policy and governance of integrated services digital network (ISDN), or cross-border data flows over private leased telecommunication circuits, cannot be characterized as Internet governance. The Internet had its own distinctive protocols that posed unique governance problems. The Internet also evolved its own standards development organizations and governance institutions, such as the Internet Engineering Task Force (IETF) and address registries, that were outside the established institutions of global telecommunications governance.

Historical periodizations are neither correct nor incorrect; they are more or less suited to specific purposes. Our purpose is not to track communications policy in general but to reveal the trajectory of Internet governance as

a distinct arena of public policy and global governance. By doing that, we hope to assess the usefulness and longevity of the term "Internet governance" as the label for this field. It makes sense, therefore, to start with the time period after the Internet protocols had been developed and implemented and their use by the public had reached the point at which it posed problems that had to be resolved in public arenas through legal, political, and institutional means. This did not happen until the Internet was open to widespread public use and was recognized as something that could be or should be subject to public governance.

Our chapter contributes to the overarching theme of this book by analyzing the evolution of the field of Internet governance studies. We show how Internet governance research and scholarly participation appeared at stages of the Internet's development, the emergence of distinct Internet governance problems, and how and why they became important research topics. This can help scholars identify emerging topics that relate to Internet governance. We have also identified how various disciplines got involved with Internet governance research. For example, early on, the Internet governance field was mostly rooted in legal studies, but as the Internet became more widespread, its governance started to intersect with other fields such as political science and international relations. We briefly mention the emergence of theories of Internet governance, new research methods, and the use of new research tools to analyze Internet-generated data.

Phase One (1993–1997): Discovery and Exceptionalism

The term "Internet governance," as far as we can tell, does not appear in any scholarly or news articles before 1995 (Kowack 1995). But the words "governance" and "law," on the one hand, and "cyberspace," "Internet," and "the Net," on the other, started to be used in close association with each other several years before that, roughly from 1993 on (see, for example, Braman 1995). That period corresponds to the emergence of the Internet as a mass public medium. That emergence was contingent on three events: the development and adoption of the World Wide Web protocol from 1989–1993, the publication of freely downloadable web browser software after 1991, and the privatization of the Internet backbone and its opening to commercial use by the US National Science Foundation in 1995. Together, these developments

made the Internet accessible to ordinary businesses and end users. (For an early newspaper account of this transition, see Lewis [1994].)

The most notable and interesting feature of the earliest Internet governance discourse is its vigorous debate on conceiving of cyberspace as its own place, or what some have called Internet exceptionalism. John Perry Barlow (1996) is usually put forward as the paragon of exceptionalism, but typically this is done to discredit the idea on the cheap. Barlow is a convenient strawman for antiexceptionalists because he was a rock lyricist, not a social science scholar, and his *Declaration* was a manifesto and rallying cry, not a carefully developed, theoretically grounded argument.

But contemporary to Barlow, legal scholars were having a far more serious debate about the extent to which cyberspace was a terrain that should develop its own rules and institutions. David Johnson and David Post were also exceptionalists (Johnson and Post 1996), and they were among the first to ask explicitly, "How shall the net be governed?" (Johnson and Post 1997). Focusing on the Internet's operational reliance on voluntary transborder cooperation, they developed an argument for decentralized, emergent law as an alternative to traditional hierarchical, state-centric control. The word "governance," which was also gaining credence in UN documents at the same time (UNDP 1997), was a softer term than "government" and implied a more polycentric order.

Johnson and Post's argument is often unfairly equated with a cruder, technological determinist argument that the Internet is inherently resistant to state control. But the emergent law argument was normative, not positive: it asserted that the Internet could and probably *should* follow a new model of nonnational governance, not that it necessarily *would* be governed in that way.

Even before Johnson and Post, in what is perhaps the earliest law review article on cyberspace governance, Hardy (1994) also opted for the exceptionalist camp. Like others in this period, he does not use the term "Internet governance" but refers to cyberspace law, or the customs and rules associated with its governance. His paper asks whether we should treat (the whole of) cyberspace as a separate jurisdiction. While inspired by law and economics scholars and judges, Hardy also refers to multistakeholder collaboration and bottom-up rulemaking. He rejects established intergovernmental organizations as unsuitable for resolving transjurisdictional

disputes on the Internet and instead puts forward the idea of having a world cyber court. He calls for "international cooperation among a wide array of groups" for the court, which seems to imply a multistakeholder governance system. Similarly, Tim Wu addressed the issue of cyberspace sovereignty—not the sovereignty of states, but of cyberspace itself—in 1997 (Wu 1997). Wu's treatment contained a remarkably prescient discussion of the application of international relations theory to cyberspace governance. As with Hardy, cyberspace governance, not Internet governance, is the dominant label. It was, as the next section explains, the formation of the Internet Corporation for Assigned Names and Numbers (ICANN) that cemented the term "Internet governance" into place.

Aside from the broad discourse about the new world created by cyberspace, legal scholars were attuned to the less sweeping but still novel and intellectually exciting problems raised by the commercialization of the Internet. Novel legal issues were posed by the nascent online economy:

- Trademark law and domain names (Burk 1995)
- Intermediary responsibility and copyright protection (Boyle 1996; Hardy 1994; Samuelson 1996)
- Censorship and filtering of Internet content (Resnick 1997; Resnick and Miller 1996)
- Private contract law versus public law and jurisdictional conflict (Perritt 1996)

As the fascination with cyberlaw studies burgeoned, conservative legal scholars reacted against it, insisting that there was no new cyber jurisdiction or territory or that calls for a new jurisdiction constituted a call for "cyber-anarchy" (Goldsmith 1998). Cyberlaw was ridiculed as tantamount to the study of "the law of the horse" (Easterbrook 1996). Such an effort, a prominent legal scholar proclaimed, was bound to be "shallow and to miss unifying principles" (Easterbrook 1996, 207).

