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

June 18, 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.

Third International Engineering Symposium
CESUN 2012, Delft University of Technology, 18-20 June 2012

Cyber International Relations as an Integrated System[1][2]

Chintan Vaishnav, Nazli Choucri, David Clark
Massachusetts Institute of Technology
chintanv@mit.edu, nchoucri@mit.edu, ddc@csail.mit.edu

Abstract. *International Relations (IR) – whether in pursuit of wealth or power – have been traditionally predicated upon the dominance of the State and the effectiveness of geographical boundaries. The Internet has shattered these assumptions. Consequently, the properties of information goods such as information security, control, or freedom, or those of international activities such as trade, or diplomacy must be framed in the context of emergent behaviors of a system where the Cyberspace interacts with traditional IR.*

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 Cyber International Relations (Cyber-IR) System, and to identify and analyze its emergent properties utilizing the methods of engineering systems. Our work is an exploration in both theory and methodology.

We begin by identifying important actors in Cyberspace and IR, and the core functions they perform for their respective systems. In doing so, we disambiguate important questions of system boundary. We then create a domain structure matrix (DSM) of the interdependencies among the core functions of the various actors. This method enables us to integrate the domains of Cyberspace and IR that we then examine in two ways. First, we qualitatively analyze DSM to show how Cyber-IR is characterized by the activities of multiple actors who are interdependent in various ways, and who are highly heterogeneous in their roles and capabilities. Second, we perform quantitative analysis using several matrix-based techniques to illustrate and verify how certain core functions are more important than others, and why attributes such as geographical location, economic status, etc., of the actor shape their 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, Domain Structure Matrix, DSM*

1.0 Introduction: Cyber-IR as a Problem of Complex Systems

Over the past decade, the dependence of individuals and businesses on Cyberspace has grown consistently. Recent events such as Wikileaks[3], Stuxnet[4], and the "Arab Spring"[5], however, has made it clear that Cyberspace[6] is interwoven with and has important implications for international relations as well. At the highest level, behind each of these incidents is the fact that, in the information-related domains of international relations, Cyberspace weakens the traditionally held notion that the State is the most powerful actor and boundaries of the State are dependable.

As yet, very little literature directly has teken on the problem of studying Cyberspace and International Relations jointly. Recently, an extensive paper, *Cyberspace and International Relations: Toward an Integrated System*, by Nazli Choucri and David Clark, has begun studying this topic from theoretical perspectives in both engineering and political science. The Choucri-Clark paper develops a candidate framework—combining *layered* model 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

[1] 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.

[3] http://en.wikipedia.org/wiki/WikiLeaks
[4] http://en.wikipedia.org/wiki/Stuxnet
[5] http://en.wikipedia.org/wiki/Arab_Spring
[6] In general terms, we accept the following concept of Cyberspace that is commonly accepted: *Cyberspace is the collection of computing devices connected by networks in which electronic information stored and utilized and communication takes place.* The term "Cyberspace" was coined by fiction writer, William Gibson, and popularized in his book *Neuromancer* (1984).

integrated Cyber International Relations system (jointly, Cyber-IR). *The present research is a direct descendent of the Choucri-Clark paper.*

In this paper, we view the challenge of understanding Internet's implications for the future of International Relations as fundamentally that of understanding interdependencies of these two domains, as *understanding interdependencies is foundational to understanding how any two domains influence each other*. For systems where both technological and human complexities are present, such as one that combines Internet and International Relations, Design Structure Matrix (DSM) has emerged as a useful technique for jointly analyzing such disparate domains.[7] In this paper, we will utilize it for studying the interdependencies of Internet and International Relations.

The remainder of the paper proceeds as follows: we begin by discussing research questions that arise when looking at Cyber International Relations as an integrated system from the perspective of their interdependencies. In section 3, we develop a method for studying questions we raise and apply the method to the joint Cyber-IR domain. The result of this exercise produces a Cyber-IR Dependency Matrix (see Appendix). In section 4, we present analyze the matrix to answer questions raised in this paper. In section 5, we draw conclusions.

2.0 Research Questions

Complexity in Cyber-IR arises due to two factors: multiple actors operate in both Internet and IR domains, and that these actors are heterogeneous in their attributes and in functions they perform (i.e., in the roles they play).

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 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 vs. 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.

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 the Internet. 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).

