Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

Who Controls Cyberspace?

Nazli Choucri
Political Science Department
Massachusetts Institute of Technology

David D. Clark
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

September 1, 2013

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Who Controls Cyberspace?

When Wikileaks released hundreds of thousands of Iraq War logs and diplomatic cables in 2010, a horrified US government sprang into action—but the classified information the government hoped to keep from public view quickly migrated to overseas servers, ensuring that it would likely never be suppressed.

After an anti-Islamic movie trailer was posted on YouTube in 2012, the horrified Pakistani government rushed to block its nation's access to the Internet video service—and, in the process, temporarily disrupted YouTube access around the world. Toward the beginning of the Egyptian revolution, the government of Hosni Mubarak tried to quell the cyber-based aspect of the protest by turning off the Internet, but that effort did little to alter the course of the revolt. China, however, continued to block searches for the terms "Egypt" and "Arab Spring," with at least some success.

Until recently, cyberspace was considered largely a matter of low politics, the term political scientists use to denote background conditions and routine decisions and processes. Over the last decade, though, cyberspace, with the Internet at its core, has clearly begun to shape the domain of high politics—that is, the national security considerations, core institutions, and decision systems that are critical to national governments. Those governments have long held a monopoly on high politics and are, in turn, trying to control the future of cyberspace, with, at best, very limited success.

The field of international relations, rooted in 20th-century issues and theories, has not kept pace with the emerging significance of cyberspace; and as the empowered non-state groups and individuals of cyberspace and international politics now simultaneously shape one another, the potential collisions of law, policy, and practice have barely been identified. Before the international community can begin to minimize the negative consequences of those inevitable collisions, it needs to understand how and where cyberspace and international relations intersect and influence one another, and who controls those intersections.

An Alignment Strategy

The term "cyberspace" is not well defined, generally. We, the authors, take it to describe a new arena of human interaction—focused on the Internet and the hundreds of millions of computers the Internet connects, the institutions that enable it, and the experiences it provides—that has become a fundamental feature of society, creating a new reality for almost everyone in the developed world and a growing number in the developing world. For analysis purposes, the Internet can be thought of as having four layers: the physical foundations— the Internet's bricks and mortar, from fiber-optic cables to cell towers, personal computers, and servers; the logical layer, which includes the Internet protocols, the World Wide Web, browsers, the domain-naming system, websites, and software that make use of the physical foundations; the information layer of encoded text, photos, videos, and other material that is stored, transmitted, and transformed in cyberspace; and, of course, the users who shape the cyber experience and the nature of cyberspace itself by communicating, working with information, making decisions, and carrying out plans. Detailed study of these layers reveals that they have interesting and important substructures; for example, the logical layer includes the Internet itself (along with a sub-layer associated with Internet service providers, or ISPs), and the applications that run over the Internet, which are provided by a separate set of players.

In this model, the Internet's upper layers depend on the functions of the lower layers, but not the opposite. This view of the Internet is useful in locating cyber actors and activities, highlighting significant technological changes, and identifying the conditions under which actors operate across layers or, alternatively, choose to concentrate their activities within a layer. This way of looking at cyberspace can help track and represent patterns of dependencies and influence within the cyber domain.

