International
Studies
Review

International Studies Review (2009) **11**, 205–230

THE FORUM

Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State

Edited by Johan Eriksson
Södertörn University College and the Swedish Institute of International Affairs

and

Giampiero Giacomello
Università di Bologna

Editors' Note: *Does the global diffusion of the Internet signify the final end of the state's ability to control society, or is the state on the contrary maintaining or even strengthening its hold of society? Several observers have taken the latter position, most recently Goldsmith and Wu (2006), authors of Who Controls the Internet?, while critics claim this is grossly misleading, and that international regimes and a myriad of nonstate actors such as private firms and nongovernmental organizations play a much greater role in Internet governance (Mathiason 2007). In our view, thus structured, such debate risks reiterating a much older (and largely stalemated) debate about whether the nation-state is "obstinate or obsolete" (Hoffman 1966), mirrored also in the larger debate about globalization. The goal of the present Forum*[1] *is to reexamine and ultimately problematize this debate by discussing what actors are controlling what aspects of Internet usage, and under what conditions. A brief introduction to this is given in the first essay, written by the Editors. The following contributions demonstrate that, rather than seeking a final word on who controls the Internet, it is more fruitful to unpack the complexity of control in the digital age, and indeed the diversity and preliminary nature of available analyses. It is also for this reason we have invited contributors who elaborate a variety of perspectives, including a stout defender of state-centrism (Hamoud Salhi), a contributor who unravels the complexity of public–private partnerships in Internet control (Myriam Dunn Cavelty), and advocates of more critical perspectives emphasizing complexity (J.P. Singh), interactivity and discourse (M.I. Franklin). We believe that the global scope and spatial origins of the authors in this Forum imply experiences and outlooks which help reveal new insights and cross-fertilizations, which goes beyond the dominant US-centered perspectives on international relations in general and the Internet in particular.*

[1]This is not the first journal forum on Internet governance. With remarkable forbearance, in 1999 the Swiss Political Science Review arranged a forum on this topic (Giacomello, Akdeniz, Authority, and Holitscher 1999). The contributors to that first forum concluded that the state, albeit crucial for the development of the Internet worldwide, was far from being the sole, or even the dominant, player in Internet control. The sovereign state had to confront the powerful private sector and aggressive nongovernmental organizations (NGOs), especially in the realm of free speech and privacy. Such conclusions have been reiterated in several publications since then (for example, Giacomello 2003, 2005; Latham 2003; Eriksson and Giacomello 2007; Dunn, Krishna-Hensel, and Mauer 2007).

Who Controls What, and Under What Conditions?

Johan Eriksson
Södertörn University College and the Swedish Institute of International Affairs

and

Giampiero Giacomello
Università di Bologna

With the Internet being a truly global phenomenon, understanding how this is controlled should yield observations of relevance for the study of global governance more generally. The Internet, and how it is controlled, should therefore be a concern for all students of world politics, and not only for the smaller albeit multidisciplinary community of scholars engaging in ''Internet studies.'' A first step is to acknowledge that Internet control varies across time, space, and issue-areas. To better understand such complex patterns of governance, we need to go beyond universal generalizations. In an attempt to support the middle-range theorizing, which arguably is needed, this essay introduces and briefly unpacks three analytical questions: What are the key aspects of Internet control? What actors might control what aspects of the Internet? And, finally, under what conditions are different types of actors likely to control various aspects of the Internet?

Control of What?

We suggest that the notion of Internet control[2] breaks down into three dimensions: (1) *access* to the Internet, (2) *functionality* of the Internet, and (3) *activity* on the Internet.

Access to the Internet is about whether people have basic opportunities for connecting to and using the Internet. Controlling access to the Internet can further be divided into (1a) control of the means of access (computers and Internet service providers) and (1b) control of the physical infrastructure without which Internet access is impossible, that is, satellites, cable networks, routers, communications dishes, and antennas. States and nonstate actors may to varying degrees control one or more of these aspects, although usually with a limited reach. No single actor controls every single hub of cyberspace.

While access is about whether people can use the Internet or not, *functionality* is about the technical quality of Internet usage. Controlling functionality is more specifically about (2a) the physical quality of connections (bandwidth and speed); (2b) the quality of communications software (such as browsers, e-mail, chat programs, file transfer software, voice, and video communications programs); and finally (2c) about the technical protocols of Internet communication (IP, TCP, etc.). Control of the third aspect, technical protocols, is the only one that has an exclusively global reach and, for this reason, could be interpreted as one of the

[2]Rather than engaging in a lengthy conceptual discussion of what ''control'' generally implies, and how it relates to similar concepts such as ''power'' and ''governance,'' we simply wish to clarify what dimensions of control are of relevance for our empirical focus on the Internet. It should be noted however, that the term ''control'' is commonly used in analyses of the social and political dimensions of information and communications technology (Pool 1983, 1990; Beniger 1986; Buchner 1988; Mulgan 1991:52; Chomsky 1997; Mowlana 1997; Shapiro 1999; Wright 2000; MacMahon 2002; Mueller 2002; Zittrain 2004; Giacomello 2005). Importantly, ''control'' is not only associated with general notions such as ''governance,'' ''influence,'' and ''authority,'' but is also distinctively linked to the law (Pound 1997) and technology, including the methods and means of governing the performance of any apparatus, machine, or system.

most fundamental sources of power in Internet governance (see Singh's essay). Functionality can also be negatively affected by intentional actions such as denial-of-service attacks (such as spam and Internet virus pandemics), as well as external events such as power outages (see Dunn Cavelty's essay).

The third dimension of Internet control is about *activity* online. Access and functionality are essential for using the Internet, and their importance is generally underestimated, but it is how the Internet is used by individuals, organizations, and governments, and how online activity is controlled, that has stirred the most intense political and scholarly debates. Most of these issues have a strongly moral and ethical character, concerning privacy and surveillance, and substantive questions such as online fraud and theft, pornography, videos of beheadings and rapes, extremist and racist propaganda, and practical manuals for creating explosive charges.

Control of online activity can take many different forms: (3a) filtering and blocking of particular parts or features of the Internet such as websites, search words, or online communities; (3b) surveillance of online activity, for example, surf logs, spyware, and more comprehensive eavesdropping of electronic communications (see Dunn Cavelty), which is done for instance through the much debated Echelon system; and finally (3c) attempts to shape and control social and political discourse through various means of information, propaganda, and entertainment (see Franklin's essay). This last aspect receives a considerable amount of attention in Internet research, particularly regarding the mobilization of extremism and terrorism.

Who Controls What?

A great variety of types of actors may control various aspects of the Internet—notably governments, businesses, and NGOs (especially civil liberties organizations such as Privacy International) (Herrera 2002; Giacomello 2003, 2005; Dunn et al. 2007; Franklin 2007a; Mathiason 2007). All three types of actors simultaneously operate domestically as well as internationally, which makes it intriguing to observe their interactions.

Though we advocate conditional rather than universal generalization, three general assertions can be suggested, which in fact clarify our view that variation and complexity overshadows most universal patterns of Internet control. Firstly, the significance of governmental and nongovernmental actors varies considerably across countries (in contrast, Salhi argues that the state maintains a universally dominant position also in the digital age). Albeit the Chinese government heavily relies on private firms (including several multinationals) to exert filtering and censorship on Internet usage, it is doubtlessly a more significant cyber-watchdog than most other governments in the world.[3] Yet, the reach of its control is limited to the domestic domain (Lagerkvist 2007).

Secondly, no single actor or even single type of actor has complete control of all dimensions of the Internet, not even on a domestic level (see Singh, and Franklin, respectively). Internet control is generally negotiated and shared, implying overlapping public and private authority, albeit in greatly varying degrees (Dunn et al. 2007).

Thirdly, understanding Internet control unavoidably implies focusing on public–private relations (see Dunn Cavelty's essay). While governments may exert significant control of access, functionality and activity online, mainly through regulation and monitoring activities, a myriad of private firms play significant

[3]Moreover, Chinese control is constantly challenged by computer-savvy younger generations. See, for example, Howard French, ''Great Firewall of China Faces Online Rebels,'' *The New York Times*, online version, February 4, 2008, at http://www.nytimes.com/2008/02/04/world/asia/04china.html?ref=asia (accessed February 5, 2008).

roles in providing and maintaining the infrastructure, hardware, and software which is essential for Internet usage.

The means of access to the Internet are generally though not exclusively produced and provided by private firms, including the hardware, software, and physical infrastructure. Governments exert control of access mainly by regulating, monitoring and planning access, for example, through state-run programs of developing broadband networks, and through licensing domestic Internet service providers. Governments often have the capacity to shut down incoming and outgoing Internet traffic across the domestic–international border, which is what the Estonian government did in a historically unique response to the massive cyber-attacks in May 2007. Again, however, the ability as well as the willingness to control may vary greatly over time and space.

Much like access, functionality of Internet usage is largely controlled by private interests (see Salhi's essay for counterarguments). Private firms almost exclusively control bandwidth, speed and stability of connections, and the quality of browsers, e-mail and other communications software, although governments may, again, exert control through domestic regulation, licensing, and monitoring. Notably, the control of quality of connections is extremely dispersed and localized, while software control potentially has a worldwide reach, exemplified buy the global domination of Microsoft's Internet Explorer browser.

The third aspect of functionality, namely the technical protocols of the Internet, pinpoints the significance of public–private relations on a global scale. Negotiated, developed, and maintained through the main Internet governance bodies—Internet Corporation for Assigned Names and Numbers (ICANN), World Summits on the Information Society (WSIS), and the Working Group on Internet Governance (WGIG)—governments and private actors collaborate in international regime-building (see Singh's essay for an elaboration). This emerging regime is significant not only for its global reach (Mathiason 2007), but also, we would argue, for the development and regulation of universal technical protocols providing nothing less than the ''genetic code'' of the Internet. It is still unclear, however, what form and degree of power different actors and countries have in these instances of global Internet governance. The dominance of public and private US actors in the above mentioned forums should be subjected to further scrutiny, and so should the innovative new ways of inviting a broader public in policymaking, exemplified by the United Nations Internet Governance Forum.

