Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

http://ecir.mit.edu/

A Research Collaboration of MIT and Harvard University

The Final Report

Version 1.2

Prepared by:

Nazli Choucri, Principal Investigator
Professor of Political Science
Massachusetts Institute of Technology

Cambridge, Mass. 2015

PART II

RESULTS of SCIENTIFIC INQUIRY

Part II presents a more detailed presentation of the results of ECIR scientific research. The *ECIR Research Agenda,* noted below, summarizes the research challenges and activities undertaken, and serves as a guide for the results presented in the Sections of Part II.

ECIR Research Agenda

1. **The Core: Framework and Foundations for Theory and Policy**

   Constructing the *overarching framework* essential for capturing interactions between the cyber and the physical arenas, and for clarifying how the "pieces" generate a view of the "whole." The framework is the *anchor for the ECIR investigations, i.e*. the reference for, and convergence of, all research projects.

2. **Cyber Power and Cyber Security: Control Point Analysis**

   Exploring *cyber power* and *control, people and messaging,* key features of *cyber security threats* to security and impacts of *social media* on power relations.

3. **Cyber Governance: How the Cyber System is Structured and Disciplined**

   Mapping and analyzing diverse modes of *private and public authority* managing the cyber domain, emergent cyber norms, and *resilient mechanism design.*

4. **Alternative Futures: Drivers of Change**

   Designing potential futures for cyberspace and international relations, potential *structure* and process, and the underlying *governance* principle.

5. **Cross-cutting Theme: Domain Ontology for Complex Systems**

   Three cross cutting themes help anchor ECIR contributions to the Minerva Program and Relevance for the U.S. Department of Defense

Part II (sections 4 to 8) are devoted to the results of these five components of the technical and scientific research agenda in the order presented above,

The full citation for a noted reference is presented in Section 6 of this Report where we list the knowledge materials developed throughout the ECIR Project. This allows the reader to go directly

to the source rather than to reply on a highly simplified summary, given the scale and scope of the research and the extensive nature of the result.

Important Caveat:

Since the ECIR publication record is to extensive and available on the ECIR website, this report illustrates the products and results. It does not provide coverage or summary of each published item. Further, what follows does not cover all of the results generated by the ECIR Project.

4. FRAMEWOK:

FOUNDATIONS for THEORY and Policy

The conceptual framework of the ECIR research is anchored in the intersection principle, that is, the intersection of the *layers* of the Internet, the core of cyberspace, and the *levels* of analysis in international relations, described below.

The major result is *the construction of an empirically based framework for connecting international relations and cyberspace*. This allows us to utilize one overarching frame that spans both the cyber and the IR domains. This frame is rendered operational for different purposes using different methodologies.

The key elements of this framework are the *layers* of the Internet (core of cyberspace), and the *levels* of analysis (structure of the international relations). The connection is made by the *intersection* between layers of the Internet and the levels of analysis in international relations. The overall outcome is the product of specific research activities. The result if the *Cyber-IR Model.*

4.1 The Core of Cyberspace – Layers of the Internet

Our starting point in the analysis of cyberspace is unbundling the *architecture of the Internet*, focusing on its layered structure. As defined, the Internet structure consists of physical, logical, information layers (with the operating actors) and "user" layers. The latter refers to all users of the Internet irrespective of role and function.

- Basic frame on layer structure of the Internet (Clark)

- Comparisons of automated ontologies to understand how different scientific communities' (engineers vs. social scientists) view and examine cyberspace and other derivative variables (Madnick and Choucri)

- New method and tool for automated investigations of large bodies of scholarly publications to derive mappings of structures and processes reflected in scientific publications related to cyberspace (Madnick and Daw Elbait)

4.2 Structure of International Relations — Levels of Analysis

By analogy, we view the international system in terms of the characteristic features that operate at different *levels* of analysis. Generally, these levels are seen as the individual (the first level), aggregating to the state (the second level), organized in the international system of states and non-state actors (third level), and embedded in the global system (fourth level). Traditionally, human activities were considered only in their social contexts. More recently, the field recognized all levels of analysis operate in and involve the social environment and the natural environment.

- Literature review of cyberspace and international relations (spanning 10 years and 8 major journals) Reardon and Choucri

- Theoretical framing of cyberspace as the third arena of human interactions (in ECIR book) Choucri

The above provide critical resources that are then used for conceptual and theory-building purposes. The first key step is identification of the core theoretical construct.

4.3 Theoretical Construct - The Intersection Principle

The Intersection Principle refers to the core "rule" that we have developed in order to allow us to examine who does what, and who "gets what, when, and how"—the basic premises of politics, national and international. It is defined as the intersection between the layers of the Internet and the levels of analysis in international relations.

Thus, application of the *intersection principle* allows us to identify the actors, functions-roles, actions, and target-goals. It is derived from disaggregation of the Internet layers and international relations levels. This intersection anchor for the model of the Joint Cyber-IR System, depicted in simplified form in Figure 4.1 below. This is an important step in addressing the question mark in Figure 1.1 above.

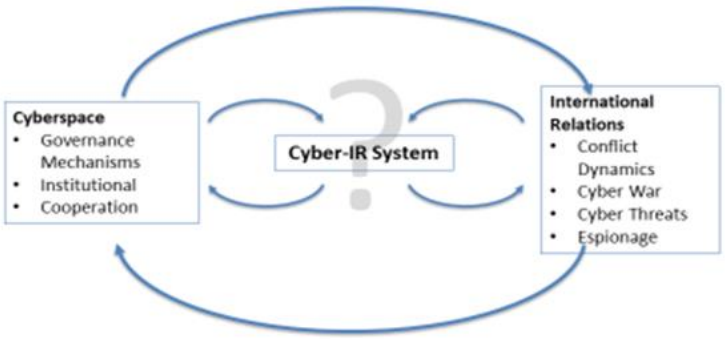

Figure 4.1 Frame of the Cyber-IR Model

Note that the Figure 4.1 is bracketed by two opposing pressures: *system threats* (conflicts, contentions, and violence) and *system supports* (governance, cooperation, collaboration). Note also that the central part of the Figure is unbundled in Table 4.2 showing a simplified view of the intersection principle in matrix form.

Table 4.1

Cyber-IR System: Layers and Levels

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

Logical

Source: David Clark

A set of further results, based on then use of different methodologies, provided added details, insights and information about the structure and dynamics of joint Cyber-IR system intersection principle framing different. These include, for example, results of:

- Empirical application of SDM architecture generated published results that enhance understanding of the interconnections among elements of the *joint Cyber-IR system* in static and dynamic terms – (Vaishnav, Choucri, Clark).

4.4 Framework of ECIR Multidisciplinary Research-In-Depth

The major product (and the derivative results) of the Core theme 1, in Table earlier -- integrated framework and model for the Joint Cyber-IR system – it is the core "whole" within and around which all other "individual" research activities cohered.

Figure 4.2 shows the "whole" in some detail. It includes many but not all of the research activities generated by the ECIR Project. These are presented in the following section is the most abbreviated form. Given the publication record of ECIR (shown later on), we found it necessary to focus on the "big picture" rather that the individual results.

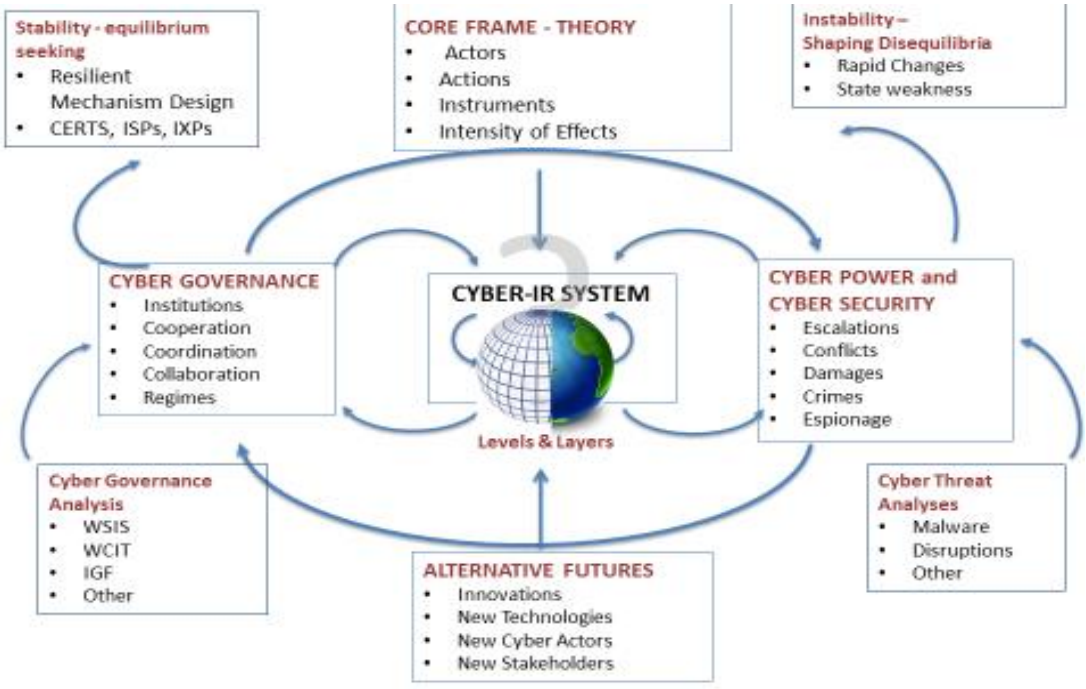

Figure 4.2 Framework for Exploring Cyber International Relations

This figure provides a detailed articulation of the question mark in Figure 1.1. It also serves as a useful context within which to situate the research activities, singly or jointly.