Easterbrook was claiming—wrongly as it turned out—that technology did not or could not transform societal interactions sufficiently to justify a specific analysis of how law related to the technology. This evolved into a debate on the sociology of technology. Legal scholars were asking whether Internet technology altered laws and institutions or were incorporated into established legal principles, just as science and technology studies had for some years before been defined by an ongoing debate between realists who

emphasize the autonomous or deterministic effect of technologies and social constructivists who focus on how societal factors shape the final form taken by technical systems. Lessig's (1999a) code-as-law argument was, in essence, an attempt by a legal scholar to reinvent the wheel of social studies of technology.

A key feature of this period is that the Internet governance field is rooted in legal studies. The literature is already addressing issues in international relations, institutional theory, science and technology studies, global governance, and the role of global civil society, but legal scholars are doing most of the work (Kowack [1995] is a rare exception). In retrospect, almost every aspect of current issues in Internet governance, including the nexus between national security and cybersecurity (Arquilla and Ronfeldt 1993), had been posed in some form in these initial years. Yet in this first phase, North America is overwhelmingly the center of research and writing. Very little attention is paid to the implications of Internet growth and policy to other nations or cultures or to how Internet governance might play into interstate rivalries.

Phase Two (1996–2003): ICANN *Über Alles*

The term "Internet governance" came to prominence in 1996–1999, when it became associated with the struggle to create a new institution to take over global coordination of Internet domain names and IP addresses. The formation of ICANN took center stage in Internet governance discourse and research, and the term "Internet governance" became widely used to describe this area.[1] Ironically, during the period in which "Internet governance" becomes widely used as the label for the conflicts over control of the root of the domain name system (DNS) and the policy battles associated with domain-name trademark conflicts, the term is also actively resisted by many involved in the names and numbers debates, especially the technical community stakeholders.[2] In what turns out to be a losing battle, they insist that "governance" is a misleading term because the Internet Assigned Numbers Authority (IANA) is not the Internet and governance of domain name and IP address resources is merely technical management, not governance or policy. A seminal book from this period, which published the results of a 1996 conference of academics and practitioners around the problem of institutionalizing the IANA, was deliberately titled *Coordinating*

the Internet and did not refer to governing it (Kahin and Keller 1997). And yet, almost all results of searching the LexisNexis Academic database for the term "Internet governance" in this period relate to the controversies over control of IANA and the formation of ICANN.

Research and writing during this period shifted away from more abstract exceptionalism debates to the question of building a real governance institution. But exceptionalism was often an unstated assumption, in that few actors in a position of influence wanted the Internet to be subsumed under existing intergovernmental regimes. Who, then, would control a global, centralized institutional framework to coordinate domain name and address assignment? How would this institution be structured? How would it be made accountable? Fulfilling the expectations and norms of the exceptionalists, the encounter with those problems culminated in an institutional innovation, the ICANN (Mueller 2002).

The formation of the ICANN regime resolved conflicts over property rights that had been created by attempts to appropriate new global technical resources (primarily domain names). It also addressed the coordination problems posed by managing critical Internet resources in a manner that would retain global compatibility. As Wolfgang Kleinwächter noted, ICANN was a "silent subversive" because of the way it altered the role of states in global governance (Kleinwächter 2001). Indeed, for a time ICANN was hailed as a paradigm of new forms of governance ushered in by the networked age (Ahlert 2001; Hofmann 2005; Levinson 2002). Others, however, while recognizing its novelty, mounted strong challenges to the model's legality and legitimacy (Froomkin 2000; Weinberg 2000).

ICANN was controversial because it was a private nonprofit corporation unilaterally delegated by the United States to be the global authority over the root of the domain name and Internet address spaces and empowered to resolve key public policy problems through the issuance of private contracts. These contracts were a means of addressing competition policy issues in the commercial market for domain names, domain-name trademark conflicts, the allocation of Internet addresses, and related problems. Klein and several others explore another interesting aspect of the ICANN experiment—namely, its early attempt to use global, democratic elections to keep its board of directors accountable (Klein 2001; Palfrey 2004; Weinberg 2001).

Given the overarching *problematique* of the relationship between internetworking and national sovereignty, the role of governments in ICANN's

formation has always been a topic of interest, and we begin to see political scientists drawn into Internet governance research. Volker Leib and Daniel Drezner, for example, examined EU–US interactions in the initial negotiations over ICANN (Drezner 2007; Farrell 2003; Leib 2002). In the real world of institutions, this *problematique* led to the creation and gradual empowerment of ICANN's Governmental Advisory Committee (GAC). The GAC was a strange beast: simultaneously a mini-intergovernmental organization composed of representatives of nation-states and an organ of a private California nonprofit public benefit corporation offering nonbinding advice to the organization (Weinberg 2011).

Phase Three (2003–2009): World Summit on the Information Society and Internet Governance Forum

In the 2003–2009 phase, Internet governance becomes fully recognized as a domain of global governance, and the boundaries of what is considered Internet governance expand beyond ICANN. In the business world, this phase also marks the rise of social media platforms around global corporations such as Facebook, Twitter, and Google. Large-scale global intermediaries residing on the Internet transform the context in which traditional communication policy issues are debated. But the key turning point in both research field formation and the actual practice of governance was the World Summit on the Information Society (WSIS).

During the WSIS, which lasted from 2002 to 2005, ICANN became the provocation for international clashes over the US role in Internet governance and the position of state and nonstate actors in shaping it. Using Google search counts as a metric, we find that the period of the WSIS corresponds to the high point of "Internet governance" as a search term with currency among the web-using public (figure 3.1). Awareness of Internet governance was raised in the developing world and especially among diplomats and government ministries, who had to learn what Internet governance (and perhaps even what the Internet) was. It led to the creation, in 2004, of the UN Working Group on Internet Governance (WGIG), which was charged with developing a working definition of the term. In the early stages of the WSIS process, definitional debates centered on the distinction between a narrow approach, encompassing only ICANN-related functions, and a broad definition, seeming to include anything and everything related