As for control of activity, most observers are mainly concerned with how national governments—independently or in collaboration—seek to monitor, filter, regulate, and influence Internet usage (see Franklin's essay for a critique of this state-centered debate). Moreover, the extent and ambition of governmental control varies considerably across the world; China is often considered the most extreme in terms of actively intervening, by simply blocking or deleting Internet content.

A great many liberal democracies have developed their own surveillance systems, including advanced systems of tracking all incoming and outgoing Internet traffic, and blocking of illegal sites (notably those containing pedophilia). Furthermore, private firms, such as multinationals Google and Yahoo and the multitude of domestic Internet service providers, log the surfing behavior of individuals.

Nevertheless, there are ways to escape electronic eavesdropping, particularly by using encryption software, which has been freely available since the early 1990s. Attempts have been made to prohibit access to this, notably by the US government, which ''securitized'' free encryption as a serious threat to national security, fearing that terrorists and criminal groups would make use of such tools (Denning 1997; Bendrath 2003). This ''securitization move'' failed, and encryption has remained widely available, mainly because of the expressed usefulness of the device for securing business communication (Schneier 2000; Levy 2001; Giacomello 2005: Chapter 2).

When we expand the perspective beyond these defensive aspects of online activity, we can give more attention to the Internet as a global marketplace of ideas, in which no single type of actor is able to exert complete discursive control (see Franklin, and Singh). States are competing and collaborating for visibility and influence with NGOs, private firms, the news media, the entertainment industry, online gaming communities, criminal networks, terrorist groups, religious communities, academia, and especially individuals.

Unsurprisingly, perceptions of vulnerability and weakness dominate when we look at discourse control through the lens of national security. Governments fear that the Internet has increasingly become a ''virtual sanctuary'' for states and nonstate groups spreading violent and subversive propaganda (Weimann 2006; Ranstorp 2007). The question that we briefly discuss in the next section is how and when various actors control certain aspects of the Internet.

Who Controls What, Under What Conditions?

Clarifying the varying conditions of control leads us firstly to the level of development of the domestic information society and to what is sometimes called ''network readiness,'' an important background factor. Network readiness is more specifically measured by the percentage of households with Internet connects, and so forth (see Singh's essay for recent statistics). The continuing discussion on the ''digital gap'' between the haves and the have-nots confirms the significance of network readiness, which emphasizes the importance of conditional rather than universal generalizations about Internet control.

If the network readiness is low or insignificant, then by all means there is not much to control, and the dependency on information and communication technology (ICT) for the functioning of society and government is insignificant. If, however, network readiness is high or clearly growing, then the issue of Internet control is of much greater importance. It becomes more interesting to consider the various dimensions of control, especially such conditions as patterns of ownership and maintenance of critical infrastructure, governmental Internet policies (including censorship), dependency on multinational cyber-companies and other foreign interests, and the significance of global Internet governance initiatives.

Though the Internet is a truly global phenomenon, the domestic context plays a surprisingly significant role. In the field of information retrieval (IR) the debate about the domestic and international levels of analysis, and indeed the connections between the two, is almost as old as the discipline itself, being one of the major issues of scholarly discussion (cf. Waltz 1959; Aron 1962). Domestic political systems and regulations do play a major role in Internet control, not least because domestic actors arbitrate international developments differently across countries. Systematic differences can be observed between democracies and autocracies, although neither democracies nor autocracies are all the same (Lijphart 1999).

In developed democracies, not only the private sector but also civil liberties NGOs play a noteworthy although variable role (Herrera 2002; Giacomello 2003, 2005). In democracies as well as in autocracies, however, the national intelligence community plays an increasingly significant role in Internet governance, albeit for partly different reasons. At the end of the day, a crucial condition for control is not only the ability to control, but also the willingness to do so (for instance, regarding censorship), which points to the significance of ideational factors such as political culture and ideology.

Until recently, the Internet was a symbol of ''OECD-ization'' more than it was an icon of globalization. The countries that originally were seen to be the most significant in the Internet world were advanced economies, that is, OECD members, which for the most part could be equated with the exclusive club of

modern democracies with advanced market economies. Autocracies were present on the Internet from the beginning, but were not considered very influential. To understand the conditions of control, it was sufficient to study the interactions of the actors *within* democracies. Ultimately, these set the ''spirit of the time'' on the Internet, including its control (Giacomello 2005).

These conditions began to change as more and more users logged in from less developed countries, several of them democratic and many certainly not, though some autocracies still pay lip service to democratic standards. Not only China but also several states in the Middle East, for example, developed programs for intrusive control of Internet usage in their own countries (Giacomello 2005). In these countries, the national government adopted a two-prong strategy. At the domestic level, they used their legislative instruments for imposing control on activity (content and the on-line conduct of users), heavily sanctioning those that did not conform to the rules.

These governments have alerted international organizations such as the UN or the International Telecommunications Union (ITU), arguing that only sovereign states have the right to control the Internet. The influence of civil liberty organizations was considered problematic in the eyes of these governments. Demand for strict control of online activity has increased also in Western democracies, as an element of the stricter legislations following the events of September 11, 2001.

The prevailing clash between radically divergent views on Internet governance is a serious obstacle for the establishment of a global Internet regime (Bessette and Haufler 2001). Advocates of stricter regulation and the right to apply intrusive control have used arguments familiar in other domains of global governance: that international law implies the need to respect cultural differences, and that Western democracies cannot ''impose'' their control standards on others. The debate on Internet governance will continue, and become increasingly significant for international relations more generally. If there is any general conclusion to be suggested regarding Internet control, it is that despite efforts to establish a global governance regime, Internet control will remain and possibly becoming increasingly diversified and dispersed.

The State Still Governs

Hamoud Salhi
California State University, Dominguez Hills

The Internet has gained ground through its engineering sophistication and its ability to regulate transnational activities in ways the state cannot. In their 2006 book *Who Controls the Internet? Illusion of Borderless World*, Jack Goldsmith and Tim Wu argue that the self-regulating Internet is a myth. They believe that governments have the resources to enforce their laws in cyberspace; that the Internet has created its own boundaries to accommodate the needs of individuals from different communities, thereby making itself amenable to state control; and that communities, including business and professional associations, have sought government intervention in cyberspace to regulate activities they deem harmful to their interests or societal ethics.

Goldsmith and Wu acknowledge the transformative potential of the Internet, but maintain that such potential has not diminished the state's ability to govern (Goldsmith and Wu 2006:180; see also Zysman and Newman 2006). Because of

the very anarchic nature of the international system, the state is best positioned to impact the new and expanding cyberspace environment. Unlike other international actors, the state has sole ownership of the legitimate use of force and the authority to regulate cyberspace within its territory.

Several propositions in the literature on Internet governance have predicted a diminishing role for the state in the Digital Age and more autonomy for the Internet. Futurists including John Barlow, John Negroponte, and Alvin Toffler optimistically predicted the end of what Barlow described as ''the tyrannies,'' that is, the governments of the Industrial World: ''You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders'' (Said Barlow, as quoted in Youm 2006:730). Negroponte believed that the state would shrink in the face of globalization, declaring that he does not have the ''recipe for managing such a world, but its laws will have to be more global. Cyberlaw is global'' (as cited in Flichy 2007:117). Social scientists had similar hopes, believing that the Internet would bring direct democracy to the public by offering the opportunity to directly participate in the decision making process (Hague and Loader 1999). It was also believed that the Internet would democratize the Third World: a study by Rand Corporation predicted a wave of political change in the Middle East ushering democracy in ways never seen before.

So far, predictions of the collapse of the state and the democratization of authoritarian regimes (in China and the Middle East, for example) have not come to pass. The state is alive and well, albeit wounded at times. The debate over who controls the Internet has become more even more nuanced and detailed, with both the state and the self-regulating Internet giving up the notion of supreme control.

From a state-centric perspective (the view that the state controls the Internet), the ability to govern and enforce laws is key to the control challenge. But is the fact that the state possesses the legitimate right to govern enough to propose that it is in control of the Internet? Furthermore, does the state really govern the Internet if it does not effectively enforce its laws on Internet activities? And can the ''informal'' self regulatory mechanisms developed by the Internet be a substitute for the formal legal authority adopted by the state to manage and resolve conflict?

The intent of this essay is not to dismiss the impact that the Internet has on the world, or to downplay its ability to impose control on some of its activities and in ways the state cannot. Rather, I will argue that in the final analysis the state is more likely to emerge as the controller of the Internet. Hence, I treat the state's control as a matter of degree, not as an either/or issue.

But framing the question in degrees poses a serious problem for empirical measurement. How do we account for the state's governance of the Internet? At what level of analysis (systemic, nation-state, government, societal, and individual) are we to assess the state's governance of the Internet? Can we weigh all levels of analysis in the same way? What is the tipping point? How do we measure the impact of the Internet on society, political change, and economic development? How much of that influence, if there is any, can be attributed to the effect of the Internet? At the other end of the spectrum, how do we measure ''the legitimate use of force''? What impact, if any, has the use of force had on Internet governance? Does it enhance the state's ability to govern the Internet or diminish it? These questions suggest that governing the Internet is a complex matter involving many intertwined social, political, and economic factors. This is why it is important to examine the context in which the state operates. We must also examine the Internet's relations to the state in a particular context.

The Internet is a tool, a medium (a mediator as in Franklin's essay), and a ''techno-economic manifestation'' of human development. As a medium, the

Internet is no more than a facilitator, a tool that has helped shorten distances and contributed to raising consciousness and forming identities (Singh's essay). But these activities do not occur in a vacuum: the Internet has had to adapt to conditions in order to be relevant to those it sought to serve.

Goldsmith and Wu argue that the Internet has mapped out its own borders to better accommodate the needs of specific communities. Using historical examples and empirical data, the authors argue that the notion of a borderless world is illusionary and that state laws have superseded those of the Internet. Moreover, in *Mapping the Borders* (Chapter 3), there is a clear argument that the Internet has had to resort to working within specific borders. The Internet has had to adapt to geographical conditions, legal prerogatives, and good business practices. The authors admit that the Internet has brought the world closer, but relative to each country, community, and individual. According to the authors, it did not make sense to have a ''borderless flowery delivery service'' (p. 59). The Internet is but a tool incorporated into an environment equipped with its own laws, cultural norms, and social order governing people's behavior by holding them accountable for their actions. In other words, while an argument can be made that the virtual world of the Internet may not have borders, the location from where it is being accessed does. Thus, the state's role becomes crucial.

