Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Cyber International Relations as an Integrated System

Chintan Vaishnav

Engineering Systems Division
Massachusetts Institute of Technology

Nazli Choucri

Political Science Department
Massachusetts Institute of Technology

David D. Clark

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of

November 17, 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.

Citation: Vaishnav, C., Choucri, N., & Clark, D. D. (2013). Cyber international relations as an integrated system. *Environment Systems & Decisions, 33*(4), 561–576.

Unique Resource Identifier: http://dx.doi.org/10.1007/s10669-013-9480-3

Version: Final published version.

Environ Syst Decis (2013) 33:561–576
DOI 10.1007/s10669-013-9480-3

Cyber international relations as an integrated system

Chintan Vaishnav · Nazli Choucri · David Clark

Published online: 17 November 2013

Abstract The purpose of this paper is to conceptualize the hitherto separate domains of Cyberspace and International Relations into an integrated socio-technical system that we jointly call the cyber International Relations (Cyber-IR) system and to identify and analyze its emergent properties utilizing the methods common to science and engineering systems adapted here for the social sciences. Our work is an exploration in both theory and methodology. This paper (a) identifies the actors and functions in the core systems, Cyberspace, and IR, (b) disambiguates system boundary, (c) creates a design structure matrix (DSM), a matrix of the interdependencies among functions of actors, (d) analyzes DSM qualitatively to show multiple interdependent and heterogeneous Cyber-IR properties, and (e) analyzes quantitatively the differential importance of core functions as well as the impact of actor attributes on influence in Cyber-IR. This work forms a baseline for further understanding of the nature of the heterogeneous influences of the various actors and the various outcomes that could result from it.

Keywords Internet · Cyberspace · International Relations · Design structure matrix · DSM

C. Vaishnav · N. Choucri (✉) · D. Clark
Massachusetts Institute of Technology, Cambridge, MA, USA
e-mail: nchoucri@mit.edu

C. Vaishnav
e-mail: chintanv@mit.edu

D. Clark
e-mail: ddc@csail.mit.edu

1 Introduction: challenges of complex systems

Almost everyone recognizes that Cyberspace is a fact of daily life. Given its ubiquity, scale, and scope, Cyberspace—including the Internet, the hundreds of millions of computers it connects, its management, and the experiences it enables—has become a fundamental feature of the world we live in and has created a new reality for almost everyone in the developed world and rapidly growing numbers of people in the developing world.

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. Cyberspace is now a matter of high politics. The new practice of turning off the Internet during times of unrest in various countries, the effective leakage of confidential government documents on Wikileaks, the cyber-attacks that accompanied recent events in Georgia and Estonia, and the use of cyber-based attacks to degrade Iran's nuclear capabilities all illustrate new challenges for the State system and the complexities created by the increasing salience of Cyberspace and its enabling capabilities.

In short, all aspects of International Relations today may well intersect with or rely upon one form of cyber venue or another. Cyberspace evolves rapidly, and these changes have occurred faster than our ability to fully appreciate their significance. The result is a powerful disconnect between twentieth century International Relations and the realities of the twenty-first century. An entirely new vocabulary has emerged surrounding the cyber features of national security, International Relations, world politics, or the global system more broadly defined.

This vocabulary operates in something of a vacuum—at least with some distance from the literatures in the field of International Relations. A critical review of the literature published in the *International Political Science Review* concludes theoretical contentions in the field such that they are "implying great difficulties for theoretical adaptation and application in analyses of the complexities of the emerging new digital world" (Eriksson and Giacomello 2006: 236). The authors reference here the contributions of the *Millennium* special issue on International Relations and the digital age (2002). A recently completed working paper for the joint MIT-Harvard University collaboration on explorations in cyber International Relations (Cyber-IR) reviewed 18 major journals in the field of International Relations over a 10-year period 2000–2012 (Reardon and Choucri 2012). It found the prevalence of pockets of discrete research activities segmented according to a specific theoretical focus in International Relations (*realism, institutionalism, and constructivism*) at distinctive specific levels of analysis (*the individual, the State, the international system, and the global system*) with few discernible, generalizable findings or propositions (Reardon and Choucri 2012).

All things considered, the fact is that the scientific community has not yet developed a "map" of cyber features in International Relations or even the basic coordinates required for such a map. While both systems are constructed by humans, they differ significantly in their characteristic features.

In this paper, we address the challenge of identifying, characterizing, and representing interdependencies within and across these two domains, as *foundational to understanding how any two domains as important and pervasive as Cyberspace and International Relations influence each other, on the one hand, and shape a joint domain on the other*.

For systems defined by both technological and human complexities, design structure matrix (DSM) has emerged as a useful technique for jointly analyzing fundamentally different domains (Steward 1981). The DSM is a simple tool to perform both the analysis and the management of complex systems. It enables the user to model, visualize, and analyze the dependencies among the entities of any system and derive suggestions for the improvement or synthesis of a system.

Minimally, creating a DSM involves (1) identifying boundaries of a system (or systems) to be analyzed, (2) identifying the elements of the system(s), (3) identifying interactions/interdependencies/inferences among the elements and representing them as a matrix, and (4) analyzing the matrix. The final step of analysis may draw from techniques of matrix algebra or other disciplines such as graph theory, engineering systems, or network and complexity science. Overall, DSM provides a compact and clear representation of a complex system and captures interactions between the elements of a single system or multiple disparate systems.

Such a system has been used in the past to analyze more deterministic environments such as product architecture or an engineering design process (Ulrich and Eppinger 2012; Eppinger and Browning 2012). By contrast, in this paper, we create a DSM to explore a relatively non-deterministic environment, formed due to interconnections and interdependencies of Cyberspace with its rapidly evolving technology, and International Relations with its complex decision-making.

Our purpose here is to utilize the DSM method for tracking and analyzing the interdependencies anchored within the Internet, which forms the core of Cyberspace, with some extensions beyond this core; within the domain of International Relations (i.e., interactions among sovereign states and other entities in world politics); and between these two domains. Thus, an important methodological contribution of this work has to do with abstracting the common elements shared by both systems, namely the actors, their attributes, functions, and connections. On this basis, a related contribution is to identify potential disconnects between the two systems.

The remainder of the paper proceeds as follows: Sect. 2 presents a brief review of International Relations, old and new, in order to provide a situational context for our investigations. Then, in Sect. 3, we define the research questions that arise when considering Cyberspace and International Relations as an interdependent and integrated system, we can call cyber International Relations. By definition, the joint system is characterized by the fundamentally different features of Cyberspace and of International Relations. However, they are connected by an important common element—*decision actors* affecting the structure and function of the separate and the joint entities. Section 4 develops a method for representing the joint domain. In Sect. 5, we analyze the matrix to answer questions raised in this paper. The conclusion in Sect. 6 synthesizes the lessons learned and discusses future research required to address the limitations of this paper.

2 International Relations: the "Old" and the "New"

A brief sketch of the traditional international system—the world of the twentieth century—helps us highlight the new features created by the construction of Cyberspace. Here we introduce briefly the traditional International Relations and then turn to the "new" changes in the international system created almost entirely by the salience of

Cyberspace and its growth and expansion since the end of the twentieth century.