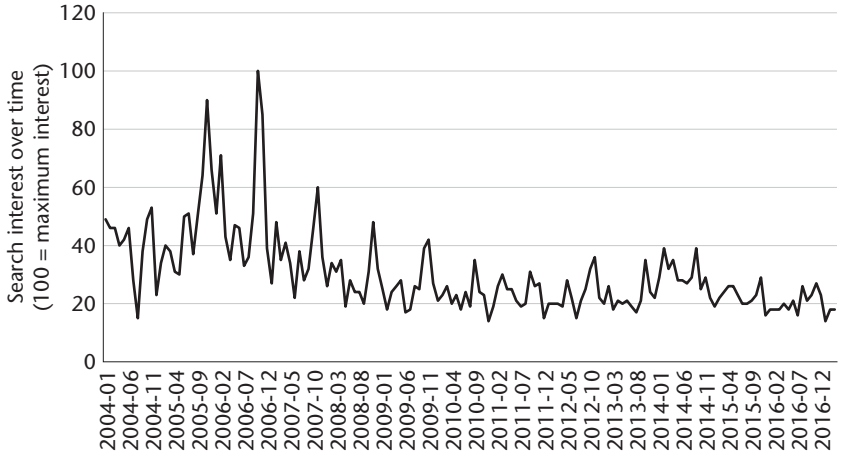

Figure 3.1
Occurrence of "Internet governance" as a search term worldwide by year.

to information and communication technologies. Both extremes missed the mark. Confining concepts of Internet governance to ICANN was justified by the undeniable fact that DNS and IP governance was central to the actual functioning of the global Internet, but it was evident that other processes also governed the global Internet, such as standardization bodies, trade in services agreements, World Intellectual Property Organization treaties, law enforcement activities related to cybercrime, and so on. On the other hand, any attempt to stretch "Internet governance" to include matters like the construction of physical telecommunications infrastructure, spectrum management, open standards, national e-government initiatives, and the like was simply based on an uncritical attempt to conflate all forms of information and communication technology with the Internet.

In its agreed definition, the WGIG expanded the meaning of Internet governance beyond ICANN, applying the term to any and all "shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (Drake 2005; MacLean 2004). The definition obviously drew on Krasner's (1983) canonical definition of international regimes but, reflecting the enlarged role of nonstate actors in managing the Internet, noted that these shared processes involve not just governments but business and civil society as well.

The WGIG-WSIS definition ratified the position of nonstate actors in Internet governance and put many of the traditional problems of communication and information policy within its frame. Reinforcing this trend, in their confrontation with states, ICANN and its defenders found it useful to emphasize the open and multistakeholder nature of ICANN processes. What had been described as private sector leadership or self-regulation in the early days of ICANN's formation was now repackaged as the multistakeholder model. Intergovernmental organizations such as the United Nations and intergovernmental processes such as the WSIS had to be opened up to civil society and the private sector. Whereas, before, ICANN's most powerful actors had scorned or marginalized civil society stakeholders, they now embraced them as evidence of their relative openness and the superiority of its private-sector-led governance model. A new line of research opened around multistakeholder governance, and Internet governance researchers began to look at other domains such as the environment for precedents and at the preexisting literature on transnational governance networks (Cave et al. 2007; DeNardis and Raymond 2013; Levinson and Smith 2008; Sørenson and Torfing 2007).

The literature on the WSIS is large and of uneven quality but contains many important insights into international institutions, the participation of civil society in global governance, the role of the United States, and of course Internet governance itself. One of the ironies of the WSIS is that it was supposed to address the full range of communication-information policy but ended up becoming almost entirely focused on ICANN and Internet governance. A good descriptive analysis of the WSIS process from the standpoint of a traditional civil society development advocate and UN system insider can be found in Souter (2007). Hans Klein (2004) provides a valuable analysis of the politics of the WSIS placed in the context of UN summits. Wolfgang Kleinwächter (2004) and Marc Raboy (2004) provide additional participant accounts of the WSIS process, while Mueller (2010) examines the post-WSIS Internet governance landscape and emphasizes the continuing tension between networks and states as forms of governance.

WSIS created a new set of expectations regarding the ability of civil society actors to participate in global Internet governance processes (Padovani and Tuzzi 2004; O'Siochru 2004; Raboy 2004). While it often disappointed stronger advocates of participatory democracy and failed to resolve the

debates about ICANN and the US unilateral role in Internet governance, WSIS did create a new institutional vehicle for carrying on discussion and debate around those issues: the multistakeholder Internet Governance Forum (IGF). There is a huge amount of policy literature and occasional papers around the IGF but very little deep scholarly analysis. Malcolm (2008) carefully traces the developments of the IGF's first two years and offers a normative analysis of how it can be reformed to fulfill the promise of multistakeholder governance.

Another immediate result of WSIS was the formation of an academic network specifically devoted to Internet governance research: the Global Internet Governance Academic Network (GigaNet) in 2006. In early 2006, during the formative stages of the new UN IGF, emails and conversations among a core group of academics led to a conclusion that within the post-WSIS environment there was no natural home for Internet governance research and education. They decided to create their own independent academic platform, introducing a sometimes awkward separation from the civil society nongovernmental organizations with whom they had been connected during the WSIS process. GigaNet has held annual symposia showcasing Internet governance research concurrently with the IGF every year since the first IGF in 2006.

The dialogue and writing about the appropriate definition of Internet governance was not entirely settled by WSIS but continues to this day. To some, Internet governance includes only those technical, legal, regulatory and policy problems that arise as a direct consequence of the involved parties' mutual use of the Internet protocols to communicate. Laura DeNardis provides a clearly reasoned basis for distinguishing between studies of Internet content and usage and the governance of the Internet per se. "Issues of Internet governance relate to Internet-unique technical architecture rather than the larger sphere of information and communication technology design and policy" (DeNardis, 2014, 19). Another issue is that governance in cyberspace is so distributed and indirect that it is often unclear where authority to govern lies. Van Eeten and Mueller (2013) initiated a critical scholarly debate about whether IGF and other forums in which Internet governance is discussed can be considered Internet governance at all. That debate is taken up by Hofmann, Katzenbach, and Gollack (2016), who attempt to introduce a distinction between governance and regulation.

Whether the IGF constitutes governance or a mere talk shop, it seems to have set in motion a process of institutional isomorphism, with multiple

national and regional Internet governance forums following in its wake (Epstein and Nonnecke 2016). Studying these forums, Epstein and Nonnecke develop a distinction between substantive and performative multistakeholder governance of the Internet. Although the IGF is more of a performative multistakeholder Internet governance process, they argue that the regional and national Internet governance forums may become the link between the UN IGF and local Internet rulemaking.