Governance and Control

This brings us to the issue of state control in the areas of access, functionality, and activity. First, when measured by access, ''the opportunities for connecting to and using the Internet'' (Giacomello and Eriksson's essay), and functionality, variations exist among states as a result of different political systems and levels of economic and societal development.

In advanced countries, access is universal and relatively affordable to the vast majority of the population. The control of the Internet reflects the capitalist nature of these societies—competitive, corporate-based, and geared towards profit making. Some states in the Western world have abdicated some of their powers to the private sector. In the United States, for example, then-President Bill Clinton and Vice President Al Gore believed that the US government should avoid regulating cyberspace activities, and urged the private sector to lead the way in transforming the digital world (Framework for Global Economic Commerce as cited in Zysman and Newman 2006:277; also Kenny 2004:69–106). In Europe, other states were similarly inclined (Dumez and Jeunemetre 2004:381–405). Governments entrusted nonstate actors to set rules, fearing that the rigidity of their own institutions would slow or obstruct the development of information technology. It was also believed that the commercialization of the Internet was good for its survival. The private sector, with its free enterprise and competitiveness, was considered better suited to take the Internet to the next stage, producing a network for the general public and not just for selected universities and the military, as it was originally conceived. From a capitalistic market perspective, this was a logical sequence for any idea to achieve its full potential.

In contrast, in nondemocratic societies the Internet has been placed under the tutelage of the state, and access has been limited. In the Middle East, it has become common practice for the government or a relative of the governing elite to own the licensing of the Internet. This has accentuated the powers of the state, enabling governments to control the spread of the Internet by limiting access through higher subscription fees, membership applications, and computer pricing and, in turn, preempting challenges to the existing political order. The rulers' fear is that the opposition may use the Internet to spread information that could devastate the rulers' position in power (rallying the masses against the rulers, portraying them as corrupt or violators of human rights), potentially

leading to their isolation worldwide. Hence, it becomes imperative for the state to exercise its authority in order to promote the status quo.

Additionally, even in cases where Middle East states have sought deregulation in an attempt to expand access and lower the cost of Internet services, deregulation has helped the state to extend its influence to new areas. Information technology, including the Internet, has been placed under the ministries of information and culture, notorious for their strict censorship and authoritarian regulations. Deregulation has increased the number of Internet cafés and the degree of public access, expanding the domain of public debate to include chat rooms and blogs. However, because of established political barriers, the new privatization licensing laws—issued and promulgated by the same state—did not provide nonstate actors the means or the opportunity to navigate cyberspace without government interference. The Internet has been governed by the same rules that monitor the media, ''either through explicit laws or via a direct ownership in state monopolies'' (Warf and Vincent 2007:89).

Regulating the Internet

Goldsmith and Wu attempt to debunk the proposition that the Internet can regulate its activities, and they are successful to a degree. Internet companies and others can control users' activities online. Take Google for example. Google allows users to access its map data and functionality by assigning them a ''key.'' Google reserves the right to revoke that key at its own choosing. Here the state is not playing a dominant role.

Wikipedia is another example. Wikipedia allows users to write, edit, and publish reference articles without gatekeepers (Zittrain 2008:133). In the beginning, there were no rules for submissions, just a code: ''Be conservative in what you do; be liberal in what you accept from others.'' But steps have been taken to preempt mishaps or vandalism to the pages. For instance, edits are introduced in sequences so that users can go back and follow what was originally discussed. Similarly, Wikipedia provides a discussion page next to the main page for the authors to explain the rationale behind their edits. Hence, problems were resolved as they arose. But as Wikipedia grew, it became essential to have its own regulations. Wikipedia developed its own administrative hierarchy with its own board of administrators to supervise the editorial process.

The Internet has even played in important role in e-government. The recent UN E-Government Survey 2008*: From E-Government to Connected Governance* notes that governments in several countries worldwide are increasingly relying on information technology and the Internet to better serve their citizens. The study uses three overlapping layers to assess the readiness of a government to be electronically adept. These are: (1) infrastructure based on the reliability and affordability of connectivity to citizens and businesses in a specific country; (2) integration to assess how well citizens, businesses, and government are linked by a system both to the internal and outside world; and (3) transformation to measure the impact a connected e-government service may have on the country's democratic and economic development.

The study reveals large discrepancies among the five regions sampled in terms of their readiness to provide e-government services to their citizens. Europe led the pack, followed by the Americas, Asia, Oceania, and Africa. In terms of specific countries, Sweden was ranked the most e-government ready, followed by Denmark, Norway, and the United States, respectively. No country of the Third World, including Africa and Central America, was among the top 35; according to the survey, this is partially a result of the high cost of IT infrastructure and budget constraints forcing governments to prioritize more pressing issues, such health care and education. (UN E-Government 2008:20) The study also shows that e-participation—that

is, the extent to which governments offer citizens opportunities to impact the decision making process—is on the rise. Here too the less developed countries trail the developed countries (UN E-Government 2008:59).

Clearly the data show that the Internet is contributing to better governance and greater participation by citizens. In fact, the study notes that ''citizens groups have come to expect a 24/7 convenient user interface with ease of use, in a language the user understands and which is tailored to individuals needs'' (UN E-Government 2008:2). To the Neoliberal this is more power to the citizens: the Internet has helped the government to function in a faster, smoother, and more efficient way.

But Goldsmith and Wu are not convinced. They argue that in the final analysis the state is in charge because of its legitimate legal authority. They introduce numerous legal examples to demonstrate how the state has been able to regulate the Internet. The case of Yahoo is illustrative because its shows how the French government forced Yahoo, a US giant, to comply with French law. Yahoo was sued for in France for advertising the sale of Nazi memorabilia online. Since this violates French law, a French judge ruled that Yahoo had to remove those materials or pay a hefty fine. Yahoo removed the Nazi-related content from the French version of its portal, and turned to US courts to protect its right to free speech. Goldsmith and Wu use the Yahoo case to make another point: that Internet presences like Yahoo have allowed themselves to become tools of the state. Yahoo filters anti-Communist content on its Chinese portal, as directed by China's government.

Most of the criticisms leveled against Goldsmith and Wu (that they overestimate the power of the state, that they ignore international regimes) are warranted, to a degree, and are discussed in depth elsewhere (Mathiason 2007; Salons 2007; Kerr 2007). Orin S. Kerr (2007) argues that the issue of control is one of compliance and enforceability. Simply put, the state does not have control of the Internet because it cannot always enforce its laws. Others have raised the issue of transparency as it pertains to encryption, which users employ to protect themselves from government interference. Finally, there is a concern that the law is soft on software authors and operating system makers, whose products are susceptible to viruses and malware, while the cost of repairs usually falls to the end-user (Zittrain 2008). But these criticisms suggest that the state is adapting to the challenges brought on by the proliferation of the Internet. The state has worked in concert with the private sector, but has largely retained its capacity to maintain its authority.

National Security and the Internet: Distributed Security through Distributed Responsibility

Myriam Dunn Cavelty
Center for Security Studies, ETH Zurich

The aim to move ''beyond universal generalizations'' when it comes to Internet control issues, as expressed in the introduction to this forum, is both timely and necessary. Indeed, ''no single actor controls'' any given aspect of the Internet. Rather, the impression of a complicated or even complex pattern of overlapping governance structures, stemming from diverse actors approaching the Internet in different ways, is far more suitable to characterize the state of the art of Internet control. This diversity requires an analysis of the peculiarities of

specific issues in various settings rather than elusive parsimony or reductionist explanations, as political scientists are sometimes prone to strive for (and of which the recent book by Goldsmith and Wu 2006 is an example). To move beyond an ''unfruitful deadlock'' in the debate about whether or not the state is becoming obsolete in the digital realm, more studies of specific empirical nature rather than more general philosophic ones are needed. In an attempt to move in this direction, this chapter address aspects of Internet control in relation to security threats in more detail rather than addressing Internet control as a whole (in contrast to the other essays on this Forum).

There are some difficulties for studying information age security issue from an academic perspective, mainly because the majority of books and articles on national security aspects of the Internet published over the last 10–15 years tend to be highly specific and policy-oriented, are US-centric, and do not communicate with more general international relations theory and research (prominent examples for this kind of literature include Arquilla and Ronfeldt 1997; Alberts and Papp 1997; Henry and Peartree 1998. For a broader discussion of IR theory and information age security, see Eriksson and Giacomello 2007). A common feature of most of the literature on the information revolution is the particular belief that in the ''information age,'' information is becoming the major resource of power. One of the core arguments in this literature is that the technological development enhances two trends that diminish the importance of the state, both of which have implications for security: increasing internationalization and increasing privatization. Two central conflicts reveal the nature of an ongoing redistribution of power: first, the notion that the information revolution empowers new forms of international actors, such as NGOs and activists, thus challenging the state's status as the major player in the international system; and second, the idea that the emergence of a global electronic marketplace would inevitably imply a collapse of the state's economic pillar of power as companies increasingly become global citizens and economic boundaries no longer correspond to political ones. Both of these trends have particular implications for nation-states' room for maneuver when it comes to security.

More recently, some scholars have focused on the construction of information-age security threats by using frameworks informed by constructivism, particularly securitization theory (Eriksson 2001; Bendrath 2003; Dunn Cavelty 2008). From this, valuable insights can be gained with regard to threat perceptions and policy reactions, but more research is warranted particularly with regard to comparative studies of threat constructions in countries other than the United States. Post-structuralism has influenced another body of literature, which focuses on so-called ''Postmodern War'' (Hables Gray 1997, 2005; Der Derian 2001), seen as a discourse on technical–military interaction that also focuses on the centrality of information. Information becomes the ''new metaphysics of power'' (Dillon and Reid 2001:59), with various implications of such a conceptualization for the military itself and society as a whole. This kind of literature focuses less clearly on the loss of control by state actors, but, by their very nature, strongly on questions of power and control more generally (see also Franklin).

