Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Integrating Cyberspace and International Relations: The Co-Evolution Dilemma

Nazli Choucri

Political Science Department
Massachusetts Institute of Technology

David D. Clark

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

November 6, 2012

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.

Citation: Choucri, N., & Clark, D. D. (2012). *Integrating cyberspace and international relations: The co-evolution dilemma* (ECIR Working Paper No. 2012-3). MIT Political Science Department.

Unique Resource Identifier: ECIR Working Paper No. 2012-3.

Publisher/Copyright Owner: © 2012 Massachusetts Institute of Technology.

Version: Author's final manuscript.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

INTEGRATING CYBERSPACE and INTERNATIONAL RELATIONS:

The Co-Evolution Dilemma

Nazli Choucri

Department of Political Science
MIT

David D. Clark

Computer Science & Artificial Intelligence Laboratory, MIT

Abstract

As cyberspace and international politics now start to shape each other, we have few conceptual anchors to understand the mutual influences and dependencies. This paper proposes a way of integrating international relations and cyberspace: Specifically, we (1) develop an *alignment strategy* to connect the Internet, the core of cyberspace, and international relations (2) introduce the *control point analysis,* a method to explicate dynamics among cyber-actors, in terms of their relative power and influence, and (3) highlight *co- evolution parameters* shaping the joint future.

.

ECIR Workshop on
Who Controls Cyberspace?

November 6-7, 2012

Electronic copy available at: http://ssrn.com/abstract=2178586

Introduction

Cyberspace is a fact of daily life. Until recently cyberspace was considered largely a matter of *low politics* – the term used to denote background conditions and routine decisions and processes. By contrast *high politics* is about national security, core institutions, and decision systems that are critical to the state, its interests, and its underlying values. We now see cyberspace shaping the domain of high politics, and high politics shaping the future of cyberspace. The field of international relations, rooted in 20th century issues and theories, has not kept pace with the emerging significance of cyberspace.

This paper addresses what we call the *co-evolution dilemma:* as cyberspace and international politics now start to shape each other, we have few conceptual anchors to fully identify, let alone model, the potential collision of law, policy and practice in the cyber arena with shared norms, common practices, and modes of interactions in international relations that have evolved over time. At a minimum, we need to develop a map of the joint domain of cyberspace and international relations.

Our purpose here is to (1) develop an *alignment strategy* to connect the Internet, the core of cyberspace, and international relations (2) introduce the *control point analysis,* a method we have developed to explicate dynamics among cyber-actors, in terms of their relative power and influence, and (3) highlight critical *co-evolution parameters* embedded in the fabric of world politics.

Foundations: Alignment Strategy

Our foundational alignment strategy is built on the intersection of the *layers of the Internet* architecture and the *levels of analysis* in international relations.

The Layers Architecture

We begin with a model that gives more structure and form to the Internet, which we take as the core of cyberspace. While use of a layered model to describe the Internet is well understood there is no common consensus, so we use a four-layer model that captures the features of interest for alignment purposes.

- The *physical foundations* – the Internet's bricks-and-mortar, from fiber-optic cables to cell towers, personal computers and servers.
- *The logical layer* –the Internet protocols, World Wide Web, browsers, domain-naming system, websites and software that make use of the physical foundations.

Electronic copy available at: http://ssrn.com/abstract=2178586

- *The information layer* –the encoded text, photos, videos, and other material that is stored, transmitted, and transformed in cyberspace.
- *The users* – the people and constituencies who shape the cyber-experience and the nature of cyberspace itself, by communicating, working with information, making decisions and carrying out plans.