2.1 Changes in traditional International Relations

By definition, the traditional international system consists of interactions among sovereign states. The organizing principle, sovereignty, is the anchor upon which the entire system rests. Also by definition, all other actors and entities are derivative, legitimized at their origin by the State. At the end of World War II, there were 55 sovereign states. Today, there is more than three times that number. The State remains the dominant actor but it is increasingly subject to pressures from various types of non-state actors. Below is a brief, illustrative review of recent changes in International Relations to provide a context for the investigations that follow.

Among the important legacies of the twentieth century are the end of the Cold War, the consolidation of the United States as the only "hegemony" and the growth in the number of sovereign states (due to the decolonization process, the breakup of the Soviet Union, and common consensus), all with new claims on the international community. There are new regional centers of power with new political aspirations and new competitions on a global scale. In addition, the evolution of new norms and the proliferation of international organizations—with diverse functions and responsibilities to facilitate development and sustainability—provide a legitimate basis for intrusion and influence deep into the structure of the State system.

The traditional systems of twentieth century International Relations—such as those with bi-polar, multipolar, or unipolar structures, and generally characterized by hierarchical power relations—have gradually given way to new structural configurations characterized by different types of asymmetries and relatively weak hierarchies, if any, thus replacing the well-known "vertically organized" structures of power and influence.

We have seen the expansion of private and public interests coupled with the creation of new markets and innovative practices that create overlapping spheres of influences and ever-fluid "playing fields"—each governed by distinctive rules and regulations—making it ever more difficult to understand and track the various systems of interaction. In some cases, we observe something akin to different entities behaving as if they were competing "sovereignties" seeking to expand their control and establish their legitimacy within and across the same territorial domains.

Various types of non-state actors—such as those focusing on development assistance and humanitarian needs, religious groups, those with various ideological or political agendas—seem to be growing faster than our ability to track and assess their roles and responsibilities, constraints and contributions, as well as threats and vulnerabilities.

We have also witnessed changes in the nature of conflict and war in all parts of the world. Large-scale war among major powers no longer seems likely, but we have seen the State seeking to retain control in its efforts to contain or prevent the evolution of new types of conflict and violence with varying degrees of formal organization. For example, wars for national liberation from colonial rule have gradually been superseded by conflicts waged by non-state actors, expansion of civil conflicts, and a wide range of terrorist initiatives. Conflicts between major powers over spheres of influence are replaced by contentions over control of these spheres by various local entities. (Afghanistan is a good case in point.)

Toward the end of the twentieth century, we saw a gradual appreciation of the unintended consequences of economic growth as the prime target for all future developments and a shift toward a quest for "sustainable development"—an improvement in the human condition devoid of the most damaging by-products of growth. The potential for sustainability is now a central feature of the international agenda.

In sum, each one of these changes in traditional International Relations is embedded in its own situational context and is important in its own right. Jointly they are fundamental features of our world today. The important point is this: *none of these powerful shifts are due to the construction of Cyberspace nor are they contingent on the expansion of cyber venues or the increase in cyber access*. But together they constitute the context within which the construction of Cyberspace has already contributed to new and unprecedented shifts in power and influence and forged new types of threat and new forms of vulnerability.

2.2 Cyberspace and "New" International Relations

Many of these features are already influencing, if not challenging, traditional theory, policy, and practice of International Relations. We also point to notable shifts and political realignments to date. Of the many changes triggered by the expansion of cyber venues, the following are ranked among the most important implications of Cyberspace as a new domain of interaction.

One Technological innovations aside, the single most distinctive feature of this new reality is the *dominance of the private sector* in an international system defined by the principle of sovereignty and shaped by the demands and capabilities of sovereign states. In many if not most countries, Cyberspace is organized, managed, and maintained entirely by private sector entities. Specifically, the Internet is constructed and operated by private sector actors

(Internet service providers) located in various legal jurisdictions and minimally regulated in many contexts. The standardization and governance of the Internet is carried out by organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF), which are, to some extent, private actors. At this point, the entire cyber system rests on the integrity and effectiveness of their performance—and increasing their legitimacy as well.

Two The major actor that constitutes and defines International Relations—the *State*—is unable to control the cyber domain to any meaningful extent or to insulate itself from the implications of the new cyber realities. There are unmistakable new challenges to national security, with new sources of vulnerability (cyber threats), new dimensions of national security (cybersecurity), and new sources of fear and uncertainty. Concurrently, we see the growing use of cyber venues by non-state groups whose objectives are to undermine the security of the State or to alter its foundations. The recent Wikileaks episodes showed, with no uncertainty, the politicization and disruptiveness of Cyberspace.

Three The increasing evidence of *cyber threats* to security reinforces the politicization of Cyberspace and its salience in emergent policy discourses. Among the problems with security today is that we do not yet have a full understanding of the sources of threats, the venues, or the targets. Moreover, we do not have a common agreement on the concept of cyber "security" itself. As a result, the tendency is to draw upon known measures and recombine them in arguably more effective ways. In the United States, for example, the Patriot Act adopted by Congress in response to the tragic events of September 11, 2001, included provisions enabling the government to monitor Internet communications without obtaining prior permission from the Justice Department. President Obama's *Sixty Day Review* of the cyber situation in early 2009 also recognized vulnerabilities and was designed to bring Cyberspace into the policy domain.

Four New types of *asymmetries*—notably the extent to which weaker actors can influence or even threaten stronger actors (such as press reports of anonymous penetration incidences of the US government computer systems)—have little precedence in world politics. At the same time, however, such asymmetries may actually point to the emergence of new symmetries (such as the ability of a weaker actor to penetrate the computers of stronger actors).

Five The creation of *new actors*—some with formal identities and others without—and their cyber empowerment is altering the traditional international decision landscape in potentially significant ways. More specifically, growth in the number of actors increases the density of decision-entities—each with new interests and new capabilities to pursue their interests—and thus increases potential for intersections in spheres of influence, with possibilities for new and different types of contention and possible conflict. Among the new non-state entities are commercial entities, creators of new markets, proxies for State actors, cyber-criminals (generally too varied to list and too anonymous to identify), and not-for-profit actors (faith groups, international interest groups, agenda setters, etc.), and the anonymous actors—"good" and "bad" as the case may be—whose anonymity itself conflicts with traditional principles of international interactions.

Six The growing *contestation of influence and control* over cyber venues between the new institutions established to manage Cyberspace (ICANN, IETF and others) and the traditional international institutions [such as the International Telecommunications Union (ITU) or other United Nations organizations] creates new tensions of legitimacy and responsibility, which further complicates the already thorny issue of international accountability. International organizations are drawing on their established legitimacy—based on their traditional mandate and legal status buttressed by sovereign support—to influence the private sector. Often, such contestations are reinforced by ambient stress as some (developed) states object to what they regard as excessive American control over cyber management, and other (developing) states seek influence in the international management structures already in place, traditional as well as new.

Seven Various types of *cyber conflicts* (between and within states, of known and unknown identity and provenance) are becoming apparent with the potentials for new modes and manifestations thereof. Many contaminate the traditional calculus of conflict and cooperation and the assumptions that are anchored in the physical domain, largely derived from the historical experience of major powers, and based on the assumptions that the military instruments of power dominate. The identity of the contenders is known and that, in the last analysis, "might" be relied upon to make "right," and so forth.

Eight Concurrently, we are also observing different modes of *cyber collaboration* in the effort to reduce uncertainty and introduce some measure of order in an "environment" that is increasingly perceived as "anarchic." Among the most notable initiatives is the development of Computer Emergency Response Teams (CERTs), a loose network of organizations around the world seeking to take stock of and reduce breaches of cyber security. Another important development is the Cyber Crime Convention, but there are, as yet, no initiatives that span the entire domain of Cyberspace.