How National Security and Cyberspace Became Interlinked

In order to understand the security debate surrounding the Internet today, we need to consider two interlinked and at times mutually reinforcing debates that have largely shaped the current discussions and are also reflected in the literature as discussed above. The first is the expansion of the threat spectrum after the Cold War, especially in terms of malicious actors and their capabilities. During the Cold War, threats were mainly perceived as arising from the aggressive intentions of states to achieve domination over other states. Among other things, the end of the

Cold War also heralded the end of unambiguous threat perceptions: following the disintegration of the Soviet Union, a variety of ''new'' threats were moved onto the security policy agendas of most countries. The main distinguishing quality of these ''new'' challenges is the element of uncertainty that surrounds them. The notion of ''threat'' as something imminent, direct, and certain no longer accurately describes these challenges. Rather, they can be characterized as ''risks,'' which are by definition indirect, unintended, uncertain, and situated in the future, since they only materialize when they occur in reality (Rasmussen 2001).

As a result of these diffuse risks and due to difficulties in locating and identifying enemies, parts of the focus of security policies has shifted away from actors, capabilities, and motivations towards general vulnerabilities of entire societies. The catchphrase in this debate is ''asymmetry,'' and the US military has been a driving force behind the shaping of this threat perception in the early 1990s (Rattray 2001). The US, as the only remaining superpower, was seen as being predestined to become the target of asymmetric warfare. Specifically, those adversaries who were likely to fail against the American war machine might instead plan to bring the United States to its knees by striking against vital points at home that are fundamental not to the military alone, but to the essential functioning of industrialized societies as a whole. These points are called *critical infrastructures* (CI). They are deemed critical because their incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a nation (Abele-Wigert and Dunn 2006; Dunn Cavelty and Kristensen 2008).

Fear of asymmetrical measures against such ''soft targets'' was aggravated by the second debate, revolving around new kind of vulnerabilities due to modern society's dependency on inherently insecure information systems. Under the heading of vital system security, protection concepts for strategically important infrastructures and objects have been part of national defense planning for decades, though they played a relatively minor role during the Cold War (Collier and Lakoff 2008). Around the mid-1990s, however, the possibility of infrastructure discontinuity caused by attacks or other disruptions attracted fresh attention among security strategists, mainly due to the information revolution. ''The Internet'', understood here as a network of networks linking computers to computers that share protocols for communication, seemed to add a variety of novel aspects to the older debate about vital system security (Eriksson 2001).

Aspects of Control: The Internet as Target and Weapon

Subsequently, the question of whether the Internet was becoming the new Achilles' heel of modern societies began to be discussed in earnest. In this debate, information infrastructures are regarded as the backbone of critical infrastructures, given that the uninterrupted exchange of data is essential to the operation of infrastructures in general and the services that they provide. Centralized Supervisory, Control and Data Acquisition (SCADA) systems are widely employed to remotely monitor and control infrastructures. But SCADA-based systems are not secure: once-cloistered systems and networks are increasingly using off-the-shelf products and IP-based networking equipment, and require interconnection via the Internet, which opens the door to attackers from the outside in addition to the inside.

The complex interdependence of liberal (risk) societies and their growing technological sophistication have transnationalized and technologized the types of security problems that they face. We seem be witnessing scalar changes moving in opposite directions: the power to resist vulnerability moves *outwards* to international markets and international organizations while the power to cause vulnerability moves *inwards*, through classes and groups to the individual. Representations of this security threat are very broad and also very vague, both in terms of what or who is seen as the threat and of what or who is seen as being

threatened. Global information networks, so the argument goes, make it much easier to attack even the strongest powers, as such an attack no longer requires big, specialized weapons systems. In theory, attacks can be carried out in innumerable ways by anyone with a computer connected to the Internet, and for purposes ranging from juvenile hacking to organized crime, political activism, or strategic warfare. The technology employed for attacks is simple to use, inexpensive, and widely available. The methods of attack have become increasingly automated and more sophisticated, resulting in more damage from a single attack. In addition, Internet attacks in general are quick, easy, inexpensive, and may be hard to detect or trace, especially since the globe-spanning networks grant a great deal of anonymity.

In this debate, ''the Internet''—or rather the information infrastructure—plays three different roles: first, the Internet is used for controlling aspects of critical infrastructures (often remotely); second, the Internet is seen as an attractive target; third, the Internet can be a weapon or at least a kind of ''delivery system'' for attacks. In an attempt to control what the consider to be ''malicious activity'' online and to increase security, states (i) aim to enhance the security of the control infrastructure to ensure reliable functionality of services and (ii) strengthen national law-enforcement capacities and international cooperation. There are also sporadic calls for arms control efforts or multilateral behavioral norms for the military use of computer exploitation (Denning 2001a,b; Rathmell 2001). Due to the breadth of issues subsumed under the virtual threat, all three dimensions of Internet control mentioned in the introduction (*access* to the Internet, *functionality* of the Internet, and *activity* on the Internet) are implied.

Actors: Distributed Security Through Distributed Responsibility

Considering its framing as national security issue or ''high politics,'' forceful attempts by nation states to control undesirable effects in this domain could be expected. What we do see, however, is that governments fail to provide security by themselves so that policies are predicated on the concept of voluntarily sharing responsibility with private actors.

There is little consensus among a variety of public and private actors regarding both the nature of the problem and the approaches to be taken. Depending on their viewpoints, they may see information infrastructures as tools for maintaining a competitive edge over business adversaries, as technical–operational systems, as facilitators of criminal activities, or as defense-relevant strategic assets. This leads to tensions between different stakeholders when it comes to addressing necessary control and security measures. On the one hand, turf battles among government actors are frequent. As is the case for every ''new'' threat that needs negotiation in the political process, different government agencies compete with each other by bringing their own perspective to bear on the problem and try to shape future policies accordingly (Bendrath 2001; Dunn Cavelty 2008). This also has specific implications for how the issue can be addressed theoretically (see below).

On the other hand, governments see themselves in need to engage with the technological community and the private sector as the main proprietor and operator of the critical information infrastructure. In many countries, the provision of energy, communication, transport, financial services, and health care have all been, or are being, privatized as previously protected markets are deregulated. In a nonliberalized economy, the state assumes the responsibility as well as the costs of guaranteeing functioning systems and services. In a liberalized global economy, however, assigning responsibility for securing such systems and services is becoming a major issue (Andersson and Malm 2006). It comes as no surprise, therefore, that governments seek to integrate the private owners of critical infrastructure in CIP practices by means of so-called public–private

partnerships and information-sharing initiatives (Suter 2007). This is, however, not an easy task: In many countries, discontent between the private sector and government is deeply rooted and there are continuing struggles over the question of whether ''security'' means the security of the state as a whole, or whether it only refers to the security of individual users or technical systems, and should therefore be handled by authorities other than national security bodies. We can thus argue, by re-quoting Salhi, that state not only ''allowed nonstate actors to take on crucial roles''—but that they actually *need* nonstate actors in order to provide one of the core tasks of the nation state: security for their citizens.

Material and Immaterial Conditions

Following the arguments made above, it is important to consider both material and immaterial factors with influence on Internet control. When it comes to security critical infrastructures, ''network readiness'' does not play a significant role. Even countries usually considered among the ''have-nots'' in terms of information technology, most notably a number of African countries, are showing a great interest in critical infrastructure protection (CIP) issues. This clearly points to the importance of threat perceptions of state actors: it could be expected that the bigger the threat perceived, the greater the efforts to secure by various means. Other factors that seem to be of import are (i) the degree of liberalization in the infrastructure sectors defined as critical in the respective countries; (ii) the amount of actual (or imagined) dependability of critical infrastructures on ''the Internet''; (iii) the propensity of a state to regulate; and (iv) the level of trust between state actors and the private sector.

Taking into consideration the turf battles and differing viewpoints among a variety of actors, it is necessary to ponder the conditions influencing the process by which key actors subjectively arrive at a shared understanding of how to respond to a security threat (Buzan, Wæver, and de Wilde 1998). In accordance with approaches understand the interactions and processes that form reality as conflicts and struggles between antagonistic and competitive forces over ''the structuring of social meaning'' (Howarth 1995:132), a multiplicity of positions leads to struggles over legitimacy and primacy between competing discourses. At some point in the process, one group will emerge as the ''winner'' of this struggle and will be able to shape its social representation accordingly. Factors that play a role in this process are, among others: (i) the characteristics of the broader environment that shape the threat perception, including technological development; (ii) institutional settings, especially rules, norms, habits as well as culture, as Singh also points out; (iii) the broader political context, and the characteristics of the actors involved, including their beliefs and the resources at hand (Eriksson and Noreen 2002); but also (iv) the way in which the issue is discursively framed (Dunn Cavelty 2008:24–40).

What is Being Controlled on the Internet?

J. P. Singh
Georgetown University

The resurgence of the state in controlling Internet conduits was predicted and predictable (Spar 2003). Let's be fair. When academics first heard the early calls of a ''limitless frontier,'' no one dropped her valise full of structures and

inequalities to start packing in a whole new flat world, despite Friedman's clarion calls to do so (Friedman 2000, 2005). Nevertheless, some hope was expressed for genuinely transformative international governance, economic interdependence, and social organizing and identity politics.[4] Proving John Perry Barlow (or Friedman) wrong was the easy part (Barlow 1996). The hard part involved documenting the political, economic, and social transformations that *were* taking place and the evidence continues to roll in (Dunn Cavelty, Mauer, and Krishna-Hensel 2007; Eriksson and Giacomello 2007; Mueller, Kuerbis, and Page 2007). An equal deluge of scholarship conforms the status quo of state control (Goldsmith and Wu 2006), the triumph of great powers (Drezner 2007), resurgence of (long-distance) nationalism and, to some extent, barriers to electronic commerce.

The question is not whether the state can or cannot control the Internet. Of course, it can control the Internet: in the same way that in the famous retort to Ruggie's (1993a) seminal article about the emergence of extraterritoriality, one academic quipped that state presence, adaptation, and regulatory capacities could be observed in security and economic circumstances everywhere (Kapstein 1993). Ruggie retorted that medieval rulers could break up the trade fairs and gather taxes from them from outside the city walls but who knew then that these new forms of commerce would also herald a whole new way of life and the beginnings of modernity (Ruggie 1993b). If instrumental control were all that mattered, the proper names of town governors alone would alone comprise every city's history.

