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

JOINT RESEARCH TEAM

M.I.T

Nazli Choucri – PI	Political Science
David D. Clark	Computer Science and Engineering
Roger Hurwitz	Political Science
Stuart Madnick	Business and Management – Sloan School
John Mallery	Political Science
Silvio Micali	Computer Science and Engineering
Michael Siegel	Business and Management – Sloan School
Patrick Winston	Computer Science and Engineering

Research Associates - MIT

Daniel Goldsmith
Shirley Hung
Chintan Vaichnav
Cindy Williams

Harvard University*

Venkatesh Narayanamurti – Co-PI	Science and Technology – Kennedy School
Richard Clarke	Government – Kennedy School
Jack Goldsmith	Law School—Harvard University
Melissa Hathaway	Government – Kennedy School
Joseph Nye	Government – Kennedy School
Eric Rosenbach	Government – Kennedy Schoo

*Members of the core research team at its origin. Richard Clarke and Eric Rosenbach took on other responsibilities early in the project period.

ECIR Joint Policy Committee

Nazli Choucri
David D. Clark
Stuart Madnick
Venkatesh Narayanamurti

CONTENTS

APPENDIX

A-1 PRODUCTION of NEW KNOWLEDE MATERIALS

- List of Publications, Papers, Research Results

A-2 BOOK PUBLISHED

CYBERPOLITICS in INTERNATIONAL RELATIONS

- Table of Contents

A-3 BOOK COMPLETED

ECIR STUDIES: CYBERSPACE and INTERNATIONAL RELATIONS

- Table of Contents
- Chapter Abstract

A-4 BOOK COMPLETED

THE CO-EVOLUTION DILEMMA: CYBERSPACE and INTERNATIONAL RELATIONS

- Table of Contents

A-5 Report on: PERSPECTIVES on CYBERSECURITY

- Table of Contents

A-6 ECIR WORKSHOPS

- Co- Sponsors
- ECIR Workshops
- Affiliated Workshops

A-7 HARVARD POLICY SEMINAR

- List of Speakers

PART I

BRIEF OVERVIEW

Part I presents a high level view of the Final Report. Beginning with a brief Introduction it identifies the research challenges, the methods used, the basic results, and the publication.

It also presents a brief note on sharable resources generated and information about courses developed.

Especially relevant is the education of students, researchers, and policy analysts.

Each of these, and related topics, is addressed in greater details in other Parts of this Report.

INTRODUCTION

In international relations, the traditional approaches to theory and research, practice, and policy were derived from experiences in the 19th and 20th centuries. But cyberspace, shaped by human ingenuity, is a venue for social interaction, an environment for social communication, and an enabler of new mechanisms for power and leverage. Cyberspace creates new conditions—problems and opportunities—for which there are no clear precedents in human history. Already we recognize new patterns of conflict and contention, and concepts such as cyberwar, cybersecurity, and cyberattack are in circulation, buttressed by considerable evidence of cyber espionage and cybercrime.

Research Challenge

The research problem is this: distinct features of cyberspace—such as time, scope, space, permeation, ubiquity, participation and attribution—challenge traditional modes of inquiry in international relations and limit their utility. The interdisciplinary MIT-Harvard ECIR research project explores various facets of cyber international relations, including its implications for power and politics, conflict and war.

Our primary *mission* and principal goal is to increase the capacity of the nation to address the policy challenges of the cyber domain. Our research is intended to influence today's policy makers with the best thinking about issues and opportunities, and to train tomorrow's policy makers to be effective in understanding choice and consequence in cyber matters.

Accordingly, the ECIR *vision* is to create an integrated knowledge domain of international relations in the cyber age, that is (a) multidisciplinary, theory-driven, technically and empirically; (b) clarifies threats and opportunities in cyberspace for national security, welfare, and influence;(c) provides analytical tools for understanding and managing transformation and change; and (d) attracts and educates generations of researchers, scholars, and analysts for international relations in the new cyber age.

Research Agenda

The research agenda converges around five topics:

- *Framework: Foundations for Theory and Policy*
- *Cyber Power, Cyber Security, and Cyber Conflicts*
- *Cyber Governance: How Behavior is Disciplined*
- *Alternative Futures: Drivers of Change*
- *Cross-cutting Issues: Methods and Techniques*

These are discussed in some detail in Part II. Note that the cross-cutting issues are four-fold, as follows: (1) contribution of a joint cyber-IR knowledge system; (2) Integration of the

cyber-IR system in the complexities of world politics; (3) Systems of interactions as interconnected vulnerability domains, and (4) Foundations of 21st international relations theory.

Methodology:

By necessity, we draw upon a diverse set of methods, theories, and tools—from social sciences, international studies, policy and risk analysis, communication studies, economics, management, computer science, and law—to explore utility of existing methods and to develop new techniques. These include:

- *Domain Representation* – Integrating Empirically Cyberspace and International Relations
- *Data Development and Empirical Analysis*: Focusing on and analyze actors, actions and impacts
- *Dynamic Modeling, Simulation, and Policy Analysis:* Providing tools for analysis and policy
- *Cross-School Participation:* Involving MIT and Harvard faculty, research fellows and affiliates
- *New cyber system and cyber policy courseware*, case studies, scripting, and delivery

Sharable resources generated:

Data Resources:

Cyber System for Strategy and Decision (CSSD) Second generation of MIT's Global System for Sustainable Development spanning the Cyber-IR domain Ontology-based and curated evolving knowledge data base consisting or tagged searchable abstracts with links to source.

Cybersecurity Wiki Harvard's Berkman Center for Internet & Society (with Science, Technology, and Public Policy Program) http://h2odev.law.harvard.edu/playlists/633

ECIR Data Dashboard designed to provide scholars, policymakers, IT professionals, and other stakeholders with a comprehensive set of data on national-level cyber security, information technology, and demographic data. (See http://coin.mit.edu:8080/Dashboard).

Computational Taxonomy Generation System to extract taxonomies or ontologies from large-scale data base systems of journals. Tested and applied to "cybersecurity" and "cyberspace".

Courses and Materials:

Cybersecurity Model Curriculum Harvard's Berkman Center's tool providing resources with elements of the course plans and "drag and drop" to create customizable syllabi.

Cyber Politics in International Relations, MIT Political Science with participation from Computer Science and Management.

International Relations Theory in the Cyber Age, MIT Political Science MIT

Cybersecurity and the Future of Cyberspace, MIT Political Science Department. MIT Political Science with participation from Computer Science and Management.

Publications through this Minerva research:

Books:

- Choucri, Nazli. 2012. *Cyberpolitics in International Relations.* Cambridge, MA: MIT Press
- Choucri, Nazli, David D. Clark and Stuart Madnick edited. volume. ECIR Studies on *Explorations in Cyber Politics for the Cyber Age,* completed.
- Choucri, Nazli and David D. Clark**.** *The Co-Evolution Dilemma: International Relations in the Cyber Age***,** completed
- Ellis, Ryan. *The Politics of Critical Infrastructure Protection*, book ms submitted for review, 2015.

Articles: other Publications, and Solicited Book: See Publication List in Appendix A-1

Education of Student, Researchers, and Policy Analysts

Fifty-Six (56) individuals graduated from ECIR -- *excluding* student participants in the new courses. The list of individuals is presented in Part III – Section 10 – along with basic information.

1. SCIENTIFIC and TECHNICAL OBJECTIVES

1.1 Introduction

Everyone recognizes the salience of cyberspace in the world today – the threats, challenges, and opportunities – but there is limited understanding of how cyberspace influences international relations and how power and politics in international relations influence the conduct and management of cyberspace. Cyber threats to national security are apparent after the fact, and little anticipatory capability has been developed to help shape policy responses under different contingencies. For the most part everyone tends to be operating under the dominant assumptions of the 20th century politics and policy in an increasingly uncertain world of the 21st century whose parameters are still in the making. We are now deeply rooted in the cyber age, and its rapidly changing configurations.

To simplify, cyberspace is a new arena of interaction with many features still fluid and subject to development and change. International relations, is a well-established domain of activities for state and non-state actors of unequal power and capabilities, operating in physical environments beyond their own territorial boundaries, and whose behaviors are shaped by long traditions of norms, principles and institutional directives.

So far, they have been viewed largely as independent arenas of interaction. But realities impinge, and we now appreciate their interconnections and interdependence. The details have yet to be developed. In response to new 21st C realities shaped by the salience of cyberspace, the goal is to construct a cyber-inclusive view of international relations (Cyber-IR System) – with theory, data, analyses, simulations – to anticipate and respond to cyber threats, impacts on power politics, and challenges to national security and international stability.

1.2 Need for New Knowledge

While many features of international relations can be explained and understood without reference to the overall cyber domain, many more, if not most, require a cyber-centered perspective that intersects with and bears directly upon international relations. We have excellent maps and visual materials for international relations and its various facets. We also have maps of cyber access, different representations of traffic, and different features of cyberspace.

There is limited understanding of how cyberspace influences international relations and how power and politics in international relations influence the structure, process, and management of cyberspace. Dominant assumptions of the 20th century politics and policy are severely undermined by the 21st century and the cyber age with its dynamic and changing configurations. The knowledge gap is profound: There are excellent maps and visual materials for international relations and for different features of cyberspace.

Missing, however, is a combined view so essential for understanding today's realities and anticipating future directions. Without a "map" to navigate its joint international relations and cyber features and their interdependence, a viable theory thereof, and mechanisms for tracking potential threat, it is unlikely that we can fully understand what it is, let alone identify threat points and their underlying trajectories.

The ECIR Project responded to a critical need at this point in time, that is, a rethinking of core assumptions of structure and process in international relations as well as a reassessment of methods and tools required for navigating through the joint complexities of cyberspace as these bear on the security of the nation, and the stability and wellbeing all individuals, societies and states, as well as the entire international community.

1.3 Vision for Theory

The major objective of the ECIR research program is to develop approaches to international relations – with theory, data, and methods – responsive to the cyber realities of the 21st century. Its vision is to understand the *mutual and reciprocal interconnections of cyberspace and the international relations* and *create a body of knowledge* that is theory-driven, empirically sound, and technically anchored such that it:

- Clarifies threats and opportunities of cyberspace for national security, welfare, and influence;
- Provides analytical tools for understanding and managing cyber based transformation and change; and
- Attracts and educates a new generation of researchers, scholars, and analysts.