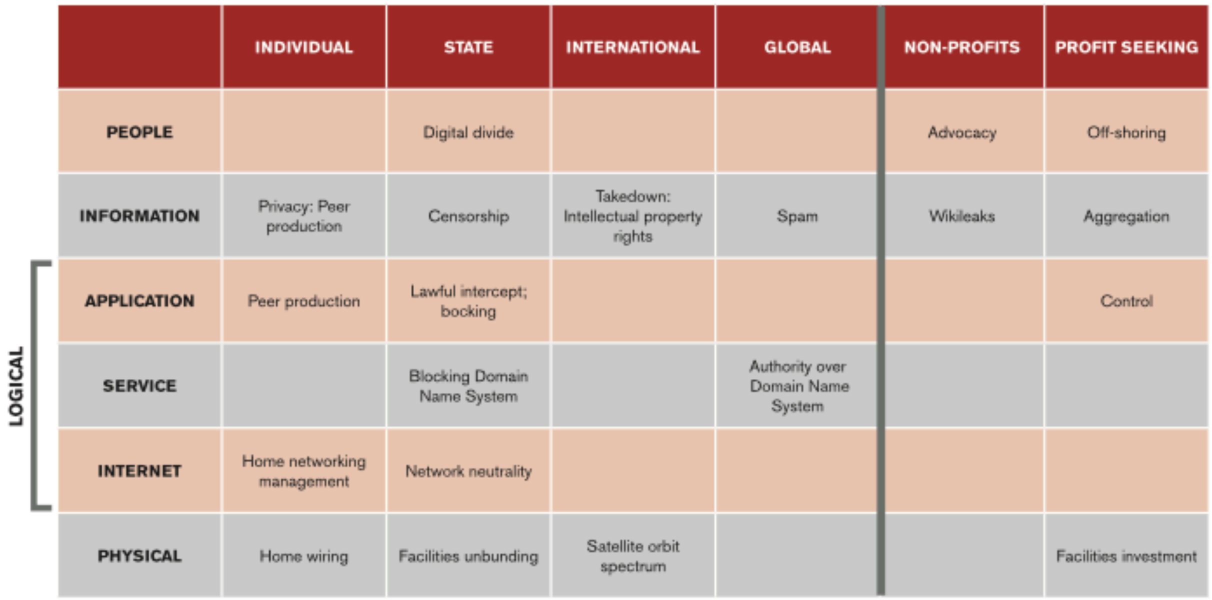
A common way of taking stock of structure and process in international relations, meanwhile, involves a focus on levels of analysis. Traditionally, political scientists have looked at levels consisting of the individual, the state (acknowledging the existence of nonstate actors), and the international system (Waltz, 1959). This view is anchored in the principle of sovereignty, which distinguishes between the state and other entities and provides the legal basis for the modern system of international relations. In recent years, a fourth level has been recognized, the overarching global system (North, 2000).

By using this model, we see some notable implications of cyberspace. Cyber access empowers the individual, providing new and powerful ways to articulate and aggregate individual interests and mobilize them for action. The individual, therefore, begins to matter in the state-based sovereign system of international relations. From a theoretical perspective, this means that the first level in international relations theory is as important as other levels of analysis, a change from traditional theory.

The construction of cyberspace also changes the traditional security calculus of the state, adding the notion of cyber security—that is, protection against threats to online information, espionage, sabotage, and fraud, among other things— to the internal, external, and environmental dangers that states have long faced (Choucri, 2012). Cyberspace has accelerated the formation of private interests, including transnational and multinational non-state actors, that become influential entities in their own right. It has empowered international institutions with new tools to support communication and performance. But it has also created a new arena of conflict and contention among member states, best exemplified by discussions at the World Conference on Information Technology aimed at renegotiating the 1988 International Telecommunication Regulations, a treaty created in a pre-Internet era when many telecommunications firms were state-owned (WATTC-88, 1988).

As a fourth level of analysis of international relations, the global system is a relatively new feature of world politics. Transcending and incorporating other levels, this level consists of the Earth's population and its global society, supported by all the life-supporting properties of nature. It now spans cyberspace, the most pervasive system of interaction ever constructed by human science and engineering. One addition is required to the levels of-analysis model to capture a central aspect of cyberspace. The traditional levels comprise a state-centered model; cyberspace is, to a large extent, a creation of the private sector. Private-sector actors do not fit neatly into the analysis levels—some may be domestic, some transnational; some are profit-making, others are not. But these actors must be included as a part of our model in order to offer a realistic framework for analysis.

Combining these analyses of Internet layers and international relations levels reveals a wealth of relationships (see Figure 1) that could be useful to policy makers who are managing the fractious co-evolution of both systems.



		INDIVIDUAL	STATE	INTERNATIONAL	GLOBAL	NON-PROFITS	PROFIT SEEKING
	PEOPLE		Digital divide			Advocacy	Off-shoring
	INFORMATION	Privacy: Peer production	Censorship	Takedown: Intellectual property rights	Spam	Wikileaks	Aggregation
LOGICAL	APPLICATION	Peer production	Lawful intercept; bocking				Control
	SERVICE		Blocking Domain Name System		Authority over Domain Name System		
	INTERNET	Home networking management	Network neutrality				
	PHYSICAL	Home wiring	Facilities unbunding	Satellite orbit spectrum			Facilities investment

Figure 1. The four-column matrix to the left of the gray vertical bar shows some of the relationships involved in the combined system of cyber international relations. The two columns to the right of the gray bar reflect the activities of private-sector entities, both for-profit and non-profit, within the layers of cyberspace.