The meaningful questions to be asked in the long run would surely include those that help us ascertain the tremendous diffusion of the Internet globally and the cultural meaning of this technology for people. We would then need to ask ourselves if the state's control of the Internet, of the type offered by Goldsmith and Wu, is emblematic of the status quo or the transformation in the cultural capacities of the people to make the world meaningful to themselves. For such analyses, obviously taking a bottom-up than a top-down state-centric one, emerging social norms locally and globally through interaction may be in conflict with the world states perceive. The manipulative capacity of the state to survive even such an interactive technology surely speaks highly of the state (Rosecrance 1996; Slaughter 2004) but need not necessarily tell us much about the effects of the Internet in the long run. Technology diffusion and its effects are not the purview of states alone.

Take a simple instrumental insight: the oft-hailed ''unprecedented'' growth of the Internet is undeniable but it is unclear if this diffusion can be explained with recourse to US state or great powers interests alone. The diffusion of this technology, that found its early origins in the US defense establishment, would be counterintuitive to the way the US or any other government seeks to guard its security technologies. Even the terminology used to describe the proliferation of the Internet globally breaks ranks with its predecessors; it would be archaic to speak of the Internet as a ''dual-use'' technology or restrict the export or proliferation of Internet.[5] As of November 2007, there were 1.3 billion users of the Internet out of total world population of 6.6 billion.[6] While Internet penetration was 71% in North America and only 5% in Africa, Africa's growth rate was 880% in the 2000–2007 period as opposed to 119% for North America in the same period. While all kinds of indicators can be produced here to support or invalidate the great power control hypotheses, the point of the diffusion rates is different. Household diffusion of the Internet was far greater than other

[4]For early examples, see Klein (2002) for governance, Rosenau and Singh (2002) for economic transformation, and Castells (1997) and Harcourt (1999) for social organizing and identity politics.

[5]Of course, there are information technologies in general that do remain on sensitive lists. See, of example, http://www.dtic.mil/mctl/ (accessed June 1, 2008).

[6]Statistics cited from http://www.internetworldstats.com/stats.htm (retrieved January 18, 2007).

comparable demand driven technologies such as the telephone or electricity and it is unclear how this diffusion rate can be reduced to great power interests alone.

What led the US government to diffuse this technology throughout the world, which had its origins in the country's security apparatus? The clues to this can be found in the demands for networking and, especially since the Clinton administration, in electronic commerce. Neither of these purposes leads to straightforward equations of state control or state interests. If anything, the assertion of state control in these arenas must be viewed in the context of this loss or potential loss. For each story of the re-assertion of state control one can furnish a counter example. Both narratives are correct but it's too early to tell if state control and electronic commerce are co-joined. If commerce has supported the efforts of the US administration to maintain its control over DNS and ICANN, it is not because commercial enterprises are driven by the prerogatives of their flag but because they are driven by profit and fear that control exercised by the United Nations, as for example, proposed by the World Summit for Information Society (WSIS) and Working Group on Internet Governance (WGIG) processes, would translate into unnecessary regulations and barriers to interoperabilities. Electronic commerce and state control are moving in tandem for now but not because commerce is following flag or because the flag clearly understands its interest in electronic commerce terms.[7]

Furthermore, the profoundest shift in Internet control issues, at the cultural level, comes from the *epistemes* of those purportedly being controlled but nevertheless interacting and networking on the Internet. Can we say for sure that Internet users affirm the precedence of the state in commanding due obedience and legitimacy? If we answer in the affirmative, as a few academics do, this instrumental understanding of the power of technology misses its transformative effects, the change in the identity of the issues and the actors themselves through the interactive circumstance of the Internet. That we have been negligent in attending to the interactive effects of technology is because we have argued interactions away by holding actor identities, interests, and preferences constant in dominant liberal, realist, and radical paradigms. The constructivist and ''reflective'' traditions open up the constitutions of identities and interests.[8] I have argued elsewhere that what instrumental and structural notions were to liberal and radical analyses respectively, *meta-power* is to constructivism in accounting for the effects of interaction on identities of actors and issues (Singh 2002). In the short space of this essay it is not possible to delve into the effects of networking or interaction on social identities, but suffice it to say that political scientists by and large do not want to engage with sociological theories of communication. If they did, they would be discovering formation of identities in the spaces of flows (Castells 1997), interstitialities (Deibert 1997) or in virtual spaces. The unfettered legitimization of state control in these spaces and flows is far from clear.

If interactions change actor identities and meaning of the issues they pursue, actor preferences cannot be taken as constant as do structural analysis where power structures determine preferences prior to any interaction. An example might be illustrative. Despite the Bush administration's attempts to transform ''terror'' into a national category by waging wars on a nation-state, images and narratives on the Internet did not legitimize this conceptualization. These ranged from anti-war chat rooms and protests, to the images of Abu Gharaib, and militant web sites. In conflict here were contending notions of ''security''

[7]See Singh (2008/forthcoming) for the variety of international negotiations underway in the unraveling of electronic commerce.

[8]Keohane (1988) used the term reflective early on in reference to the constructivist, gender, post-modernist, and interpretative traditions in international relations.

and ''threat'' that would not be settled even if the US were to ''win'' its self-defined ''war on terror.'' While the interactions that are leading to new definitions of security are not limited to the Internet, the latter's role in proliferating and deepening the new cultural understandings globally is undeniable. It may not be a mere coincidence that notions of human security, rather than national security, are coming to fore in the age of the Internet. To be sure, human security norms have not (yet) replaced national security norms but the co-presence of the two is among the many cultural conflicts of our age.

This short essay does not deny that state control over the Internet exists. If anything, not only does the United States control crucial nodes with a concert of great powers, but also as is becoming clear, at least in terms of Internet governance, states are finding new and creative ways of reasserting their control. However, in order to obtain a complete picture of control or its opposite, we must attend to dominant factors leading to Internet diffusion and its long-term transformational effects. This essay points toward the tremendous growth of electronic commerce and the changes in cultural identity of actors and issues as a result of the inter-actional circumstances of the Internet. Networked identities might be a useful metaphor to capture the transformational dynamics as revealed through the workings of the networked state (Slaughter 2004) or networked human beings, as opposed to discrete nation-states or other global actors that come with predefined preferences. The term ''network'' redefines both their solitude and their strategies. A particularly poignant example recently was the protest in Colombia on February 4, 2008, against both left-wing guerillas movements and right wing paramilitaries. What led to one of the biggest ever protests in Colombia—estimated 500,000 protesters in Bogotà alone—and many other cities around the world, began as an idea promoted over the Internet social networking tool, Facebook, that quickly drew pledges from 100,000 people from around the world to protest (Kraul 2008). We scholars are quite right in noting that teenagers and young people primarily use Facebook. However, we are quite behind in understanding the transformational effects of this technology on the way Facebook users understand their political and cultural identities. A generational gap, indeed!

Who's Who in the 'Internet Governance Wars': Hail the Phantom Menace?

M. I. Franklin
Goldsmiths, University of London

Opening Credits

Now that the specter of interdisciplinary theory and research once haunting *fin-de-siècle* IR is safely locked away in its academic crypt, unfettered state-centeredness can once again hog the limelight. Twenty-first century *realpolitik* is alive and kicking; not only in (neo-)conservative (US) foreign-policy terms (Grandin 2007) but also in emergent computer-mediated ones. It would be disingenuous for critics of longstanding state-centric IR paradigms and great power muscle-flexing to claim otherwise, either in ''real-life'' or ''virtual'' world affairs, a truism that all contributors to this forum take on board in one way or another. In the latest

history of the Internet, Goldsmith and Wu (2006) set themselves a straightforward task of stating the obvious in this regard. Their normative—political—aim, however, is to relegate contending notions of the Internet (however defined), as a *viable* ''nonstate'' actor or transformative nexus, to the dustbin of recent history. To do this they have to write out of their narrative the existence, and persistence of a plethora of other, nonstate agencies, techno-economic powers, cultures of use, IT ideas and software designs, corporate interests, media-reform platforms, cultural and political activities on or through the Internet.

Whether or not History is on their side, locking all the action, players, and dénouement into the grand narrative of an ''older and stronger'' state-system (op cit: iii) this polemical account grossly overplays not only the *intentions* but also the *foresight* of said ''state-actors'' in its version of who (really) controls the Internet. As one reviewer notes, this offensive could herald the start of the *Internet Governance Wars*. Be that as it may, when it comes to technological change, facts and fictions have always been almost impossible to disentangle from one another; real-life all too often mimics art.[9]

Like my co-contributors, this taking up of this particular gauntlet speaks from the intersection of a diverse literature on the shifting powers of the ''State,'' as conceived in traditional IR theory (Eriksson and Giacomello, Salhi in this forum) vis-à-vis contemporary ''global governance'' institutions on the one hand and, on the other, the supraterritorial, transnational, or global dimensions of the contemporary world (see Scholte 2000; Appadurai 2002) and how these are ''overdetermined'' by information and communication technologies (ICTs or the Internet for short). Contra to Salhi, picking up where Dunn Cavelty leaves off, and taking Singh's skepticism to its logical conclusion, this contribution looks to problematize the terms of debate even further.

Main Plot and Cast Members

Given that 20/20 vision comes with the benefit of hindsight, Goldsmith and Wu's claims that States (*viz.* the US) have inviolable sovereignty over their *Own Private Internet*, ''rogue states'' excepted, compels a response in kind; for or against the *State*. However, debates about *who* controls the Internet, let alone *how*, are not just about locating the exercise of direct—coercive—''power over'' infrastructures, content, access-points, or uses (Eriksson and Giacomello). They are also struggles over *artistic* control of the ''prequel''; of futures-past now that the halcyon days of the World-Wide Web cyber-optimism are over. As wars have been won and lost on the battleground of ideas, leverage over the narrative is paramount. Goldsmith and Wu's *Die Hard* version of ''How The Internet Was Won,'' albeit set in a post-9/11 *Star Wars* galaxy lays a finger on some sore spots. This calls for a sturdy rise to the challenge nonetheless. Even more so as the object of analysis and location, the ''Internet''—a slippery target anyway, morphs into its second if not third incarnation.