Nine There is a new cyber-based mobilization of *civil society* (the aggregations of individuals in their private capacity as well as organized elements of the private

sector) and its potential empowerment across jurisdictions and in all parts of the world.

Ten The *intersection in spheres of influence*—with the private sector managing order in Cyberspace and sovereign authority managing order in the traditional domain worldwide—provided much of the rationale for organization of the first World Summit on the Information Society (WSIS). In part to avoid contentions over power and legitimacy, WSIS was conceived as a high-level, inclusive, and overarching meeting of all relevant entities and interests—organized under the auspices of the State system in International Relations.

These are some of the more notable influences of Cyberspace in International Relations. While the proverbial skeptic will argue that "plus ça change, plus c'est la même chose," it is difficult to envisage a world in which we can effectively "roll back" any one of these factors to their pre-2000 status.

3 Research questions: in search of an integrated system

We argue that the interwoven nature of Cyberspace and International Relations require the properties of information goods such as information security, control or freedom, or those of international activities such as trade or diplomacy to be framed in the context of emergent behaviors of a system where Cyberspace interacts with traditional IR.

As yet, very little literature directly has taken on the problem of framing and examining Cyberspace and International Relations jointly. *Cyberpolitics in International Relations* (Choucri 2012) provides a detailed analysis of the impacts of Cyberspace on International Relations, and to some extent, ways in which the cyber domain has begun to influence world politics. Drawing on a traditional framework in the analysis of world politics, first introduced by Waltz (1959) and developed further by North (1990). Choucri (2012) also addressed propensities for cyber conflict and cooperation, as well as contending models for the future of cyber politics. This provided the basis for exploring the interconnections between these two domains.

A joint paper entitled, "Cyberspace and International Relations: Toward an Integrated System" (Choucri and Clark 2011) addressed this issue from theoretical perspectives in computer science, engineering and political science. The Choucri–Clark paper develops a candidate framework—combining *layered* models of the Cyberspace familiar to engineers, and *levels* of analysis familiar to political scientists—to position actors, functions, and current issues and concerns in the integrated cyber International Relations system. The present research takes its inspiration from these earlier works and develops a theoretically driven and empirically based framework of the joint domain of Cyberspace and International Relations.

Of the many complexities of Cyber-IR, we focus on two fundamental features of the *multiple actors* who perform in the joint domain: (1) *role heterogeneity*, in that the multiple actors operating in both Cyber and IR domains perform a variety of functions, and (2) *attribute heterogeneity*, because these actors are heterogeneous in their attributes.

3.1 Role heterogeneity

The modular architecture of the Internet enables multiple actor types, as defined by the different roles they play in the design, provisioning, management, and usage of Cyberspace. For example, equipment providers design network equipment, Internet service providers (ISPs) build networks and provide Internet service, applications providers create Internet applications, standards organizations develop and coordinate Internet standards, and so on. Each actor type performs a unique set of core functions (discussed further in the next section).

3.2 Attribute heterogeneity

Cyber-IR actors can be heterogeneous in their attributes. One dimension of attribute heterogeneity is the geographical location of the actor. For example, ISPs are local actors, but information platforms such as Facebook are international actors from the perspective of many states. Another dimension of attribute heterogeneity is the economic status of the actors. For example, ISPs are for-profit, private entities in some nations, but are not-for-profit, public entities in others. Finally, attribute heterogeneity could arise due to the State versus non-state nature of actors. For example, International Telecommunications Union (ITU) as a standards body is a State actor that represents interests of the various nation states, but Internet Engineering Task Force (IETF) as a standards body is a private, non-state actor.

The above factors motivate the overarching query driving our research. It is this: *Does heterogeneity of the actors (their attributes and the functions they perform) create opportunities to gain advantage in the joint domain of Cyberspace and International Relations?* In this paper, we will focus on three specific questions related to this overarching query:

1. Are some actors/functions more important for the structure and performance of the Cyber-IR system than others? This question is important because many other functions in the Cyber-IR system depend on such functions. Therefore, muting of such a function

hampers many dependent functions, and enabling it accentuates them, and thereby, the whole system.
2. What dependencies are critical for functioning of Cyberspace, IR, and the relationship between the two? Given that Cyberspace is rapidly changing, highly fluid, and increasingly subject to technological innovations in some cases, and to State policies and interventions in others, the purpose of identifying such critical areas of dependencies is so that they can be tracked over time and studied in more detail in future work.
3. How do actor attributes such as location (local vs. non-local) or status (State vs. non-state) inform (support, reject or qualify) findings of questions 1 and 2? This question is especially relevant as it provides insights into the relative importance of select attributes for the relevance and performance of an actor at any point in time.

4 Method and application

Our purpose in using design structure matrix (DSM) method is to construct the Cyber-IR interdependency matrix. However, to appropriately frame the scope of the matrix and make its structure and interpretation more relevant and meaningful to the overall investigation, we must create several additional constructs, meanings, rules, and assumptions.

4.1 Overview of methodology

The "raw" application of DSM generates a critical anchor for the remainder of the investigation. This anchor provides internal consistency in the logic of interconnections between the cyber domain and International Relations. However, it is only an entry point for our investigation. More must be done. In Table 1, we provide an overview of the overall methodology and its application. Each step in Table 1 can be viewed as "belonging" to one of two distinct phases of inquiry: (a) creation of the interdependency matrix (steps 1–3), and (b) analysis of the interdependencies (step 4). Please note that the somewhat abstract description of rules in Table 1 is discussed with concrete examples of their application in Sect. 4.2 to follow.

Table 1 Overview of methodology

Step 1: Identify important actors in Cyberspace and International Relations
Rule 1: Differentiate actors based on a set of functions they perform with respect to the Internet, not the bases of functions they could potentially own
Step 2: Identify core functions performed by the actors
To enlist core functions of an actor ask the following question: can the actor be that actor without performing a given function?
Rule 2: When attribute heterogeneity does *not* determine core functions performed: take core functions that the actor type performs
Rule 3: When attribute heterogeneity does determine core functions performed: take the union of all core functions that the actor type could perform
Step 3: Identify interdependencies among core functions
To identify interdependency between any two core functions ask the following question: Is "Function B" necessary to fully or partially perform "Function A"? If yes, then A depends on B
Rule 4: Capture only the direct dependencies of core functions. Indirect dependencies of core functions are derived from the direct ones, as mediated by other core functions
Rule 5: Disaggregate an actor type to avoid loss of interdependency information
Step 4: Code and analyze the structure of interdependencies
Code and analyze two types of matrices
Qualitative Matrix
Binary Matrix

4.2 Operational details: application of the "Rules"

We now turn to a brief discussion of each step:

Step 1: Identifying important actors in Cyberspace and International Relations

To begin, we must identify the functional categories of Cyberspace and International Relations-related actors. For Cyberspace, the first set of actors are those who provision the various functions of the Internet, namely equipment providers (e.g., Cisco, Ericsson), Internet service providers or ISPs (e.g., Comcast and Verizon in the United States), information communications and applications platforms (e.g., Google, Facebook), device makers (e.g., Apple, Nokia), application providers (e.g., Skype), and individuals (e.g., individual users or businesses). The first set of actors (functional categories) is well accepted when discussing Internet architecture, supply chains, or policy (Vaishnav 2010).