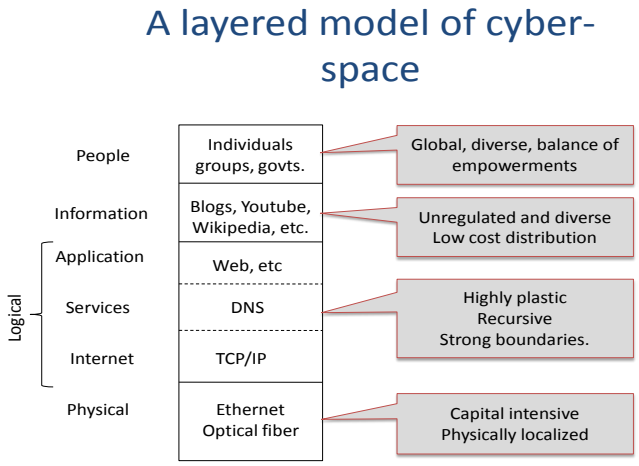

Figure 1. Defining the Layers of Cyberspace

In the *layered* model the upper layers depend on the functions of the lower layers, but not the opposite. This model is a useful device to (a) locate cyber actors and activities, (b) highlight significant technological changes, (c) identify the conditions under which actors operate across layers or, alternatively, chose to concentrate their activities within a layer, and (d) thus help track and represent patterns of dependencies and influence within the cyber domain.

The Levels of Analysis

A common way of taking stock of structure and process in international relations is to focus on *levels of analysis*. Traditionally, the levels consisted of the individual, the state (acknowledging the salience of non-state actors), and the international system. This hierarchical view is anchored in the principle of sovereignty that 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 was recognized, namely the overarching global system.

By using this model, we see some notable implications of cyberspace. Cyber access empowers the *individual*. It provides new and powerful ways to articulate and aggregate their interests and mobilize for action. The individual 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 privileged as other levels of analysis, a change from traditional theory.

Electronic copy available at: https://ssrn.com/abstract=2178586

The construction of cyberspace creates new imperatives for the traditional security calculus of the state, the second image. It complicates an already complex security calculus which is anchored in *external* security (defense against military threats), and generally includes *internal* security (stability and legitimacy of governance) and *environmental* security (the resilience of the life supporting properties of nature). At this point, we are faced with growing threats to *cyber* security (security of online information and knowledge, and protection against cyber threats, espionage, sabotage, crime and fraud). Indeed, cyber security has become an increasingly salient issue in national and international contexts.

At the third level of analysis, the international system consists of sovereign states also includes non-state actors enfranchised by the state, and non-state actors those commonly thought of as transnational (operating across boundaries) or multinational (rooted in different states). Cyberspace has accelerated the formation of private interests that become influential entities in their own right, with goals and objectives, priorities and problems. It has empowered international institutions with new tools to support communication and performance. It is also creating a new arena of conflict and contention among member states, best exemplified by the upcoming World Conference on Information Technology (WCIT-2012) to renegotiate the 1988 International Telecommunication Regulations.[1]

As the fourth level, the global system is a relatively newly appreciated feature of world politics. Transcending and incorporating other levels, the fourth 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 – and challenging social, regulatory and policy practices.

The limits of the level of analysis in international relations are well recognized, but the relationships to cyberspace remain obscure. It is useful to signal (1) the permeability of influences across levels of analysis; (2) the extent to which conditions and behaviors at one level influences structure and process across others vary considerably; and (3) despite evidence of increasing cyber access world-wide, the operational norms and practices also vary within levels and across jurisdictions.

The Combined Cyber-IR System

The alignment strategy yields an integrated system—a cyber-IR frame in Figure 2. At a minimum, this system can be used to represent and situate a wide range of issues and contentions spanning both domains. The extent to which these issues are not well understood illustrates some of the power and nuances of the alignment framework.

Electronic copy available at: https://ssrn.com/abstract=2178586

		Individual	State	International	Global	Non-profits	Profit-seeking
Logical	People		Digital divide			Advocacy	Off-shoring
	Information	Privacy; Peer production	Censorship	Takedown; IPR,	Spam	Wikileaks	Aggregation
	Applications	Peer production	Lawful intercept; blocking				Control
	Services		Blocking DNS		Authority over DNS		
	Internet	Home network mgt.	Network neutrality				
	Physical	Home wiring	Facilities unbundling	Satellite orbit spectrum			Facilities investment

Figure 2. Integrated Cyber-IR System: Situating issues or concerns

Several high visibility cases illustrate how events in the cyber arena intersect with (or permeate) the traditional levels of international relations and ways in which activity at various the layers of the Internet shape issues and contentions in international relations

High Visibility Cases

Here we highlight four different types of cases to reflect the diversity and complexity.