5. CYBER POWER, CYBER SECURITY and CYBER CONFLICT

The second core theme or research challenge focused on power, influence and security. The results include the construction of new methods, the development of new knowledge materials, and the convergence of new answers to emergent puzzles about cyber power and threats to security. More specifically, results pertain to:

5.1 Cyber Power in International Relations

We have identified the scale, scope, and domain of cyber "power," the leverages and actions–for different types of actors and motivations. The results include:

- Identifying and understanding the *drivers* for the diffusion of public and private cyber power and influence (Nye, Sewell)

- Clarifying the mechanisms shaping *people power* and social networking, how mobile technologies create pressures on state control, and how the state responds to such pressures (Goldsmith and Siegel)

- Capturing the collective insights and evidence about *social media impacts* derived from ECIR Workshop on *People, Power, and Cyber Politics* with respect to:

    - How we listen to messages
    - New threats and opportunities for governance
    - Effects of cyberpolitics on democracies
    - What can we learn from uses social media and social action
    - New visions for the future

5.2 Control Point Analysis

We developed a process-based method we call *control point analysis* to identify the actions and actors involved in executing a user request. To demonstrate its effectiveness we illustrate with cases such as to "create a web-page," "search across web-pages" and "retrieve information" and the like. There results include:

- *Specific applications* to show how to identify actors, actions, potential locations, and expected outcomes at each control point throughout the entire cyber-IR space (Clark)

- Comparative investigations show *differences in control policies* and mechanisms for states (USA vs. China) and for a dominant cyber entity (Google). Figure below shows the application to China.

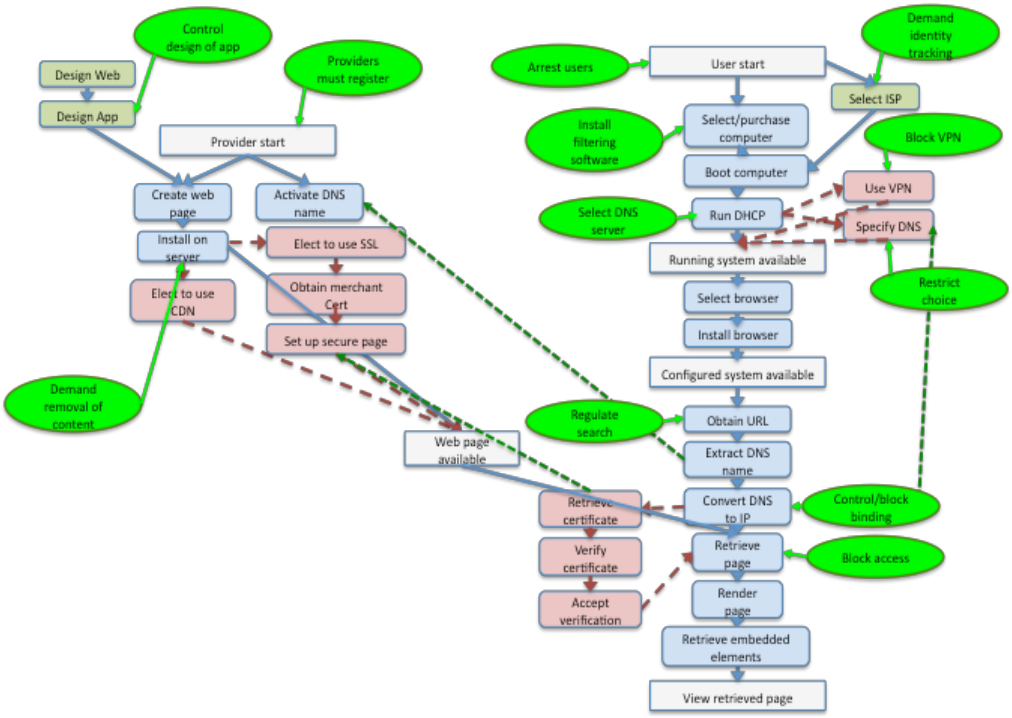

Figure 5.1; Control Points in China to Retrieve a Web Page
Source: David D. Clark

When applied to the case of Google, a *private sector actor*, we determined how this entity exerts its control and influence.

These results provide a detailed view of who controls a cyber access, how, where, and with what effect. In a sense, this can be seen as the view from the "top".

5.3 Cybersecurity – New Tool for Knowledge Exploration

We have constructed a new tool for extracting knowledge from large-scale repositories. Results include construction of a new computer based technology for *comprehensive analysis of massive materials* ("big data"), reporting on the issue of "cybersecurity"

- Application of the methods provided a "proof of concept" for a new research tool based on a close examination of a large corpus of scholarly knowledge, to generate new knowledge

about cybersecurity, notably about the multidimensionality thereof. Choucri, Daw Elbait, Madnick

Below in Figure 5.2 we show the profile of the automated system developed for this purpose. Later in this Report, we shall present the results of the application to cybersecurity

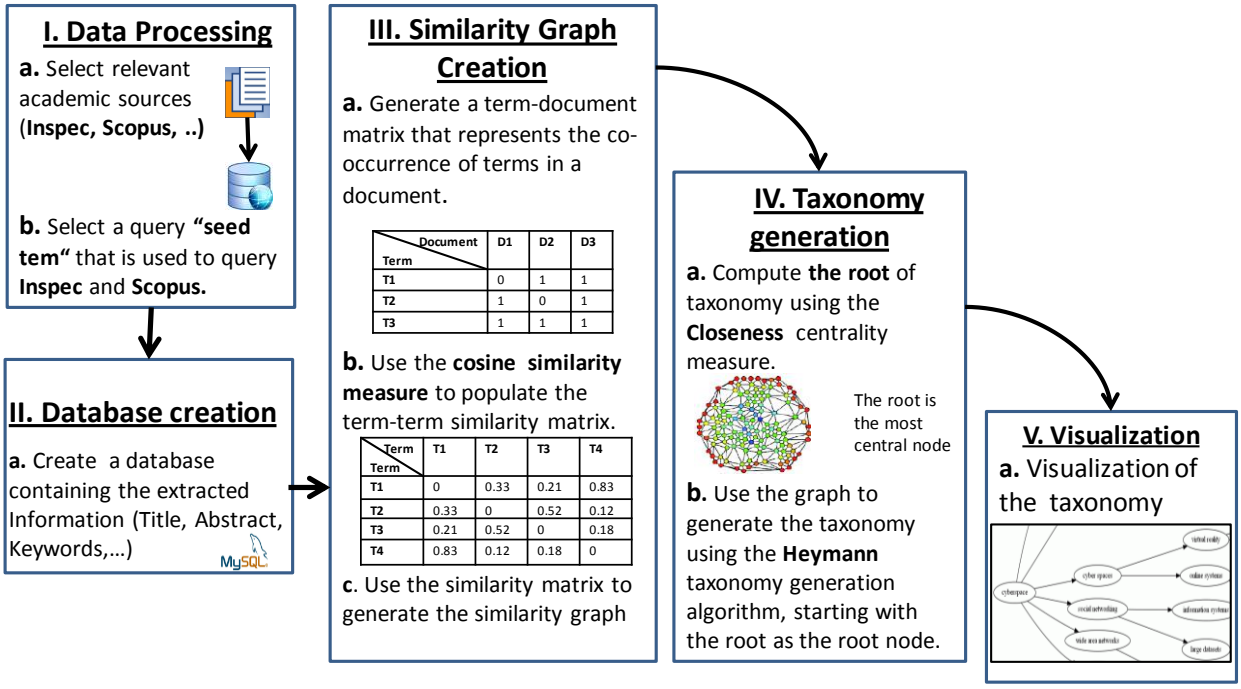

Figure 5.2 New Method for Automated Knowledge generation
Source: Daw Elbeit, Madnick, Choucri

5.4 *System Dynamics- Modelling Cyber Threats and Corporate Responses*

Development of a system dynamics simulation models of the cyber organizational "ecosystem applied to a set of challenges. The research focused on two questions:

- The first question is: *What are corporate responses to cyber attacks?* This model highlights the "sluggish" reactions whereby patching is used "after the fact" with little anticipatory actions. The basic model is shown in Figure 5.3 below.

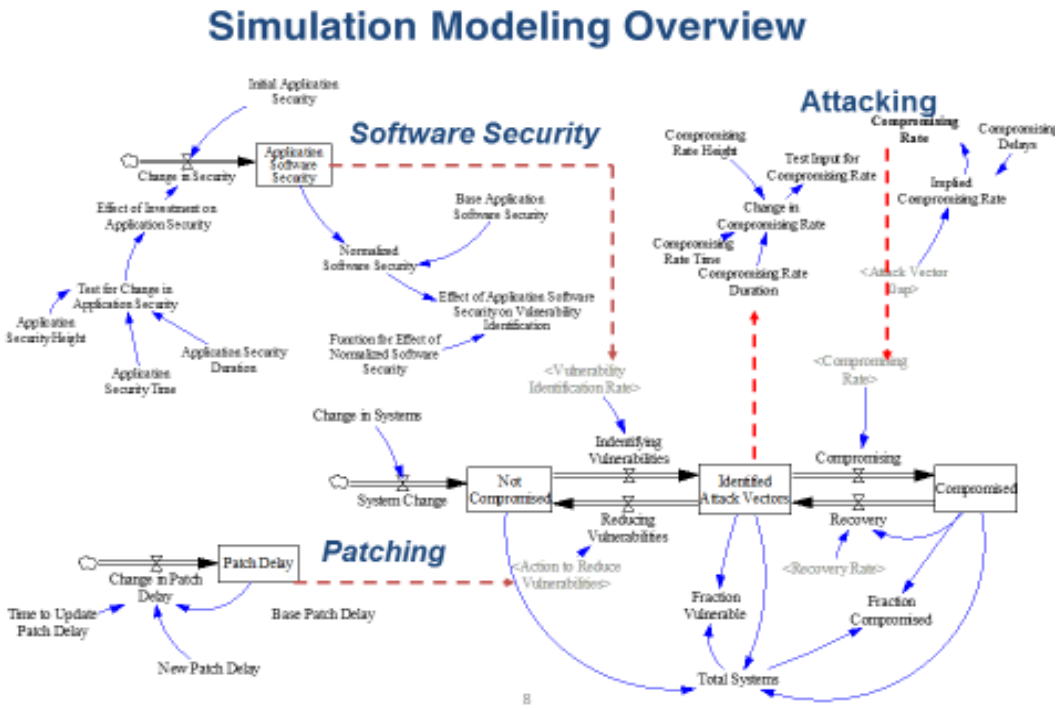

Figure 5.3: Patching not Solving Security Breaches
Source: Siegel and Houghton

- The second question is: *How can we model the complexity of cyber security?* The answer to this question is shown in Figure 5.4 showing the first order segmentation used to address this question. Several different threat systems examined illustrate the diversity of the underlying dynamics.