The above factors motivate the overarching question of our research: *Does heterogeneity of the actors (their attributes and the functions they perform) create opportunities to gain advantage in cyber international relations?* In this paper, we will pose three questions related to this overarching question:

(1) Are some actors/ functions more important in Cyber-IR than others?
(2) What dependencies are critical for the Internet, IR, and the relationship of the two?
(3) How do attributes such as actor's location (local vs. non-local) or status (state vs. non-state) inform findings of questions 1 and 2?

3.0 Method and Application

At the heart of our method is the creation of the Cyber-IR Interdependency Matrix, which uses Domain Structure Matrix (DSM) as a tool. That said, to appropriately bind the scope of the matrix and make its interpretation more meaningful, we have had to create several additional constructs, meaning, rules and

[7] *Product Design and Development*, McGraw-Hill, New York; *Design Structure Matrix Methods and Applications*, MIT Press, Cambridge, forthcoming in spring 2012 Steven D. Eppinger and Tyson R. Browning. The DSM. Don Steward was the first in publishing a set of process interdependencies as a DSM in his 1981 reference *Systems Analysis and Management: Structure, Strategy, and Design*, New York: PBI.

assumptions. Figure 1 provides an overview of our methodology, which we apply to Cyber-IR next. The steps involved in our methodology could be viewed as belonging to two distinct phases: creation of the interdependency matrix (steps 1-3), and analysis of it (step 4).

Step 1: Identify important actors in Internet 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 function that the actor type performs.
- Rule 3: When attribute heterogeneity does determine core functions performed: take the union of all core function 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.

- Qualitative Matrix
- Binary Matrix

Figure 1 Methodology Overview

Step 1: Identifying important actors in Internet and International Relations

The first step is to identify the functional categories of Internet and International Relations related actors. For the Internet, 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 second set of Internet actors are those who create and manage standards or other operational issues, namely, 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 North American Network Operators' Group (NANOG)[8]. The first set of actors (functional categories) is well accepted when discussing Internet architecture, supply chains, or policy (REF).[9] We are beginning to discuss the importance of the second set of actors in the context of Cyber-IR.[10]

For International Relations, our list consists of actors who perform Internet-related functions that could have international implications; namely, the State, International Telecommunications Union (ITU), and World Trade Organization (WTO). (REF)[11]

Step 2: Identifying core functions performed by the actors

The second step is to identify the core functions of an actor 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. Figure 2 shows all actors and their core functions. We enumerate core functions of each actor by asking the following question: Can the actor be that actor without performing a given function?

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

[9] Chintan Vaishnav, *'The End of Core: Should Disruptive Innovation in Telecom Invoke Discontinuous Regulation'* PhD Dissertation, Engineering Systems Division (ESD), MIT, 2010.

[10] Choucri-Clark Paper discussed in the Introduction section of this paper.

[11] We base our selection of IR actors on 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.

Internet Actors and Core Functions	IR Actors and Internet-related Core Functions
Equipment Providers • Design and develop Network Equipment • Generate funds to survive **ISPs** • Connect with individuals and businesses • Connect with domestic ISPs • Connect with international backbone ISPs • Provide Internet service • Secure links and servers • Develop capacity to meet demand • Generate funds to survive **Information/Communications/Applications Platform** • Generate content[13] • Store content • Provide access to content • Provide communications platform[14] • Distribute applications[15] • Secure content • Develop capacity to meet demand • Generate funds to survive **Device Makers** • Design and develop end devices for communications • Generate funds to survive **Application Providers** • Design and develop Internet applications • Generate funds to survive **Individuals** • Access content • Generate content • Share content[16] • Develop Internet applications • Secure links/content • Invest in Internet technologies **IEEE** • Develop hardware standards • Coordinate hardware standards[17] • Generate funds to survive **IETF** • Produce Internet standards	**State** • Grant private equipment providers[12] • Grant private ISPs • Grant grant Information/Communications/ Applications Platform • Grant private device makers • Grant private application providers • Own and operate network equipment manufacturing • Own and operate ISP functions • Own and operate Information/Communications/Applications Platforms • Own and operate device manufacturing and maintenance • Own and operate application development • Import hardware/software products • Export hardware/software products • Censor content • Filter content • Physically secure Internet access, services, and information flows • Generate funds **ITU** • Produce Internet and Telecom Standards • Coordinate Internet and Telecom Standards • Coordinate Radio Communications Services • International management of radio spectrum and satellite orbits • Facilitate initiatives in emerging market • Publish ICT Statistics • Generate funds to survive **WTO** • Produce trade agreements for goods, services, and intellectual property • Implement and monitor trade agreements • Dispute settlement

[12] "Granting" private provisioning of any actor type is construed broadly to include situation 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 Untied States, whereas a license is necessary to do so in most other nations.
[13] 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.
[14] Examples of a communications platform are the likes of email platform (e.g., Hotmail), or social networking platform (e.g., Facebook).
[15] A platform may distribute applications generated by it or someone else (e.g., Apple's iTunes Store).
[16] Generation and sharing of content is construed broadly here to include content generated and shared between users, or between by a user and a machine.
[17] Coordination of hardware standards is to ensure interoperability among hardware devices.