A related objective is to provide the U.S. government with useful tools and insights into the emergent complexity of the new realities. These realities are increasingly shaped by the interdependence between the physical world and the cyber domain.

1.4 Core Challenge

The contrast between the characteristic features of *cyberspace,* on the one hand, and those of *international relations*, on the other, creates significant challenges for theory and policy, nationally and internationally. While both domains are created and driven by human activity the characteristic features of cyberspace are at variance with conventional understanding of, and interactions, in the international arena. Figure 1.1 shows a simplified view of the core challenge for the ECIR initiative.

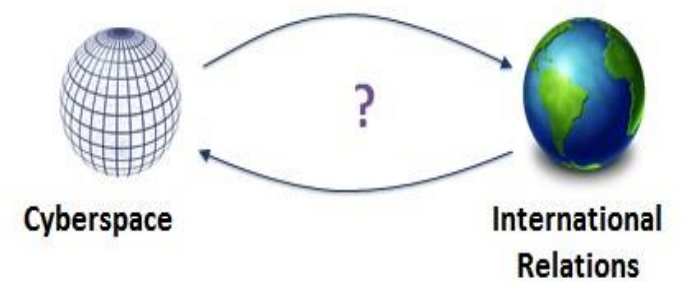


Figure 1.1 The Overarching question

Addressing the question mark in Figure 1 is particularly daunting since the properties of the international system are fundamentally different from those of cyberspace. This challenge is at the core of the ECIR research agenda.

At this time, a *cyber-inclusive view of international relations* has become a necessity rather than simply a convenience. Such a view is missing from the current corpus of scientific knowledge and tools for policy analysis. It must be developed if we are to manage the complex challenges of the 21st century defined in large part by the complexity and the co-evolution of cyberspace and international relations.

Table 1.1 below identifies key cyber features that are particularly problematic for all facets of International relations and world politics related to theory, policy, and practice.

Table 1.1
Cyberspace Challenges to International Relations

- *Temporality* – Replaces conventional time with near-instantaneity
- *Physicality* – Transcends constraints of geography and physical location
- *Permeation* –Penetrates boundaries and jurisdictions
- *Fluidity* – Sustains persistent shifts and reconfigurations
- *Participation* – Reduces barriers to activism and political expression
- *Attribution* – Obscures identities of actors and links to action
- *Accountability* – Bypasses established mechanism of responsibility

Source: Adapted from N. Choucri *Cyberpolitics in International Relations,* MIT Press, 2012.

It is not difficult to appreciate that these features, individually and collectively, challenge the core principles of sovereignty, authority, jurisdiction as well as a whole range of fundamentals that

provide order and stability in the modern world order. Simplistic as that might seem, the essence of ECIR research is signaled by the question mark in Figure 1.1.

1.5 Research Products and Potential Impact on DoD Capabilities and National Defense

Among the products of ECIR are new tools to (a) capture emergent dynamics of the joint Cyber-IR domain; (b) anticipate, track, and clarify cybersecurity and cyber threats; (c) understand and manage worldwide cyber transformation. This enables (d) uses of new "hands on" analyses; (e) strengthens analysis of 21 C. realities; and (f) supports U.S. Grand Strategy.

The following section summarizes the overall research approach – from the basic assumptions to operational methods – and is followed by a concise statement of results.

2. APPROACH and METHODS

In this section, we present the overall ECIR approach and its characteristic features. Here we focus is on the overarching methodology rather than on the details of a particular method or technique. This is dictated by the diversity of techniques utilized as well as those that have been developed in the course of the investigations.

2.1 Basic Assumptions

The ECIR research program is built upon three basic assumptions: (1) the interdependence of technology and policy, (2) the conjunction of uncertainty and regularity in human interactions, and (3) salience of technological change.

2.2 Multi-disciplinary and Multi-methods

ECIR adopts a *multidisciplinary approach* that draws on theories, methods and insights from different fields. These include, but are not limited to Political Science, Economics, Business and Management, Engineering, Computer Science, Artificial Intelligence, and Law and Government. Our approach is based on the view that diversity of perspectives, theories, data and modes of inquiry is essential for our purposes.

The research design is *modular* as it focuses on a set of substantive and methodological issues that are significant in their own right. It is also *interconnected* because the individual pieces are linked to an overarching "whole". The research is organized around *core themes,* defined as distinct investigations. In some cases, the research itself resulted in new methods and tools necessary for navigating through these new complex arenas. By necessity, it is also *multidimensional* to accommodate the features noted in Table 1.1.

First, we present the overarching research challenge or *core themes* (operational goals) of the ECIR research initiative, then we introduce the *cross-cutting issues,* that is, those that bear on all of the core themes. In a later section of this report, we elaborate on each of the core themes and identify the *specific individual projects* – the inquiries and products – with completed reports or nearing completion within each theme.

2.3 Core Research Challenges: Focus and Topics

The first research challenge is constructing the *framework* to represent and explore the interconnections between cyberspace and international relations, based on the *intersection principle* and its application. The results include not only the interconnections between the cyber and the international domains but also the construction of an overarching joint cyber-IR system. All aspects of the research program are derived from and connected to the overall

framework – the foundation for theory. This is the foundation to which all other aspects of ECIR research are connected.

The second challenges focuses on the nature of *cyber power, cybersecurity* and *cyber conflicts,* broadly defined. Among the key questions examined are: Who controls cyberspace? What are the dominant threats to security and stability, for the nation and for the international community? What are the drivers of potential cyber-based conflicts and contentions in international relations? Addressing these questions serves to illustrate the emergent *cyberpolitics* and to consider, for example, how technological innovations associated with expansion of social media affect and external distribution of power and influence, and the political issues that emerge as result.

The third is on *cyber governance*, and examines how behavior is disciplined, taking into account the existing regulatory and institutional frameworks in place as well as those that might be emerging. It also considers different mechanisms to facilitate decisions under various conditions and constraints.

The fourth is to explore *alternative futures* for cyberspace and international relations, with special attention to the future of to cyberpolitics.

The fifth and final research challenge consists of three *cross-cutting issues*, as follows:

2.4 Cross-Cutting: Domain Ontology for Complex Systems

Early on we identified a range of broad issues that are sufficiently compelling as to cut across all research themes and provide the basis of domain ontology for complex systems

2.5 Operational Basics

All of the research activities – for all of the research challenges, core themes and cross cutting themes – involve:

- Development of a *theoretical* approach for integration of cyberspace and international relations.
- Extensive *use of data* and/or data generation techniques, for example, for empirical investigation, or modelling and dynamic simulation, or ontology construction.
- Investigation with different forms of *policy analysis, simulation and modeling*)
- *Relevance for DoD* – the focus is *on* ensuring the *relevance of ECIR research and its products* for U.S. Department of Defense concerns and priorities, as currently expressed in the Minerva Program statements.

3. CONCISE ACCOMPLISHMENTS

The section presents a concise statement of research accomplishments, noting only the highlights in terms of substantive issues and implications. It also provides some basic statistics regarding products. The concise accomplishments can best be framed as follows:

3.1 Results of Scientific Research

First we present an overview of results, then we highlights specific results:

3.1.1 Overview

Results include theory development, data generation, empirical analysis, and new technologies for analytical and quantitative investigations – presented in published form.

Among these are foundations for a theory of cyber-international relations, which identify:

- Actors, actions and outcome
- "Who controls" where, when, and how in the cyber domain
- Types of cyber conflicts and dimensions of cybersecurity
- Modes of cyber governance, among other critical factors
- Domain ontology for complex systems of Internatoinal Relations and cyberspace

The conceptual, empirical, and policy aspects of the ECIR scientific inquiry are summarized in Part II of this Report.

3.1.2 Specific Results

The ECIR Project has:

(a) Constructed an empirically based *method to integrate cyberspace and international relations,* anchored in the layers of the internet and the levels of international relations;

(b) Demonstrated value of *control point analysis* with strategic and policy relevance;

(c) Identified *empirical patterns* of *internet control* by different actors (countries like China, and firms, like Google);

(d) Developed new system automated knowledge generated from large scale collections;

(e) Generated new empirical evidence of the power of *private authority* in management of cyberspace, with applications;

(f) Created and delivered robust *cyber-IR courseware* and exercises on cyber policy and management;

(g) Conducted interdisciplinary discussion of *cyber policy issues*;

(h) Identified new issues of *law and regulation* as potential control points; and

(i) Achieved *frequent publication* in widely read and popular media.

3.2 Publications and Related Knowledge Products

These include course development, workshops, directed research – available on ECIR website, MIT course materials, and Harvard websites – consistent with institutional practices. These materials include tested detailed curricula for four new courses, case studies two published books, one in draft, and another consisting of the compilation of research results by the individual researchers. They are highlighted in section 4.2 of this Report of new scholars and researchers, nationally and internationally, as well as new policy analysts. Basic summary is as follows:

Books:

- Choucri, Nazli 2012. *Cyberpolitics in International Relations.* Cambridge, MA: MIT Press See Appendix A-2

- Choucri, Nazli, David D. Clark, and Stuart Madnick *et al*. Editors. *Studies in Explorations in Cyber Politics for the Cyber Age,* in ms form. Information on contents and chapter summaries presented in Appendix A-3

- Choucri, Nazli and David D. Clark**.** *The Co-Evolution Dilemma: International Relations in the Cyber Age***,** completed, in manuscript form See Appendix A-4

- Ellis, Ryan. *The Politics of Critical Infrastructure Protection*, book ms submitted for review, 2015.