The second set of Internet actors are those who create and manage standards or other operational issues, namely the Institute for Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), World Wide Web Consortium (W3C), and the North American Network Operators' Group (NANOG).[1] They are critical to the overall configuration of Cyberspace. Some were established long before the construction of the

[1] As a representation of other similar groups such as SANOG.

Internet and are thus cyber-centered rather than Internet-focused. We are beginning to identify and examine the importance of the second set of actors in the context of Cyber-IR.[2]

For International Relations, we focus on established actors who perform Internet-related functions with direct international implications, namely the sovereign State, International Telecommunications Union (ITU), and World Trade Organization (WTO; Choucri 2012).[3] There are other actors, to be sure, but for the sake of parsimony, we highlight the most relevant.

Step 2: Identifying core functions performed by the actors

The second step is to identify the core functions of an actor. These are a set of functions it must perform to be that actor type. For example, providing connectivity and Internet service are core functions of an ISP, without which it would cease to be an ISP. Table 2 shows actors to date and their core functions. The core functions listed here are derived based upon the following process. A rather exhaustive list of functions performed by the Internet actors like equipment makers, ISPs, devise makers, and application providers is available in Vaishnav (2010), chapter 2. A similar list for the role of individual, standards organizations, and the State that allows us to derive the core functions of these actors is available in Choucri and Clark (2011). Finally, the role of organizations such as IEEE, IETF, W3C, ICANN, NANOG, ITU, and WTO is further crystalized by their mission statements. Such an exhaustive list of core functions is then further pruned to list just the essential functions of each actor by asking the following question: Can the actor be defined as that actor without performing a given function?

Several aspects of the core functions listed in Table 2 are especially relevant to this inquiry. First, all actors perform both technical and economic core functions. For example, for ISPs, developing capacity to meet demand and generating funds to survive are primarily economic functions, even though capacity expansion could sometimes depend upon technological advance. By contrast, the rest of the functions performed by an ISP are primarily technical functions, even though they have economic implications.

Second, the final core function—generate funds to survive—is relevant for all actors, except possibly the State. We interpret this function broadly. While financial viability is important for all, mechanisms for survival could be different for different actors. For example, with the exception of individual users, for all Internet-related actors "to survive" means remaining profitable by managing revenues and costs (when the actor is private) or being supported by the State (when State-owned). By contrast, for a State, the notion of fund generation in this matrix is limited to funds necessary to support viable cyber access where such funds may be generated through a combination of taxation of individuals and businesses, import, and export, etc. The survival of a State is a concept that has implications far beyond this inquiry, so it is not addressed here.

Third, for many actors, the attribute heterogeneity does not change the core functions they must perform. For example, equipment providers, device makers, and application providers must perform the same core functions whether they are small, medium, or large, for profit or not-for-profit, local or international. In this case, we simply use Rule 2 described in Table 2. By contrast, for some actors, attribute heterogeneity does determine the core functions they perform. For example, small ISPs may not directly connect to the Internet backbone, not all individuals develop Internet applications, or all states do not own ISPs, and so on. In this case, we apply Rule 3 described in Table 2 to take a union of core functions an actor type performs to arrive at the complete list.

Finally, two methodological issues must be noted. First, as stated in Rule 1 of Table 2, the Internet actors and their functions were identified according to the functions they *do* perform, and not functions they *could* potentially own. For example, an ISP could also decide to become an information platform, but the majority does not.

The second methodological issue is whether the functional classification is identified at the appropriate level of aggregation. For example, is it better to aggregate equipment providers, device makers, and application providers into a single actor called hardware/software providers? Conversely, could we not disaggregate platform providers into information platforms, communications platforms, and applications? We argue that the disaggregation of actor type produced here is appropriate, as any further aggregation would result in loss of information (Rule 5, Table 2). For example, if we were to combine equipment providers and device makers into an aggregated actor, ISP's unique dependencies on equipment providers and individual's unique dependencies on the device makers will not have to be attributed to this new aggregated actor, thereby inflicting some loss of information. Such choices related to the levels of aggregation raise important qualitative issues that must be kept in mind when interpreting the results.

[2] Choucri–Clark Paper discussed in the Introduction section of this paper.

[3] We base our selection of IR actors on the Choucri–Clark Paper. Here we have eliminated a few new actors, namely IGF and WSIS, as it is unclear what operations of the Internet would cease to exist in the absence of these organizations as yet.

Table 2 Actors and core functions

Internet actors and core functions	IR actors and Internet-related core functions
Equipment providers	*State*
Design and develop network equipment	Grant private equipment providers[a]
Generate funds to survive	Grant private ISPs
ISPs	Grant information/communications/applications platform
Connect with individuals and businesses	Grant private device makers
Connect with domestic ISPs	Grant private application providers
Connect with international backbone ISPs	Own and operate network equipment manufacturing
Provide Internet service	Own and operate ISP functions
Secure links and servers	Own and operate Information/communications/applications platforms
Develop capacity to meet demand	Own and operate device manufacturing and maintenance
Generate funds to survive	Own and operate application development
Information/communications/applications platform	Import hardware/software products
Generate content[b]	Export hardware/software products
Store content	Censor content
Provide access to content	Filter content
Provide communications platform[c]	Physically secure Internet access, services, and information flows
Distribute applications[d]	Generate funds
Secure content	
Develop capacity to meet demand	
Generate funds to survive	
Device makers	*ITU*
Design and develop end devices for communications	Produce Internet and Telecom Standards
Generate funds to survive	Coordinate Internet and Telecom Standards
Application providers	Coordinate Radio Communications Services
Design and develop Internet applications	International management of radio spectrum and satellite orbits
Generate funds to survive	Facilitate initiatives in emerging market
Individuals	Publish ICT Statistics
Access content	Generate funds to survive
Generate content	
Share content[e]	
Develop Internet applications	
Secure links/content	
Invest in Internet technologies	

Table 2 continued

Internet actors and core functions	IR actors and Internet-related core functions
IEEE	*WTO*
Develop hardware standards	Produce trade agreements for goods, services, and intellectual property
Coordinate hardware standards[f]	Implement and monitor trade agreements
Generate funds to survive	Dispute settlement
IETF	
Produce Internet standards	
Generate funds to survive	
ICANN	
Coordinate Internet addresses[g]	
Coordinate the DNS[h]	
Generate funds to survive	
W3C	
Develop Web standards[i]	
Generate funds to survive	
NANOG	
Identify and solve problems of Internet operations and growth[j]	
Generate funds to survive	

[a] "Granting" private provisioning of any actor type is construed broadly to include situations where no formal permission is necessary to perform as that actor. For example, it is not necessary to obtain a license to become an ISP in the United States, whereas a license is necessary to do so in most other nations

[b] Content is construed broadly here to include that generated by humans and machine, pure content and content about content, and content in text, voice, and video formats

[c] Examples of a communications platform are the likes of email platform (e.g., Hotmail), or social networking platforms (e.g., Facebook)

[d] A platform may distribute applications generated by it or someone else (e.g., Apple's iTunes Store)

[e] Generation and sharing of content is construed broadly here to include content generated and shared between users, or between a user and a machine

[f] Coordination of hardware standards is to ensure interoperability among hardware devices

[g] An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication

[h] The design name system (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide

[i] "Web standards" is a general term for the formal standards and other technical specifications that define and describe aspects of the World Wide Web

[j] Concerns interconnection and peering in the Internet backbone

Step 3: Identify dependencies among core functions

Having identified and listed the core functions of actors, we now seek to identify the interdependencies among the core functions they perform. To identify interdependency between any two core functions, we ask the following question: Is "Function B" necessary to fully or partially perform "Function A"? If yes, then A depends on B. This inquiry generates a dependency matrix of all functions performed in the Cyber-IR system.