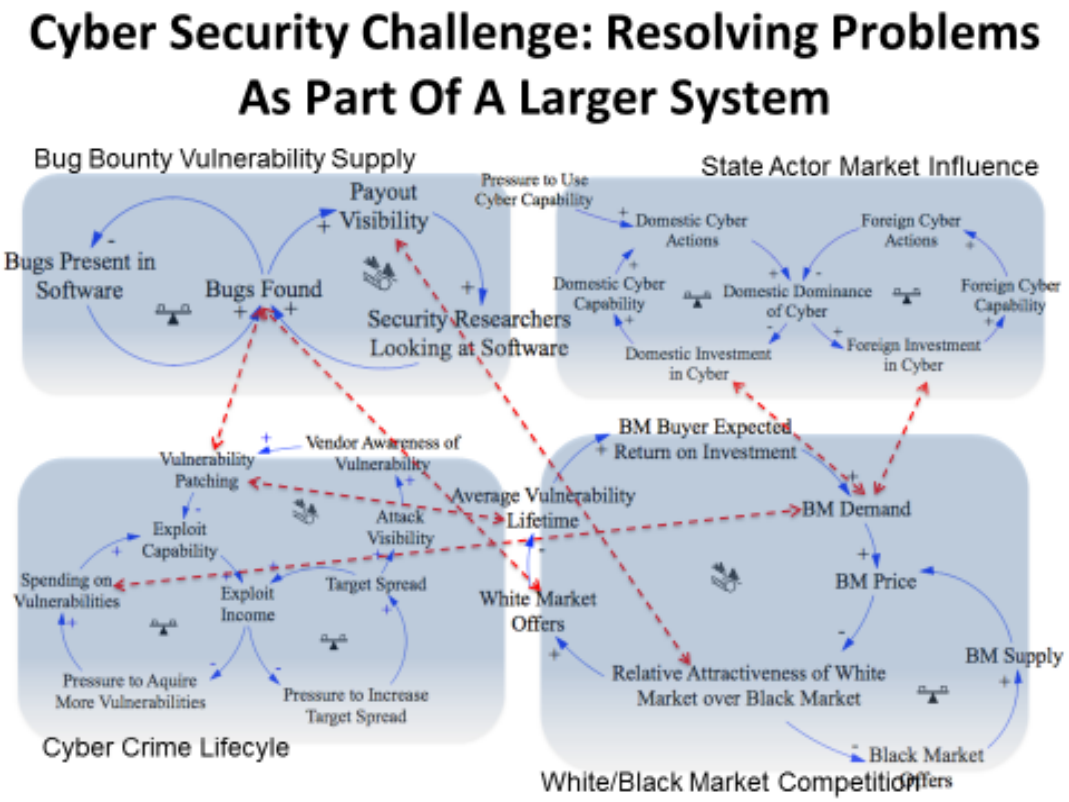

Figure 5.4: Select "Whole" of the Cyber Security Problem
Source: Siegel and Houghton

Such in models help us toi nvestigate the nature and requirements of effective deterrence in the cyber domain. Moving forward from a nuclear-era doctrine, cyber strategy must be encompass a broad spectrum of options for deterrence rather than a stand-alone strategy for cyber, applying not just elements of punishment and denial but also of entanglement, and soft power.

5.5 Modelling the vulnerability of the undersea cable system

Very little is known about the vulnerabilities of undersea cables. For this reason, we developed a model to represent the sources, the interconnections, and the effects of different forms of intrusions on cyber-based operations (Siechrist, Viahnav, Goldsmith)

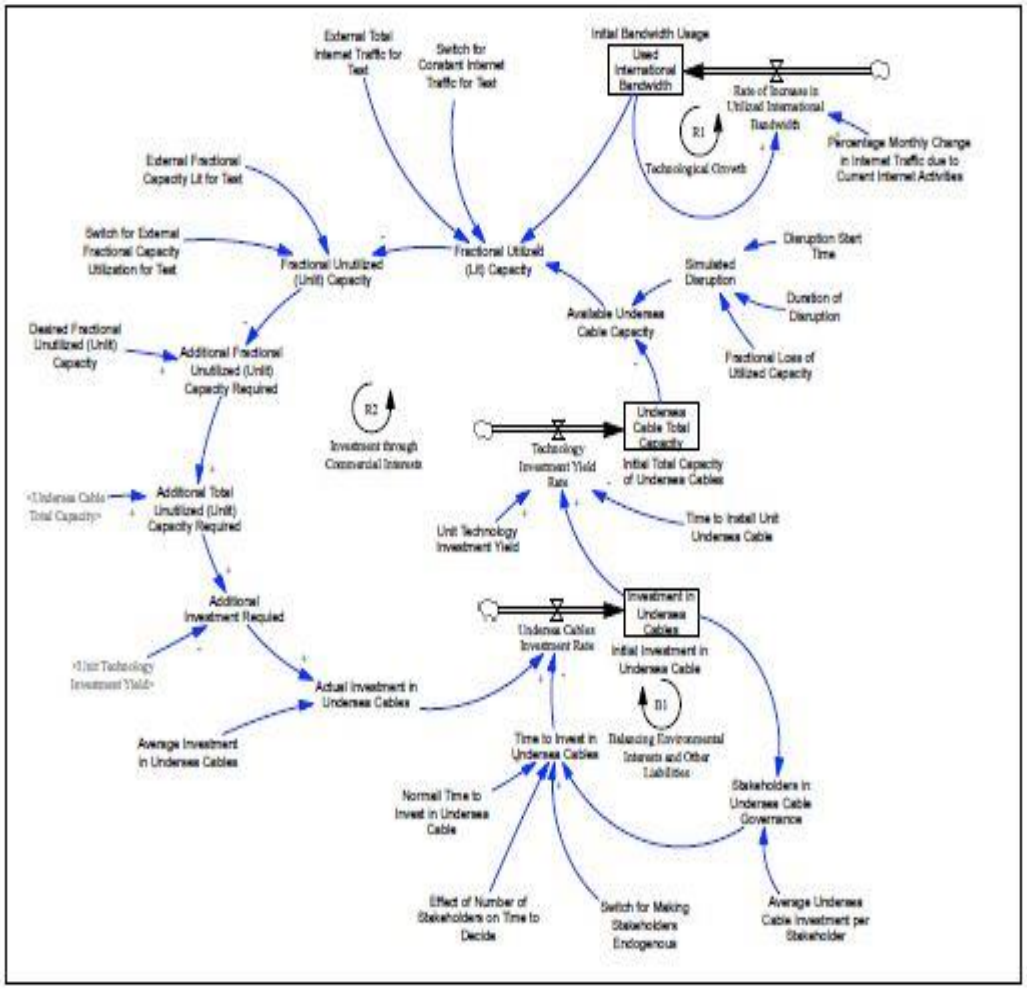

Figure 4.9: Modelling the Vulnerability of Undersea Cables-Dynamic Process
Source: Siechrist, Viashnav, Goldsmith

5.6 Comparative Analysis of Cyber Conflicts

ECIR conducted a systematic re-analysis of cases developed by the Atlantic Council yielded information about the targeted layers of the Internet and attendant implications. Based on materials from the Atlantic Council, we developed a case study for each conflict based on a common framework designed to facilitate comparison. These are in Table 5.1 below.

Table 5.1 Comparative Analysis of Cyber Conflicts

CASE	TARGET LAYER(S) of the INTERNET
1.Cuckoo's Egg	**Physical**. Hess accessed data stored on hardware at the target installation.
2. Morris Worm	**Physical**. The worm overloaded the infected hosts resulting in disabled hardware [4]. **Application**. Morris's spread mechanism used applications such as SEND MAIL [92].
3. Dutch Hackers and British Hackers	**Information**. Espionage operations that seemingly do not attack infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
4. Operation Solar Sunrise	**Logical** and **Information**. The former due to the implantation of malware for espionage purposes, and the latter because of the espionage operation.
5. Moonlight Maze	**Information**. Espionage operations that seemingly do not attack infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
6. Electronic Disturbance Theater	**Physical** and **logical**. Distributed Denial of Service (DDoS) attacks affect both the infrastructure (physical) and its ability to carry traffic (logical).
7. ILOVEYOU	**Information**, **logical** and **physical**. The primary intent of the virus destroyed files (information), while the secondary DDoS resulted in an attack to both the physical (infrastructure) and logical (ability to carry traffic) layers.
8. Patriotic Hackers	P**hysical**, **logical**, **information** and **user**. DDoS resulted in an attack to both the physical and logical layers. Altering data on hosts with malicious intent relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.
9. Chinese Cyber Espionage	**Information**[1]. Espionage operations that seemingly do not attack _ infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
10. Estonia receives cyber attacks	**Physical**, **logical**, **information** and **user**. DDoS resulted in an attack to both the physical and logical layers. Posting data on hosts (websites) relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.
11. Russo-Georgian War	**Physical**, **logical**, **information** and **user**. DDoS resulted in an attack to both the physical and logical layers. Altering data on hosts (for defacement or otherwise) with malicious intent relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.
12. Operation Buckshot Yankee	**Information**. Espionage operations that seemingly do not attack infrastructure (physical) or protocols and applications (logical) are classified as targeting the information layer.
13. Conficker	**Physical**, **logical** and **information**. Conficker takes part of the computing capabilities of its victims, and transmits using removable media [59] resulting in an attack to the physical layer. It modifies the software of the host to prevent being detected (information), and spreads through the Internet (logical).
14. Stuxnet, Flame and Duqu	**Physical**, **logical**, **information** and **user**. DDoS (on third parties) resulted in an attack to both the physical and logical layers. Stuxnet also caused malfunction of hardware (physical). Altering data on hosts (for avoiding detection or otherwise) with malicious intent relates to the information layer. Finally, the attacks were targeted at actual groups, affecting the user layer.