Articles, Chapters, Reports and other

Statistics

- 27 Published articles or Chapters in Books
- 10 Scheduled for Publication or in Press
- 20 Published in Conference or Workshop Proceedings
- 4 Working Papers or in Progress

- 37 Posted on ECIR Website
- 9 Posted on SSRN (Backlog in SSRN Posting)
- 7 Theses and Dissertations

Policy Publications

11 Online Editorials

Publication list is attached to this Report as Appendix A-1

3.3 New Methods and Applications

(1) Created a *domain structure matrix* as a tool for empirical investigations
(2) Developed model and methods to analyze the combined *cyber-IR system*
(3) Designed *control point analysis* to identify actors, actions, outcomes at key decision points
(4) Developed *automated taxonomy methods to* create new of cyber-knowledge
(5) Created Web-based system of joint cyber-IR knowledge with new ontology, database, and interactive functionalities

Extending Frontier Methods

(1) Explored *malware*
(2) Extended *resilient mechanism design* (i.e., reverse game theory) for cyber agreements
(3) Extended automated applications of *alternative algorithms* for taxonomy on cyber security
(4) Engaged in multi methods analysis of cyber conflict
(5) Completed field work on *private authority* in cyber management and governance,

3.4 Sharable Resources, Data, and Analytical Tools

The major resources and tools developed are:

- **Cyber System for Strategy and Decision (CSSD)** Second generation of MIT's Global System for Sustainable Development, an ontology based system representing the Cyber-IR domain, and curated for an evolving knowledge base consisting or tagged searchable abstracts with links to original knowledge source.

- **Cybersecurity Wiki** Harvard's Berkman Center for Internet & Society (with Science, Technology, and Public Policy Program) http://h2odev.law.harvard.edu/playlists/633

- **ECIR Data Dashboard** designed to provide scholars, policymakers, IT professionals, and other stakeholders with a comprehensive set of data on national-level cyber security, information technology, and demographic data. (See http://coin.mit.edu:8080/Dashboard).

- **Computational Taxonomy Generation System** to extract taxonomies or ontologies from large-scale database systems of journals. Tested and applied to "cybersecurity" and "cyberspace".

3.4 New Courses

ECIR Project has created nine (9) new courses: Curricula available upon request.

- **Cybersecurity Model Curriculum** Harvard's Berkman Center's tool providing resources with various elements of the course plans and "drag and drop" to create customizable syllabi.
- **Cyber Politics in International Relations,** MIT Political Science with participation from Computer Science and Management (on line)
- **International Relations Theory in the Cyber Age,** MIT Political Science (on line)
- **J-Term Course,** Harvard with all supporting materials.]
- **Cybersecurity and the Future of Cyberspace** MIT Department of Political Science, with participation from Sloan School and Computer Science.

3.5 Education of New Scholars, Researcher, and Policy Analysts

Section 10 in Part III below presents an overview of new scholars and researchers, listing individuals and areas of work. A total of 55 scholars, researchers and policy analysts participated in the ECIR Project. *This figure excludes participation or registration for courses.*

Total of 56 students, post docs, research collaborators

- MIT List = 35
- Harvard University List = 21

For details see Section 10 of this Report.

3.6 ECIR Policy Outreach

Policy outreach is designed to make ECIR research relevant for government and the private sector. These activities include

(i) Four Annual ECIR Workshops (See Appendix A-5)

(ii) Regular Harvard Policy Seminar

(iii) MIT ECIR Research Seminar.

In addition, the lead researchers regularly contribute to deliberations in national and international organizations focusing on cyberspace, cybersecurity, and transformations in international relations. The details are presented in Section 4.4 of this Report.

3.7 Relevance to the Minerva Initiative

3.7.1 Contributions to the Minerva Program

We note here three types of contributions

(i) New methods for *policy and strategy* (such as method to identify leverage points);

(ii) *New tools*, modeling and methods;

(iii) Foundations for new *theory for the cyber* age (such as framework for 21st C.. international relations theory, and alternative futures predicated on integration of cyberspace and international relations).

See Part V of this report for contributions to Department of Defense and to the Minerva Initiative. priorities are presented in Section 5 of this Report.

3.7.2 Potential Impact on DoD Capabilities and Broader Implications for National Defense:

New tools are now available to: (a) construct robust understanding of emergent dynamics surrounding the Internet and cyberspace; (b) anticipate, track, and clarify cyber threats, and; (c) understand and manage worldwide cyber transformation.

These help to: (d) construct methods with "hands on" use; (e) provide foundations for 21st C. international relations and; (f) support analyses for U.S. Grand Strategy.

3.8 Collaboration with Business and Industry

A notable product of the ECIR Project is the creation of the MIT Interdisciplinary *Consortium for Improving Critical Infrastructure Cybersecurity (IC)³ Consortium.* As a result of the ECIR initiative, IC3 is filling a critical need for critical infrastructure. Security of conventional information systems is recognized as important, but is still not fully effective. The number and magnitude of recent cyber-attacks (Target, Home Depot, SONY, etc.) is growing weekly. Details are in Section of this Report.

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.

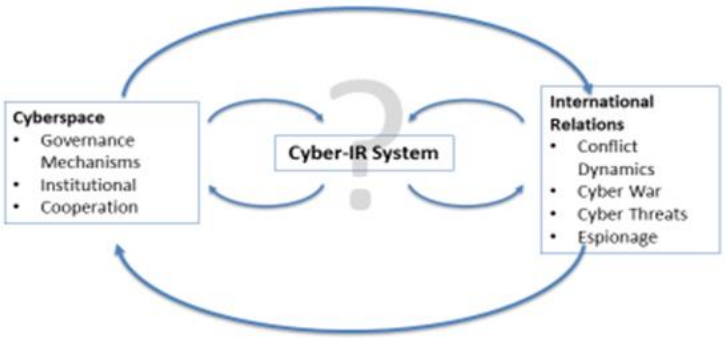


Figure 4.1 Frame of the Cyber-IR Model

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

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.

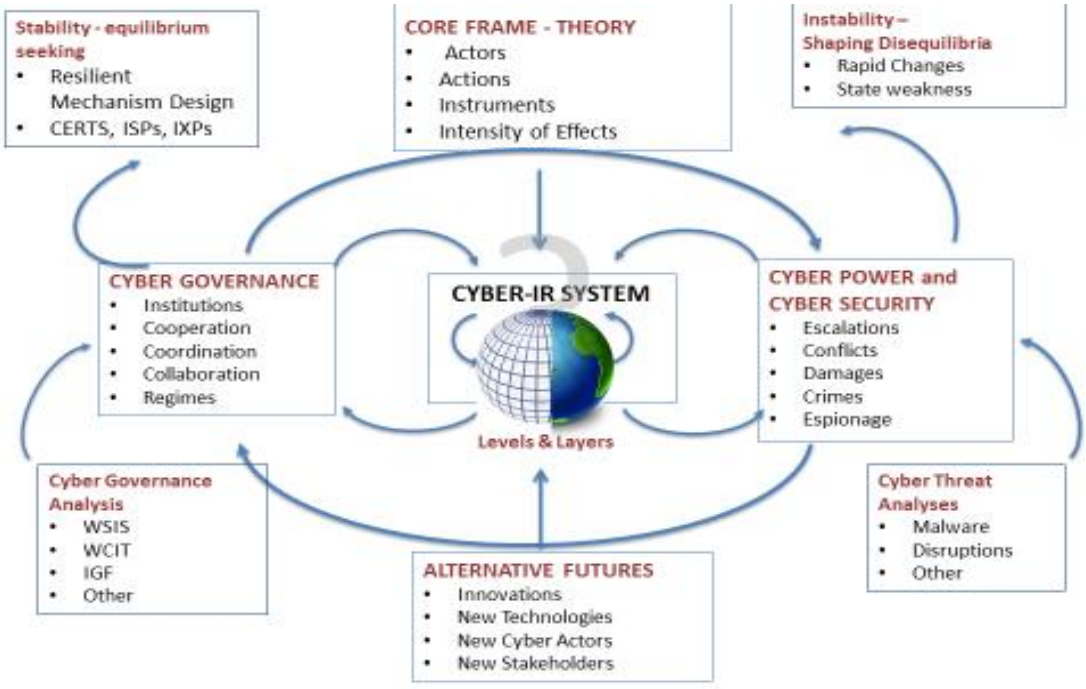


Figure 4.2 Framework for Exploring Cyber International Relations

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.

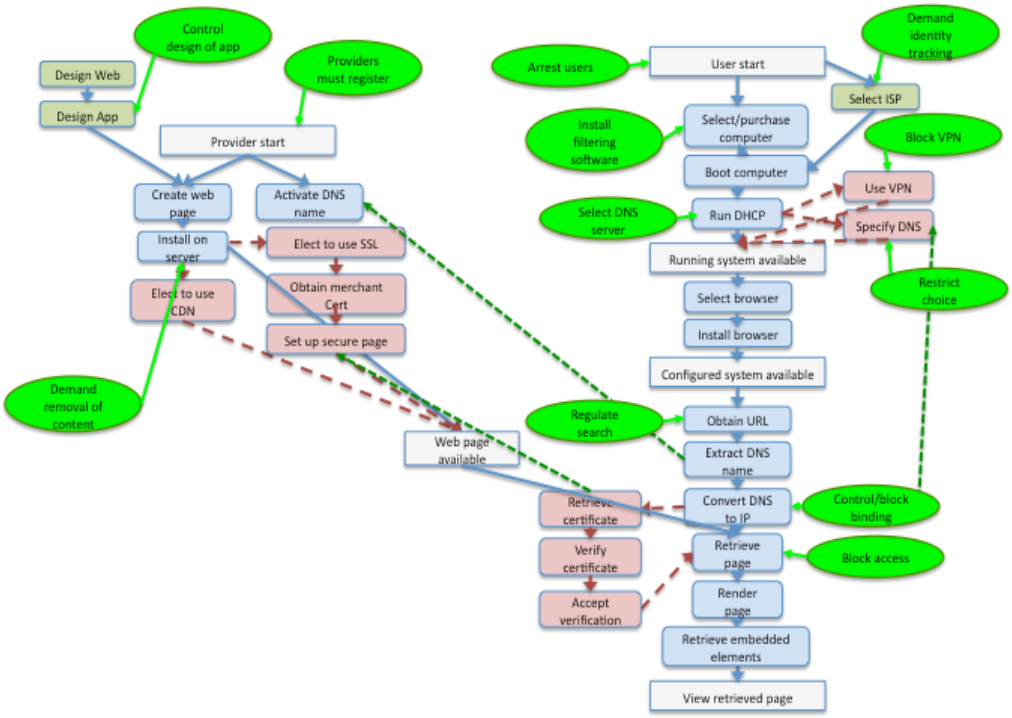


Figure 5.1; Control Points in China to Retrieve a Web Page
Source: David D. Clark