A: Wikileaks: Information Release and Reaction

The Wikileaks releases of highly sensitive classified information, such as the Iraq war logs and diplomatic cables, were an issue at the *information* layer of the internet architecture. It might initially be seen as a domestic (state) issue with respect to levels of analysis. However, it was in fact an international issue, since the Wikileaks operator was overseas. It has been speculated, but not confirmed, that the U.S. government influenced the domestic provider of the Wikileaks DNS name (wikileaks.com) to disable it. In response, Wikileaks registered a variant of their name in Switzerland. Wikileaks was also attacked at the *physical* level when the company hosting the web site terminated its hosting agreement. In response, the data was moved overseas, and various advocates hosted copies of the information across the globe, more or less assuring that the information could never be suppressed.

Electronic copy available at: https://ssrn.com/abstract=2178586

B: Pakistan's YouTube Fight

The second case, Pakistan and YouTube, is typical of various *nation-specific* attempts to block access by their citizens to content that they deem offensive, disruptive, or illegal. However, there was a global twist to this story. Pakistan, offended by a video degrading to Islam, decided to block access to YouTube internally, and instructed their domestic ISP to take this action. However, ISPs have no control over YouTube (Google) and what it posts. So the Pakistan ISP took the approach of injecting a false routing assertion into the local region, which would redirect packets being sent to the address of YouTube to a local site that would inform the viewer that YouTube was blocked. Due to a technical error, this move leaked out of Pakistan and disrupted access to YouTube in various parts of the globe. A global effort was required to "fence off" Pakistan's disruption. This effort was carried out by the collective and cooperative action of ISPs across the globe. The response was not an *international* (multi-state) action, but a large-scale voluntary *global, non-state* action carried out by a loose, non-hierarchical organization of ISPs.

C: The Global Battle Against Spam

Spam is a problem that arises at the *application/information* layer. While many companies and research groups have helped combat spam, a significant and effective response has arisen at an institutional *global, non-state* scope: an organization called Spamhaus, which collects lists of sites known to be spammers, and passes this list on to email operators who then have the option of blocking email from those sites. Spamhaus is lightweight (performing only this function, it has essentially no assets) and it can easily position itself in jurisdictions that are unsympathetic to lawsuits from enraged spammers.

D: Social Media and the Arab Spring

The "Arab Spring" of 2011 refers to the resistance movements in Tunisia and Egypt (and then in other Arab states) that changed the normal course of politics in these countries and the region as a whole. This is a case of mobilization of *individuals*, the concentration and expansion of activities in the people layer. *Users* leveraged their Internet connection via various applications and online services, such as Facebook, to mobilize political protest and create a relatively non-violent but dramatic and effective demand for internal political change. In Tunisia secular politics prevailed; in Egypt the popular vote yielded an Islamist President.

These events, and other attempts in other countries, fit into the layer model at the "*people"* layer, and might (on first inspection) have remained at the *individual* level of analysis, but they had a powerful impact on the *state* level of analysis. These events also created spillover effects from one country to another, and to the *international* system. Interestingly, China is now blocking such search terms as "Egypt" and "Arab Spring". These events involved many layers. At the *physical* layer, Egypt tried (briefly and ineffectively) to quell the cyber-based aspect of the protest by turning off the Internet; at the *information* layer, China blocks responses to politically sensitive search terms; and at the *people* layer, the phenomenon is no longer a cyber-event but a physical event in the streets and the seats of government.

Electronic copy available at: https://ssrn.com/abstract=2178586

Gains from Alignment

Based on the forgoing, we put forth initial propositions about the combined cyber-IR system and its value:

- The lower layers of the Internet architecture are more amenable to state regulation, since they are more "physical." The activities are also capital intensive, and thus associated with large, established actors. The higher layers are often populated by private actors that are smaller and which can more easily escape from 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 DNS, 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 (aggregated protest) impact upon the state level (threats to stability), which in turn, lead the state to control cyber access through denial of service or other policies.
- 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 cyberspace architecture—they are more concerned with people and information than with fibers and simple 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 multi-national non-state actors.
- The non-state international organizations, sometimes poorly institutionalized, have shown the nimble and flexible character necessary to deal effectively with salient issues. These entities can position themselves as competitors to international institutions as the proper venue for oversight and governance of cyberspace.