• Generate funds to survive	
ICANN	
• Coordinate Internet addresses[18]	
• Coordinate the DNS[19]	
• Generate funds to survive	
W3C	
• Develop web standards[20]	
• Generate funds to survive	
NANOG	
• Identify and solve problems of Internet operations and growth[21]	
• Generate funds to survive	

Figure 2 Actors and Core Functions

Several aspects of the core functions listed in Figure 2 are important to discuss. 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 present for all actors, except State. We interpret this function broadly. While financial viability is important for all, mechanisms for survival could be different for different actors. For example, for all Internet related actors except Individuals, "to survive" could equate to 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 a viable cyberspace, where such funds may be generated though 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 matrix, so it is excluded here.

Third, for many actors, attribute heterogeneity does not change the core functions they must perform. For example, Equipment Providers, Device Makers, Application Providers must perform the same core functions whether they are small, medium, or large in size, for profit or not-for-profit, local or international. In this case we simply use Rule 2 described in Figure 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, or all individuals do not develop Internet applications, or all States do not own ISPs, and so on. In this case, we apply Rule 3 described in Figure 2 to take a union of core functions an actor type performs to arrive at the complete list.

Finally, two methodological issues are appropriate to consider here. First, as stated in Rule 1 of Figure 1, the Internet actors and their functions in the above list were identified considering functions they *do* perform, and not functions they *could* potentially own. For example, an ISP could also decide to become an information platform, but majority do not.

[18] 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.
[19] The Domain 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.
[20] "Web standards" is a general term for the formal standards and other technical specifications that define and describe aspects of the World Wide Web.
[21] Concerns interconnection and peering in the Internet backbone.

Second methodological concern is whether the functional classification is at the right 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 platforms. Step 3, Rule 5 is created to arrive at the above functional classification of actors we present above.

Step 3: Identify dependencies among core functions

Having listed the core functions of actors, we 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. The Appendix at the end shows a version of the Cyber-IR Dependency Matrix produced from this step.[22]

Step 4: Code and Analyze the Structure of Interdependencies

We then code and analyze the matrix in two ways. We first produce a heavily annotated version of the dependency matrix to footnote each dependency. Form 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, which we will discuss in the Analysis and Results section.

The second way we analyze the matrix is by converting the qualitative matrix to a binary matrix, where a populated cells is marked as "1" and empty cells as "0." We then analyze the binary matrix using various techniques of matrix algebra.

4.0 Analysis and Results

We now turn to analysis of the dependency matrix to answer the research questions we raised in section 3. Please note that below we discuss Question 1 and 2, and in discussing them interweave the implications of Question 3.

Q1: Are some actors/ functions more important in Cyber-IR than others?

To answer this question, let us look at two different views of the dependencies: functions most depended upon (Figure 3), and most dependent functions (Figure 4). We argue that functions shown in Figure 3 should be considered important because many other functions in the Cyber-IR system depend on them. Absence of such a function hampers many dependent core functions, and leveraging it could influence the same ones positively. The chart can be interpreted as follows: (1) for that States that neither owns manufacturing of devices, network equipment, application providers, nor hosts information and communications platforms in its jurisdiction, import of such hardware and software is critical for a stable Internet experience; (2) ISP's ability provide connectivity and survive economically is critical for all states; and curiously, (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 a more varied dependencies across all layers of the Internet than any other standards organization such as IEEE, IETF, or W3C.

[22] 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.