Goldsmith and Wu rest their case for the prosecution in their staging of *State Actors vs. NonState Actors* on the unabashed optimism of many authors from the previous decade (the heyday of the world-wide-web), accusing them of pie-in-the-sky thinking. On so doing they end up underscoring the shaky ground upon which even the most coercive governments, democratic or autocratic, stand when faced with layers of computer encoded pathways, operational incompatibilities of

[9]For a summary of Goldsmith and Wu's argument and a regime theorist's riposte see the review by John Mathiason (2007), one in which he makes full use of allusions to the Star Wars series of Hollywood blockbuster movies. Popular culture, particularly science fiction, is a rich allegorical source for many a commentary on the Internet, society, politics nexus; albeit an ambiguous one given the predominance of US cultural industries and military-industrial complex in this cultural domain as well.

ICT day-to-day interconnections, millions of ordinary users refusing to do as they are told, global financial behemoths defying fiscal regimes, and violently inclined parties parading their counter-hegemonic programs online. The body of evidence actually underscores the inadequacy and limits of traditional powers' ability to cope with the unruliness of the myriad (non-)uses, misuses and applications of ICTs (see Dunn Cavelty and Singh), of which ''the Internet'' and its ''governance'' are but parts of a larger puzzle.

Meanwhile, already argued in the previous contributions, ICT/media policy-making continues to unfold in multiplex settings, assigning a less pre-eminent role for Westphalian-style statehood in the proceedings as a matter of course; e.g., the UN's *World Summit on the Information Society* (WSIS). Translocal, transnational, and supraterritorial trajectories and alliances overlay domestic–international demarcation lines as multilateral institutions broker ''multi-stakeholder'' meetings (e.g., the *WSIS*), supraterritorial arbitrage (for example, the *World Trade Organization*), and transnational monitoring bodies (e.g., the *Scientific Expert Group on Climate Change and Sustainable Development*). The *modus operandi* of these initiatives is that ''nonstate actors''—corporate and ''civil''—are indispensable to ''global agenda-setting,'' monitoring, and enactment (Jørgensen 2006).

These trends are further complicated by the way on-the-ground, face-to-face negotiations and political rituals are spliced with *cyberspatial*, web-based ones (Jordan 1999; Jones 1999; Franklin 2004, 2007a,b). The terrain (the whereabouts), the actors (the ''who''), the stakes (what is it all about), and the *means*, are increasingly multi-sited and multidimensional rather then vertically integrated, geographically contained, analogically disseminated. That certain governments are ready to rush onto the stage at propitious moments, Anglo-US scuttling of the 1980s *New World Information and Communication Order* (NWICO) initiative or Tunisian authorities' interventions in WSIS events for instance, are not sufficient evidence that they have *unmitigated* control over the course of events, let alone hold some higher moral ground. Besides, notions of political administrations having executive power over R&D trajectories or multi-media sectors, in OECD countries at least, is virtually extinct after the liberalization-privatization strategies of past decades. The double standards shown by ''good guy'' and ''bad guy'' regimes and ''private sector'' partners, if not willful undermining of these more inclusive multilateral moments, are more indicative of a geriatric ''phantom menace'' than a reinvigorated State riding to the rescue with his cyber-spurs on.

Back-Stories and Sub-Texts

What we are dealing with here is not just complex wrangles over technoeconomic jurisdictions, democratic accountability, or the fate of the state but, rather, inchoate visions of computer-mediated futures and their underlying ethos. The Internet cannot be captured in its thing-ness; as hardware, software packages, distributed servers, wires and cables, or even the way in which this object can be (better) apprehended discursively (see Dunn Cavelty). It is all of these things. And more, as its material-symbolic constitution becomes a signifier, an allegory, for how ''we,'' whoever we are, want to live on the planet, under what conditions, and by what means. Power and influence over all this, as much an affair of state as a transnational corporate concern, implicates ordinary users and non-users as well. The political is deeply personal here as practices of everyday life online continue despite Pro-Am sabotaging of functionalities, quasi-legal monitoring and commercial filtering of Internet content, activities, and relationships that criss-cross national borders and international legal niceties (see Singh, Dunn Cavelty, Eriksson and Giacomello). At this juncture not only the terms of debate, the means by which it takes place but also speaking rights need to be rigorously

renegotiated, incumbent political and techno-economic powers' sense of entitlement hotly contested accordingly.

While the jury is still out, the verdict is not a *fait accompli*. It is at a critical juncture nonetheless; critical because in all its symbolic and techno-economic manifestations, the Internet operates as both a means and mediator for all manner of global, *trans*-local, and nonbordered interactions. This ''double-life'' of Internet technologies inculcates high politics, corporate strategizing, political platforms (neoconservative, [neo]liberal, and ''old Left''), and social activism. If the Internet is indeed a new locus for the ''long-standing theoretical debate about the nature of the world'' (Mathiason 2007:152; Sahli and Singh) endemic to IR, then there is an urgent need to engage politically and theoretically in this latest version of the *Realism vs. Idealism* standoff. Much as I beg to differ, I applaud this *politicization* of the *meaning-making* that comprises any notion of Internet control and/or ''governance.''

Battle of the Script-Writers in Five Parts

The first problem is that the Internet, in itself and corollary issues, has only just caught the eye of IR scholars. Frameworks germane to the *Third Debate*[10] have generally shown a sturdy disinterest in such ''techie'' matters. Roughly the same age as the Internet, this body of literature extended the cast of actors, story-lines, and locales pertinent to international studies in arguing that it would no longer do to write practices, flows, locations, and agents that cannot be dealt with by state-centric paradigms/levels of analysis out of the script. *In toto* these *intra*disciplinary moves have failed to effectively problematize the underlying hi-tech essentialisms permeating both (neo)realist and critical theoretical explanatory frameworks of world politics (cf. Der Derian 1995; Hardt and Negri 2000; Franklin 2004; Dahlberg and Siapiera 2007). Cyber-based, on-the-ground, and supraterritorial technological and political realities have been *co*-constructing one another for some time now. For instance, global agenda-setting or protest is very much a *hyper*textual, computer-generated affair (Franklin 2007a), Internet access and ''computer literacy'' are integrated into Human Development ideas as the latter are effected by and through ICTs, multilateral institutions consummately create and replicate online content, the Internet is becoming a global repository for human memory and site for neuro-marketing (Lazuly 2003; Bénilde 2007; Lévy 2007).

One way to make sense of all this, particularly in light of the return of a hearty neorealism, is through a radical, not simply utilitarian understanding of *discourse* (see also Singh, Dunn Cavelty, and Eriksson and Giacomello). This is not to substitute material realities with an abstract, socially disembedded ''text''—technical or cultural artifact. Emergent discursive practices of digitality, hypertextuality, and cyberspatiality are embedded in actually existing sociocultural and political economic power relations. This more thorough notion of discourse folds the thing-ness of the Internet into ideational contestations, the ''immateriality'' of virtual domains into the nitty-gritty of media law, physical access, uses, palpable albeit diffuse ''media effects,'' activities, and functionalities. The Internet and its constitutive practices and structures need to be construed not just as-a-technology but also as-an-idea, integral to the ''scriptural economies'' that reproduce the ''modern mythical practice'' (Certeau in Franklin 2007a:315) of the Westphalian Imaginary and its representational regimes—*machineries* (Hall in Franklin 2004:15–16). The Internet, its so-called governance or control, is integral to such meaning-making practices, and vice versa. Rather than appear inexorable,

[10]This is a broad rubric for varieties of critical, constructivist, (see Singh in this forum), post-modern, and post-positivist IR, feminist and postcolonial streams included (Lapid 1989; Der Derian 1995; Franklin 2004).

seemingly monolithic ICT networks, architectures, and digital components can be demystified, rendered contestable in their contingency; an amalgam of individual and societal socialization processes (''onlineness''), normalization (the Internet was a novelty once), institutionalization (multilateral and national policy agendas), singular ideas (the ''information society''), and grander narratives (globalization).

This brings us to a third problem; what to do with actually existing state agencies nonetheless, let alone their reincarnation as private-sector partnerships. A fuller conceptualization of discourse recognizes that the ''State,'' just like the ''Internet,'' crystallized over time, in haphazard and contingent ways: neither arrived on the scene ready-made. Michel Foucault puts it this way; ''the State does not have an essence. The State is not universal. The State is not in itself an autonomous source of power. The State is nothing other than the effect, the outline, the moving cross section of a perpetual process of State formation … [of] practices of *governmentality*'' (Foucault 2004a:79; emphasis added).[11] Within this notion of discourse and in light of the forum editors' tripartite delineation of internet control, thinking in terms of governmentality means putting state-apparatuses in their place; as accumulations over time rather than granting them a priori rights of entitlement. Control of the Internet, and its conceptualization (Mattelart 2007) is subject to, and object of this ''triangle, sovereignty—discipline—government, which has as its primary target the population and as its essential mechanism the apparatuses of security'' (Foucault 1984:102). In short it means approaching the ''State'' and/or the ''Internet'' as ''singularly paradoxical'' (ibid: 103) phenomena.

The next issue concerns the flip-side of state-centric takes on ''Internet Governance.'' Responding in kind—for or against the state—lead to the real and present danger of ''overvaluing the problem of the state'' (ibid: 103) even as numerous parties are trying to (re)write the script, wrest leverage over the final cut if not buy up the copyright or distribution rights. In these shifting sands, some more clarion calls against state-control can become complicit in the continued expansion rather than contraction of modernist governmentality (Foucault op cit, Douglas 1999). Goldsmith and Wu actually have a point here in their assessment of the 1990s'' generation of cyber-enthusiasts. The new millennium's generation of transnational ICT and media-reform activism and advocacy networks are not immune to these impulses either.

Reducing everything to a Manichean battle between the State and its Discontents, then, can also mean missing crucial nuances, opportunities, and moments for resistance and change as the script, casting, location, and final production are finalized. For struggles over artistic control are occurring in the writing and ownership of software, where servers filter or monitor Internet traffic, under Wi-Fi umbrellas or in satellite arrays, in reruns of Star Wars defense discourses in outer-space, and in the intimate spheres of interpersonal practices online. To speak of this as discourse—the politics of representation in other words—is to see the Internet as a fluid and multiplex cluster of systems, infrastructures, practices, meanings, and regulations. The latter being piece meal and, by tradition, reactive rather than proactive, are based on a not always happy marriage between political representatives, regulatory bodies, and corporate interests. Techno-historical and socio-economic accidents such as the Internet-as-we-know-it can proffer alternative futures. It need not be subservient to the seemingly inexorable march of the Westphalian-Capitalist telos.