The foundational alignment strategy gives us a static model within which actors and actions can be positioned and evaluated. In principle all actors and all cyber-functions can be positioned within this framework. How do actors interact? To what ends, with what means? With what political or other effects?

Power and Influence: Control Point Analysis

To answer these questions we developed a method of analysis that is complementary to, and extends, the levels and layers system, a method we call *control points analysis* that explicates the dynamics among the actors – in terms of relative power and influence. This method identifies

Electronic copy available at: https://ssrn.com/abstract=2178586

critical features of technology (structure and process) and actors (roles and function) inherent in the pursuit of a particular task or objective.

Reference Case

To illustrate control point analysis we use a simple user task as a reference case: the steps taken to first create and then retrieve a selected webpage. Figure 3 shows the "normal" sequence of steps. Each step is a potential point of control, and the figure also shows which actors have immediate authority, access, or technological responsibility for each control point.

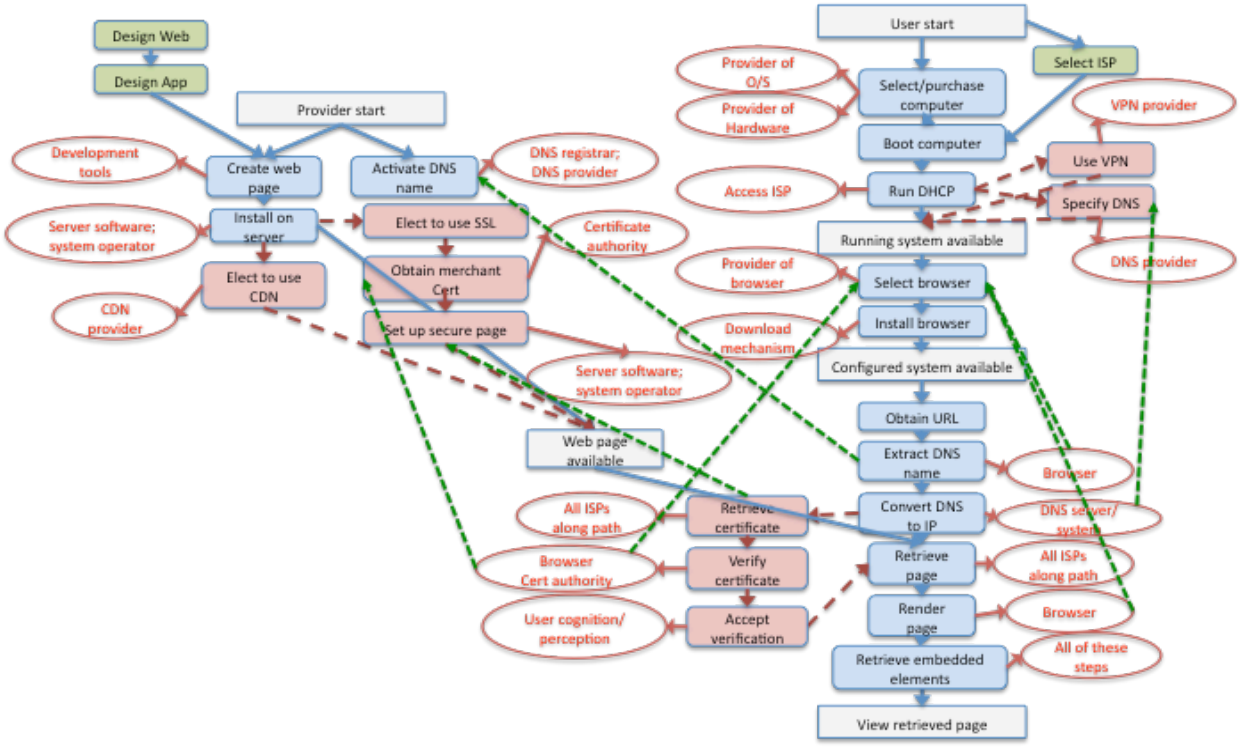

Figure 3: Steps in the retrieval and viewing of a web page.

Blue arrows indicate the normal sequence of steps. Green arrows capture dependencies on prior steps. Red ovals catalog the actor(s) that have immediate control of the outcome of each step. Green boxes are parts of the overall logic method and of the diagram that are not elaborated in this paper for reasons of space.