Figure 1 shows the components of the Cyber-IR dependency matrix: two types of actors (Cyber and IR), core functions they perform, and the resulting four types of dependencies (within Internet (Cyberspace), Internet on IR, IR on Internet, and within IR). The "Appendix" at the end shows a populated version of the Cyber-IR dependency matrix produced from this step.[4]

Step 4: Code and analyze the structure of interdependencies

The next step is to code the data and then analyze the matrix. This is done in two ways. The first is to construct a heavily annotated version of the dependency matrix and footnote, in detail, each individual dependency. From this matrix, we produce a descriptive document on the nature of dependencies faced by each core function. Such a bottom-up process allows us to identify equivalence classes of dependencies (discussed later). It allows us to analyze the question we raised earlier about the nature of dependencies within the Internet, within IR, and between the two domains.

The second way we analyze the matrix is by converting the qualitative matrix to a binary matrix, where a populated cell is marked as "1" and empty cells as "0." From the binary matrix, we can begin to study the nature of interdependencies algebraically. Doing so allows us to analyze the question we raised earlier about the relative importance of actors and functions in the Cyber-IR system.

5 Analysis, results, and "Lessons"

We now turn to analysis of the dependency matrix to answer the research questions we raised in Sect. 3. Procedurally, we focus on Question 1 and 2 and in discussing them interweave the implications of Question 3.

Question 1 Are some actors/functions more important in Cyber-IR than others?

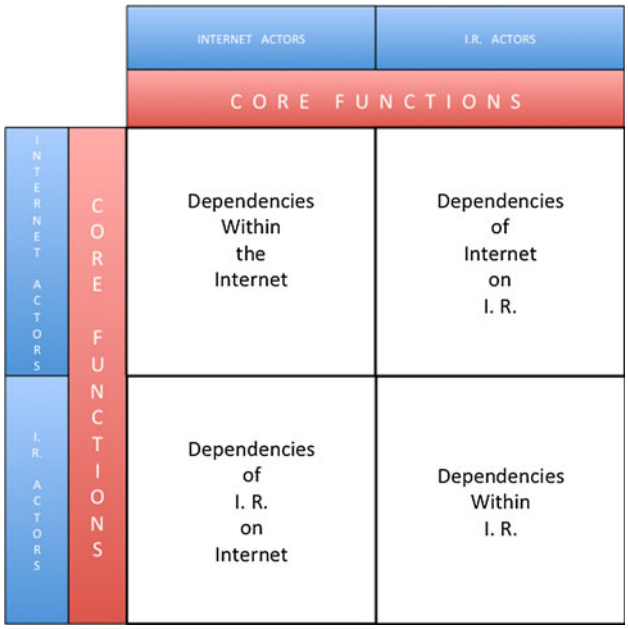


Fig. 1 The components of cyber-IR dependency matrix

To answer this question, let us look at two different views of the dependencies: functions most depended upon (Fig. 2) and most dependent functions.

Figure 2 should be considered important because many other functions in the Cyber-IR system depend on them. So, muting of such highly depended upon functions hampers many dependent functions, and enabling it accentuates them, and thereby, the whole system.

Figure 2 can be interpreted as follows: (1) for those States that neither own the manufacturing of devices, network equipment, application providers, nor host information and communications platforms in its jurisdiction, import of such hardware and software is critical for a stable Internet experience; (2) ISP's ability to provide connectivity and survive economically is critical for all states; and (3) because it engages in standards creation and coordination that caters to a variety of interests at the State level; put together, ITU activities have more varied dependencies across all layers of the Internet than any other standards organization such as IEEE, IETF, or W3C.

Figure 3 shows functions that are most dependent on other functions. These functions are important because they are the most complex to produce or perform. In some cases, it is easier to grasp why their production may be more difficult than others. For example, the State's decision to import hardware and software, the individual's decision to invest in Internet technologies, and ITU's ability to facilitate initiatives in emerging markets necessarily depend upon many other activities. Similarly, core functions such as survival of ISPs and equipment makers are complex

[4] As discussed in the next section, we produce qualitative and binary versions of the dependency matrix. The matrix shown in the "Appendix" is the binary matrix with all the cells with 0's turned into empty cells, to enhance readability.

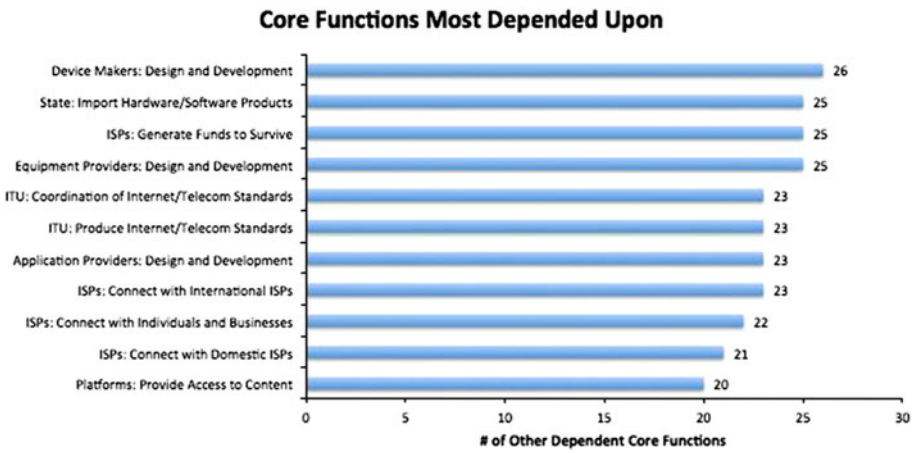


Fig. 2 Core functions most depended upon

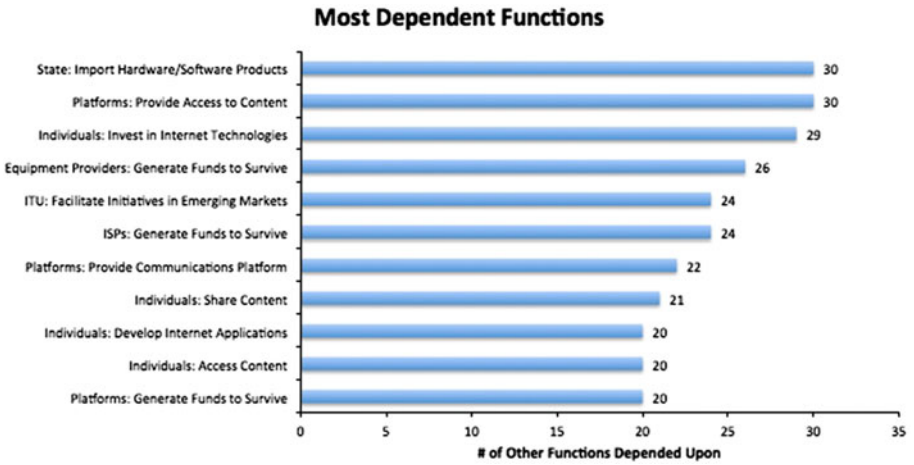


Fig. 3 Most dependent core functions

because these actors are deep into the communications supply chain.