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

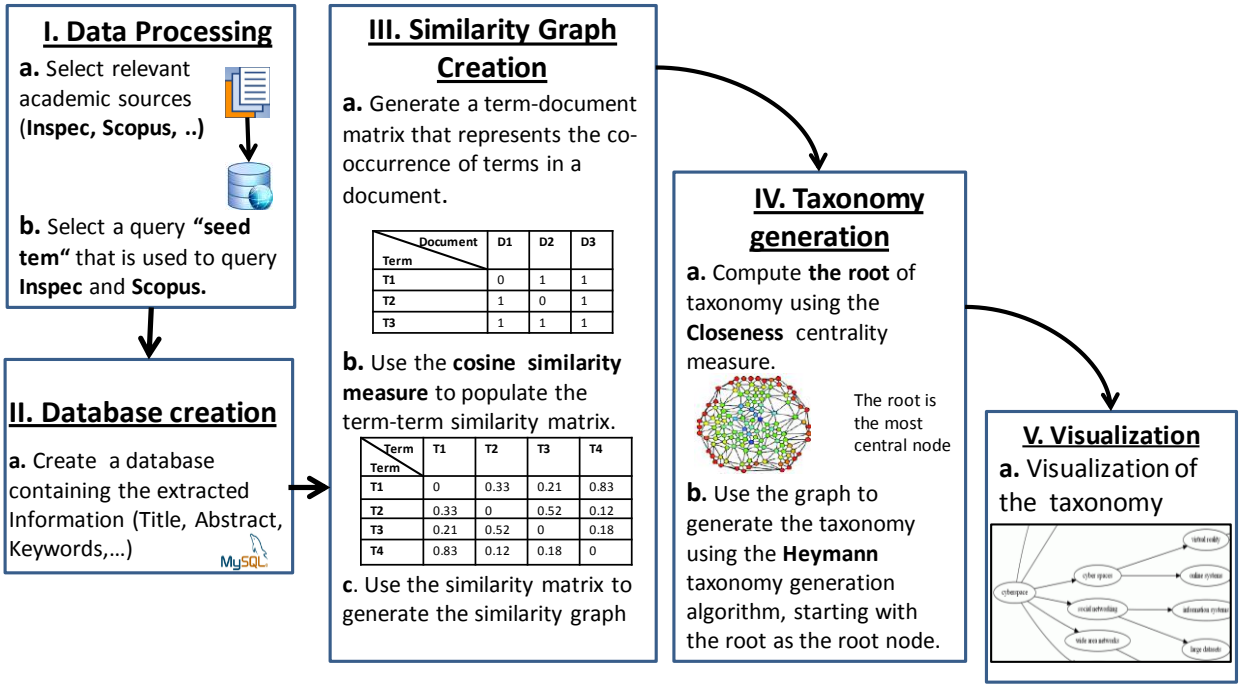


Figure 5.2 New Method for Automated Knowledge generation
Source: Daw Elbeit, Madnick, Choucri

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.

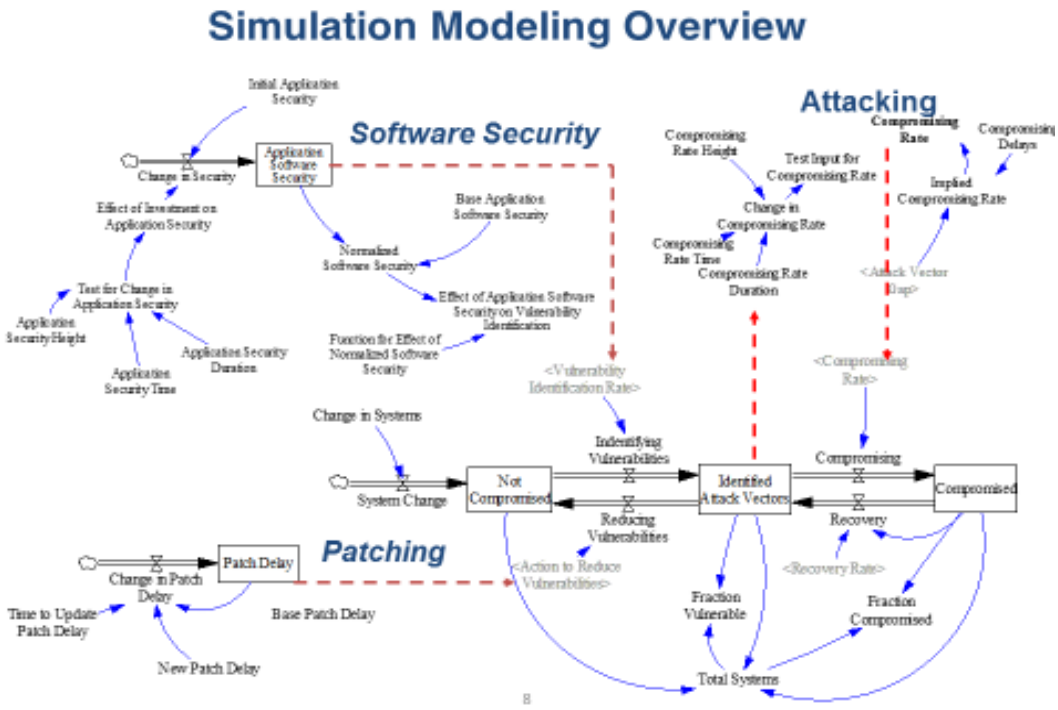


Figure 5.3: Patching not Solving Security Breaches
Source: Siegel and Houghton

- 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.

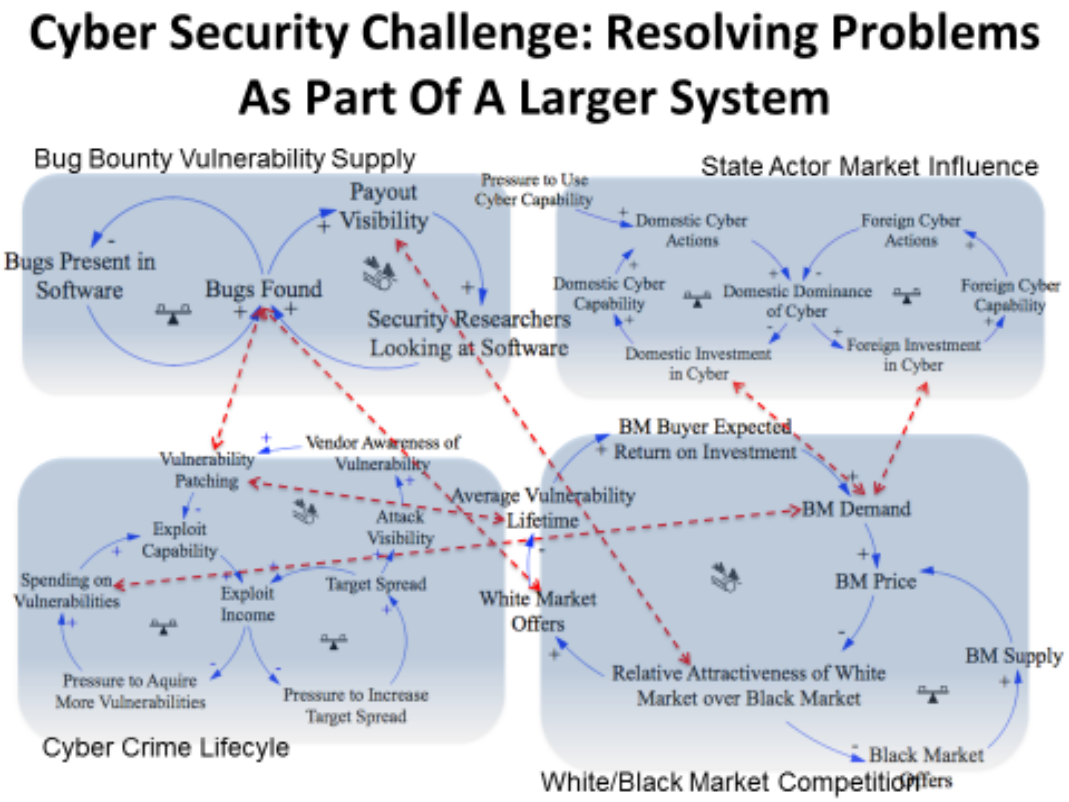


Figure 5.4: Select "Whole" of the Cyber Security Problem
Source: Siegel and Houghton

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)