While WSIS captured the attention of scholars who self-identified as Internet governance researchers and analysts, a whole new set of governance problems was brewing in the largely noninstitutionalized space formed by transnational Internet services and commerce. There was growing awareness of the power of states to shape Internet governance, led by an oft-cited work by Goldsmith and Wu (2006) arguing that states are still in control and everything will return to normal. At the same time, other scholars emphasized the ways the Internet had altered the nature of global governance of information and communication and that new forms of governance were developing.

One key area of development was Internet content regulation—that is, blocking and filtering. As nation-states gradually learned how to filter and block websites from outside their jurisdiction as an attempt to maintain sovereign control of information—and users and external actors explored ways to circumvent those barriers—an important empirical body of literature grew up around efforts by scholars to track and understand these practices. Ronald Deibert's Citizen Lab at the University of Toronto developed technical tools and methods for the systematic global analysis of Internet filtering by states (Deibert et al. 2008, 2010, 2012). Computer scientists also joined the fun, using automated Internet measurement techniques to collect data on censorship and circumvention practices (Leberknight et al. 2010; Wolfgarten 2005). Growing attention was also paid to the way private intermediaries regulated content (Wagner 2016).

A school of research focused on the economics of information security also developed during this period. While this began with a more traditional information security focus (Anderson 2001), the growth of cyberspace and the movement of ever-more social capabilities onto the Internet meant that these researchers increasingly intersected with cybersecurity and Internet governance issues, although they rarely used those labels to describe their work (Anderson and Moore 2007; Moore 2008). The new field was based on

the insight that the Internet's security problems are not simply technical but are driven by the economic incentives of actors and firms. Work in this area feeds into policy discourse by analyzing, for example, the cost-benefit trade-offs of Internet service providers' efforts to secure their networks and customers, the assignment of liability to software producers or Internet service providers, the impact of network externalities or tragedies of the commons, and the ways in which markets interact with government action in response to security problems.

Intermediary liability had been considered an Internet governance issue since the earliest days of the commercial Internet (Hardy 1994), but discussions of the topic became more prevalent with increases in Internet usage and the growing profitability of Internet intermediaries. The rise of online market intermediaries (e.g., eBay and Amazon), search engines such as Google, and social networks such as Facebook and Twitter brought to the fore new policy issues around topics such as defamation, copyright and counterfeit goods, and e-commerce (see, e.g., Mann and Belzley 2005). In this period, the immunity of intermediaries from liability was extensively discussed (Lemley 2007). This discussion continued into the fourth phase of the field's evolution, especially with efforts to pressure social media platforms to identify and take down terrorist content and the European Court of Justice decision on the right to be forgotten, which forced intermediaries to delink materials from their search engine results at the request of a claimant.

The tension between the Internet's capacity to quickly and easily share digital content, on the one hand, and the protection of copyright and trademarks, on the other, provided one of the major flashpoints of policy conflict and research. Media giants and national and international rights protection collectives had the resources to pursue a copyright and trademark protectionist strategy on a global basis. Incumbent copyright holders became some of the strongest advocates for imposing policing and enforcement responsibilities on Internet service providers and social media platforms (Bridy 2010; Horten 2012; Mueller, Kuehn, and Santoso 2012). The DNS also became an arena where rights holders sought preemptive protections for rights to names (Froomkin 2002; Galloway and Komaitis 2005).

If the rise of the Internet has mobilized copyright and trademark owners, it also sparked a new social movement that pushed in the opposite direction (Benkler 2006; Boyle 1997; Lessig 2005). This access to knowledge (A2K) movement was inspired by institutional analyses that view a

commons as a desirable governance model (Kranich 2004). Open, nonproprietary access to information was seen as especially appropriate because consumption of information is nonrivalrous. The movement had its origins in the developers of free and open source software, who pioneered new contractual mechanisms deliberately designed to prevent informational resources from being privately appropriated (O'Mahony 2003; Raymond 2001; Stallman 2002; Weber 2004). By the middle of the first decade of the 2000s, this actor network had become a full-fledged social movement that melded the free software movement with critics of the patent system in drugs and biotechnology and opponents of copyright and trademark maximalism. The A2K movement, like its opponent, was transnational in scope and self-consciously took its cause into international organizations (notably the World Intellectual Property Organization) and national legislatures (May 2007). These two forces had a historic collision in 2011–2012 over two proposed laws in the United States that would have implemented domain-name blocking mechanisms similar to China's in the service of copyright enforcement (Benkler et al. 2015; Sell 2013).

Phase Four (2010–): Surveillance, Securitization, and Alignment

In the fourth phase, ongoing as we write, issues of surveillance, privacy, and cybersecurity have become increasingly central to Internet governance politics and research. The Internet is going through a process of securitization (Cavelty 2007; Deibert and Rohozinski 2010), which further reinforces the linkages between the nation-state and Internet governance. As this happens, interest in and explicit mentions of "Internet governance" in the fields of political science and international relations grow exponentially (figure 3.2). In the research explicitly focused on the national and transnational power implications of the Internet's vulnerabilities, the term "security" no longer refers to more narrow technical forms of security but starts to mean exactly what it does in mainstream international relations research. Internet governance research now overlaps with studies of war and interstate conflict, deterrence, foreign policy, espionage, terrorist groups, and the threat to critical infrastructures that might be posed through cyberspace vulnerabilities. These concerns are often explicitly linked to the international diplomatic and policy conflicts over Internet governance (e.g., Segal 2016). Well-known international relations (IR) scholars such as Joseph Nye, who were unfamiliar