In other cases, our findings may appear surprising at first. For example, platforms such as Google depend upon many functions to provide access to content. As an individual user, it might appear that much of what one could do depends upon platforms such as Google or Facebook. But, from the perspective of the Cyber-IR system, these platforms depend too heavily on the individual user's ability to generate and share content and the availability of Internet connectivity and service. While we have come to a point where individuals easily share and access content and develop applications, arriving to this point has taken time, as all of these functions depend upon many others. For this reason, individual-level activity is marginal in states where Internet architecture is weak.

Question 2 What dependencies are critical for (a) the Internet and Cyberspace and (b) International Relations, and (c) the relationship of the two?

We address this question by noting results and drawing lessons about the nature of dependencies in four domains: Within Cyberspace, within IR, and those at the seams (of Cyberspace on IR, and of IR on Cyberspace). Below, we highlight these findings sequentially as classified in these four domains.[5] As noted earlier, the purpose of identifying such critical areas of dependencies is so that they can be examined in greater detail when needed.

(a) Results on dependencies within Cyberspace

First Technological dependencies run from upper (e.g., applications) onto the lower Internet layers (e.g., service), which is a fact that engineers have known for long since each layer of the Internet is relatively autonomous. However, this is not always true. For properties such as security, the dependencies are at all layers of the Internet. Further, *economic dependencies* such as survival of actors who provide technology for the Internet run in the opposite

[5] The lessons discussed in this section are deduced from the analysis of the qualitative matrix in the "Appendix". The footnotes to follow detail the analysis behind each of the ten lessons in this section. *Please read these methodological notes in conjunction with matrix in the "Appendix".*

direction, that is, from lower onto the upper Internet layers.[6]

Second While much of the literature on *standards* focuses on how the various technology providers depend upon standards organizations, the converse is also true—standards organizations also depend upon technology providers for standard creation and the economic viability of the standards body altogether. This point is not merely an artifact of how the dependency matrix is coded; rather it highlights the importance of leverages in standards creation and coordination. For example, if a monopolistic power emerges on any layer of the Internet, it is bound to bias the nature of standards because of the standards organization's dependency on the monopolist not just for the adoption of technology but also for its own economic survival.[7]

(b) Results on dependencies within IR

Third Public *provisioning of Internet* functions occurs in most cases when depending upon the provider of communications infrastructure, public provision remains the only viable option of Internet provisioning in large parts. Such states are in turn likely to be heavily dependent upon their ability to import necessary technology. Special cases are states like China where public provisioning is done with the added objective of controlling information content and flow.[8]

Fourth While there is currently little evidence of whether ITU depends upon the activities of WTO, the matrix suggests that managing international communications over the Internet and international trade will likely become increasingly common. For example, as Cyberspace becomes further woven into the fabric of international trade, ITU functions such as coordinating radio communications services, international management of radio spectrum and satellite services, or coordinating emerging markets must normatively have involvement of WTO through their functions such as implementing and monitoring trade agreements, and dispute resolution is inevitable.[9]

(c) Results on dependencies at the seams (of Cyberspace on IR)

Fifth In many cases, provisioning of technological functions for the Internet still depends upon *State permission*. State-level regulatory machinery is often ill equipped to systematically deal with all new Internet technologies such as Voice over Internet Protocol (VoIP), Facebook, etc.[10]

[6] Methodological note for the first lesson: This lesson can be analyzed in three parts. Part one states that technological dependencies run from higher to lower layers of the Internet. This fact can be visualized in the Cyber-IR Dependency Matrix by staring at the functions of the Internet actors (i.e., the square matrix formed by functions A1-F6, equipment makers to individuals). Even without any descriptive analysis, one can see that in this sub-matrix, there are more cells marked below the diagonal as compared to above it. This situation visually represents how functions at higher layers of the Internet depend on lower layers as compared to the other way around (e.g., ISPs depend more on equipment providers more than on device makers or application providers). One might argue that this notion is not strictly adhered to, so let us discuss some exceptions. The second part of lesson one states that security depends on all layers of the Internet. To understand this point, study security related functions of each actor (viz. dependencies of functions B5 for ISPs, C6 for platforms, and F5 for individuals). In all cases, we see dependency on all the rest of the actors, meaning, on all layers of the Internet. Finally, part three of lesson states that economic dependencies run from the lower to higher layers of the Internet. To visualize this point, look at economic functions performed by each Internet actors (viz. dependencies of the final function for each Internet actor, "Generate funds to survive", i.e., functions A2, B7, C8, D2, E2, F6), we will then see two types of dependencies for such functions, (a) on other functions performed by that actor, but (b) on functions performed by the higher layer actors. For example, economic health of ISPs depends more on functions performed by platforms, device makers, application providers, and individuals as compared to those performed by the equipment providers.

[7] Methodological note for the second lesson: This conclusion is learned from rows G1–J2, which show how standards organizations depend upon technology providers and others, and from columns G1–J2, which show how technology providers and others depend upon standards organizations.

[8] Methodological note for the third lesson: This conclusion is inferred from dependencies at three levels. At the first level, whether to provision the Internet publicly and privately depends upon how economically viable will be the various actors provisioning the Internet (equipment providers, ISPs, platforms, device makers, and application providers). Therefore, State's decisions to grant private provisioning or to ownership of a certain Internet function depends upon the economic viability of the actor performing that function This situation is represented by the dependencies of grant versus own decisions in row pairs Z1 & Z6, Z2 &Z7, Z3 & Z8, Z4 & Z9, and Z5 & Z10, on various actors ability to generate funds to survive. At the second level, any Internet actor's ability generates funds to survive is in turn dependent upon the functions it performs. For example, ISP's ability to generate funds and survive (row B7) depends upon all the technical functions it performs (rows B1–B5). At the third level, technical functions of an actor in turn depend upon being able to import (study column Z11 to understand technical functions dependent on import).

[9] Methodological note for the fourth lesson: This conclusion has an element of prediction. Today, there is very little evidence of any clear interdependencies between ITU and WTO (see the matrix created by rows and columns Y1–X4). However, as one thinks about dependencies, several of the ITU functions, such as coordinating radio communications services, international management of radio spectrum and satellite services, or coordinating emerging markets, must normatively have, involvement of WTO through their functions such as implementing and monitoring trade agreements, and dispute resolution is inevitable. In this sense, our conclusion predicts that the matrix Y1–X4 is likely to become denser, and it would be better if the interactions between these two institutions are put in place proactively rather than as an afterthought.

[10] Methodological note for fifth lesson: This lesson simply reflects the operationalization of Rule 3 we discussed in Table 1. A great diversity exists in regulatory oversight in provisioning Internet functions across the many states. For example, ISP functions may

This finding is somewhat at odds with—or provides a constraint on—our statement about the dominance of the private sector early in this paper. Such a contradiction is a representation of the impact of attribute heterogeneity, where Internet actors are private entities in some states, but not in all.