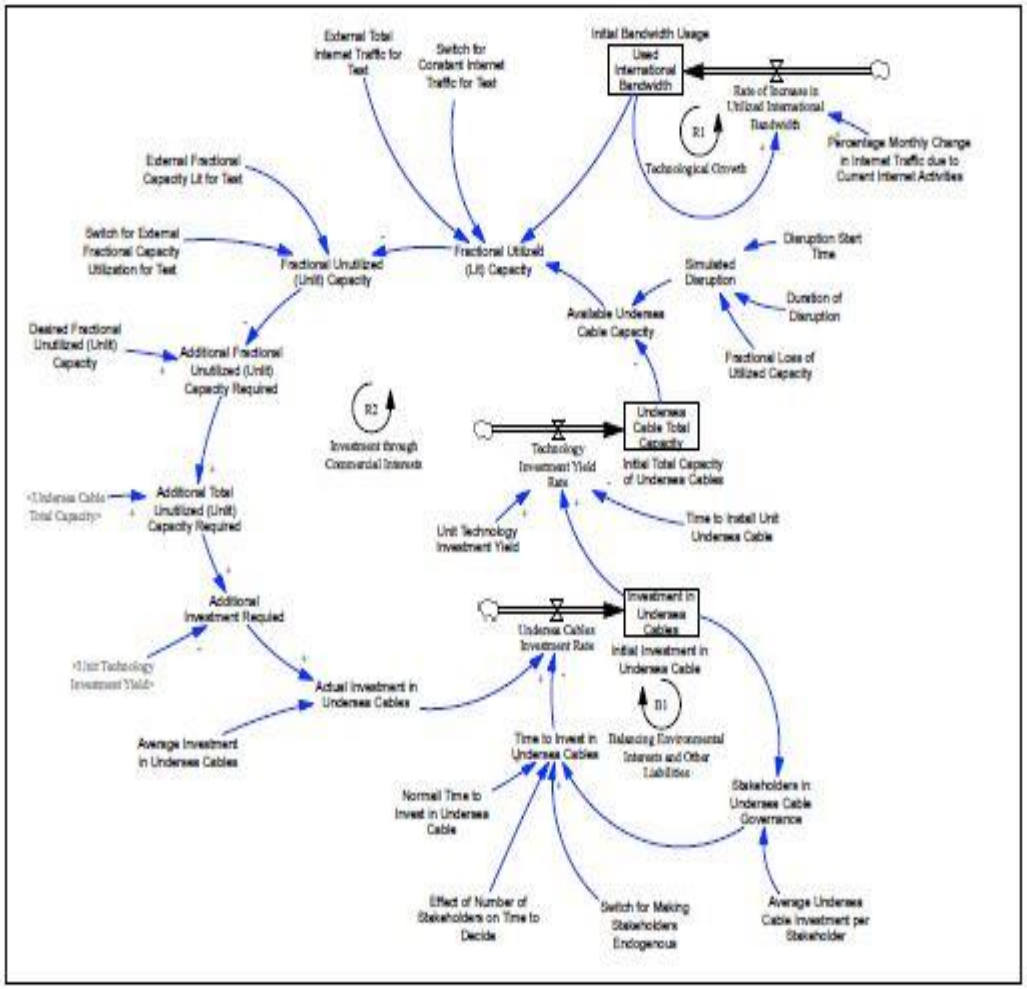


Figure 4.9: Modelling the Vulnerability of Undersea Cables-Dynamic Process
Source: Siechrist, Viashnav, Goldsmith

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?

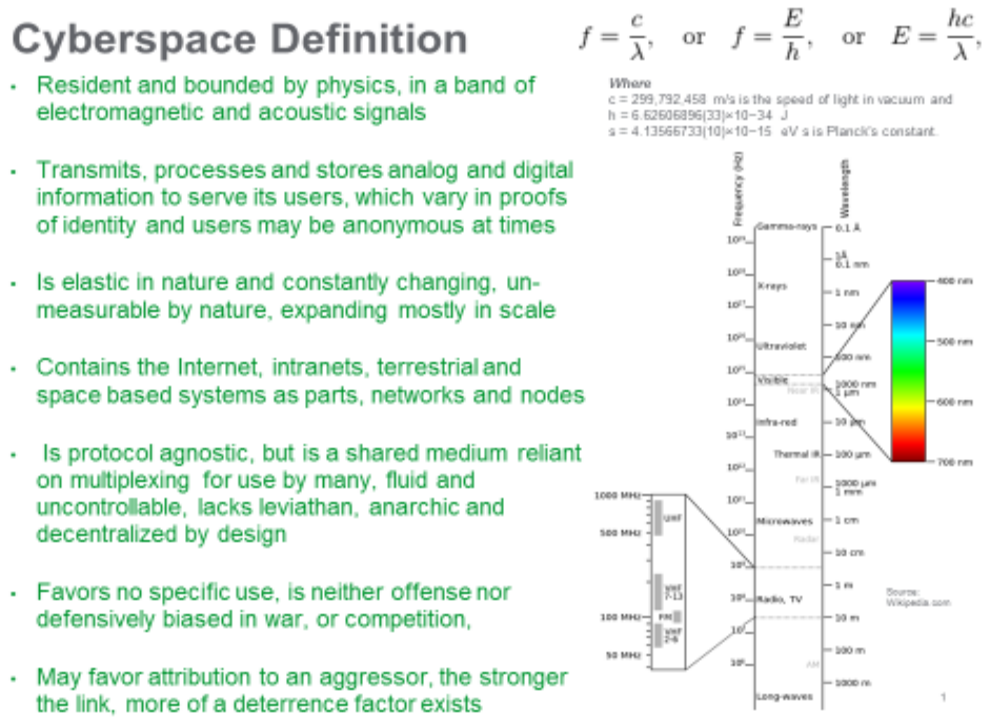


Figure 5.1

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?

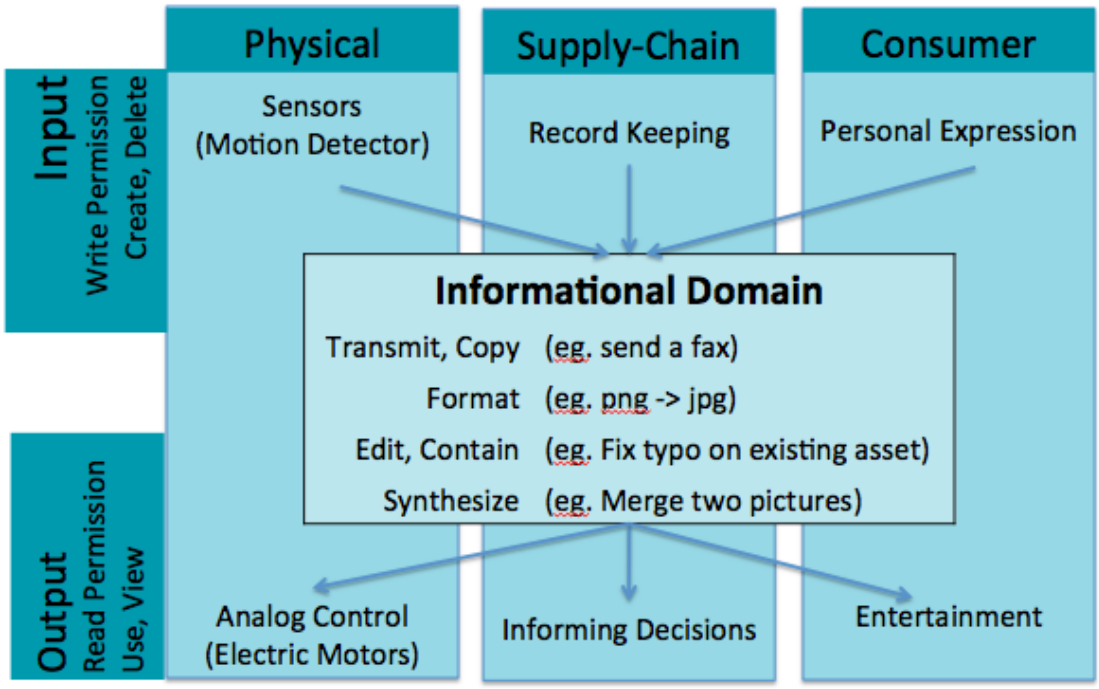


Figure 5.2

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?

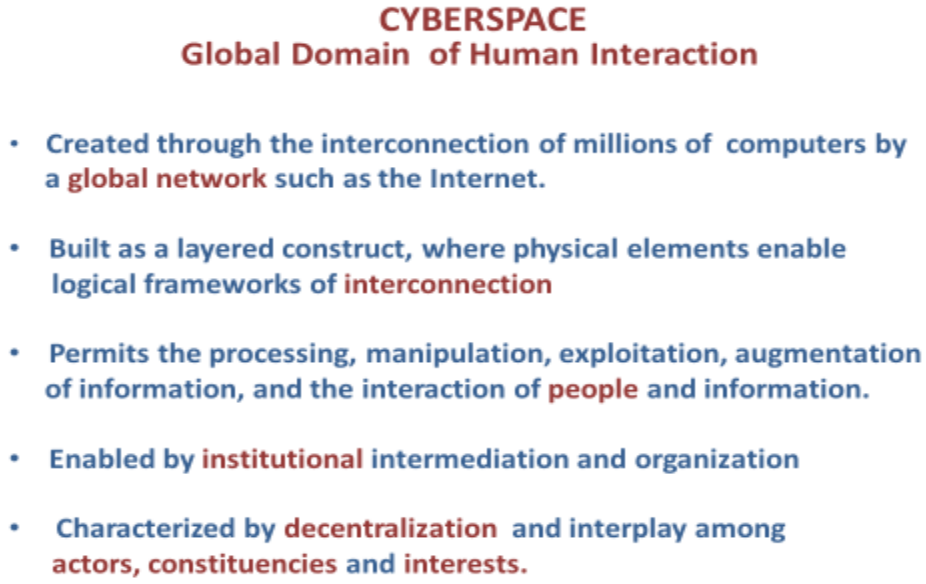


Figure 5.3

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)

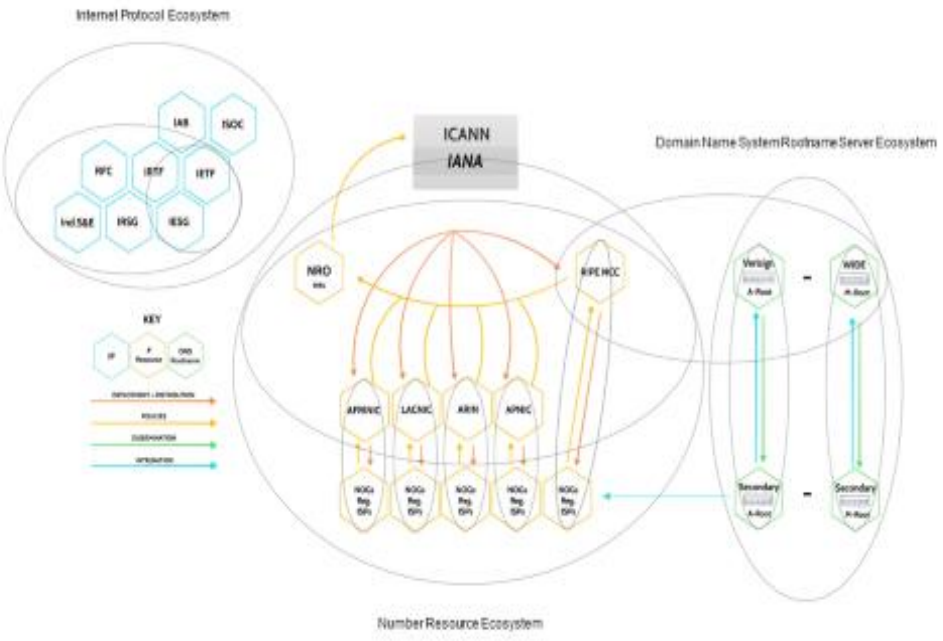


Figure 6.1: Governance of the Cyber Domain
Source: Cheung

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)