Figure 3 focuses only on the actors that have immediate, most proximate, influence over the actual character and features of the Internet. For example, the actors that actually construct, build and operate regions of the Internet are Internet Service Providers, or ISPs. Within their regions, they control topology and completion of connections (e.g., who talks to whom under what circumstances). ISPs exercise ultimate operational control: if they do not forward packets, 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—they must change the experience of using the Internet or they are not material.

Electronic copy available at: https://ssrn.com/abstract=2178586

We can now show how different actors use the various control points in the structure and process to shape or influence the user experience in cyberspace. For illustrative purposes we compare two different cases: broad distributed control (the United States) and centralized concentrated control (China).

Distributed control—a U.S. example

Surrounding the actors with direct control over the Internet are a larger set of actors that attempt to exercise control, usually *indirectly* by influence over one or another of the actors shown in Figure 3. We illustrate some examples of the U.S. case, looking at four types of actors: the ISPs themselves, the federal government, the private sector holders of copyright (who are very concerned with control of infringing copies of content) and a powerful actor with many dimensions of influence over cyberspace: Google. These are shown in Figure 4.

In general, few governments exercise direct control over cyberspace. They can exert great influence by their ability to influence other actor using regulation, legislation, investment (procurement and research) and standards. In the United States, the government and the ISPs are separate entities in law and in practice. 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) 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 exercise control of the Internet. It has developed a new operating system for mobile devices, Android, developed a browser called Chrome, and is a provider of 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 the content providers generally focus on regulating content on the net, Google seeks to increase the diversity and choice in the ecosystem, to ensure that customers have many ways to reach their services—Google recently purchased Motorola Mobility in part to gain patents relevant to mobile communications, for example—and in the process expand their business and increase their profits.

Electronic copy available at: https://ssrn.com/abstract=2178586

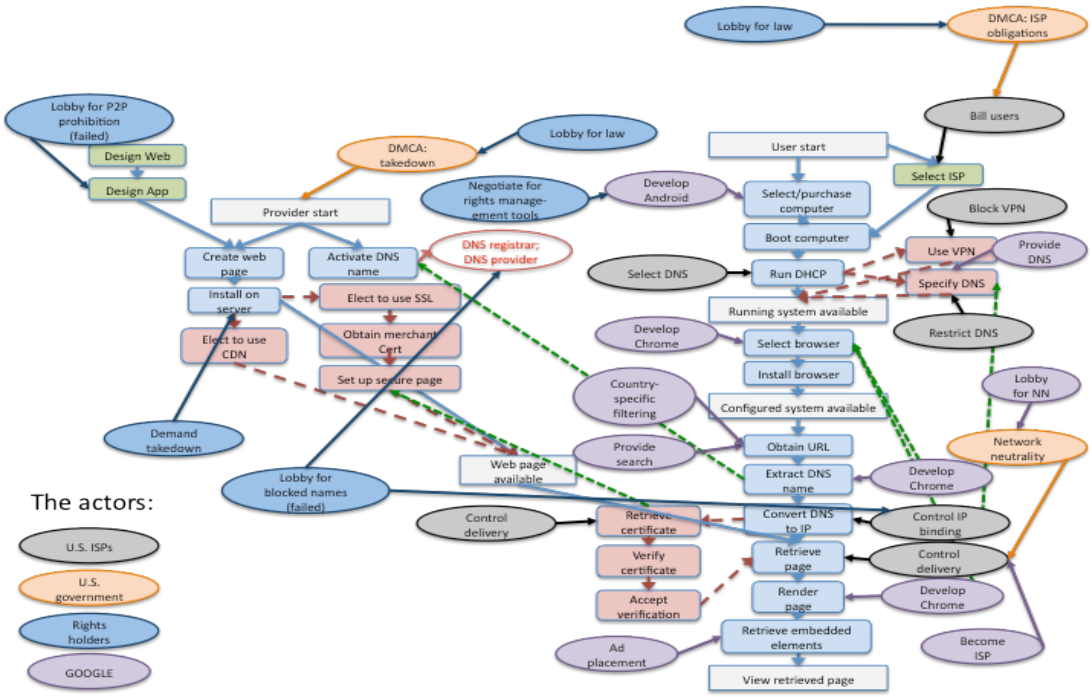

Figure 4. The U.S. Case: Examples of actors that exercise control, direct or indirect, over the Internet

Centralized Control— a China Example

The control points for the government of China are shown in Figure 5. The state controls 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 hot-spots, obtain permits. China regularly blocks protocols such as virtual private networks (VPNs) and more sophisticated bypass software such as The Onion Router (TOR), either by blocking the protocol or the destination port number. China instructs its ISPs to control routes, especially at their borders, block access to certain applications (e.g., Facebook, Google, Twitter, and so on), block access to specific websites, block circumvention protocols, and use deep packet inspection (DPI) to look for specific keywords in the packets and terminate the connection.