Sixth For poorer states with little production capability, provisioning all technological functions could especially depend upon *imports and subsidies*. Of course, such dependence on imports is not limited to poorer states. In technologically advanced states, a complex web of dependencies on global supply chains determines the necessary import.[11] For example, shutting down the semiconductor manufacturing in Japan during the 2011 Tsunami hampered the shipments of highly desirable Apple products.[12]

Seventh Information access depends upon State censorship and content filtering. This is an area of growing interest. States like China are far ahead of other states in censorship and content filtering on the Internet. Most other states, especially those where citizens use information platforms (such as Facebook) that are outside the State's jurisdiction, are trying hard to align their ability to protect information with what they have decided their citizen's rights are. A manifestation of such concern is India's demand for locating Facebook's servers within their sovereign territory.[13]

Eighth Our matrix indicates that parallel streams of decisions are likely to create a dependency of the standards organization on the balance of *State versus non-state interests*. One stream consists of various states that permit more private or State-owned Internet actors (ISPs, Platforms, etc.). The other stream is the increasing number of these Internet actors that participate in the non-state standards organizations such as IETF, ICANN. Such dependency increases coordination costs and reduces speed at which decisions can be made.[14]

(d) Results on dependencies at the seams (of IR on Cyberspace)

Ninth State censoring and filtering capabilities depend on actors at *all* Internet layers as well as the standards organizations, many of whom today are non-state, private actors (e.g., IETF, IEEE, ICANN). This means that the proverbial State is constrained in its decisions pertaining to content control. Again, China is a special case where control of information is created, by what appears like a conscious decision of the State, at all layers of the Internet.[15]

Tenth Security of *State cyber infrastructure* depends upon security at *all* layers of the Internet. For many states, however, one or more Internet layers are located outside territorial boundaries and legal jurisdiction. This type of situation creates a new set of problems in International Relations, as evident in episodes such as Google's pulling out of China, Stuxnet attack on Iran, etc.[16]

6 Conclusion

We began this paper with three questions: (1) Are some actors/functions more important for the structure and

Footnote 10 continued
be provisioned in the United States without a license but such market entry is regulated in many other nations. We have taken a union of these possibilities (per Rule 3) to show that most Internet functions, when thought about in aggregate, continue to depend upon State.

[11] Methodological note for the sixth lesson: This lesson is learned from a qualitative understanding of the matrix, where the meaning of dependencies on importing hardware/software products (column Z11). Imports for provisioning various Internet functions may be necessary because a State simply does not have indigenous capability to manufacture equipment or develop software, or they may be necessary because cost reasons as core competencies for manufacturing various hardware components and software is certainly distributed across various nations. Once again, column Z11 takes the union of all such possibilities.

[12] http://www.computerworld.com/s/article/9214687/Japanese_disaster_could_affect_Apple_say_experts.

[13] Methodological note for the seventh lesson: This lesson is learned from a qualitative understanding of the State's functions censor content (row Z13) and filter content (row Z14). Both functions depend upon technical capability of Internet actors as well as the State's control over these actors. The lesson here highlights that while functions such as ISPs are more amenable to State because they much locate their hardware within the State's jurisdiction, such is not the case for provisioning information platforms. Similarly, while states importing network equipment or devices can easily put them through appropriate approval process, doing so for software applications if far harder. These differences directly import State's ability to filter and censor content.

[14] Methodological note for the eighth lesson: This lesson is inferred from two levels of dependencies. First, much of the standards activity by IEEE, IETF, W3C, ICANN, and ITU depend upon activities of various Internet actors (see dependencies of rows G1–J2 and Y1–Y7 on columns A1–E2). The Internet activities (A1–E2) in turn can be provisioned privately or be owned by the State (columns Z1–Z10). When taken in aggregate across all states, standards organizations begin to experience private versus public interests. For example, repercussions of such changing balance are increasingly felt by ICANN as more states get interested in who controls the Internet DNS. Or similarly, by IETF as it encounters growing interest from states and not just the private who increasingly encounters State interest it hardly did two decades ago.

[15] Methodological note for the ninth lesson: Further to the methodological note accompanying lesson seven (footnote 30), this lesson observes that the State's ability to filter or censor content depends on *all* layers of the Internet. Consequently, some layers may be more important in rendering the desired control, but no layer can be excluded.

[16] Methodological note for the tenth lesson: This lesson is learned from the dependencies a State has in physically securing Internet access, service, and applications (row Z15) on functions performed by actors at all layers of the Internet (A1–F6).

performance of the Cyber-IR system than others? (2) What dependencies are critical for the functioning of the Internet, IR, and the relationship between the two? (3) How do actor attributes inform the findings pertaining to questions (1) and (2)? The body of the paper addressed each question and presented the results. In this conclusion, we take a step further to highlight some of the implications.

Our analysis began with an observation that, because cyber and International Relations are sufficiently interwoven in various ways, they best be viewed as an integrated system. This can only be done if their interconnections and linkages are systematically identified. Furthermore, it is essential that we first identify and understand the properties of the joint system in its static form before we can improve our understanding of dynamic change or emergent behaviors—as well as sources and consequences thereof.

6.1 The logic of inquiry

In the absence of quantitative foundations for an integrated investigation, we selected to utilize a methodology that allows us to represent the structure of a system. We have selected to use the design structure matrix method (DSM) and to augment (extend or enhance) its core features in order to address the challenge at hand. By augmenting DSM with several essential functions, we derived an empirically based representation of a joint system cyber-IR system.

As we proceeded, our investigation exposed clusters of dependencies that are most critical to the conduct of activities in the cyber domain and in International Relations. We focused on four specific areas: (1) within Cyberspace, (2) within IR, (3) Cyberspace dependence on IR, and (4) IR dependence on Cyberspace. We have found that the two domains "at the seams"—meaning, where Cyberspace depends upon IR and vice versa—are most revealing of potential changes in each of the individual domains. In addition, the revealing signals "at the seams" are due largely to the interactions between the two domains, the cyber and the international.

Furthermore, by synthesizing the lessons learnt about the dependencies "at the seams" (answer to Q2) in conjunction with the relative criticality of these dependencies (answer to Q1), we are able to derive some predictive inferences, despite the fact that our inquiry created a dependency matrix that is purely *static* in form.

6.2 Cyber dependence on the state

It is true that in its early years, the Internet grew in the United States in research laboratories followed by the private sector (Abbate 1999). This is the reason for the regulatory dilemma about whether and how much to regulate it (Vaishnav 2010). At the global scale, however, our analysis reveals that the growth of the Internet, or more fully the Cyberspace, has not been as independent from the State as we usually believed.

First, not in all states are the entities provisioning physical and logical layers of Cyberspace public and state-owned. This situation is also prevalent in those states where the technological capacity is limited. And the understanding of the regulatory implications of new technologies at the cyber information layer (e.g., VoIP, Facebook) is also limited. There may even be an unwillingness to adopt a "hands off" approach to Cyberspace.

Another cyber dependence on the traditional State relates to imports and subsidies. In poorer states, it is the very provisioning of the physical layer of Cyberspace that depends upon imports. But even technologically advanced states must rely on imports given the complex web of dependencies created by global supply chains associated with the cyber-centered structures and functions.

Finally, even in states with the best of cyber infrastructures, the very access to information ultimately depends upon the State's politics on censorship and content filtering. Even China, for example, has demonstrated that despite being more complex than previous communications technologies, controlling information in Cyberspace is not impossible.

Arguably, as the State becomes more cognizant of the criticality of Cyberspace in performing some of its important functions, they may become even more strategic and possibly effective in preserving and managing these points of control. Thus, while the cyber domain has always been dependent on the State, such dependence may grow further.