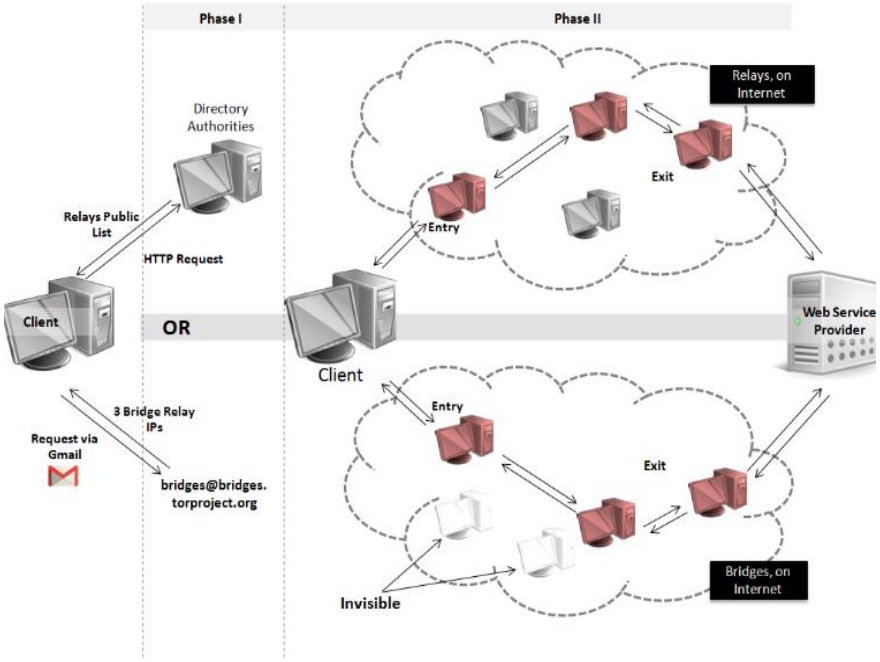


Figure 6.2: Overview of the TOR Mechanism
Source: Rady.

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).

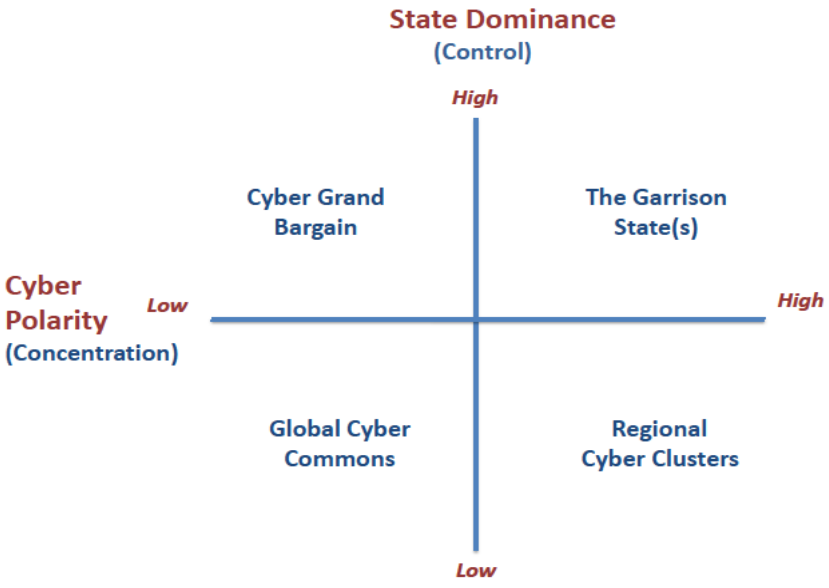


Figure 7.1 Four Futures for Cyberspace
: Source: Choucri

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.

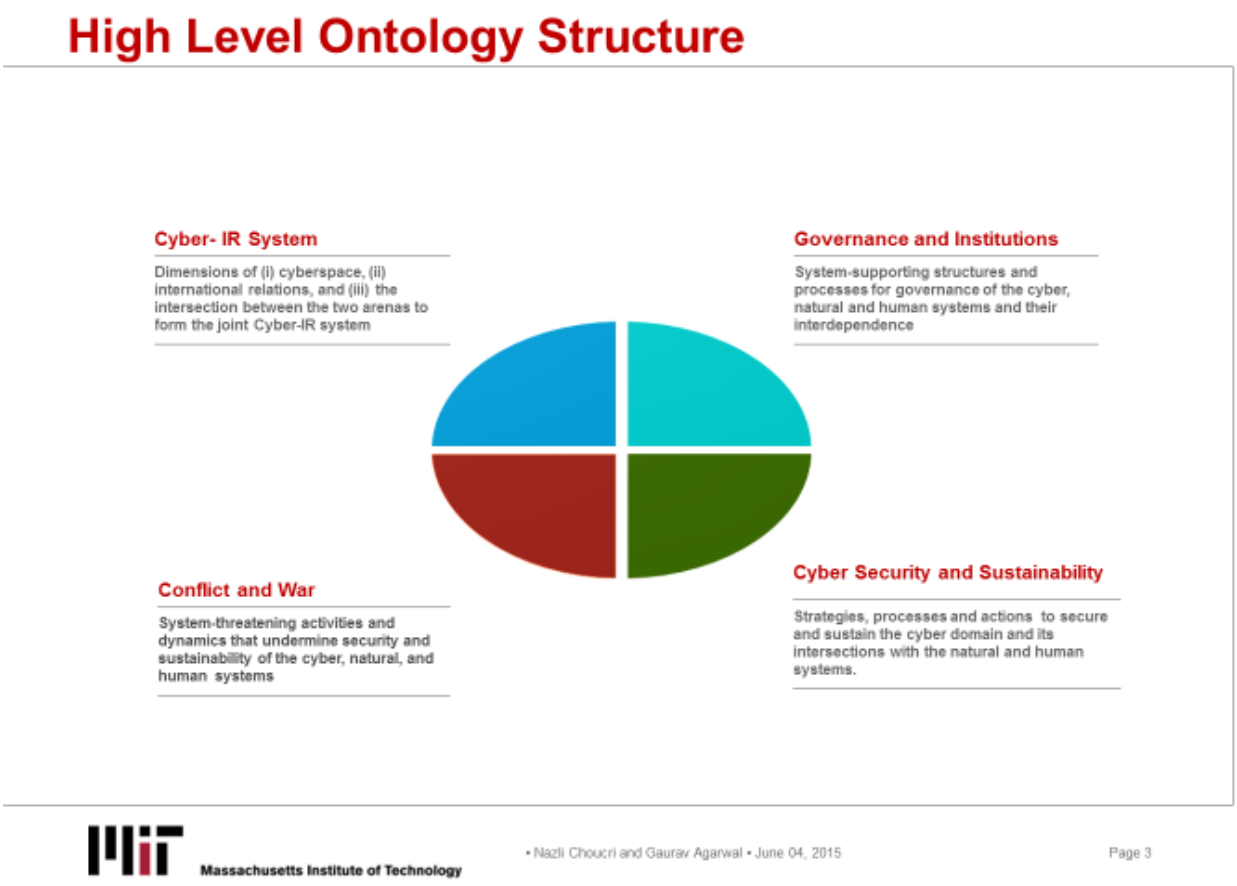


Figure 8.1: High Level View of Ontology Structure
Source: Choucri and Agarwal

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.