[11]Foucault is hardly unfamiliar to international relations theory and research since the Third Debate. The publication of a swathe of new material (Foucault 1994, 2004a,b) has seeing notions such as *governmentality* and *biopower* being furthered. For Internet-related matters this body of work, along with his contemporaneous ''practice theorists,'' are well worth the visit (Jordan 1999; Franklin 2004, 2007b).

Final issue, or twist in the plot; where does this line of thought leave critical scholars and activists in the face of increasingly commodified and proprietary spins being put on current Internet Governance discourses? Who, or what forces are the guardians of the future?

Getting to grips with the symbolic-material practicalities of Internet control—*de facto* or *de jure*—also entails serious consideration of how thinking-machines, artificial intelligences, and their specific network structures impinge on pre-existing assumptions about the nature of politics and human agency in computer-mediated and cyberspatial domains. The contemporary world order is increasingly constituted by automated—cybernetic—systems run by, and for computers (Kelly 1994, Haraway 1991, Shapiro 1999; Stefik 1999). Hence ''nonstate actors'' can also be ''thinking machines'' (Quintas 1996). These emergent actors/change-agents are still subject to organic intelligence; human agency. Just. Automation, computerized systems, robotics, Artificial Intelligences, are neither new nor inconsequential to this story. Incorporating these elements ups the ante accordingly. Questions about the specifics of ''what it is to govern'' thereby means finding out ''a little more about what type of power is covered by this notion'' (Foucault 2004b:119). In this respect, it bears noting that incumbent and emergent (counter) powers can be resisted, subverted, exercised, redirected and abdicated by remote control through automated systems or by nonhuman agents just as well.

Control: The Final Cut?

Summing up in light of these reflections, the editors' explications, and points raised by the previous contributions, three delineations to this plea for incorporating more radical notions of discourse, and governmentality bear mentioning. First, *who* controls is starting to blur into questions about *what* controls in computable terms (Kelly 1994:23–24). Second, ascertaining *how* control is exercised let alone circumvented, or subverted is analytically distinct from the ''who'' and the ''what.'' In ICT-mediated, cybernetic practice such distinctions are becoming harder to make. Third, shifting the axis of the current debate away from state-centric notions of control (power, influence) where the latter are either a question of physical possession or an instrument of ''C31'' military operations (Haraway 1991:164) onto practices, institutionalizations, and socializations, self-aggrandizing actors get put in their place. As the Internet/Internet discourses become disciplined, domesticated and ultimately corporatized, debates need to refocus. Nonhuman agents, cybernetic organisms, computer-automated systems, and Internet-embedded media messages are not extraneous to these debates. As for references to governance *wars*, well, all of the aforementioned devices and techniques are being deployed in military theatres around the world, online and offline, as I write.

To conclude, let me recall Donna Haraway's prescience when she noted way back in the 1980s how ''late twentieth century machines have made thoroughly ambiguous the difference between natural and artificial, mind and body, self-developing and externally designed …. Our [thinking] machines are disturbingly lively, and we ourselves are frighteningly inert (1990:194). Time to take this liveliness more seriously into account along with cybernetic systemic logistics and machine-organic-microchip hybrids when considering the politics of design and purpose that inform *whose* Internet is at stake in all this. Without incorporating these imminent ''nonstate actors'' into the scenario in what is an age of digital-human ''embeds, effective responses to *Return of the State* accounts can overlook how cybernetic organisms, artificial intelligences, may well end up overriding the manual controls thereby rendering state, market, and civil society obsolete. But that is another story, and another genre of science fact-fiction.

References

Abele-Wigert, Isabelle, and Myriam Dunn. (2006) *The International CIIP Handbook 2006. An Inventory of Protection Policies in 20 Countries and 6 International Organizations*. Zurich: Center for Security Studies.

Alberts, David S., and Daniel S. Papp, eds. (1997) *The Information Age: An Anthology of Its Impacts and Consequences*. Washington, DC: National Defense University.

Andersson, Jan Joel, and Andreas Malm. (2006) Public-Private Partnerships and the Challenge of Critical Infrastructure Protection. In *International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects*, edited by M. Dunn and V. Mauer. Zurich: Center for Security Studies.

Appadurai, Arjun. (2002) Disjuncture and Difference in the Global Cultural Economy. In *The Anthropology of Globalization: A Reader*, edited by J.X. Inda and R. Rosaldo. Oxford: Blackwell.

Aron, Raymond. (1962) *Paix et Guerre entre les Nations*, 3rd edition. Paris: Calmann-Levy.

Arquilla, John, and David Ronfeldt, eds. (1997) *In Athena's Camp Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND.

Barlow, John Perry. (1996) *A Declaration of the Independence of Cyberspace*. Davos, Switzerland. Available at http://homes.eff.org/~barlow/Declaration-Final.html

Bendrath, Ralf. (2001) The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. *Information & Security: An International Journal* 7:80–103.

Bendrath, Ralf. (2003) The American Cyber-Angst and the Real World—Any Link? In *Bombs and Bandwidth. The Emerging Relationship Between Information Technology and Security*, edited by Robert Latham. New York/London: The New Press.

Beniger, James. (1986) *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA: Harvard University Press.

Bénilde, Marie. (2007) *On achète bien les cerveaux. La publicité et les medias*. Paris: Raisons d'agir.

Bessette, Ràndi, and Virgina Haufler. (2001) Against All Odds: Why There Is No International Information Regime. *International Studies Perspectives* 2(1):69–92.

Buchner, Bradley. (1988) Social Control and the Diffusion of Modern Telecommunications Technologies: A Cross National Study. *American Sociological Review* 53(3):446–453.

Buzan, Barry, Ole Wæver, and Joop de Wilde. (1998) *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Castells, Manuel. (1997) *The Power of Identity. The Information Age: Economy, Society and Culture*, Volume I. Oxford: Blackwell.

Chomsky, Noam. (1997) *Media Control: The Spectacular Achievements of Propaganda*. New York: Seven Stories Press.

Collier, Stephen, and Andrew Lakoff. (2008) The Vulnerability of Vital Systems: How ''Critical Infrastructure'' Became a Security Problem. In *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security*, edited by M. Dunn C. and K. Søby Kristensen. London: Routledge.

Dahlberg, Lincoln, and Eugenia Siapiera, eds. (2007) *The Internet and Radical Democracy: Exploring Theory and Practice*. New York/London: Palgrave Macmillan.

Deibert, Ronald J., Johnpalfrey, Rafal Rohozinski and Jonathan, Zitrain, eds. (2007) *Access Denied: The Practice and Policy of Internet Filtering*. Cambridge, MA: MIT Press.

Denning, Dorothy. (1997) The Future of Cryptography. In *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, edited by Brian Loader. London: Routledge.

Denning, Dorothy. (2001a) Is Cyber Terror Next? In *Understanding September 11*, edited by Craig Calhoun, Paul Price and Ashley Timmer. Available at http://www.ssrc.org/sept11/essays/denning.htm.

Denning, Dorothy. (2001b) Obstacles and Options for Cyber Arms Controls. Paper presented at Arms Control in Cyberspace Conference, Heinrich Boell Foundation, Berlin, 29–30 June 2001. Available at http://www.nps.edu/Faculty/DorothyDenning/publications/Berlin.pdf.

Der Derian, James, eds. (1995) *International Theory: Critical Investigations*. London: Macmillan Press.

Der Derian, James. (2001) *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Complex*. Boulder, CO: Westview.

Dillon, Michael, and Julian Reid. (2001) Global Liberal Governance: Biopolitics, Security and War. *Millennium Journal of International Studies*, 30(1):41–66.

Douglas, Ian Robert. (1999) Globalization as Governance: Toward an Archaeology of Contemporary Political Reason. In *Globalization and Governance*, edited by A. Prakash and J. Hart. London/New York: Routledge.

Drezner, Daniel. (2007) *All Politics is Global: Explaining International Regulatory Regimes*. Princeton, NJ: Princeton University Press.

Dumez, Herve, and Alain Jeunemetre. (2004) Regulation in Europe. In *The Global Internet Economy*, edited by Bruce Kogut. Cambridge, MA: MIT Press.

Dunn Cavelty, Myriam. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.

Dunn Cavelty, Myriam, and Kristian Søby Kristensen. (2008) Introduction: Securing the Homeland: Critical Infrastructure, Risk, and (In)Security. In *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security*, edited by M.D. Cavelty and K. Søby Kristensen. London: Routledge.

Dunn Cavelty, Myriam, Victor Mauer, and Sai Felicia Krishna-Hensel, eds. (2007) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot, UK: Ashgate.

Dunn, Myriam, Sai Felicia Krishna-Hensel, and Victor Mauer. (2007) *The Resurgence of the State: Trends and Processes in Cyberspace Governance*. Aldershot: Ashgate Publishing.

Eriksson, Johan. (2001) Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management* 9(4):211–222.

Eriksson, Johan, and Giampiero Giacomello, eds. (2007) *International Relations and Security in the Digital Age*. London: Routledge.

Eriksson, Johan, and Erik Noreen. (2002) *Setting the Agenda of Threats: An Explanatory Model*. Uppsala Peace Research Papers 6. Available at http://www.pcr.uu.se/publications/UPRP_pdf/uprp_no_6.pdf.

Flichy, Patrice. (2007) *The Internet Imaginaire*. London, UK, Cambridge, MA: The MIT Press.

Foucault, Michel. (1984) *The Foucault Reader*, edited by P. Rabinow. New York: Pantheon Books.

Foucault, Michel. (1994) *Dits et écrits*, Volumes 1–4. Paris: Gallimard.

Foucault, Michel. (2004a) *Naissance de la biopolitique*. Cours au Collège de France. 1978–1979. Paris: Gallimard.

Foucault, Michel. (2004b) *Sécurité, Territoire, Population*. Cours au Collège de France, 1977–1978. Paris: Gallimard.