[1] The attack on cyber sites might have involved other layers, but there isn't enough information available (from the sources reviewed for this paper) to assess it. In general, this case deals with extraction of information.

15. WikiLeaks	**Physical**, **logical**, **information** and **user**. The main operation of WikiLeaks was public release of information. Anonymous targeted DDoS attacked the remaining layers. Defensive measures dealt with users.
16. Edward Snowden NSA leaks	**Information** and **user**. Snowden's actions were focused on releasing secret information, related to specific agencies in the United States and elsewhere (user).\
17. Hackers Intrude into New York Times	**Physical**, **information** and **user**. Installing malware tools resulted in an attack to the physical layer. The episode was targeted, affecting the user layer. Accessing non-public information resulted in an attack to the information layer.

Source: Alex Gamero

5.7 Perspectives on Cybersecurity

Almost everyone recognizes the emergence of a new challenge in the cyber domain, namely *increased threats to the security of the Internet and its various uses.* Seldom does a day go by without dire reports and hair raising narratives about unauthorized intrusions, access to content, or damage to systems, or operations. And, of course, a close correlate is the loss of value. An entire industry is around threats to cyber security, prompting technological innovations and operational strategies that promise to prevent damage and destruction.

Explanations as why cybersecurity has attained such a high degree of salience are far greater than is our understanding of the basic parameters in any matter touching on security, at all levels of analysis, namely: *who does what, when, why, how, and with what effect.* Most of the time it is possible to reconstruct the damage-episode and develop some hypotheses about several of the basic factors. But seldom, if ever, do we obtain a full reconstruction of the episode in all of its manifestations.

A "reasoning exercise" undertaken by students in the new class at MIT on *Cybersecurity* in the Department of Political Science at MIT examined this issue from multiple perspective. Appendix A-6 presented the Table of Contents. The full report is on the ECIR website.

In this introduction we begin with a simple example to illustrate the reasons surrounding ambiguity or absence of definition, as well as what might be some attendant implications. Then we highlights, in a sentence or two, the contributions of each of the essays that follow.

5.8.1 The Cyber Domain: Alternative Views

Our "reasoning excessive" was designed as a multidisciplinary and multidimensional initiative and, to the extent possible, empirical grounded and policy relevant. At least three different "definitions" of cyberspace were put forth.

First is the *technical focus*, put forth as the engineer's view, in Figure 1.1 below. All of the properties noted are critical and relevant. These may be necessary but are they sufficient to help shape effective framing of "cybersecurity". If so how? If not why not?

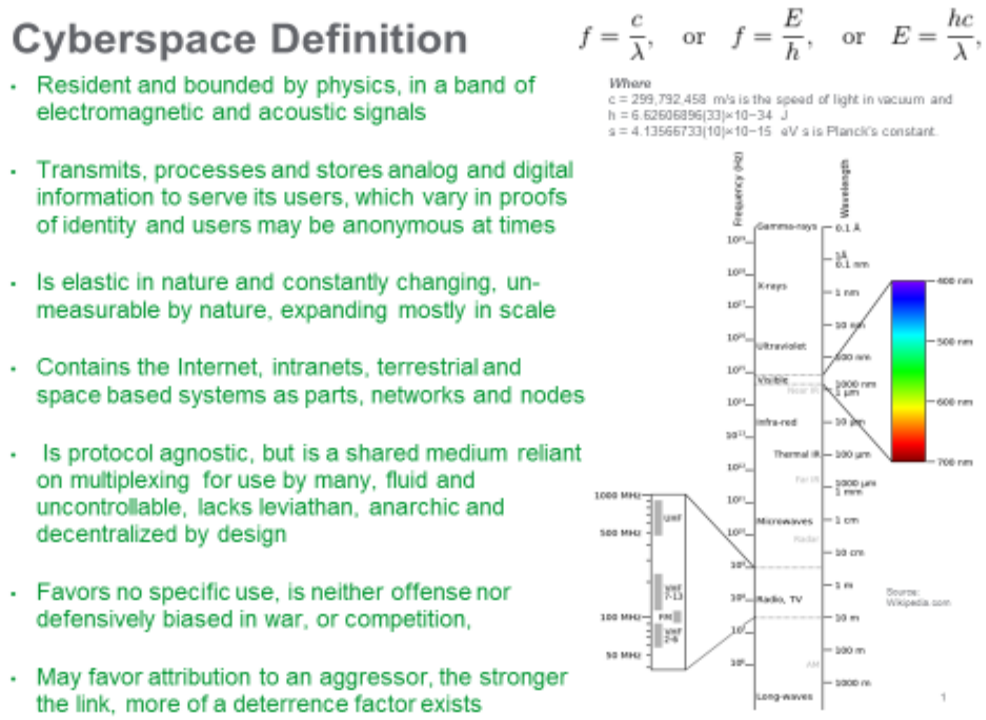

Figure 5.1

Source: George Wren. MIT Cybersecurity Seminar, Spring 2015.

Second is the *content focus.* Without undermining the technical infrastructure and underpinnings, this perspective on cyberspace broadens the framing and structures it around matters of information. As with the first focus, it is reasonable to state that all the features in future 1.2 may be necessary, but are they sufficient to help framing cybersecurity? If so how? If not why not?

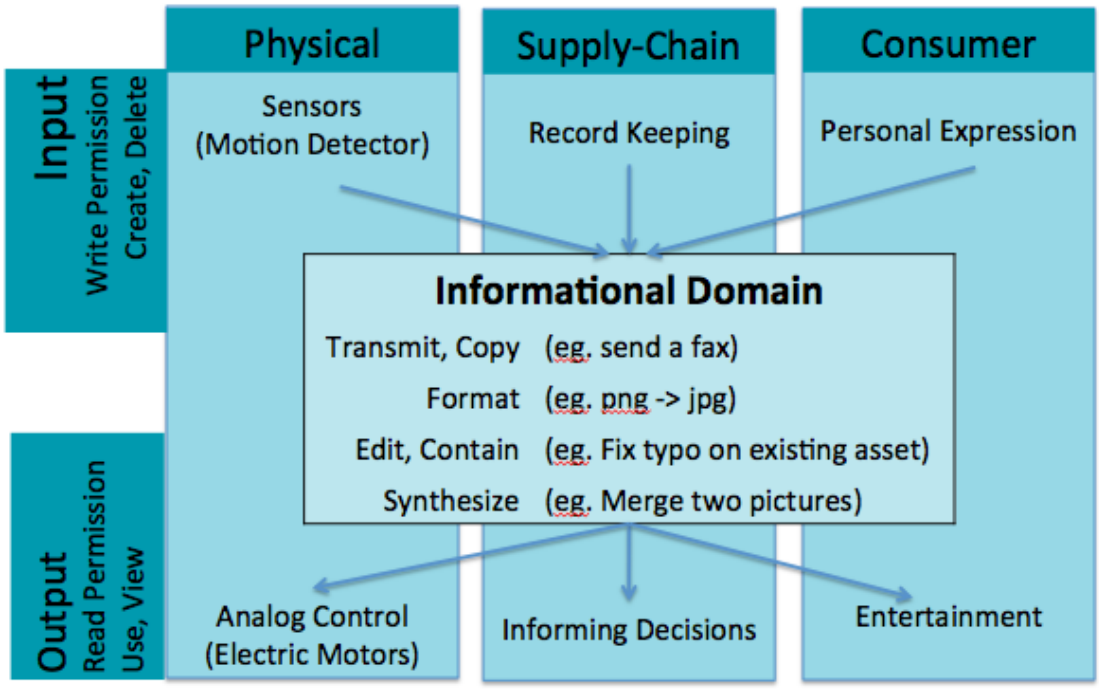

Figure 5.2

Source Lyla Fisher, Cybersecurity Seminar, 2015.

Third is the *global view* this view sees cyberspace as a constructed domain of interaction. Shown in Figure 6.3 its scale and scope is greater than the first and second views. But we must still ask the question: These features are all necessary but are they sufficient to help frame "cybersecurity?

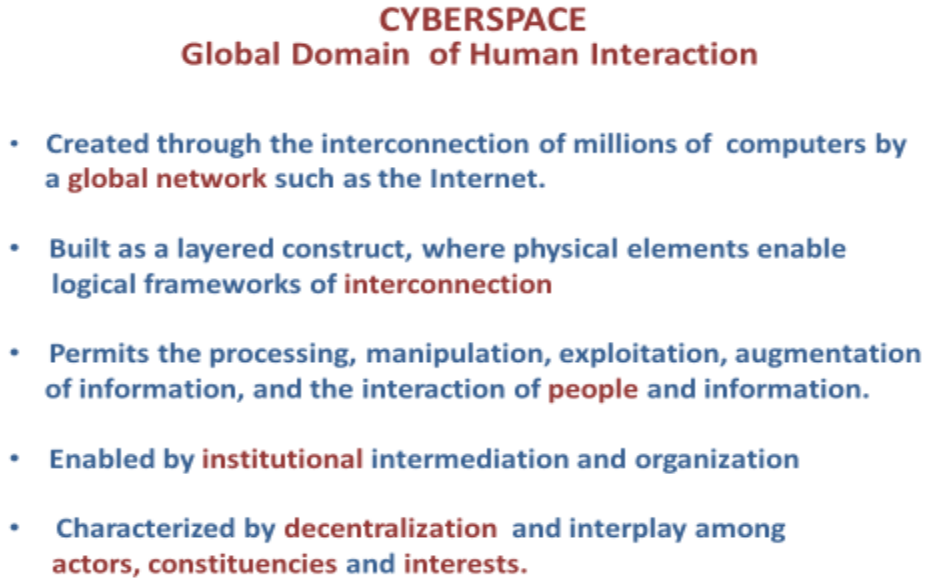

Figure 5.3

Source: Nazli Choucri , MIT Cybersecurity Seminar, spring 2015

5.8.2 Implications

Each of these perspectives focuses on different manifestations of the cyber experience. It should come as no surprise that there are differences, or that the in the best of all possible worlds, the conception of cybersecurity derived from each of the above should be mutually supportive and integrative rather than mutually exclusive and competitive. Interestingly, each appears to be predicated on different phases in the construction and diffusion of the internet worldwide.