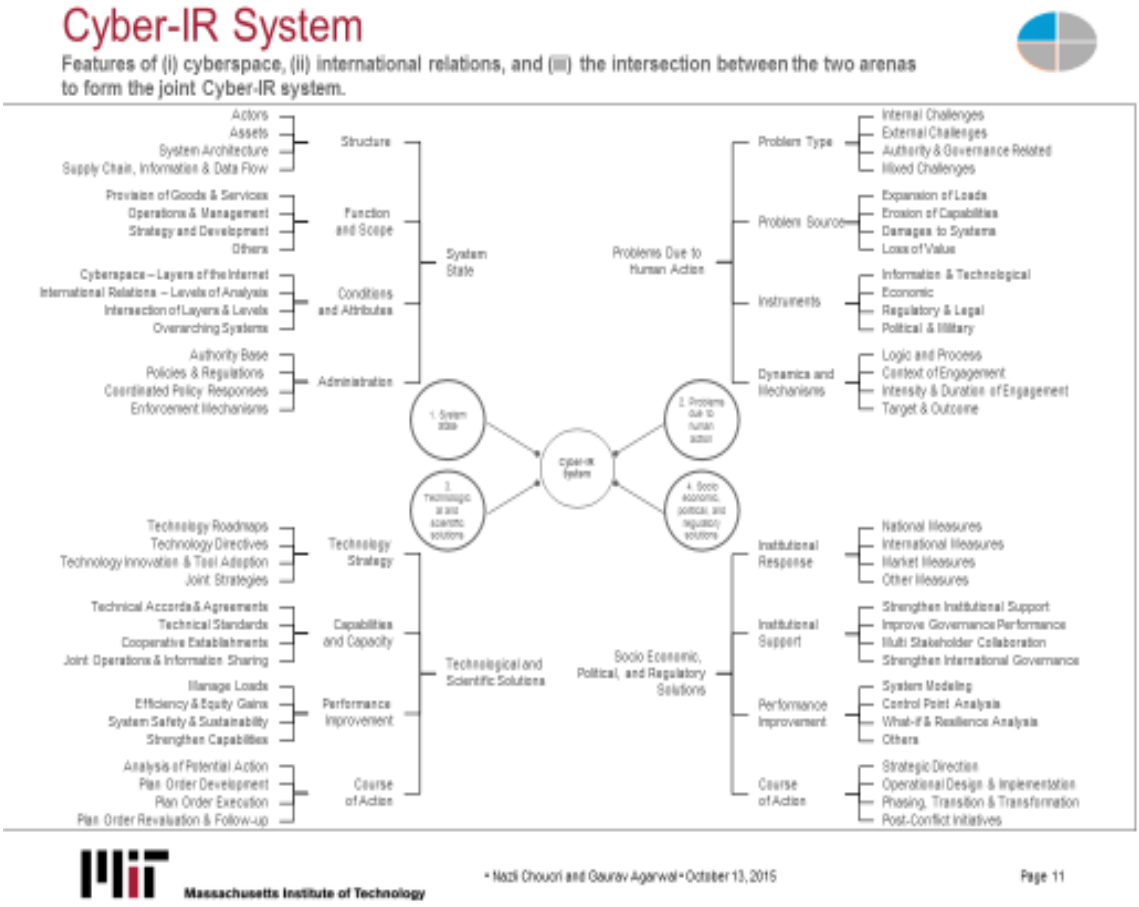


Figure 8.2: The Cyber-IR System
Source: Choucri and Agarwal

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

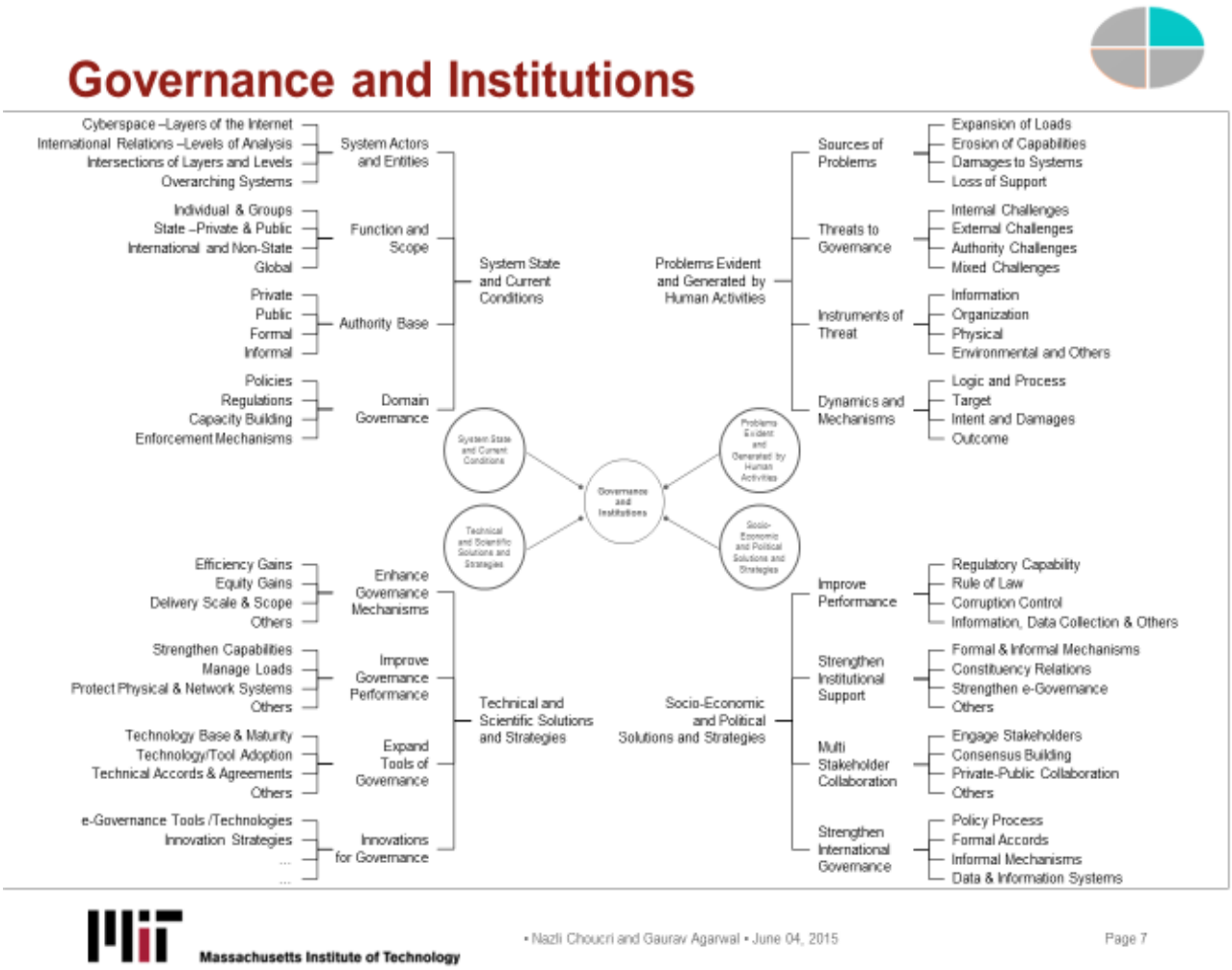


Figure 8.3 Governance and Institutions
Source: Choucri and Agarwal

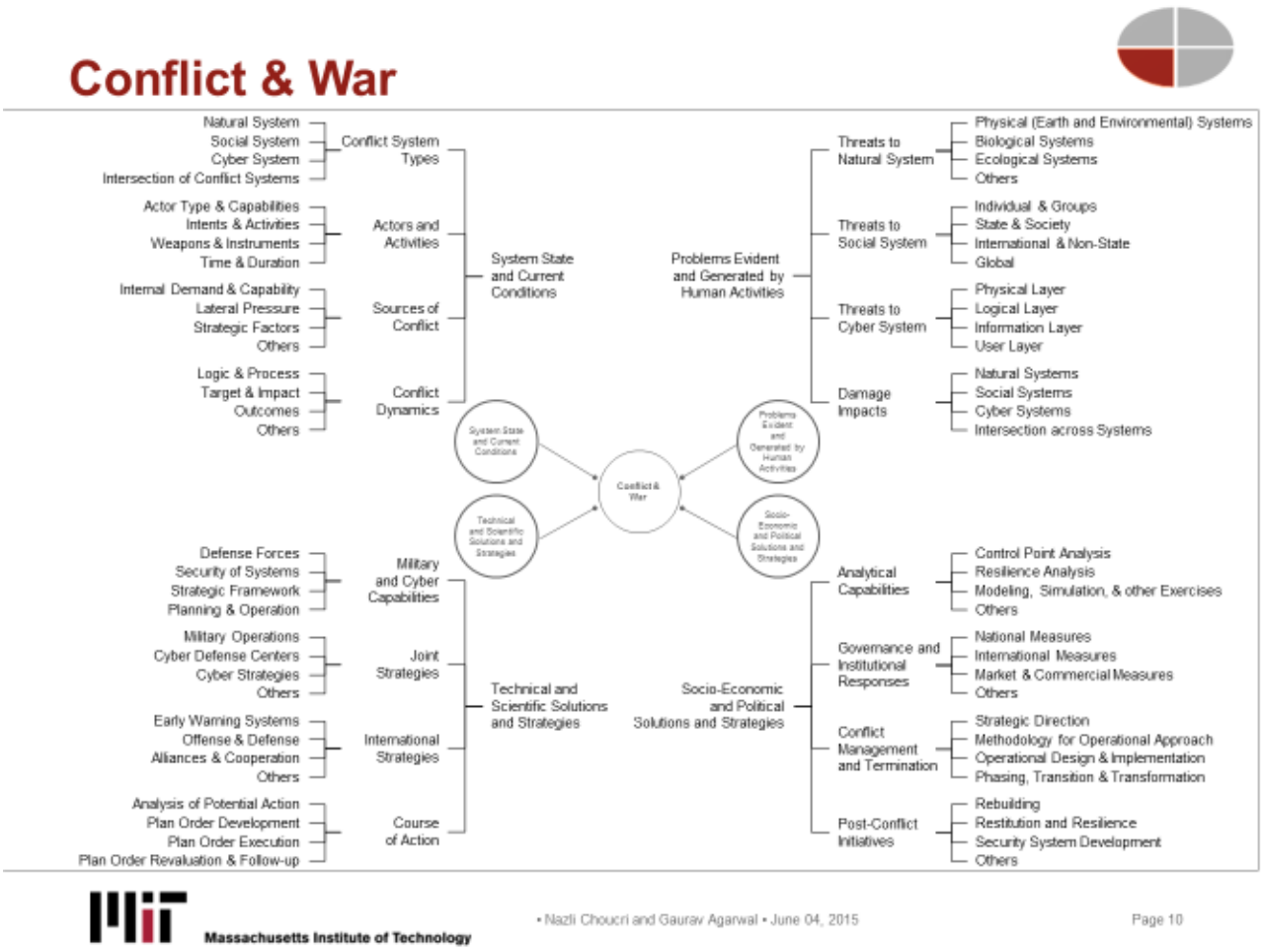


Figure 8.4 Conflict and War
Source: Choucri and Agarwal

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

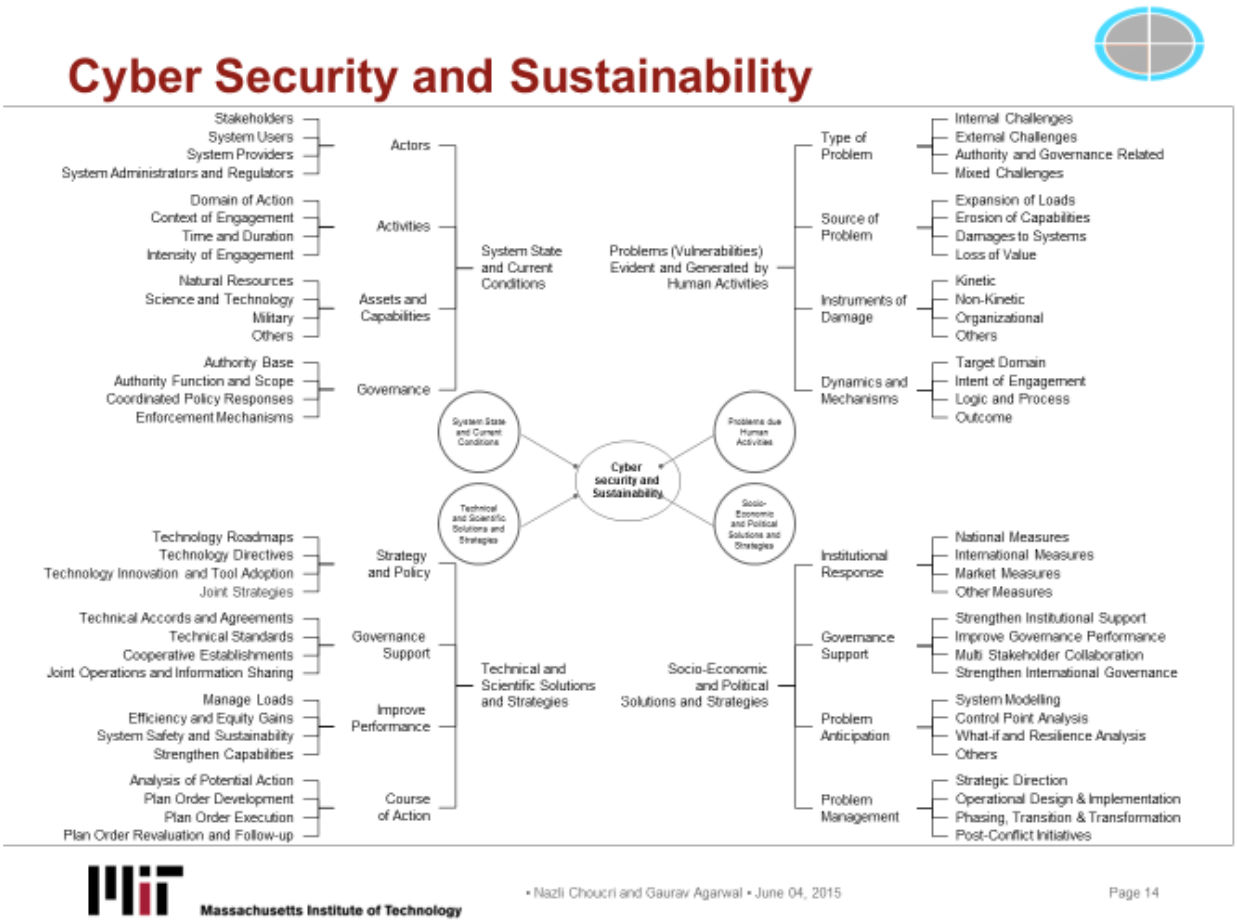


Figure 8.5 Cyber Security and Sustainability
Source: Choucri and Agarwal

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).

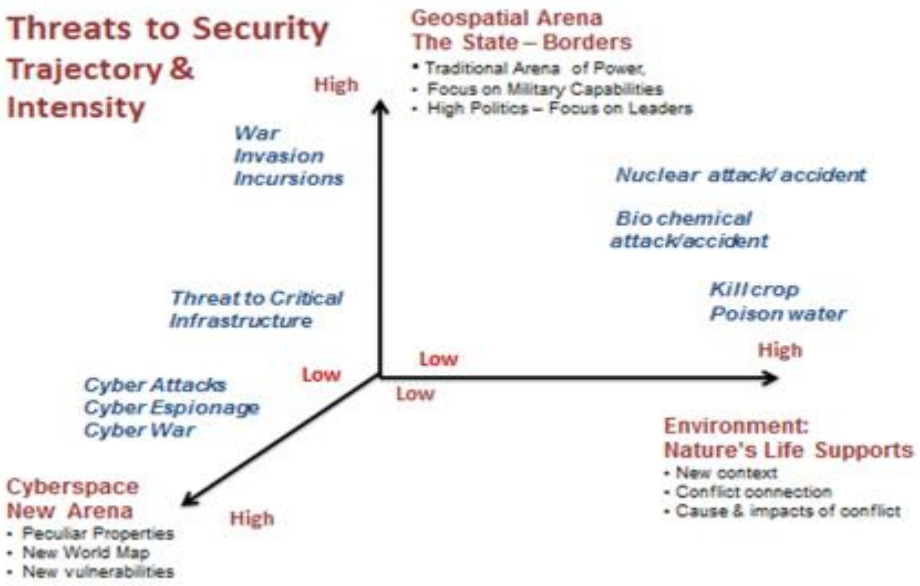


Figure 8.6 Interconnected Vulnerabilities
Source: Choucri

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.

PART III

EXPANDED ACCOMPLISHMENTS

The "expanded accomplishments" highlighted in Part III refer to s specific aspects of the collaborative initiative. These consist of:

- The production of knowledge materials, such as books, papers, and the like, as well as and any publications reflecting the overall activities, as well as the development of new courses; and the development of new courses; and
- The education of new scholars, researchers and analysists at MIT and Harvard University
- The development of sharable resources.
- Policy outreach
- Targeted relevance to the Minerva Program Priorities
- Collaboration with business and Industry

9. PRODUCTION OF KNOWLEDGE MATERIALS

Here we consider the production of knowledge materials to include (a) publications (including theses and dissertations) (b) development of course materials and (c) ECIR Workshop Reports and Poster Sessions. A brief note on each follows.

9.1 Publications

Earlier in this Report we highlighted some features of the production of knowledge, and presented some summary statistics. Here we provide a more detailed view of the types of knowledge materials generated by the ECIR Project. These consist of:

(1) Books

(2) Published chapters and articles etc.

(3) Scheduled publications

(4) Proceedings of ECIR Workshops for ECIR outreach.

(5) Working Papers - in progress

(6) Research Paper on the ECIR website

(7) Papers posted on SSRN

(8) Papers presented at Conferences and in Workshop Proceedings

(9) Editorials

(10) Graduate Student Theses

A detailed list of these items is in the Appendix to this Report. All are available on the ECIR website.

9.2 Development of New Courses

A total of nine (9) new courses were developed during the ECIR Project period. The breakdown is as follows:

9.2.1 MIT Courses

The MIT courses developed during the ECIR project period are full courses.

International Relations Theory for the Cyber Age
Faculty: Professor Nazli Choucri

Cyberspace and International Relations
Faculty: Professor Nazli Choucri, Dr. David Clark, and Professor Stuart Madnick

Digital Evolution
Faculty: Professor Stuart Madnick

Cybersecurity and the Future of Cyberspace
Pilot version: Designed by Professor Nazli Choucri, Dr. David Clark, and Professor Stuart Madnick

9.2.2 Harvard University Courses

Below is the list of Harvard Courses offered during the Project period. These include term modules as well as full courses.

Full Course

International Cybersecurity: Public and Private Sector Challenges
Faculty: Professor Jack Goldsmith

J-Term

IGA-339M – J-term 2011 –
The Future of Cybersecurity
Faculty: Professor Jack Goldsmith

IGA-236M - J-term 2013
Technology, Security, and Conflict in the Cyber Age