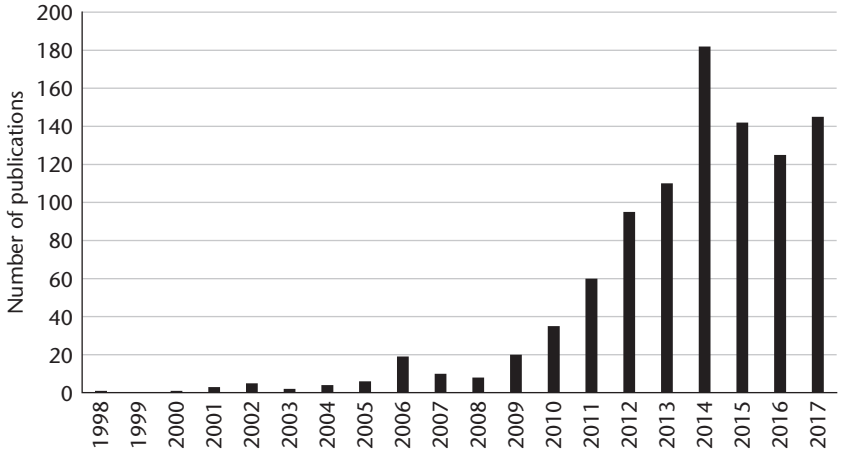

Figure 3.2
Occurrence of "Internet governance" in journals in ProQuest political science database by year.

with the decade of Internet governance research preceding the involvement of political scientists, reinvented certain themes, characterizing Internet governance as a "regime complex" (Nye 2014). There is even a systematic application to cyberspace of the classic IR concepts of the security dilemma (Buchanan 2016) and deterrence (Gartzke, Lindsay, and Nacht 2014).

The Edward Snowden revelations, which exposed internal documents about the pervasive global surveillance of the US National Security Agency, were a watershed in this process. The classified documents confirmed the surprisingly large scale and scope of digital surveillance, rekindling long-standing debates about privacy, encryption, and the powers of the state relative to the individual. But they also solidified the link between military and national security and the Internet; reinforced notions that one government, the United States, was preeminent or hegemonic in cyberspace; opened the veil on how the United States leveraged the extensive data collection that its private intermediaries gather about their users (Lyon 2014); and undermined US moral authority in Internet rights and norms (Farrell and Finnemore 2013). Snowden generated new forms of "data nationalism" from allies and rivals alike (Chander and Lê 2015).

In addition to sparking a vibrant debate about the possibility of a Balkanized or fragmented Internet (Drake, Cerf, and Kleinwächter 2016; Hill 2012;

Mueller 2017), the Snowden revelations contributed to a major institutional change in Internet governance—namely, the IANA transition (Becker 2019; Mueller 2014; Scholte 2016). US control of ICANN via the IANA functions contract had been controversial since the early days of WSIS. The post-Snowden crisis of legitimacy finally prompted the United States to relinquish its control of the DNS root and its contractual control of the IANA functions, owing to fears that many countries would defect from the ICANN-led Internet governance regime. The transition also brought in its wake major reforms in ICANN's accountability arrangements (Kruger 2015).

Despite its drift toward state-centric approaches, the cybersecurity literature does overlap with Internet-governance-related research on networked and multistakeholder governance. Empirical research on the actual mechanisms of cybersecurity production reveals a great deal of private action and collective action by Internet service providers, standard-setting organizations, and governments and law enforcement agencies (Asghari et al. 2015). Traditional hierarchical state action is the exception rather than the rule (Kuerbis and Badiei 2017; Schmidt 2014).

Surveillance and privacy were also key factors in the civilian debate over policy responses to the ubiquity of social media. While traditional privacy advocates adjusted their norms and policy ideas to the new conditions (Trottier 2016), neo-Marxists spoke of surveillance capitalism as a new type of economy (Zuboff 2015, 2019). The governance of data protection loomed ever larger in Internet governance, as the right to be forgotten, the breakdown of the US-Europe safe harbor agreement, and Europe's General Data Protection Regulation transformed the regulatory environment for major platforms offering free services in exchange for the value of users' data (Bennett and Raab 2017).

Data-localization laws were also analyzed as a digital trade issue. Legal scholars studied how data localization can affect digital trade and cross-border data flow, framing it as a trade barrier without achieving the desired privacy and security on the Internet (Chander and Lê 2015). Others took a different approach, discussing the legitimacy of data-localization laws by countries such as Brazil, India, China, and Russia. Assessing the tension between data localization and free trade, Selby argues that data-localization laws engage both Internet governance and international trade law (Selby 2017).

Another recent development in the field of Internet governance and trade is tech-nationalism. The US attack on Chinese telecommunications

equipment manufacturer Huawei pushes the next generation of mobile telecommunications into the fray of nation-state rivalry. Russia has also taken an approach to the Internet that is explicitly nationalist and sovereign (Stadnik 2019). These actions against free trade are taken in the name of national security and cybersecurity. As nations ramp up more tech-nationalistic tendencies, the effect of sanctions and trade protectionism on technologies that are used to operate the Internet might become a more prevalent research topic.

Methodologically, the field trends toward a growing use of computer science–based measurement techniques. Some of the most promising new research comes from scholars who exploit the information-generating tools of the Internet itself to compile and analyze data about the Internet. One sees reverse engineering of spyware by Deibert's Citizen Lab and efforts by researchers to gain control of the command-and-control infrastructure of a botnet. Scholars of the economics of security such as Tyler Moore and Michel van Eeten also are increasingly able to mine huge computer-generated databases of phishing activities, routing information, spam sources, and the like. It is possible to imagine a broader diffusion and further evolution of these methods to bear more directly on the problems of Internet governance. This implies a synthesis of technical knowledge and social science that is still too rare.

Conclusion

Internet governance as a label and field of study has undergone a remarkable evolution over the last 20 years. Once a term applied narrowly to debates around the control of the DNS root—and hotly contested and rejected as a label even then—it has now become an accepted designator for a broad range of policy issues, institutional developments, and geopolitical phenomena. The need to define the term even generated a special UN working group as part of a UN summit process.