The first view is clearly architecture based. It implies that the "solution" to the cybersecurity problem (however defined) is to be found in the design itself and that the "flaws" can be corrected in that context thus reduce threats to cybersecurity. This is a view that minimizes the human or the institutional and organizational elements, but it reminds us that during the early design phase of the Internet matters of security were not salient. Of importance was building an operational global network rather than a network that is operational, global, as well as secure.

Implied in the above is something of an explicit trade-off. But there was no tradeoff at the time, as there was no security issue at stake then. Interestingly, cybersecurity became an issue as the global network extended its scale and scope, and users with different norms, values, and preferences took stock of the cyber possibilities and potential "venues" for pursuing their objectives. None of this reduces the value of the first view, rather it provides a contest for its importance.

The second view reflects the phase at which the Internet became reliable worldwide – at least relative to earlier experience – and content rather than reliability is viewed by users to be the central value. With increasing evidence unauthorized access – and the apparent ease with which this can be done – an added dimension of concern emerged, namely the protection of content. At this point, the Internet is

no longer in "US hands" so to speak, but its very success as a revolutionary technology empowers others in ways that were not possible earlier.

And this leads to the consolidation of the third view. The proverbial "others" are conceivably anyone that has access to the Internet. And with this eventuality can a concern about the intent of those "others" as well as the sanctity of the global network and the reliability of the institutions established to manage different parts of the Internet and sustain its globalization.

The following proposition is put forth: *a coherent view of cybersecurity is one that spans conditions in the technical and operational domain, incorporates all matters of content, and extends its scope throughout the "supply chain"*. Here the notion supply chain is used in a figurative rather than literal sense. It refers, *at a very minimum*, to the properties of both structure and process "turned on" by user in the course of engaging in unauthorized access, the intents of the user, and the nature of the content accessed.

It goes without saying that concerns for cybersecurity are driven by the need to protect our own security in the cyber domain. Thus it may be important to distinguish between cybersecurity as the attribute of an actor versus an attribute of the global network as a whole. States and firms generally place their own self-interest first and foremost, and only if necessary do they find it relevant to adopt a broader perspective.

The one critical implication of the above is that different actors are likely to view cybersecurity in different terms. The set of "ingredients" in the overall "mix" of concerns shaping their own conception of cybersecurity may have a common or shared core, or they might not. It is less important to resolve this matter than it is to better understand what might be the perspective of other actors. At this point in time, the salient "other" is China. It intents are suspicious and its capabilities are growing.

6. CYBER GOVERNANCE:

HOW the CYBER SYSTEM is STRUCTURED and DISCIPLINED

This segment of the ECIR scientific research consists of distinct investigations, each generating specific results about the nature of cyber governance. We summarize here three research activities based on different methods and analytical tools.

6.1 Mapping Authority and Governance for the Cyber Domain

The increased density of decision entities worldwide creates challenges for governance in the physical as well as cyber arenas. Results include:

- *Mapping the new global parameters* created by (i) the state system as a latecomer to matters of cyber governance; (ii) intersections with the private sector entities; (iii) the role of non-state actors; (iv) emergent contentions between established institutions (such as ITU) and the cyber-centered ones (such as ICANN), and (iv) consolidated political contentions with potentials for strong cleavages worldwide (Choucri, Clark)

- *Generating Empirical evidence* of the growth of actors managing cyberspace and the contentions created by the increasing density of decision-entities (Choucri)

- *Mapping the governance "ecosystems" of cyberspace provides* an overarching perspective on how the virtual domain is managed, i.e. who does what how and why, Figure 4.10 Below shows a stylized view of the results we have obtained. Note the core functions of each of the three individual ecosystems, and the linkages among them. (Chueng, Bradner, Choucri)

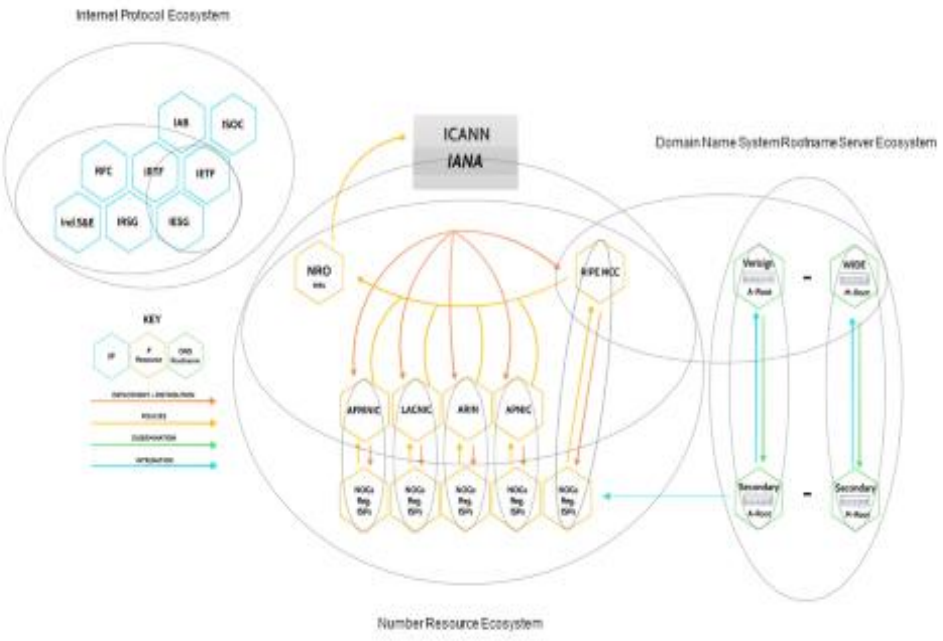

Figure 6.1: Governance of the Cyber Domain
Source: Cheung

6.2 *Norms for Cyberspace*

The role of norms is a critical element in the development of international cooperation. This issue was explored in three different contexts:

- *Framing and exploring* two different hypotheses: cyberspace lacks operational norms vs. norms are already in place,
- Differentiating between norms for *management of the Internet,* vs) norms for interaction and *conduct in cyberspace;* and
- Identifying the specific *formal and informal norms* among Internet technical operators (Hurwitz, Sowell)

6.3 *Power of Private Authority*

The management of the Internet is currently done by a wide range of private sector and informal close-knit organizational modes. These informal systems are under pressure from the more established entities, in both the cyber and the traditional domains. Based on diverse methods, results showed:

- The structure of *hidden vs. formal* operational governance of the Internet at the local levels based on detailed cases and interview methods (Sowell)

- The *self-damaging tendencies* in business responses to cyber intrusion or damages demonstrated via the use of system dynamics modelling and simulation (Goldsmith and Siegel)

- The *action-reaction chain* across cyber and physical domains as governments seek to resist pressure or prevent revolution (Rady)

- The use of *anonymous* proxy networks to support pressures on governments, with applications to revolutionary movements, case studies of Egypt and Iran See Figure 4.11 (Rady)

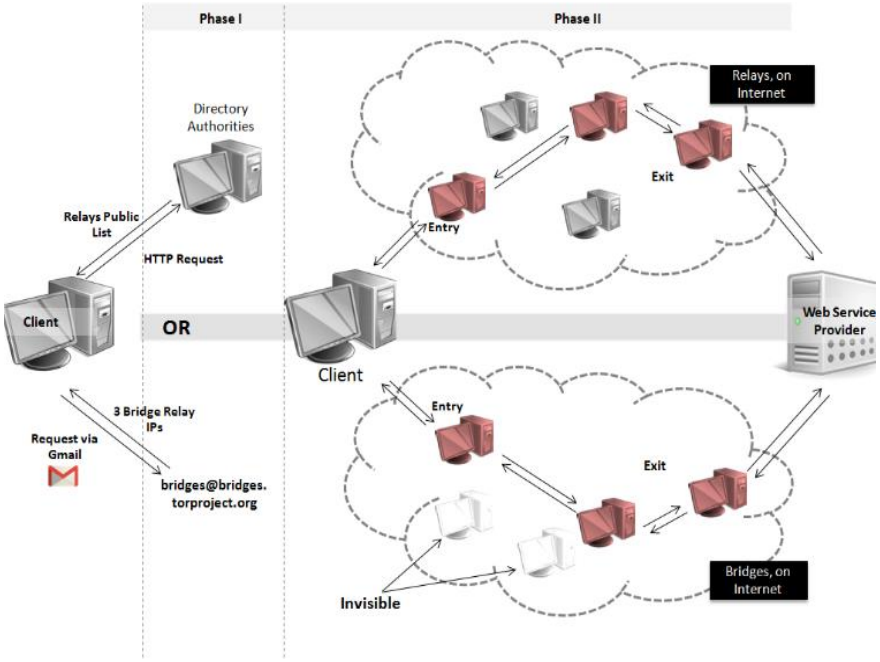

Figure 6.2: Overview of the TOR Mechanism
Source: Rady.

6.3 Resilient Mechanism Design

Mechanism design is about framing a negotiation context that will enable good *outcomes*, under conditions of incomplete but crucial information held by the players, and to do so with realistic assumptions. Establishing the rules under which negotiations will take place is an essential prerequisite to the process itself. The assumptions are that (a) the players only approximately

know what they want; (b) they do not want to tell the overarching arbiter or decision maker; and (c) they will collude if this may make them better off. The results consist of:

- *Improved framing* of such mechanisms – often seen as a mixture of game theory, secure protocols, and algorithms – to facilitate policy-relevant application (Micali).

- Initial application to *evolving negotiations* on cyber management in the context of international organizations (Micali, Chen, Choucri).