6.3 State external functions dependence on Cyberspace

Our analysis shows that two functions traditionally considered critical in IR are deeply intertwined with Cyberspace today. First is the security of State cyber infrastructure that is determined by the level of security at *all* layers of the Cyberspace. For many states, however, the information and the logical layers of the Cyberspace are located outside their territorial boundaries and legal jurisdictions. Such situation creates a new set of issues, even problems or dilemmas, in International Relations—such as Google's withdrawal from China, or Pakistan turning off YouTube stream to many South Asian nations, among others.

Second, the State's ability to censor and filter information depends upon actors at *all* layers of the Internet as well as the standards organizations, many of whom today are non-state, private actors (e.g., IETF, IEEE, ICANN). This means that the proverbial State is constrained in its control

over content. Indeed, the complexity of controlling information is apparent even in China, where the State has seemingly made a conscious effort to create controls at all layers of Cyberspace. Such an effort requires far more coordination when the actors are private.

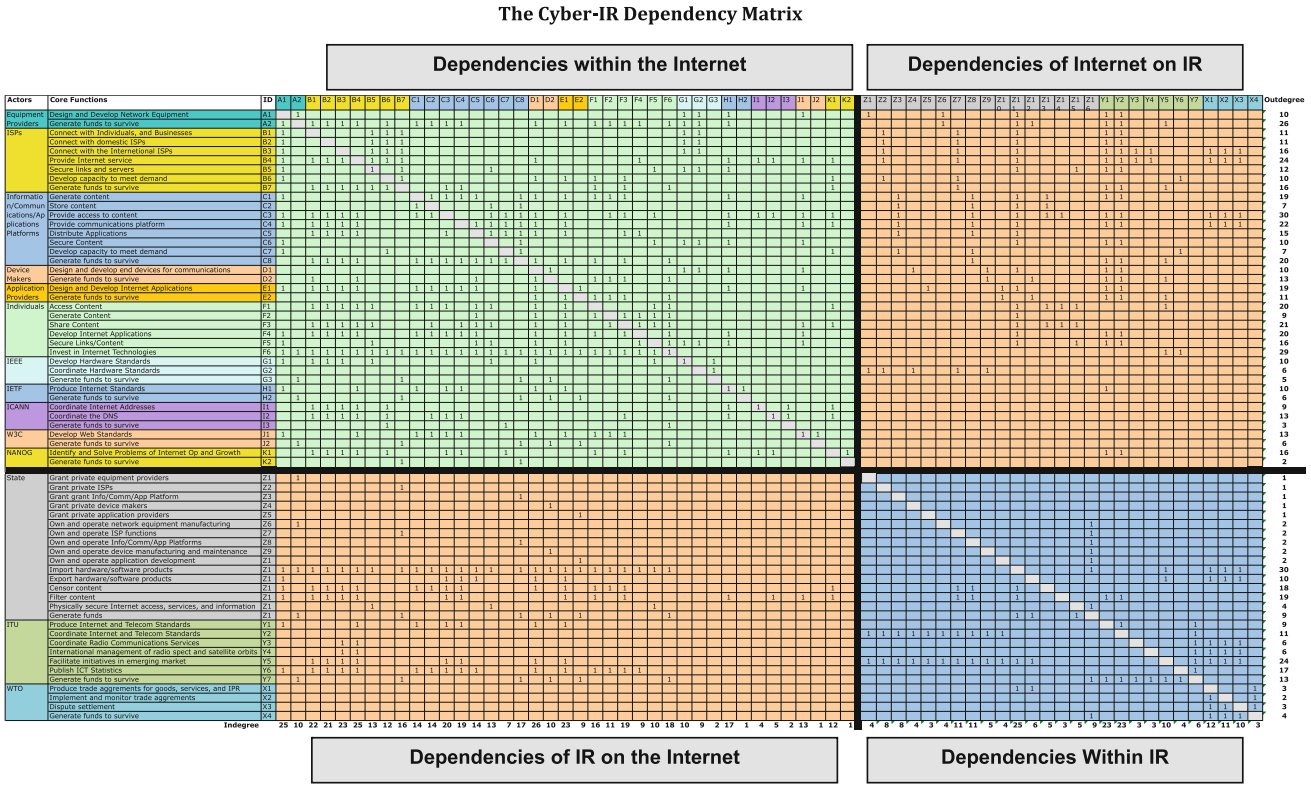
6.4 Dynamic inquiry necessary

The interdependencies of the State and cyber examined in this paper—and the methodology that we have employed—are based largely on a static logic. Nonetheless, we have been able highlight some important features of structure and function in both domains and in their interconnections. Clearly, this is only a first but important foundational step. At the same time, however, it signals the critical challenge of addressing the dynamics of change. More to the point, this challenge amounts to a necessity if the full connections and the evolutionary trajectories of this integrated system are to be explored, and perhaps in time even understood.

The urgency of developing a dynamic view to understand the trajectory of the cyber International Relations system can be appreciated by understanding the limitations of the current approach. Consider the predicament of standards organizations such as IETF, ICANN that have been the key to developing the present Cyberspace. The nature of standards setting—not what standards to set, but the process of standard setting that will lead to a resolution that will satisfy all actors—is likely change in a way that cannot be captured in the static view of interdependency we created in this paper. The reason for it is that, over time, the decisions by states worldwide to provision Cyberspace either privately or publicly dynamically alter the mix of state versus non-state voices participating in standards setting at any given layer of the Cyberspace, thus, altering the nature of standards setting. To study such an evolution with the present method would mean creating multiple snapshots of the interdependency matrix over time and studying how various dependencies appear and disappear. Studying such a dynamic evolution would be our next step.

Acknowledgments This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Appendix: The cyber-IR dependency matrix



In the above matrix, actors and their core functions from Table 2 are listed along rows and columns. A marked cell of the matrix represents a dependency of the corresponding

row core function on the column core function. Blank cells in the matrix indicate no dependency of the corresponding row and column functions.

References

Abbate J (1999) Inventing the Internet. MIT Press, Cambridge

Choucri N (2012) Cyberpolitics in international relations. MIT Press, Cambridge

Choucri N, Clark DD (2011) Cyberspace and international relations: toward an integrated system (working paper no. 8-25 for ECIR Internal Review). Retrieved from: http://ecir.mit.edu/images/stories/Salience%20of%20Cyberspace%208-25.pdf

Eppinger SD, Browning TR (2012) Design structure matrix methods and applications. MIT Press, Cambridge

Eriksson J, Giacomello G (2006) The information revolution, security, and international relations: (IR)relevant theory? International Political Science Review 27(3):221–244

North RC (1990) War, peace, survival: global politics and conceptual synthesis. Westview Press, Boulder c1990

Pragmatism in International Relations (2002) Millennium Special Issue 31(3). Retrieved from: http://www.lse.ac.uk/internationalRelations/Journals/millenn/abstracts/31-1.aspx

Reardon R, Choucri N (2012) The role of cyberspace in international relations: a view of the literature. Paper prepared for the 2012 ISA Annual Convention, San Diego, CA. Retrieved from: http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_2012.pdf

Steward DV (1981) Systems analysis and management: structure, strategy, and design. PBI, New York

Ulrich KT, Eppinger SD (2012) Product design and development. McGraw-Hill/Irwin, New York

Vaishnav CH (2010) The end of core: should disruptive innovation in telecom invoke discontinuous regulation (PhD Thesis). Massachusetts Institute of Technology (MIT), Cambridge, MA

Waltz K (1959) Man, the state, and war: a theoretical analysis. Columbia University Press, New York