Electronic copy available at: https://ssrn.com/abstract=2178586

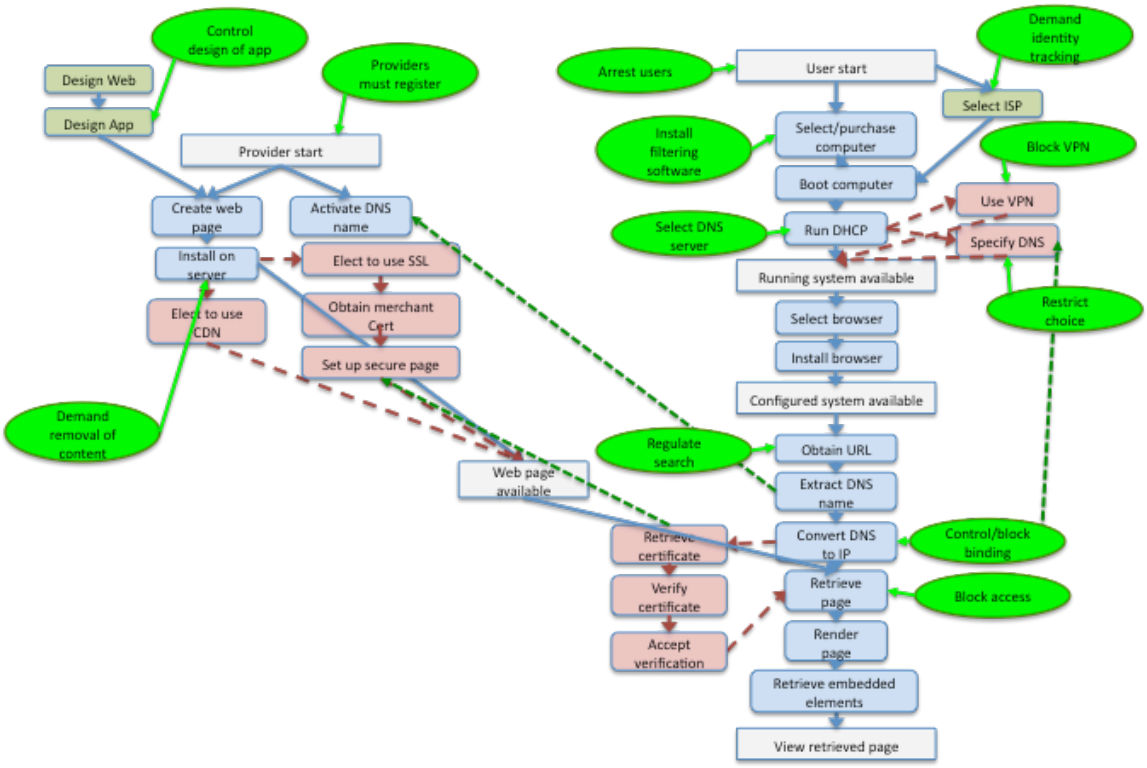

Figure 5. The China Case: Points of control exercised by the Chinese government and their related actors (e.g., ISPs) over the Chinese Internet.

Relating control point analysis to alignment strategy

Each point of control, and the options for control, can be located in the cyber-IR system, the alignment of levels and layers in Figure 2 above. For example, inspecting and blocking packets occurs at the logical IP layer, but demanding takedown of content occurs at the information layer. As well, actions can be positioned within levels of analysis: takedown of content is normally at the domestic scope, because the laws that define the rules that govern content hosting sites and rights holders are usually specific to a country. Rights holders have had to fight more or less a country-by-country campaign to protect their property from piracy.