The Combined Cyber International Relations System

At a minimum, a system that combines fundamental analyses of international relations and core features of cyberspace can help situate a wide range of issues and contentions spanning both domains. Several high-visibility cases illustrate how events in the cyber arena intersect with (or permeate) the traditional levels of international relations.

Wikileaks: Release and reaction

In 2010, Wikileaks, which styles itself as a nonprofit media organization, released hundreds of thousands of highly sensitive, classified US government documents. The release of the Iraq War logs and State Department diplomatic cables was an issue residing at the information layer of the Internet architecture. In terms of international relations analysis, it might initially be seen as a state issue, because the documents originally belonged to the US government. However, it was in fact an international issue; the Wikileaks founder and spokesman, Julian Assange, lived overseas. It has been speculated, but not confirmed, that the US government influenced the domestic provider of the Wikileaks domain name (wikileaks.com) to disable it. In response, Wikileaks registered a variant of the name in Switzerland. Wikileaks was also attacked at the physical level when the company hosting the Wikileaks website terminated its hosting agreement. In response, the dataset was moved overseas and various advocates hosted copies across the globe, more or less assuring that the information could never be suppressed.

Pakistan and the YouTube problem

In 2012, in response to the release of the anti-Islamic film trailer known as Innocence of Muslims on the Internet, the Pakistani government made an attempt to block domestic access to YouTube. The move was typical of various nation-specific attempts to block citizen access to content that is deemed offensive, disruptive, or illegal. In this case, however, there was a global twist to the story: Pakistan instructed its domestic Internet service provider (ISP) to take action against YouTube; but ISPs have no control over YouTube, which is owned by Google, and what it posts. So the Pakistan ISP took the approach of injecting a false routing assertion into the local region of the Internet, redirecting digital information packets being sent to the YouTube Internet protocol address to a local site, which would inform the viewer that YouTube access was blocked. Due to a technical error, this redirection command leaked out of Pakistan and disrupted access to YouTube in various parts of the globe. A worldwide effort by ISPs was required to "fence off" Pakistan's disruption. The response was not a traditional international action, then, but a large-scale, voluntary, global, non-state action.

Spam: Less is more

Spam—that is, unsolicited e-mail— arises at the application and information layers of cyberspace analysis. Many companies and research groups have helped combat spam, but a significant, effective response has arisen at an institutional, global, non-state level, via an organization called the Spamhaus Project, which collects lists of sites known to produce spammers and passes the lists on to e-mail operators, who then have the option of blocking e-mail from those sites. Spamhaus is lightweight (performing only this function, it has very few assets), and it can easily position itself in jurisdictions that are unsympathetic to lawsuits from enraged spammers.

Social media and the Arab Spring

The Arab Spring resistance movements began in Tunisia, and Egypt (and subsequently other Arab states) also had uprisings that changed the normal course of politics through the concentration and expansion of activities of humans (that is, at the people layer of Internet analysis). Users leveraged their Internet connection via Facebook and other online services to mobilize political protest and create a relatively nonviolent but dramatic and effective demand for internal political change. In Tunisia, secular politics prevailed initially; in Egypt, the popular vote yielded an Islamist president, but one year later, a massive mobilization demanded his resignation, and the Egyptian army removed him from office. In terms of international relations, these events and other attempts in other countries might, on first inspection, have remained at the individual level of analysis, but they had a powerful impact on the state level. These events also created spillover effects from one country to another, and to the international system. In terms of Internet analysis, Egypt tried briefly and ineffectively to quell the cyber-based aspect of the protest by turning off the Internet at the physical layer; at the information layer, halfway around the world, China blocked responses to politically sensitive search terms related to the uprising; and at the societal layer, the phenomenon is no longer just a cyber event, but a real-life event in the Egyptian streets and in the seats of that country's government.