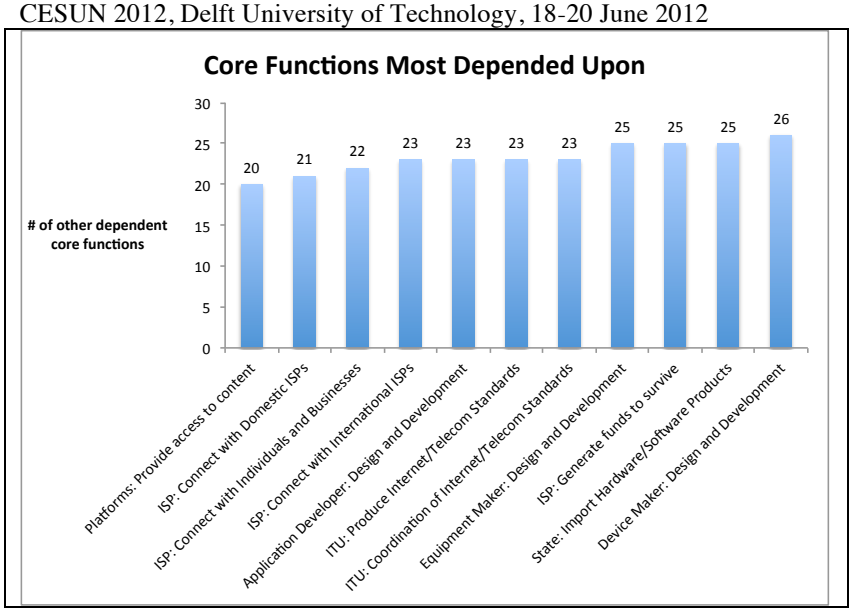


Figure 3 Core functions most depended upon

Figure 4 shows functions that are most dependent on other functions. We argue that these functions are important because they are the most complex to produce.

In some cases, it is easier to grasp why their production may be difficult. For example, State's decision to import hardware and software, individual's decision to invest in Internet technologies, and ITU's ability to facilitate initiatives in emerging markets necessarily depends upon many other activities. Similarly, core functions such as survival of ISPs, and equipment makers are complex because these actors are far deep into the communications supply chain. However, some findings are surprising at first sight.

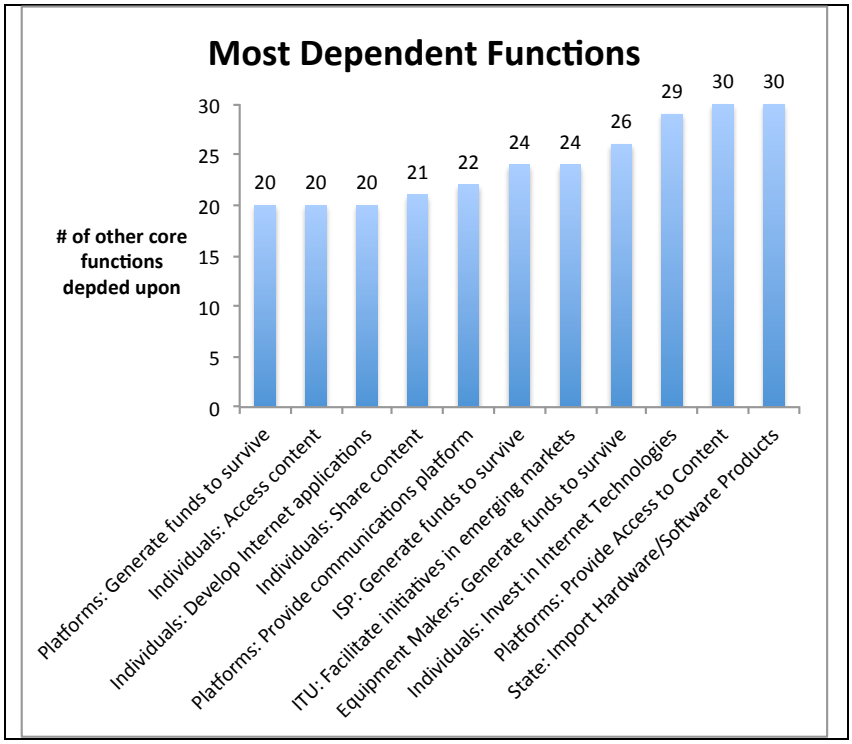


Figure 4 Most dependent core functions

Platforms 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, Facebook, but from the perspective of the Cyber-IR system, these platforms too depend heavily on individual user's ability to generate and share content as well as on the availability of Internet connectivity and service. Further, while we have come to a point where individuals share and access content easily, and some also develop applications; arriving here has taken time as all of these functions depend upon many others. This is the reason why individual-level activity is marginal in States where Internet architecture is weak.

Q2: What dependencies are critical for the Internet, IR, and the relationship of the two?