6.4 Institutions for Cyber Security

In response to increasing threats to cyber security, the international community established formal mechanisms to identify, monitor, and mitigate the damages. ECIR empirical and comparative investigations show that:

- While the institutional landscape is becoming increasingly dense; coordination integration, and shared responses *mechanisms lag far behind*.

- Despite the expansion of these institutions, we have found there are major inconsistencies among them in conceptual orientation and data making capability (Ferwerda, Choucri, Madnick)

- Built-in limitations are created initially by their "bottom-up" institutional design and then reinforced by business as usual (Ferwerda, Madnick)

7. ALTERNATIVE FUTURES:

CYBERSPACE and INTERNATIONAL RELATIONS

Many actors influence the present and the future trajectory of the Internet and cyberspace. These include *private* sector actors, *states* and governments*, commercial non-state* actors, *non-commercial* entities, *international institutions,* and various types of *Internet users,* to name the most prominent. The eventual outcomes of power and leverage designed to shape the future could create alternative types of outcomes.

ECIR results include the construction of potential futures based on critical principles of *governance* (sovereign authority vs. private order), on the one hand, and of mode of *interaction* (propensity toward conflict vs. toward cooperation), on the other. The result in Figure 6.1 below signals four different trajectories, each with distinctive features and implication. (Choucri).

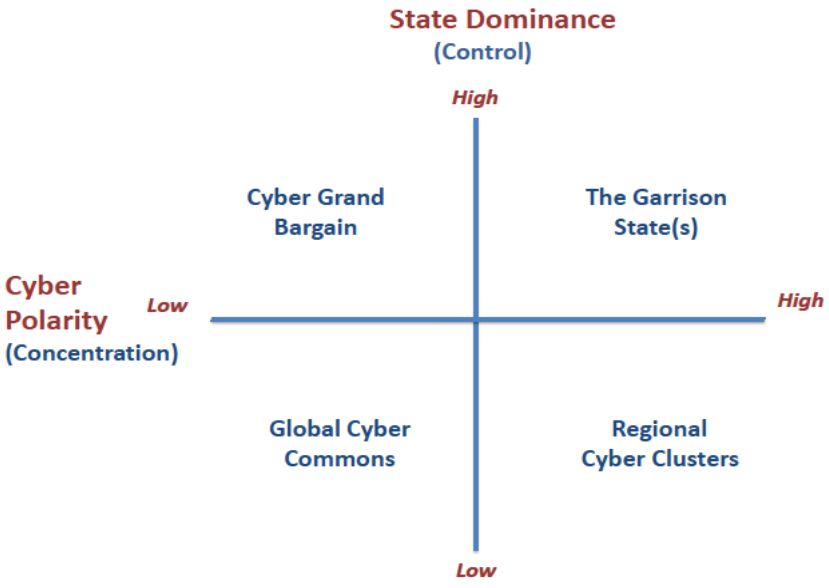

Figure 7.1 Four Futures for Cyberspace
: Source: Choucri

8. CROSS CUTTING ISSUES:

Knowledge System and 21st Century IR Theory

The cross-cutting research issues provide thematic linkages across the entire ECIR research agenda. Here we focus on two issues:

(1) Construction of a joint cyber-IR knowledge system and detailed ontology structure;

(2) Foundations of 21st international relations theory anchored in systems of interactions and interconnected vulnerabilities

8.1 *Construction of Cyber-IR Knowledge System*

We have constructed an operational knowledge system for the Cyber-IR domain, *Cyber System for Strategy and Decision* (CSSD) by:

- Constructing an ontology of the cyber-IR domain and of its broader global context
- Building a web-based customized interactive knowledge networking system devoted to quality-controlled content and materials generated by ECIR and other related research groups.

8.1.1. Ontology Structure

A generic and simplified view of the ontology system is shown in Figure 8.1 which defines the domains of arenas of human interaction.

The ontology is structured in four *domains*:

- Intersection of Cyberspace and International Relations (Cyber-IR)
- Cybersecurity and Sustainability
- Conflict and War
- Governance and Institutions.

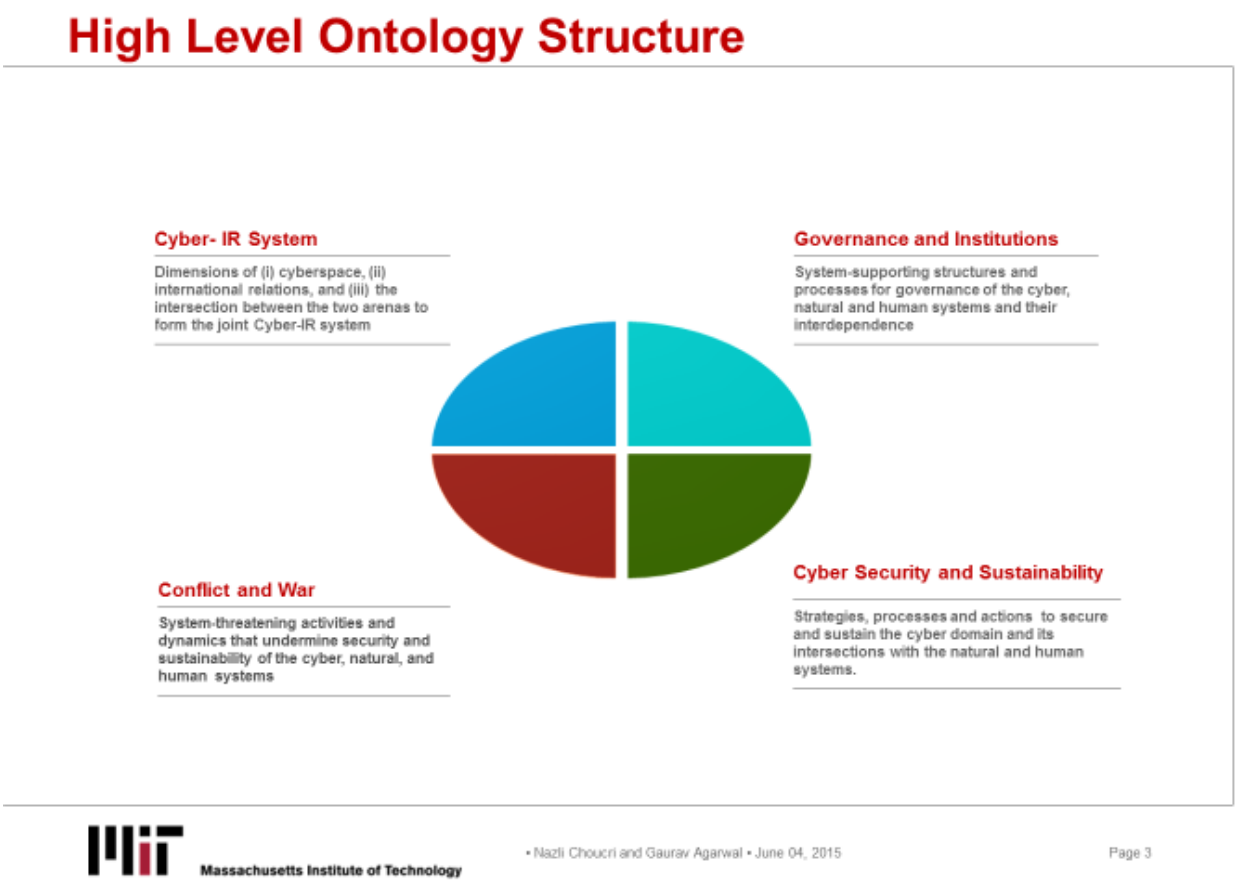

Figure 8.1: High Level View of Ontology Structure
Source: Choucri and Agarwal

Each domains is differentiated into four *dimensions* as follows:

(1) System State
(2) Problems due to human action
(3) Technological and scientific solutions
(4) Socio economic, political, and and regulatory solutions

Each of these dimensions is further differentiated in its constituent elements, not shown here.

8.1.2 The Cyber IR System

Below we show the ontology segment for the Cyber-IR domain. This figure highlights the first and second levels of differentiation beyond the basic dimensions.