Based on a combined assessment, a few preliminary conclusions about cyber international relations can be drawn:

- The lower layers of the Internet architecture are more amenable to state regulation, since they are more "physical." The activities that take place there also tend to be capital intensive and thus associated with large, established actors. The higher layers are often populated by smaller, private actors that can more easily escape governmental regulation and enforcement.
- An issue that naturally arises at one layer (e.g., the information layer) is, to date, most effectively dealt with at that layer. Attempts to deal with problems by imposing controls at another layer often fail. Efforts to control Wikileaks by disabling its name in the Domain Name System or turning off the entire Internet to block access to social networking sites such as Facebook and Twitter proved largely ineffective.
- Recent political events show how aggregated activities at the individual level and the user layer affect the state level, creating threats to stability that, in turn, lead the state to attempt to control cyber access.
- Non-state actors can be both global and small. Many of the important non-state global actors seem to be positioned at the higher layers of the Internet architecture—they are more

concerned with people and information than with fibers and packet transport. But this is not always the case: For example, some features of the physical layer, notably undersea cable, are managed in large part by multinational, non-state actors.

- Non-state international organizations, sometimes poorly institutionalized, have shown the nimble and flexible character necessary to deal effectively with cyber issues. These entities can position themselves as competitors to government-related international institutions as the proper venue for oversight and governance of cyberspace.

The system provides mainly a static model for thinking about how actors and actions can be positioned and evaluated in cyber international relations. In principle, all actors and all cyber functions can be positioned within this framework. But how do actors interact, with what means, and to what political or other effect?

Power and Influence: The Control Points

Control-point analysis complements and extends the levels-and-layers system explained above, exploring power and influence dynamics among the actors in the cyber and international relations realms. For example, the actors that actually manage and operate regions of the Internet are Internet service providers. Within their regions, they exercise ultimate control of the completion of connections: If they do not forward the digital information packets that make Internet transfers work, the operation fails. Other aspects of the Internet experience are controlled by other actors—those who develop operating systems, build browsers, make web content, and so on.

Governments can pass laws, and actors around the periphery of cyberspace can compete for power, but in the end, if these actions are to have any consequence, they must change the character of cyberspace itself in some way. Otherwise, they are not material, as is illustrated in a closer look, via control-point analysis, at Internet management in the United States and China.

Distributed control of the Internet: A US example

Surrounding those with direct control over the Internet is a larger set of actors that attempt to exercise control, usually indirectly. For the purposes of our analysis, we will look at four types of actors as they deal with the Internet in the United States: the ISPs themselves; the federal government; private-sector copyright holders, who are very concerned with control of infringing copies of content; and Google, a powerful actor with many dimensions of influence over cyberspace (see Figure 2).

In general, few governments exercise direct control over cyberspace. They can exert great influence by their ability to influence other actors, using regulation, legislation, investment, and standards. The actors representing the interests of copyright holders also cannot exercise direct control over cyberspace—they must work indirectly through other actors, in particular the ISPs.

They have lobbied the government to pass laws— in particular the Digital Millennium Copyright Act (DMCA) in the United States—to give them the authority to influence what ISPs and content hosting sites must do.

Google is a powerful, private-sector actor whose business is primarily centered on the Internet. Google has taken a wide range of actions, both direct and indirect, to use points of control to influence the character of the Internet. It has developed a new operating system for mobile devices, Android, has developed a browser called Chrome, and provides YouTube, one of the most popular sites on the Web. It has its own content delivery network with global reach and direct connection to many consumer facing ISPs.

One can see differences in intent and capabilities in these different actors. While content providers generally focus on regulating content, Google seeks to increase the diversity and choice in the ecosystem, to ensure that customers have many ways to reach its services— Google recently purchased Motorola Mobility in part to gain patents relevant to mobile communications, for example—and in the process to expand its business and increase profits.

Centralized control: The Chinese approach

In China, the state controls almost every decision point in the overall process of the Internet structure and its key institutional underpinnings, as well as any departures from sanctioned products or processes. China has constructed a complex socio-technical framework to detect unacceptable content and mandate its removal or modification. It requires that all ISPs, including mobile hotspots, obtain permits and register their users. China regularly blocks protocols such as virtual private networks (VPNs) and more sophisticated software such as The Onion Router (TOR) that seek to bypass government control of Internet access. China instructs its ISPs to control routes, especially at their borders, block access to certain applications (e.g., Facebook, Google, and Twitter), block access to specific websites, block circumvention protocols, and use deep packet inspection to look for specific keywords in digital information packets on the Internet; if disallowed keywords are found, Chinese ISPs are required to terminate the user’s Internet interaction (see Figure 3).