We analyze this question by drawing lessons about the nature of dependencies in four domains: Within the Internet, within IR, and those at the seams (of Internet on IR, and of IR on Internet). Below, we list these

lessons sequentially as classified in these four domains.[23] The purpose of identifying such critical areas of dependencies is so that they can be studied in more detail in our future work.

Lessons on Dependencies within the Internet
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; 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 provision the Internet run in the opposite direction, from lower onto the upper Internet layers.

Second: While much of the discussion on standards focuses on how the various technology providers depend upon standards organizations, the converse is also true – standards organizations too depend upon technology providers for not just standard creation but also the economic viability of the standards body altogether. This point is not merely an artifact of how the dependency matrix is coded but is representative of the importance of leverages in standards creation and coordination.

Lessons on Dependencies within IR
Third: Public provisioning of Internet functions occurs in most cases when depending upon the State is the only economically viable option. Most emerging economies where State was 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/export. Notable exceptions here are States like China where public provisioning is done with a different objective such as control of information.

Fourth: While there is little evidence currently of whether ITU depends upon the activities of WTO, such a matrix would argue that managing international communications over the Internet and international trade will likely become increasingly active.

Lessons on Dependencies at the seams (of the Internet on IR)
Fifth: In many cases, provisioning of technological functions of the Internet still depend upon State's permission. State-level regulatory machinery seems systematically throw a fit with all new Internet technologies such as VoIP, Facebook, etc.

Sixth: For poorer states with little production capability, provisioning all technological functions could depend upon imports and subsidies. Of course, such dependence on imports is not limited to poorer states, at the other end of the spectrum, in technologically advanced states a complex web of dependencies on import determine the stability of technology supply chains.

Seventh: Information access depends upon State's censorship and content filtering. This an area of growing interest. States like China are far advance in censorship and content filtering. Most other States, especially those where citizens use information platforms (such as Facebook) that are outside the State's jurisdiction, are desperately trying 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.

Eighth: Our matrix argues that while a concern such as the one we discuss here has not been recognized as critical yet, two parallel streams of decisions a) of the various States to permit more private or State-owned Internet actors (ISPs, Platforms, etc.), and b) of an increasing number of these Internet actors to participate in the non-state standards organizations such as IETF, ICANN, is likely to create a dependency of the standards organization on the balance of State vs. non-State interests. Such dependency increases coordination costs and reduces speed at which decisions can be made.

Lessons on Dependencies at the Seams (of IR on the Internet)

[23] The lessons below are deduced from the analysis of the qualitative matrix that we have not detailed here due to the short nature of this paper. With some observation, however, the same can be deduced from the matrix in the Appendix.

Ninth: State's censoring and filtering capability depends on actors at *all* Internet layers as well as the standards organizations, many of whom today are non-state, private actors. This situation makes is difficult to for any State to control content. Again, a notable exception here is China, where control of information is created, by what appears like a conscious decision of the State, at all layers of the Internet.

Tenth: Security of a State's cyber infrastructure depends upon security at *all* layers of the Internet, but for many States actors at some of the Internet layers reside outside the jurisdiction of the State. The nature of problems this situation creates is evident in episodes such as Google's pulling out of China, Stuxnet attack on Iran, etc.

A Note for Methodological Completeness

The lessons above are deduced from the analysis of the qualitative matrix. As this short paper omits the details of this analysis, for methodological completeness, we present the analysis behind lesson one (above) as a representative case. The first lesson above can be analyzed in three parts. Part ones 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 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's discuss some exceptions. The second part of lesson one states 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, take the part three of lesson one that 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.