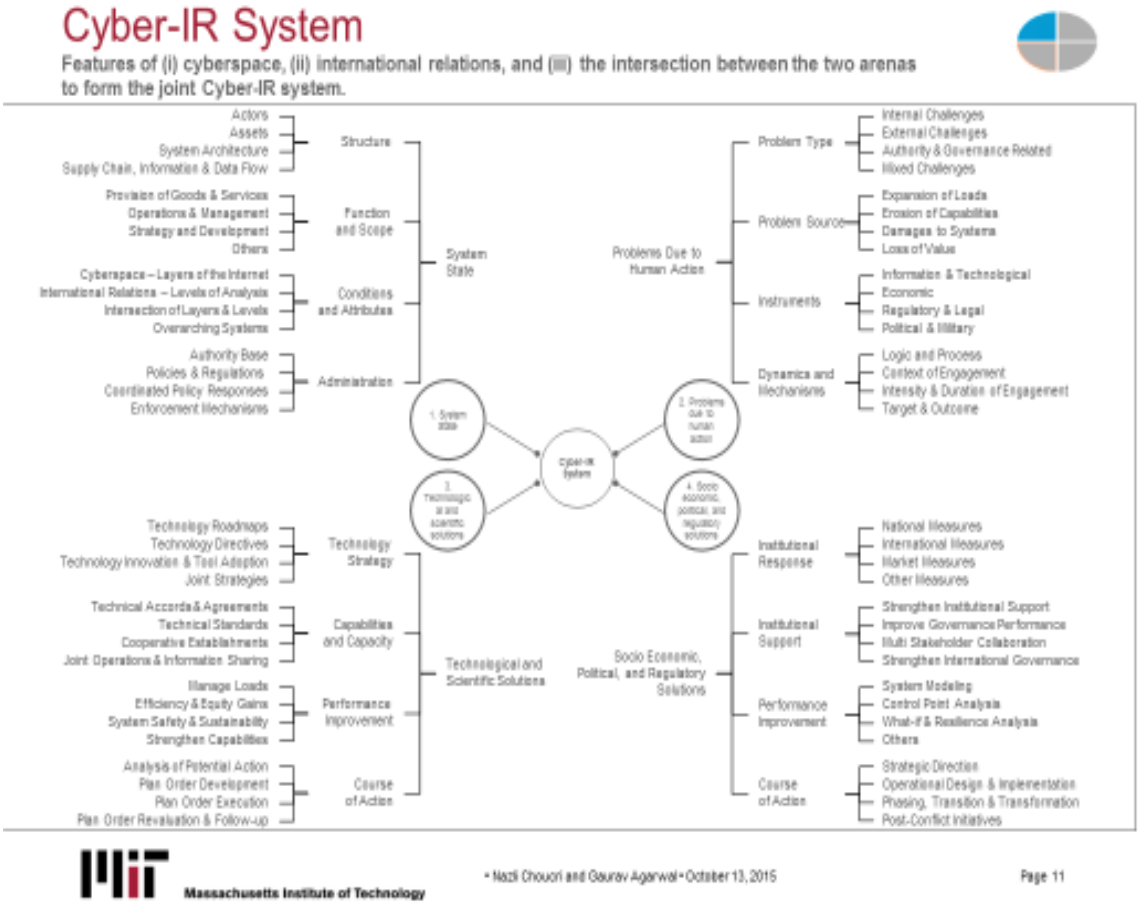

Figure 8.2: The Cyber-IR System
Source: Choucri and Agarwal

The ontology features in Figure 8.2 above are distinct but embedded in an ontology system representing high level features of world politics. In the following section we present the ontology for select complexities in world politics. These provide the context and "environment" for the Cyber-IR system.

8.2.1 Complexities of World Politics for the Cyber-IR System

Integrating the Cyber-IR system into the broader of world politics is provides a more effective view of the 21st century realities. We begin with Figure 8.3 the ontology for Governance and Institutions (top right hand corner of Figure 8.2). Figure 8.4 shows the Conflict and War segment (bottom left). Framed thus, the mechanisms of governance are designed to stabilize societies and protect them from the ravages of conflict and war