Earlier, we observed that taking an action at one layer with the goal of influencing another layer is often ineffective, because it can be circumvented and because it produces a "blunt instrument" effect with consequences much more broad than the intention. For example, we see that the rights-holders in the United States were effective at getting a law passed, the Digital Millennium Copyright Act (DMCA), that gave them take-down rights at the information layer, but were not able to get a bill passed, the Stop Online Piracy Act (SOPA), that would have tried to control access to infringing content by means of manipulation of the DNS.

Electronic copy available at: https://ssrn.com/abstract=2178586

The Co-Evolution Parameters

Returning to the dilemma introduced at the onset: invariably, the increased interconnections of cyber and other aspects of international relations will continue to shape their co-evolution along a trajectory of greater and greater interconnection. At this time, we can see several defining features of world politics that will shape the continued co-evolution of cyberspace and international relations.

The first parameter relates to *sovereignty and jurisdiction:* Traditionally jurisdiction, inherent in sovereignty, is understood in physical and geographical terms (with the usual exceptions of diplomatic and extra territorial arrangements). Jurisdiction disputes of a geographical nature can be addressed by the relevant states, or through some adjudication process if they are to be resolved. But at the very least there is some established process

Jurisdictional boundaries are weak in cyberspace, yet many notable cyber situations – such as contention over regulation of the DNS, spam and other criminal activities, or regulating the dissemination of various sorts of content – highlight 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", that is between "[m]ore global law and a less global internet."[2]

The second parameter is the *autonomy and power of the private sector and non-state actors.* While international relations theory and policy recognize the salience 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. Recall that it was the most powerful state, the United States that delegated to the private sector the operational management of the Internet. This sovereign decision set the rule of the playing field early on. 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 – that is by reasserting the dominance of state sovereignty over cyber matters.

More fundamentally, this represents a struggle between *contending principles of order.* Most, if not all of the fundamental features (or core functions) for seamless cyber interactions will continue to be controlled and managed by non-state entities.

All of this bears on the future of cyberspace. We see today several examples where 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, or an unfettered platform for innovation and commerce.

Electronic copy available at: https://ssrn.com/abstract=2178586

The third parameter pertains to the *norms and principles* – the code of conduct – for an integrated international system. Already we see some interest in various parts of the international system to develop shared norms for behavior in cyberspace. The formal deliberations at the WCIT-12 in December 2012 will invariably reflect the dominant as well as the lesser contentions over norms and principles. Many of the cleavages and contentions can be anticipated between supporters of a distributed control system versus those buttressing concentrated control. But the full outcome is difficult to predict.

End-Note

The alignment of layers and levels helps us to explore critical features of structure and process, notably to track changes in actors, functions, situations, standards and other critical factors; locate current conflicts and signal emergent interest or intersections in spheres of influence; and anticipate potential, changes in the structure of the Internet and its layers, and in the nature of the international system and its levels.

The 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. We have shown only two cases here, and thus may underestimate the diversity of control-possibilities.

Clearly, neither the Internet we have today nor the structure of the international system will remain unchanged. The co-evolution dilemma forces us to explore and anticipate the potential futures – in conceptual, empirical, and perhaps even strategic terms, and frame policy and practice on viable normative and empirical principles. It also forces us to address and resolve the difficulties created when decisions and policies pertaining to one level, global level for example, are made at the other levels of analysis – if and when the various constituencies recognize the need for decision.

References and Notes:

1. See L.B. Solum & M. Chung and K. D. Werbach.
2. Kenneth N. Waltz, *Man, the State and War* (1959); Robert C. North, *War, Peace, and Survival* (2000).
3. "Final Acts of the World Administrative Telegraph & Telephone Conference, Melbourne 1988 (WATTC-88).
4. U. Kohl, *Jurisdiction and the Internet,* (Cambridge University Press, Cambridge, England, 2007, reprinted 2010).
5. L. B. Solum & M. Chung, The layers principle: Internet architecture and the law. *U San Diego Public Law Research Paper No. 55*. (2003).
6. K. D. Werbach, A layered model for Internet policy. *J. on Telecommunications and High-Tech Law*. 1, 37-67 (2002).

Acknowledgements: 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.

Electronic copy available at: https://ssrn.com/abstract=2178586