Combining control-point analysis with cyber international relations can help visualize how some attempts to influence cyberspace are or are not successful. For example, attempts to censor content on the Web are normally domestic in scope, because the laws that define the rules that govern content hosting sites and rights holders are usually specific to a country. That is to say, rights holders may have many points of control relating to the Internet in the United States, as indicated in Figure 2; however, in China, those same rights holders have little if any influence. Overall, rights holders have had to fight more or less a country-by-country campaign to protect their property from piracy, greatly reducing the effectiveness of their efforts.

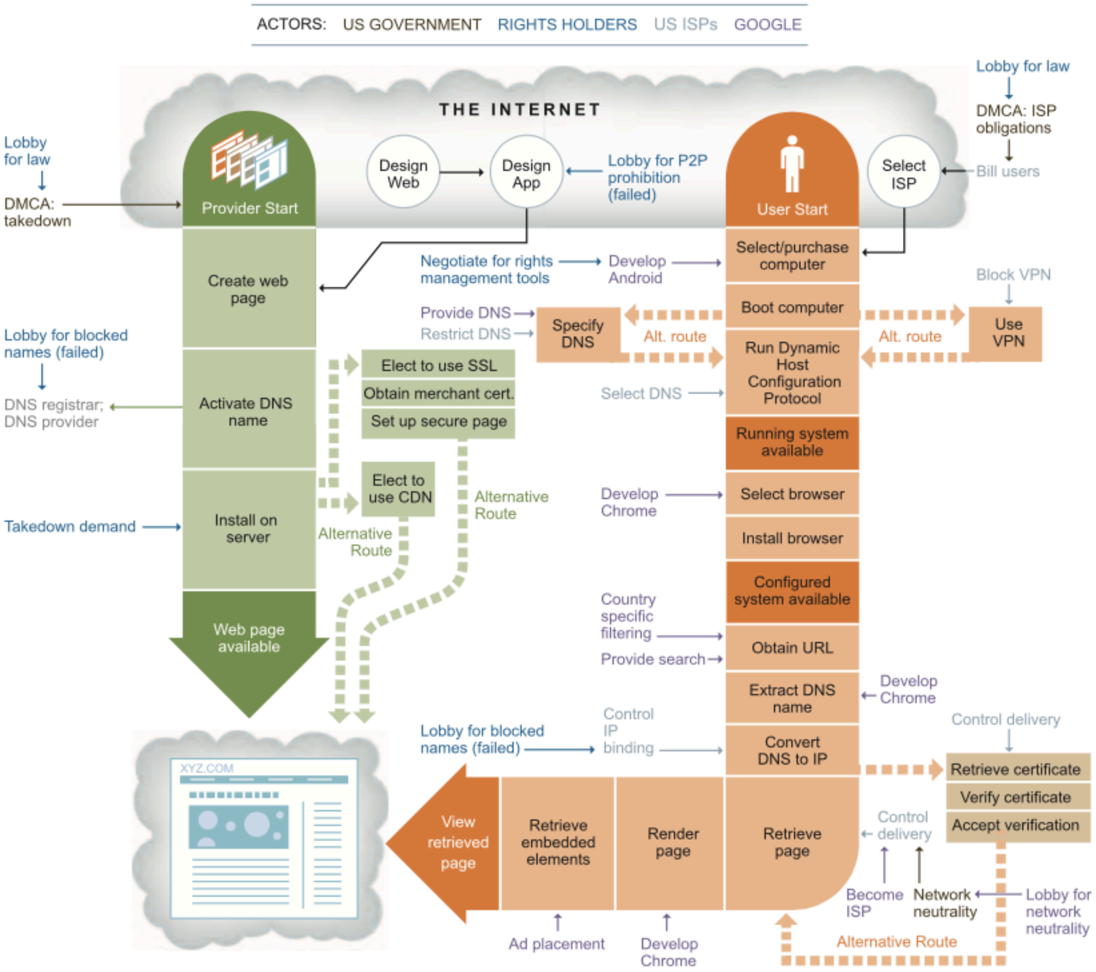


Figure 2. A control-point analysis shows how some US actors try to exercise control over the Internet for different reasons, and in different ways.