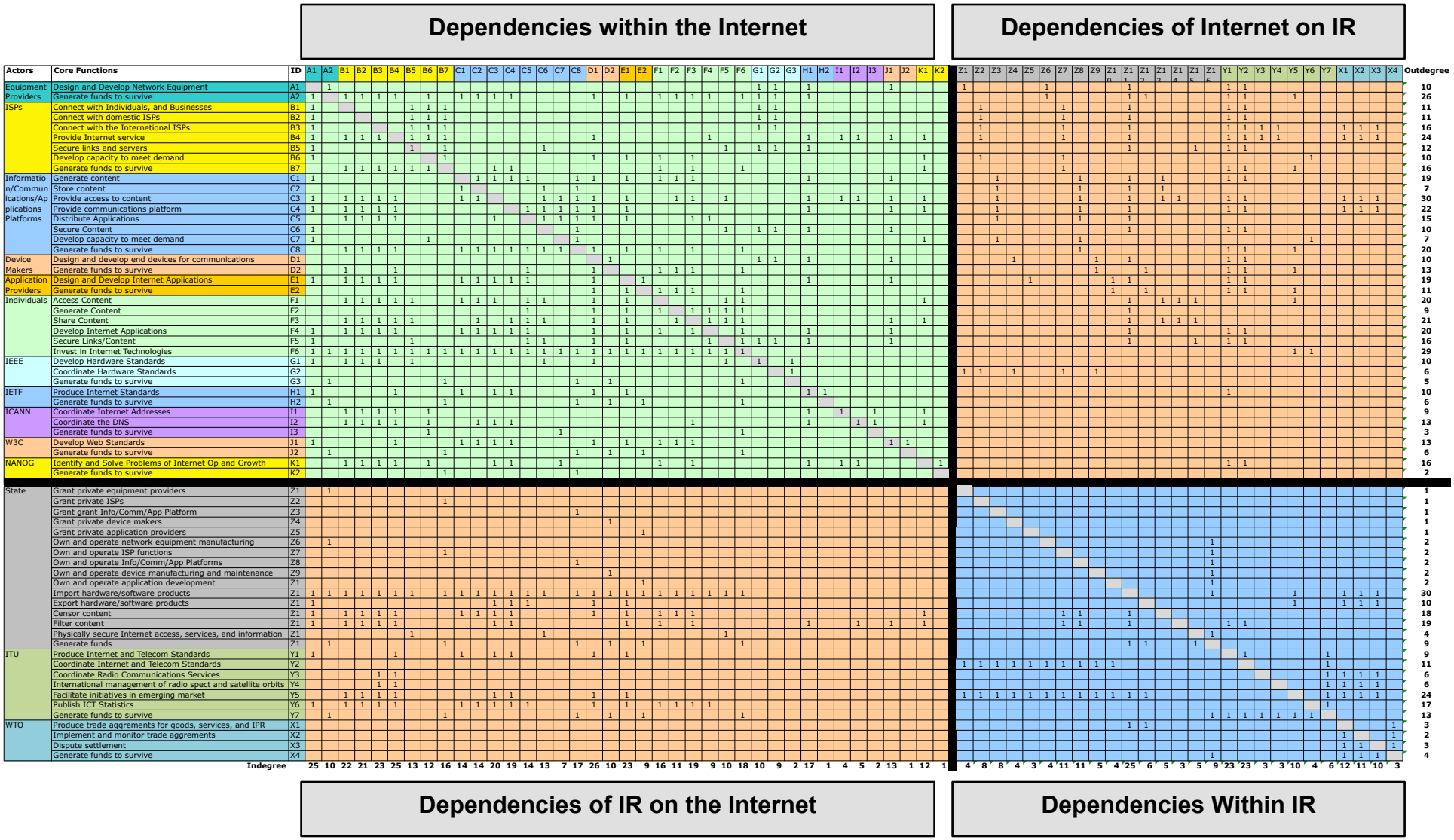
Similar discussion could be had about the other lessons listed above.

5.0 Conclusion and Future Work

In this paper, we "scratched the surface" of interdependencies between Cyberspace and International Relations. We began with an acknowledgement that in today's world, Cyberspace and International Relations are sufficiently interwoven that they ought to be studied as an integrated system, were we to understand its emergent behavior such as international security or trade. Through the research in this paper, we demonstrated that a domain structure matrix (DSM) based methodology can be used successfully to study the interdependencies in a system that combines Cyberspace and International Relations. Unfortunately, given the short nature of this paper, we kept aside two possible explorations in related literature: one demonstrating methods other than DSM that have been thrown at the problem of integrating Cyber and IR, and another exploring why DSM is appropriate given its applications to other domains. Nevertheless, our findings demonstrate ways to understand actors and functions that are important in the joint Cyber-IR system. We also expose clusters of dependencies that are most critical to study in four areas: within the Internet, within IR, of the Internet on IR, and of IR on the Internet.

Our future work will focus on understanding the ten areas of critical dependencies further, especially from the perspective of role and attribute heterogeneities of the actors. We believe, advanced DSM techniques, combined with network analysis as appropriate, will be useful in deducing further structure. At a higher level, the underlying research focuses on the operational features of cyberspace by focusing on the Internet its functions and actors first, and then includes the core institutions or entities involved in the IR domain with respect to Internet functions. In future, we also intend to take the opposite perspective.

Appendix
The Cyber-IR Dependency Matrix



In the above matrix, actors and their core functions from Figure 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.