Figure 3.3 provides an overview of how often "Internet governance" occurs in academic and research publication databases. The data are shown for four different disciplines: law (from LexisNexis Academic), economics (from EconLit database), political science (from ProQuest Political Science database, which includes international relations journals), and sociology (from ProQuest Sociological Abstracts). From this we can see that the field of law has shown the most consistent and sustained interest in Internet

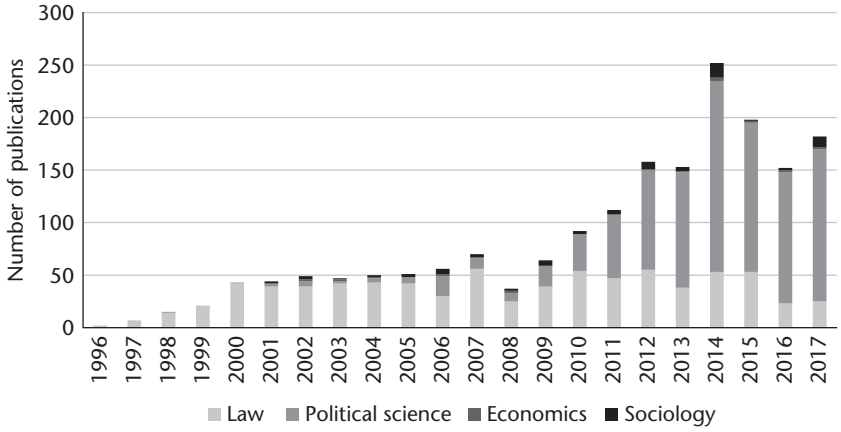

Figure 3.3
Occurrence of "Internet governance" in academic journals by year.

governance as a topic, ramping up quickly from 2 occurrences in 1996 to 49 in 2000 and maintaining a rate of about 40–50 publications per year since then. Since 2010, however, political science and international relations publications have dominated the field in terms of the sheer number of publications. We attribute this to the rise of cybersecurity as a policy and research preoccupation and the growing perception of Internet governance as a geopolitical issue. The amount of interest generated by cybersecurity and cyberspace governance in Internet research and political science fields testifies to the depth of the challenge Internet connectivity and computer technology poses to the traditional form of the state.

Economics and sociology, by way of contrast, have shown the least interest in the topic. Economics articles on the topic typically trickle in at 2 or 3 a year. Sociology averages around 4 articles a year, although it, like political science, shows more activity since 2010, notably a peak of 14 articles in 2014 and another spike of 10 in 2017. This is not, of course, because economists and sociologists have no interest in the social transformations caused by the Internet—it is simply that few of them frame their concerns as Internet governance. They are more focused on the evolution of Internet industries and the users and uses of the new media, respectively.

We conclude by raising an interesting but possibly uncomfortable question about the future of the field. In an article, Michel van Eeten claims that the rise of the Internet of Things and pervasive computing

> signal[s] the disappearance of the distinction between devices with and without connectivity and computing capabilities. Without that distinction, it also becomes less meaningful to think about cybersecurity governance as a space with a certain structural coherence. (2017, 437)

Should the governance of Internet-connected medical devices, for example, be considered Internet governance or part of health policy? Are autonomous vehicles handled as Internet governance or transportation policy? As the Internet and connected devices become ubiquitous, it is possible that most of the governance questions will be confronted and resolved in sector-specific ways that fall outside the realm of Internet governance. If this happens, ironically, it may be that the definition and scope of Internet governance once again reverts to the narrow realm of the Internet's naming, addressing, and routing infrastructure.

Notes

1. Lessig (1999b, 1407) used the term "governance" in a very general sense, and when explaining the word he mentioned the procedures for domain name registration as an Internet governance issue.

2. The NTIA green paper that eventually led to ICANN clearly reflects this tension in the following passage: "This discussion draft, shaped by the public input described above, provides notice and seeks public comment on a proposal to improve the technical management of Internet names and addresses. It does not propose a monolithic structure for Internet governance. We doubt that the Internet should be governed by one plan or one body or even by a series of plans and bodies." "Improvement of Technical Management of Internet Names and Addresses; Proposed Rule," February 20, 1998, docket number 980212036-8036-01, retrieved from https://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and-addresses-proposed-.

References

Ahlert, C. (2001). Democr@tic-Global-Governance.net: ICANN als Paradigma neuer Formen Internationaler Politik [Democr@tic-global-governance.net: ICANN as a paradigm of new forms of international government in cyberspace]. *Internationale Politik und Gesellschaft, 1*, 66–78.

Anderson, R. (2001). Why information security is hard—an economic perspective. *Proceedings of the 17th Annual Computer Security Applications Conference*. Retrieved from http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf

Anderson, R., & Moore, T. (2007, January). *Information security economics—and beyond*. Paper presented at the Fourth Bi-Annual Conference on the Economics of

the Software and Internet Industries, Toulouse, France. Retrieved from http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf

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

Asghari, H., van Eeten, M. J., & Bauer, J. M. (2015). Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy, 13*(5), 16–23.

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Retrieved from https://www.eff.org/cyberspace-independence

Becker, M. (2019). When public principals give up control over private agents: The new independence of ICANN in Internet governance. *Regulation and Governance, 13*(4), 561–576.

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

Benkler, Y., Roberts, H., Faris, R., Solow-Niederman, A., & Etling, B. (2015). Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate. *Political Communication, 32*(4), 594–624.

Bennett, C., & Raab, C. D. (2017). Revisiting "the governance of privacy." *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086

Boyle, J. (1996). *Shamans, software and spleens: Law and the construction of the information society*. Cambridge, MA: Harvard University Press.

Boyle, J. (1997). A politics of intellectual property: Environmentalism for the net? *Duke Law Journal, 47*, 87.

Braman, S. (1995). Policy for the net and the Internet. *Annual Review of Information Science and Technology, 30*, 5–75.

Bridy, A. (2010). Graduated response and the turn to private ordering in online copyright enforcement. *Oregon Law Review, 89*, 81.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford, UK: Oxford University Press.

Burk, D. (1995). Trademarks along the infobahn: A first look at the emerging law of cybermarks. *Richmond Journal of Law and Technology, 1*(1), 1–6. Retrieved from https://scholarship.richmond.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1003&context=jolt

Cave, J., Marsden, C., Klautzer, L., Levitt, R., van Oranje, C., Rabinovich, L., & Robinson, N. (2007, March 5). Responsibility in the global information society: Towards multi-stakeholder governance. *SSRN*. Retrieved from https://ssrn.com/abstract=2142027

Cavelty, M. D. (2007). *Cyber-security and threat politics: US efforts to secure the information age*. London, UK: Routledge.