The Co-evolution of International and Cyber Relations

Returning to the dilemma introduced at the beginning of this piece: The increased interconnection of cyber and other aspects of international relations will continue to shape their co-evolution along a trajectory that tends toward even greater interconnectedness. Several defining features of world politics will affect this continued co-evolution.

The first such parameter relates to sovereignty and jurisdiction: Traditionally, jurisdiction is inherent in sovereignty and understood in physical and geographical terms (with the usual exceptions of diplomatic and extraterritorial arrangements). Jurisdictional disputes of a geographical nature can be addressed by the relevant states, or through some adjudication process. At the very least, there are some established processes.

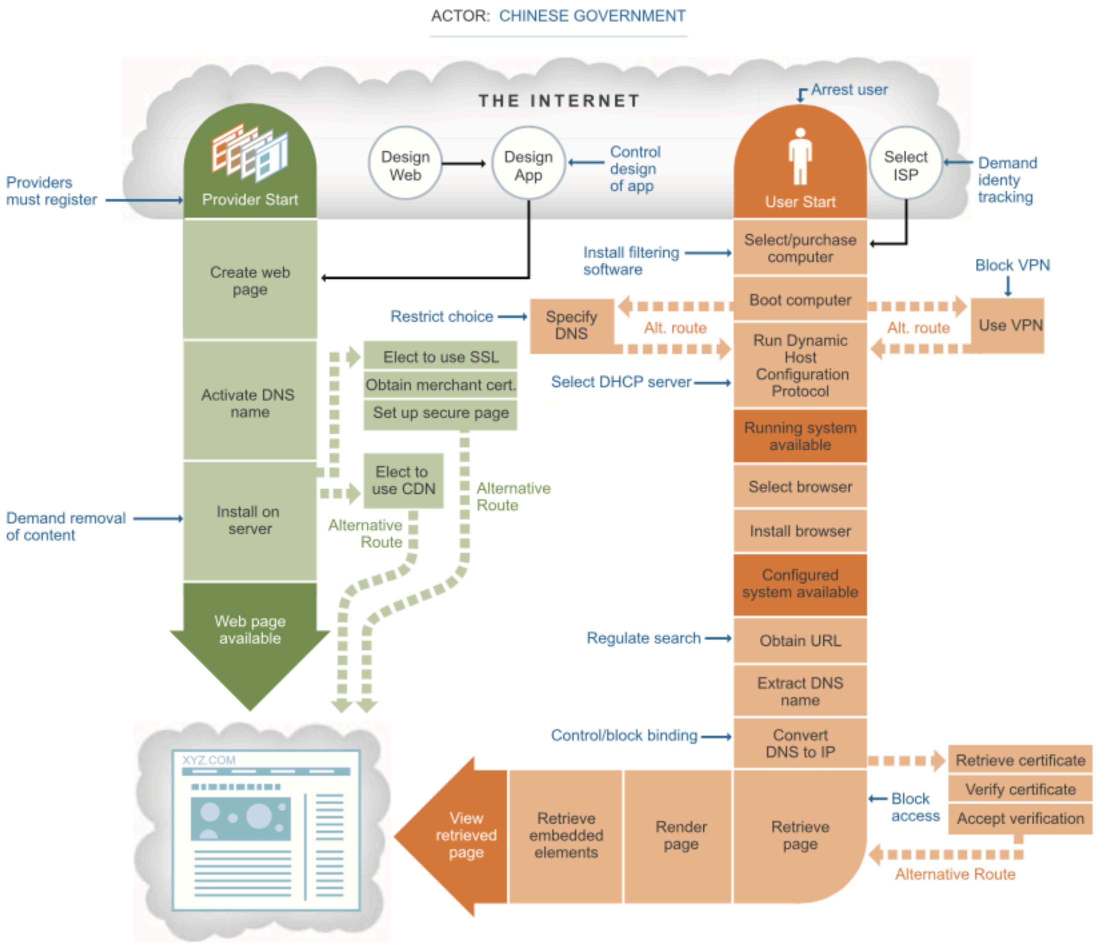


Figure 3. Control-point analysis illustrates how the Chinese government (shown in blue) attempts to control the Internet.