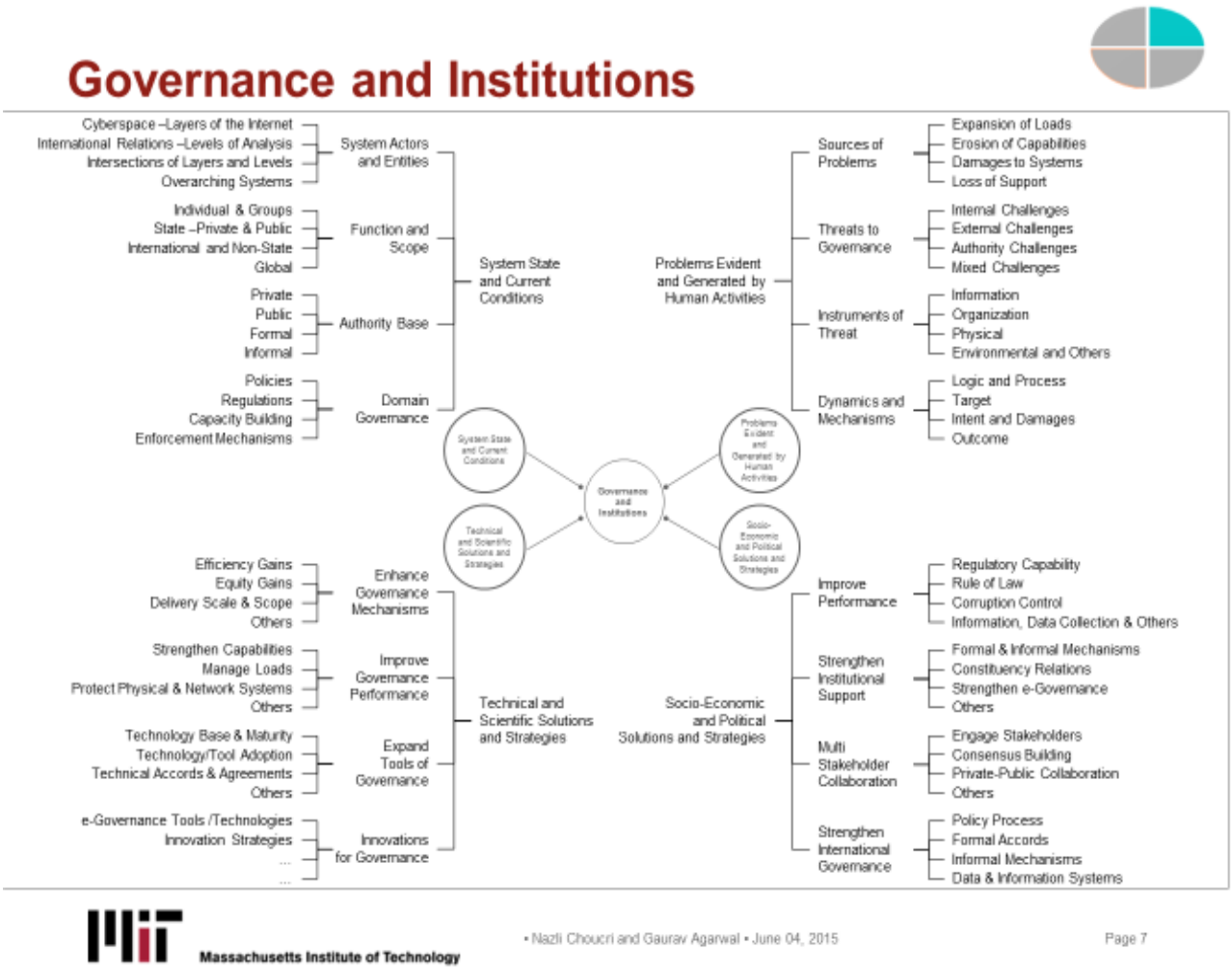

Figure 8.3 Governance and Institutions
Source: Choucri and Agarwal

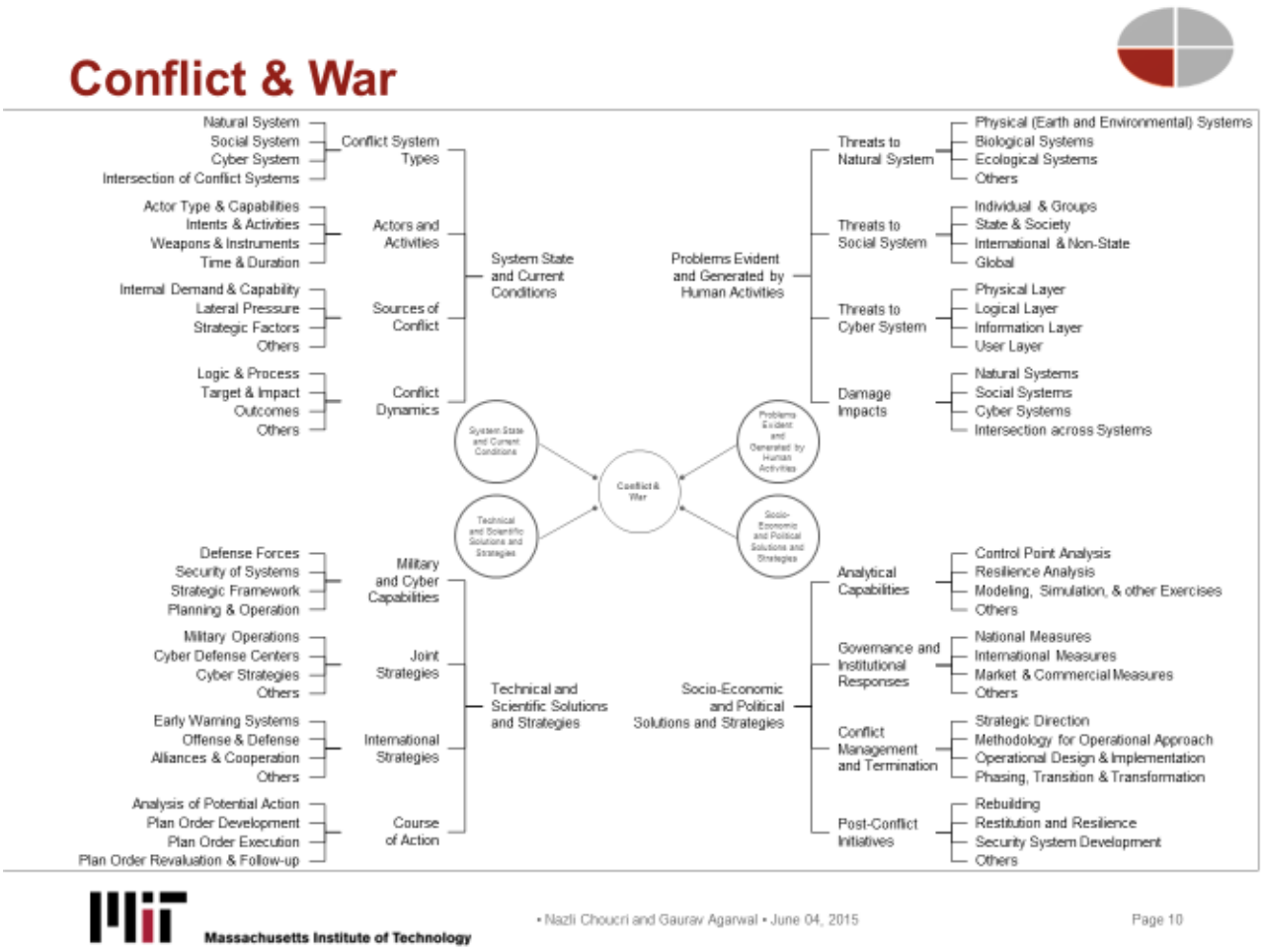

Figure 8.4 Conflict and War
Source: Choucri and Agarwal

The final segment, Cyber Security and Sustainability, is shown in Figure 8.5

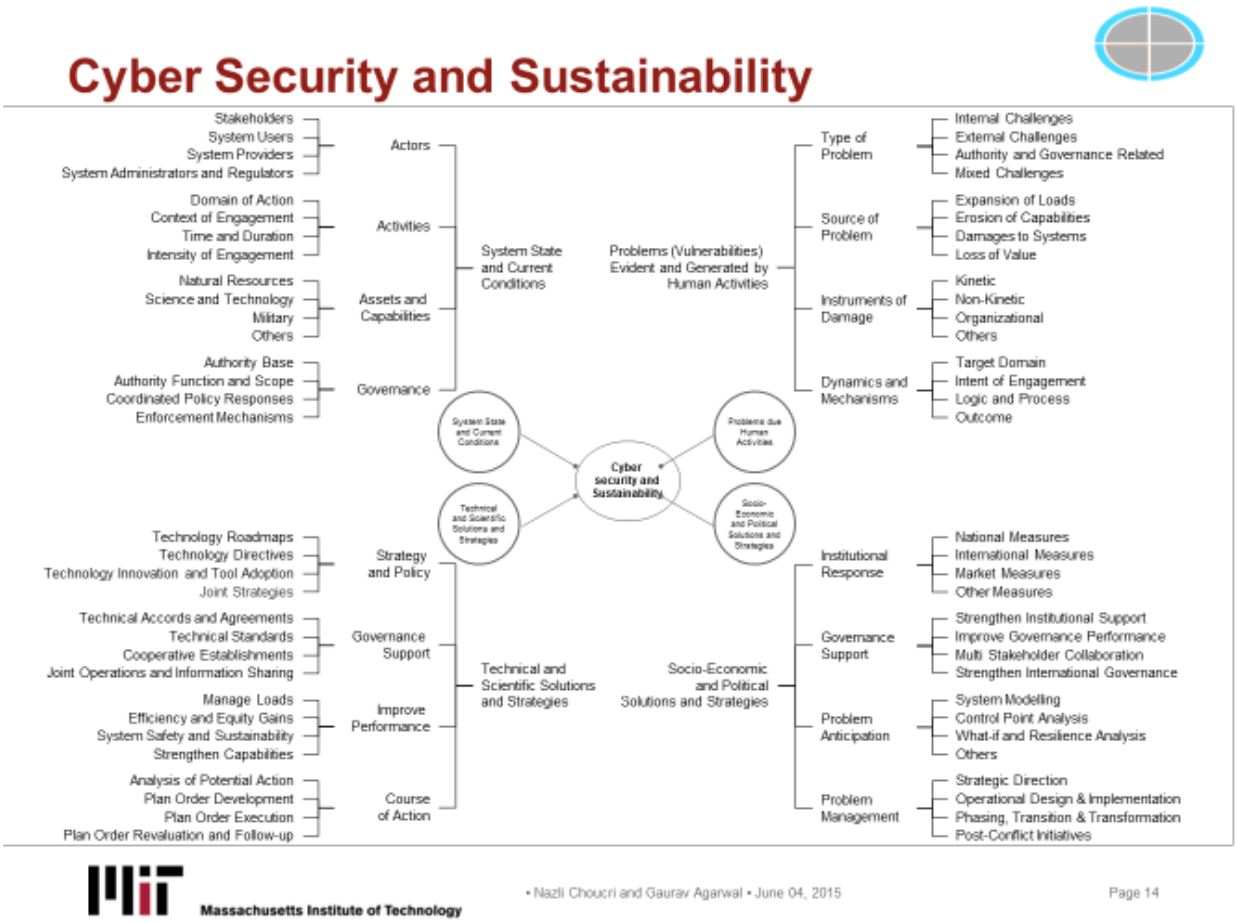

Figure 8.5 Cyber Security and Sustainability
Source: Choucri and Agarwal

8.2 Basics for 21st C Theory

At the beginning of this Final Report we presented, in Figure 1.1, a stylized view of the research challenge for ECIR. Through a set of research steps and attendant results, the question mark in the center has been replaced by the framework of the joint Cyber-IR system. This framework captures the *interconnections* among the two domains of human interactions but does not eliminate the relative autonomy and "power" of each system individually.

We have contributed to International relations theory for the 21st century by giving attention to emergent issues that transcend the bounds of traditional theory.

Recall that Figure 4.4 (in Section 4 above) that puts forth a new perspective on international relations theory, based on the results of ECIR research, a still simplified "mapping" if elements of new theory of international relations. These are only some, not all, of the critical elements for a new theory.

8.2.1 Systems of Interacting Vulnerabilities

Central to the goals of the ECIR project, and especially relevant to theory building for the 21st century is a new framing of the systems of interactions for effective decision-making. Figure 8.6 below displays the closely coupled systems– the human, environmental, and cyber – illustrated with elements that illustrate critical "spillover" effects (Choucri).

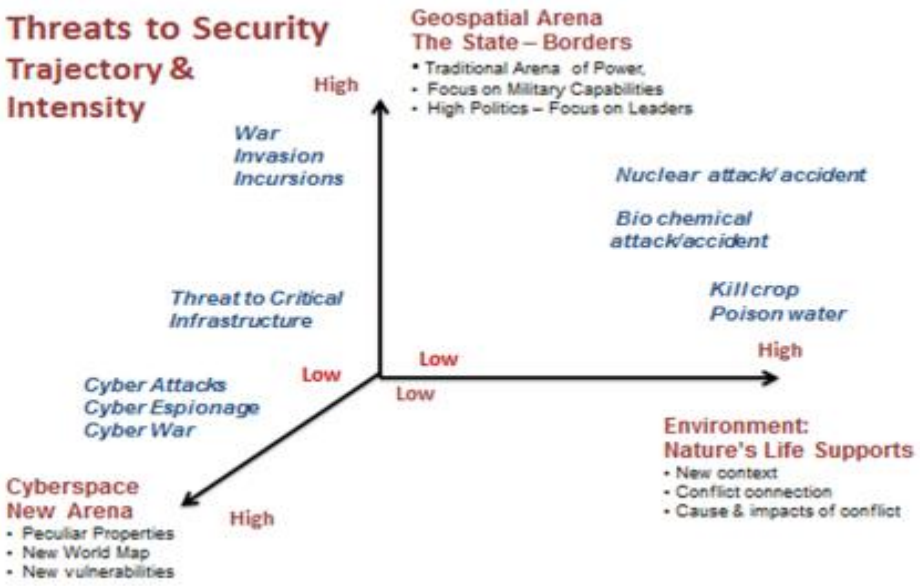

Figure 8.6 Interconnected Vulnerabilities
Source: Choucri

Given the salience of cyberspace and the natural environment as two new domains of interactions of increasing importance in world politics it is essential re reframe the parameters of theory to accommodate 21st century realities. . Put differently, the nature of the "landscape" and the ecosystem in traditional domain is rendered more complex by the creation and expansion of the cyber-based actors highlighted earlier.

Early in in this Final Relations we stated that the integration of cyberspace and international relations is rendered operational by focusing on the intersection of the *layers* of the Internet and the *levels* of analysis in international relations. We now highlight a set of propositions highlighting the new perspective on international relations theory, central to emergent policy and practice

8.2.2 Elements of the New IR Model

What follows are basic elements of the new model. Our purpose is to show how cyberspace has permeated all levels of international relations – influencing interactions within and across levels – and thus demonstrates its ubiquity in world politics. We shall proceed from "bottom-to- top", starting with

the individual. The same core logic holds when we proceed from "top-to-the-bottom". Indeed, "reversing the Images" is a well-known phrase in international relations.

The state system remains critical, but it no longer the only actor wielding the power and influence. Proceeding along the lines of the well-known levels of analysis model, we put forth a set of propositions that reflect developments of theory theory consistent with the 21st C realities.

- As the most discrete decision-maker, the *individual* is an energy-using and information-processing entity, a distinct is also embedded in diverse situational, organizational and institutional contexts, notably those pertaining to the social order, the natural environment, and the cyber arena.

- All individuals and entities generate *demands* of various sorts and are endowed with *capabilities*. Jointly these are essential requisites for engaging in *activity* of any type

- The *state*, increasingly encumbered by increasing demands and constrained capabilities, no longer dominates the international landscape.

- N*on-state* entities – for profit and not for profit – have become major, even defining, actors in world politics.

- *Civil society,* a cross-level social construct, is an aggregation of individuals with demands and capabilities that is distinct, even separate, from the state or organized non-state actors.

- Dominating the cyber domain and its management, is the *private sector* that assumes unprecedented importance in the modern era.

- As late-comer to the cyber domain, the state system is increasingly seeking to reassert a degree of control over its *sovereign domain.*

- *International relations* consists of the actions and interactions among all of the major entities operating across state boundaries – private and public – as well as all organizations composed of these respective actors.

- The *permeability* of influences across the levels of analysis conditions and behaviors at one level can influence, directly or indirectly, structure and process within and across other levels.

- Increasingly, the increasing interconnections among the *cyber, social, and natural domains* due to human activity create new complexities for policy and practice, the full nature of which is

- Differential *rates of change* in capabilities – growth and development of actors, private and public-- alter the power distribution internationally well as the salience of levels and the politicization of the domains,

- The power of *generativity* at all levels and contexts – due to interactions of people, resources, and technology -- can create new configurations of social interactions and power relations

- All entities, systems, structures and processes -- social, cyber, and natural – are embedded in an overarching g*lobal system* (a fourth level of analysis

- The basic premises of world political remain – namely the pursuit of power and the pursuit of wealth – but the actors, entities, instruments and tools are increasingly diverse and complex.

- The entire system "hangs together" through the (a) the institution of sovereignty, (b) the dynamics of feedback; (c) the power of generativity; and (d) the promise and uncertainty of technological change.

Any one of these propositions is a departure from traditional theory in international relations; jointly they contribute to forging new directions for theory, policy and analysis. It is with this set of "lenses" that we can begin to frame international relations in the cyber age. Each of these features can also be considered as "tools" to explore particular linkages of the cyber and the traditional domains, and may well create greater mutual sensitivity and interdependence among actors – the old and the new.