Chander, A., & Lê, U. (2015). Data nationalism. *Emory Law Journal, 64*, 677.

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

Deibert, R., Palfrey, J. G., 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. G., Rohozinski, R., & Zittrain, J. (Eds.). (2012). *Access contested: Security, identity and resistance in Asian cyberspace*. Cambridge, MA: MIT Press.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology, 4*(1), 15–32.

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

DeNardis, L., & Raymond, M. (2013). Thinking clearly about multistakeholder Internet governance. *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377

Drake, W. J. (Ed.). (2005). *Reforming Internet governance: Perspectives from the working group on Internet governance*. New York, NY: UN ICT Task Force.

Drake, W. J., Cerf, V., & Kleinwächter, W. (2016, January). *Internet fragmentation: An overview*. Future of the Internet Initiative White Paper. Retrieved from World Economic Forum website: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Drezner, D. (2007). *All politics are global: Explaining international regulatory regimes*. Princeton, NJ: Princeton University Press.

Easterbrook, F. H. (1996). Cyberspace and the law of the horse. *University of Chicago Legal Forum, 1996*, 207–216.

Epstein, D., & Nonnecke, B. M. (2016). Multistakeholderism in praxis: The case of the regional and national Internet Governance Forum (IGF) initiatives. *Policy & Internet, 8*, 148–173. doi:10.1002/poi3.116

Farrell, H. (2003). Constructing the international foundations of e-commerce—the EU-US safe harbor arrangement. *International Organization, 57*(2), 277–306.

Farrell, H., & Finnemore, M. (2013). The end of hypocrisy: American foreign policy in the age of leaks. *Foreign Affairs, 92*(6), 22–26.

Froomkin, A. M. (2000). Wrong turn in cyberspace: Using ICANN to route around the APA and the Constitution. *Duke Law Journal, 50*(1), 17–186.

Froomkin, A. M. (2002). ICANN's UDRP: Its causes and partial cures. *Brooklyn Law Review, 67*(3), 605–718.

Galloway, J., & Komaitis, K. (2005). Like Alice in Wonderland: Applying EC competition principles in the case of domain names. *Journal of Information, Law and Technology, 2005*(2 & 3). Retrieved from https://warwick.ac.uk/fac/soc/law/elj/jilt/2005_2-3/galloway-komaitis

Gartzke, E., Lindsay, J., & Nacht, M. (2014, March). *Cross-domain deterrence: Strategy in an era of complexity*. Paper presented at the International Studies Association Annual Meeting, Toronto, Canada.

Goldsmith, J. (1998). Against cyber-anarchy. *University of Chicago Law Review, 65*(4), 1199–1250.

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

Hardy, I. T. (1994). The proper legal regime for "cyberspace." *University of Pittsburgh Law Review, 55*, 993–1055.

Hill, J. F. (2012). Internet fragmentation: Highlighting the major technical, governance and diplomatic challenges for US policy makers. *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439486

Hofmann, J. (2005). Internet Governance: Zwischen staatlicher Autoritat und privater Koordination. *Internationale Politik und Gesellschaft, 3*, 10–29.

Hofmann, J., Katzenbach, C., & Gollack, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. *New Media and Society, 19* (9), 1406–1423.

Horten, M. (2012). *The copyright enforcement enigma: Internet politics and the 'telecoms package.'* UK: Palgrave MacMillan.

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

Johnson, D. R., & Post, D. (1997). And how shall the net be governed? A meditation on the relative virtues of decentralized, emergent law. In B. Kahin & J. H. Keller (Eds.), *Coordinating the Internet* (pp. 62–91). Cambridge, MA: MIT Press.

Kahin, B., & Keller, J. H. (Eds.). (1997). *Coordinating the Internet*. Cambridge, MA: MIT Press.

Klein, H. (2001). Global democracy and the ICANN elections. *Info, 3*(4), 255–257.

Klein, H. (2004). Understanding WSIS: An institutional analysis of the UN world summit on the information society. *Information Technology and International Development, 1*(3–4), 3–14.

Kleinwächter, W. (2000). ICANN between technical mandate and political challenges. *Telecommunications Policy, 24*(6), 553–565.

Kleinwächter, W. (2001). The silent subversive: ICANN and the new global governance. *Info, 3*(4), 259–278.

Kleinwächter, W. (2004). Beyond ICANN vs ITU? How WSIS tries to enter the new territory of Internet governance. *Gazette, 66*(3–4), 233–251.

Kowack, G. (1995). Internet governance and the emergence of global civil society. *IEEE Communications Magazine, 35*(5), 52–57.

Kranich, N. (2004). *The information commons: A public policy report* (No. 4). New York, NY: Free Expression Policy Project, Brennan Center for Justice, NYU School of Law.

Krasner, S. D. (1983). *International regimes*. Ithaca, NY: Cornell University Press.

Kruger, L. G. (2016, September). The future of Internet governance: Should the United States relinquish its authority over ICANN? (CRS Report R44022). *Congressional Research Service*. Retrieved from https://fas.org/sgp/crs/misc/R44022.pdf

Kuerbis, B., and Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance, 19*(6), 466–492.

Leberknight, C., Chiang, M., Poor, H. V., Wong, F. (2010, December 31). *A taxonomy of Internet censorship and anti-censorship*. Draft Version. Retrieved from http://www.princeton.edu/~chiangm/anticensorship.pdf

Leib, V. (2002). ICANN-EU can't: Internet governance and Europe's role in the formation of the Internet Corporation for Assigned Names and Numbers (ICANN). *Communication Abstracts, 25*(6), 755–909.

Lemley, M. A. (2007). Rationalizing Internet safe harbors. *Journal of Telecommunications and High Technology Law, 6*, 101.

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

Lessig, L. (1999b). Open code and open societies: Values of Internet governance. *Chicago-Kent Law Review, 74*, 1405.

Lessig, L. (2005). *Free culture: The nature and future of creativity*. New York, NY: Penguin.