Jurisdictional boundaries are weak in cyberspace, yet many notable cyber situations—such as contention over regulation of the domain name system, spam, and various criminal activities—involve jurisdiction issues that have been addressed largely on an ad hoc basis. If there is international law for cyberspace, it is still in the making. One analyst argues that there is a “simple choice” between “[m]ore global law and a less global internet” (Khol, 2007: 253).

A second parameter relates to the autonomy and power of the private sector and non-state actors. While international relations theory and policy recognize the importance of non-state actors, in no arena are they as dominant as in the cyber domain. These non-state actors are the essential and fundamental system organizers and managers of cyberspace. Recall that it was the most powerful nation, the United States, that delegated to the private sector the operational management of the Internet. Early on, this sovereign decision set the rule of the playing field. None of this was the result of international deliberation or international decision.

This autonomy and power of the private sector all but assures that the state system anchored in sovereign authority will make every effort to redress or to "rectify" a seeming anomaly in international relations by reasserting the dominance of state sovereignty over cyber matters.

A third parameter of world cyberpolitics pertains to the norms and principles—the code of conduct—for an integrated international system. Already some interest is noticeable in various parts of the international system in developing shared norms for behavior in cyberspace. The formal deliberations at the World Conference on International Telecommunications in December 2012 reflected the dominant as well as the lesser contentions over norms and principles. Many conflicts between supporters of a distributed Internet control system and those who favor concentrated control arose and were debated; ultimately, there was no consensus, so the debates will continue in the coming years.

All of this bears on the future of cyberspace. We see today several examples in which the state system is trying to modify the Internet to better align it with traditional interests of the state, whether these are a more accountable network (to prevent and deter unacceptable behavior), a less accountable network (to empower activists and dissidents), a network with better tools to regulate access to select content (to remove destabilizing speech or material that infringes copyright), or a network that is universally available, easier to use, and an unfettered platform for innovation and commerce.

The alignment of layers of the Internet and levels of international relations helps reveal critical features of structure and process that relate to control of cyberspace and to anticipate potential changes in the structure of the Internet, and in the nature of the international system. Control-point analysis—a method for identifying who controls what, when, and how—is useful also for comparing different cyber-policy postures in international relations and their attendant instruments of influence and control. Only two cases are described in this article, which thus may underestimate the diversity of control possibilities.

Clearly, neither the Internet nor the structure of the international system will remain unchanged. The co-evolution dilemma forces us, the authors, to explore and anticipate potential futures—in conceptual, empirical, and perhaps even strategic terms, and frame policy and practice on viable principles.

The different actors that strive to influence the character of cyberspace have different tools at their disposal and different access to the various control points of the cyber arena. In this respect, what we see is "asymmetric contention" over the future. Actions at different levels and layers interact: Our framework is a way to map out these actions and better understand their interactions, and the different expectations for success for these various actors over time.

Funding

This work is funded by the Office of Naval Research under award number N000140910597. Any opinions, findings and conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

References

Choucri N (2012) Cyberpolitics in International Relations. Cambridge, MA: MIT Press.

Khol U (2007) Jurisdiction and the Internet: Regulatory Competence over Online Activity. Cambridge: Cambridge University Press.

North RC (2000) War, Peace, Survival: Global Politics and Conceptual Synthesis. Boulder, CO: Westview.

Waltz KN (1959) Man, the State and War. New York: Columbia University Press.

WATTC-88 (1988) Final acts of the World Administrative Telegraph and Telephone Conference, Melbourne, Australia. Available at: www.itu.int/ dms_pub/itu-s/oth/02/01/S02010000214002PDFE. pdf.

Author Biographies

Nazli Choucri is a professor of political science at MIT. Her research focuses on the sources and consequences of international conflict and violence. Her most recent book is Cyberpolitics in International Relations (MIT Press, 2012). She is the architect and director of the Global System for Sustainable Development, a multilingual knowledge system on the multidimensionality of sustainability.

David D. Clark is a senior research scientist at the MIT Computer Science and Artificial Intelligence Laboratory. Since the mid-1970s, he has been leading the development of the Internet, acting as its chief protocol architect from 1981 to 1989. His current research looks at redefinition of the architectural underpinnings of the Internet, and the relation of that architecture to economic, societal, and policy considerations.