Franklin, Marian. (2004) *Postcolonial Politics, the Internet, and Everyday Life: Pacific Traversals Online*. London/New York: Routledge.

Franklin, Marian. (2007a) NGO's and the ''Information Society'': Grassroots Advocacy at the UN—a cautionary tale. *Review of Policy Research* 24(4):309–330.

Franklin, Marian. (2007b) Democracy, Postcolonialism, and Everyday Life: Contesting the ''Royal We'' Online. In *The Internet and Radical Democracy: Exploring Theory and Practice*, edited by Lincoln Dahlberg and Eugenia Siapera. New York/London: Palgrave Macmillan.

Friedman, Thomas. (2000) *Lexus and the Olive Tree: Understanding Globalization*. New York: Farrar, Straus and Giroux.

Friedman, Thomas. (2005) *The World is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus and Giroux.

Giacomello, Giampiero. (2003) The Political ''Complications'' of Digital Information Networks: A Reply to the Politics of Bandwidth. *Review of International Studies* 29(1):139–143.

Giacomello, Giampiero. (2005) *National Governments and Control of the Internet: A Digital Challenge*. London: Routledge.

Giacomello, Giampiero, Yaman Akdeniz, Singapore Broadcasting Authority, and Marc Holitscher. (1999) Debate: Internet Governance. *Swiss Political Science Review* 5(2):115–142.

Goldsmith, Jack, and Tim Wu. (2006) *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.

Grandin, Greg. (2007) Sucking up to P. *London Review of Books* 29(23):11.

Hables Gray, Chris. (1997) *Postmodern War—The New Politics of Conflict*. New York: Guilford Press.

Hables Gray, Chris. (2005) *Peace, War, and Computers*. London: Routledge.

Hague, Barry N., and Brian D. Loader (1999) *Digital Democracy. Discourse and Decision-Making in the Information Age*. London/New York: Routledge.

Haraway, Donna J. (1991) *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge.

Harcourt, Wendy, eds. (1999) *Women@Internet: Creating New Cultures in Cyberspace*. London: Zed Books.

Hardt, Michael, and Antonio Negri. (2000) *Empire*. Boston, MA: Harvard University Press.

Henry, Ryan, and Edward Peartree, eds. (1998) *Information Revolution and International Security*. Washington, DC: CSIS.

Herrera, Geoffrey. (2002) The Politics of Bandwidth: International Political Implications of a Global Digital Information Network. *Review of International Studies* 28(1):93–122.

Hoffman, Stanley. (1966) Obstinate or Obsolete? The Fate of the Nation-State in Western Europe. *Daedalus* 95(3):862–914.

Howarth, David. (1995) Discourse Theory. In *Theory and Methods of Political Science*, edited by D. March and G. Stoker. London: Macmillan.

Jones, Steveed. (1999) *Doing Internet Research: Critical Issues and Methods for Examining the Net*. London: Sage.

Jordan, Tim. (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London/New York: Routledge.

Jørgensen, Rikke Frank, ed. (2006) *Human Rights in the Global Information Society*. Cambridge, MA & London: MIT Press.

Kapstein, Ethan. (1993) Correspondence. *International Organization* 47(3):501–503.

Kelly, Kevin. (1994) *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*. New York: Addison-Wesley Publishing.

Kenny, Martin. (2004) The Growth and Development of the Internet in the United States. In *The Global Internet Economy*, edited by B. Kogut. Cambridge, MA: MIT Press.

Keohane, Robert. (1988) International Institutions: Two Approaches. *International Studies Quarterly* 32(4):379–396.

Kerr, Orin S. (2007) Enforcing Law Online. *University of Chicago Law Review* 74(2):745–760.

Klein, Hans. (2002) Global Democracy and the ICANN Elections. *Info—The Journal of Policy, Regulation and Strategy for Telecommunications* 3(2):255–257.

Kraul, Chris. (2008) Colombians Protest Rebel Kidnappings. *Los Angeles Times*. March 5. Available at http://www.latimes.com/news/nationworld/world/la-fg-march5feb05,1,955782.story

Lagerkvist, Johan. (2007) *The Internet in China: Unlocking and Containing the Public Sphere*. Lund: Lund University Press.

Lapid, Yosef. (1989) The Third Debate: On the Prospects of International Theory in a Post-Positivist Era. *International Studies Quarterly* 33(3):235–254.

Latham, Robert, eds. (2003) *Bombs and Bandwidth. The Emerging Relationship Between Information Technology and Security*. New York/London: The New Press.

Lazuly, Pierre. (2003) Telling Google What To Think: How An Online Search Engine Influences Access To Information, *Le Monde Diplomatique* (English Edition), November 2003. Original French version, ''Le monde selon Google,'' Le Monde Diplomatique, Novembre, 2003.

Levy, Steve. (2001) *Crypto: How the Code Rebels Beat the Government-Saving Privacy in the Digital Age*. New York: Viking.

Lévy, Pierre. (2007) Nouvelle responsabilité des intellectuels'. In *Le Monde Diplomatique*. Paris: Le Monde Diplomatique. 54(641): August: 22–23.

Lijphart, Arendt. (1999) *Patterns of Democracy*. New Haven, CT: Yale University Press.

MacMahon, Peter. (2002) *Global Control: Information Technology and Globalization since 1845*. Cheltenham, UK: E. Elgar.

Mathiason, John. (2007) *Internet Governance Wars: The Realists Strike Back,* book review of Who Controls the Internet? by Jack Goldsmith and Tim Wu, Oxford University Press 2006, *International Studies Review* 9(1):152–155.

Mattelart, Armand. (2007) Qui contrôle le concepts? In *Le Monde Diplomatique*. Paris: Le Monde Diplomatique. 54(641): August: 23.

Mowlana, Hamid. (1997) *Global Information and World Communication: New Frontiers in International Relations*, 2nd edition. London: Sage.

Mueller, Milton. (2002) *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Mueller, Milton, Brendan Kuerbis, and Christiane Page. (2007) Democratizing Global Communication? Global Civil Society and the Campaign for Communication Rights in the Information Society. *International Journal of Communication* 1(1):1–31.

Mulgan, Geoffrey. (1991) *Communication and Control: Networks and the New Economies of Communication*. Cambridge, UK: Polity Press.

Pool, de Sola Ithiel. (1983) *Technologies of Freedom*. Cambridge, MA: Belknap Press.

Pool, de Sola Ithiel. (1990) *Technologies Without Boundaries: On Telecommunications in a Global Age*. Cambridge, MA: Harvard University Press.

Pound, Roscoe. (1997) *Social Control Through Law*. New Brunswick: Transaction.

Quintas, Paul. (1996) Software by Design. In *Communication by Design: The Politics of Information and Communication Technologies*, edited by R. Mansell and R. Silverstone. Oxford: Oxford University Press.

Ranstorp, Magnus. (2007) *The Virtual Sanctuary of Al-Quaeda and Terrorism in an Age of Globalization*. International Relations and Security in the Digital Age, edited by J. Eriksson and G. Giacomello, London: Routledge, pp. 31–56.

Rasmussen, Mikkel Vedby. (2001) Reflexive Security: Nato and International Risk Society. *Millennium: Journal of International Studies*, 30(2):285–309.

Rathmell, Andrew. (2001) Controlling Computer Network Operations. *Information & Security: An International Journal* 7:121–144.

Rattray, Greg. (2001) *Strategic Warfare in Cyberspace*. Cambridge: MIT Press.

Rosecrance, Richard. (1996) The Rise of the Virtual State. *Foreign Affairs* 75(4):45–61.

Rosenau, James, and J.P. Singh, eds. (2002) *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. Albany, NY: State University of New York Press.

Ruggie, John Gerard. (1993a) Territoriality and Beyond: Problematizing Modernity in International Relations. *International Organization* 47(1):139–174.

Ruggie, John Gerard. (1993b) Correspondence. *International Organization* 47(3):503–505.

Salons, Deborah J. (2007) Who Controls the Internet? A Review *Federal Communications Law Journal* 59(3):615–619.

Schneier, Bruce. (2000) *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley and Sons.

Scholte, Jan-Aart. (2000) *Globalization: A Critical Introduction*. New York: St Martins Press.

Shapiro, Andrew. (1999) *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*. New York: Public Affairs—Perseus Books.

Singh, J.P. (2002) Introduction: Information Technologies and the Changing Scope of Power and Governance. In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, edited by J. Rosenau and J.P. Singh. Albany, NY: State University of New York Press.

Slaughter, Anne-Marie. (2004) *A New World Order*. Princeton, NJ: Princeton University Press.

Spar, Debora. (2003) *Ruling the Waves: From the Compass to the Internet, a History of Business and Politics along the Technological Frontier*. New York: Harcourt Books.

Stefik, Mark. (1999) *The Internet Edge: Social, Legal, and Technological Challenges for a Networked World*. Boston, MA: MIT Press.

Suter, Manuel. (2007) Improving Information Security in Companies: How to Meet the Need for Threat Information. In *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, edited by M.D. Cavelty, V. Mauer and S.-F. Krishna-Hensel. Aldershot: Ashgate.

United Nations. (2008) *UN E-Government Survey 2008. From E-Government to* Connected Governance. New York: United Nations Publications.

Waltz, Kenneth. (1959) *Man, the State and War: A Theoretical Analysis*. New York: Columbia University Press.

Warf, Barney, and Peter Vincent. (2007) Multiple Geographies of the Arab Internet. *Area* 39(1):83–96.

Weimann, Gabriel. (2006) *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press.

Wright, Scott. (2000) Political Control and the Internet. In *Human Rights and the Internet*, edited by Steven Hick, Edward Halpin and Eric Hoskins. New York: St. Martin's Press.

Youm, Kyu Ho. (2006) Who Controls the Internet? Illusions of a Borderless World (Book Review). *Journalism and Mass Communication Quarterly* 83(3):730–734.

Zittrain, Jonathan. (2004) Internet Points of Control. In *The Emergent Global Information Policy Regime*, edited by Sandra Braman. Houndmills: Palgrave.

Zysman, John, and Abraham Newman. (2006) The State in the Digital Economy. In *The State After Statism: New State Activities in the Age of Globalization*, edited by J.D. Levy. Cambridge, MA: Harvard University Press.