Lewis, P. H. (1994, October 24). U.S. begins privatizing Internet's operations. *The New York Times*.

Levinson, N. S. (2002). Internet governance and institutional change. *The Tocqueville Review/La Revue Tocqueville, 23*(2), 125–141.

Levinson, N., & Smith, H. (2008, August 28). *The Internet governance ecosystem: Assessing multistakeholderism and change*. Paper presented at the American Political Science Association 2008 Annual Meeting, Hynes Convention Center, Boston. Retrieved

from http://195.130.87.21:8080/dspace/bitstream/123456789/1020/1/The%20internet%20governance%20ecosystem%20assessing%20multistakeholderism%20and%20change.pdf

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society, 1*(2). doi:10.1177/2053951714541861

MacLean, D. (Ed.). (2004). *Internet governance: A grand collaboration*. New York, NY: UN ICT Task Force.

Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum*. Wembley, Australia: Terminus Press.

Mann, R. J., and Belzley, S. R. (2005). The promise of Internet intermediary liability. *William and Mary Law Review, 47*, 239.

May, C. (2007). The World Intellectual Property Organization and the development agenda. *Global Governance: A Review of Multilateralism and International Organizations, 13*(2), 161–170.

Moore, T. (2008). *Cooperative attack and defense in distributed networks* (Report No. UCAM-CL-TR-718). Cambridge, UK: University of Cambridge Computer Laboratory.

Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: MIT Press.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Mueller, M. (2014). Detaching Internet governance from the state: Globalizing the IANA. *Georgetown Journal of International Affairs*, 35–44.

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

Mueller, M., Kuehn, A., & Santoso, S. M. (2012). Policing the network: Using DPI for copyright enforcement. *Surveillance & Society, 9*(4), 348–364.

Nye, J. S. (2014). *The regime complex for managing global cyber activities*. Global Commission on Internet Governance Paper Series (Paper no. 1). Centre for International Governance Innovation/Chatham House. Retrieved from https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

O'Mahony, S. (2003). Guarding the commons: How community managed software projects protect their work. *Research Policy, 32*(7), 1179–1198.

O'Siochru, S. (2004). Civil society participation in the WSIS process: Promises and reality. *Continuum: Journal of Media & Cultural Studies, 18*(3), 330–344.

Padovani, C., & Tuzzi, A. (2004). Global civil society and the world summit on the information society: Reflections on global governance, participation and the

changing scope of political action. *Social Science Research Council*. Retrieved from https://ecpr.eu/Filestore/PaperProposal/268396ec-ddf8-4df3-bd32-763d314d6c65.pdf

Palfrey, J. (2004). The end of the experiment: How ICANN's foray into global Internet democracy failed. *Harvard Journal of Law & Technology, 17*(2)

Perritt, H. H., Jr. (1996). Jurisdiction in cyberspace. *Villanova Law Review, 41*, 1.

Raboy, M. (2004). The WSIS as a political space in global media governance. *Continuum: Journal of Media & Cultural Studies, 18*(3), 345–359.

Raymond, E. S. (2001). *The cathedral and the bazaar: Musings on Linux and open source by an accidental revolutionary* (Rev. ed.). Cambridge, MA: O'Reilly.

Resnick, D. (1997). Politics on the Internet: The normalization of cyberspace. *New Political Science*, 47–68.

Resnick, P., & Miller, J. (1996). PICS: Internet access controls without censorship. *Communications of the ACM, 39*(10), 87–93.

Samuelson, P. (1996). The copyright grab. *Wired*. Available at http://works.bepress.com/pamela_samuelson/240/

Schmidt, A. (2014). Hierarchies in networks: Emerging hybrids of networks and hierarchies for producing Internet security. In *Cyberspace and international relations* (pp. 181–202). Berlin, Germany: Springer.

Scholte, J. A. (2016). Process and power in Internet governance. Reflections on the IANA transition. *RIPE, Amsterdam*. Available at https://ripe72.ripe.net/presentations/20-ripe-72.pdf

Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. New York, NY: PublicAffairs.

Selby, J. (2017). Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology, 25*(3), 213–232.

Sell, S. K. (2013). Revenge of the "nerds": Collective action against intellectual property maximalism in the global information age. *International Studies Review, 15*(1), 67–85.

Sørenson, E., & Torfing, J. (Eds.). (2007). *Theories of democratic network governance*. Basingstoke, UK: Palgrave Macmillan.

Souter, D. (2007). Whose summit? Whose information society? Developing countries and civil society at the world summit on the information society. Association for Progressive Communications. Retrieved from http://www.apc.org/en/pubs/manuals/governance/all/whose-summit-whose-information-society

Stadnik, I. (2019). Sovereign RUnet: What does it mean? Internet Governance Project, Georgia Institute of Technology. Retrieved from https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/

Stallman, R. (2002). Free software, free society: Selected essays of Richard M. Stallman. Boston, MA: Free Software Foundation.

Trottier, D. (2016). Social media as surveillance: Rethinking visibility in a converging world. London, UK: Routledge.

UNDP. (1997). Human Development Report, 1997. New York, NY: United Nations Development Program.

van Eeten, M. J. (2017). Patching security governance: An empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation and Governance, 19*, 6.

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

Wagner, B. (2016). *Global free expression—governing the boundaries of Internet content*. Switzerland: Springer International Publishing.

Weber, S. (2004). *The success of open source*. Cambridge, MA: Harvard University Press.

Weinberg, J. (2000). ICANN and the problem of legitimacy. *Duke Law Journal, 50*, 187.

Weinberg, J. (2001). Geeks and Greeks, *Info, 3*(4) 313–332.

Weinberg, J. (2011). Governments, privatization, and privatization: ICANN and the GAC. *Michigan Telecommunications and Technology Law Review, 18*, 1.

Wolfgarten, S. (2005). *Investigating large-scale Internet content filtering*. (Unpublished master's thesis). Dublin City University, Ireland. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.5778&rep=rep1&type=pdf

Wu, T. S. (1997). Cyberspace sovereignty? The Internet and the international system. *Harvard Journal of Law and Technology, 10*(3), 647–666.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. New York, NY: Profile Books.