Faculty: Professor James Waldo

IGA-130M – Spring 2014
International Regimes and Cyber Issues

IGA-103M, Spring TERM Module,
Faculty: Professor J.S. Nye

The Future of Cybersecurity
IGA 339M: J-TERM Module, 0.5 credits
Harvard Kennedy School, Room L-280
Insructors Richard A. Clarke and Eric Rosenbach

10. EDUCATION of NEW SCHOLARS, RESEARCHERS, and ANALYSTS

10.1 The Record at MIT

STUDENT/POST-DOC LAST NAME	STUDENT/POST-DOC FIRST NAME	STATUS DURING THE VISIT	CURRENT AFFILIATION
AGARWAL	GAURAV	MS Student, System Design and Management, MIT	Bayer AG, Germany
ALTHUNAYYAN	HAMAD	Visiting Student to MIT from MASDAR Institute of Science and Technology (MIST)	MIST
CAMIÑA	STEVEN	PhD Student, Political Science, MIT	Product Manager, Oracle
CHEN	JING	PhD Student, Computer Science, MIT	Assistant Professor, Department of Computer Science, Stony Brook University
CHEUNG	SINEAD	Undergraduate, Wellesley College	Private Sector
CHO	YISEUL	MS Student, Technology and Policy Program, MIT	User Operation Specialist, Korean Market, Facebook
ELBAIT	GIHANDAW	Postdoctoral Associate, Department of Political Science	Independent Researcher at the MASDAR Institute of Science and Technology (MIST)
EL KHATIB	SAMEH	Visiting Professor, Masdar Institute of Science and Technology (MIST)	MIST
FABRE	GUADALUPE	Electrical Engineering and Computer Science Undergraduate, MIT	

FINLAYSON	MARK	PhD Student, Computer Science and Artificial Intelligence Laboratory, MIT	Research Scientist, Computer Science and Artificial Intelligence Laboratory MIT
FISHER	DARA	MSc Student, Technology and Policy Program, MIT	PhD Candidate, Harvard Graduate School of Education
GAMARO-GARRIDO	ALEX	Research Assistant, MIT	
GOLDSMITH	DANIEL	Research Associate, MIT Sloan School of Management, Program Manager for ECIR	Principal Consultant, PA Consulting Group
GREZEGORCZYK	LIDIA	Visiting Student, Poznan Institute of Technology, Poznan, Poland	Pozman Institute
HILL	JONAH FORCE	Fellow, Belfer Center for Science & International Affairs, Harvard Kennedy School	Consultant, Monitor 360
JOYCE	ERIC	MPP Student, Harvard Kennedy School	Senior Analyst/Policy Advisor, Computer Network Operations, Electronic Warfare Associates
KAYA	ABDULLAH	Visiting PhD Student, Masdar Institute of Science and Technology (MIST)	MIST
LINDSAY	JON	PhD Student, Political Science, MIT	Research Fellow, University of California, San Diego Institute on Global Conflict and Cooperation, Member, Project on the Student of Innovation and Technology in China
LIU	SIDNEY	Visiting Professor, National University of Defense Technology, China	
MALEKOS-SMITH	JESSICA	Undergraduate, Wellesley College	Military

MAURER	TIM	MPP Student, Harvard Kennedy School	Non-resident fellow at the Global Public Policy Institute (GPPi), program associate at the New America Foundation's Open Technology Institute
MILLER	ANDREW	Research Assistant, MIT	Ph.D. MIT
MOHAN	VIVEK	Research Fellow, Science, Technology, and Public Policy Program/Project on Technology, Security, and Conflict in the Cyber Age	Attorney, Sidley Austin LLP's Privacy, Data Security, and Information Law practice group, Washington DC
PERON	VIVIAN	Visiting PhD Student, University of Brasilia	
RADY	MINA	Research Assistant, American University, Cairo, Egypt	
RAMTIN	AMIN	MPP Student, Harvard Kennedy School	PhD Candidate, Oxford Internet Institute, Oxford University
REARDON	ROBERT	Postdoctoral Associate, Explorations in Cyber International Relations, MIT	Postdoctoral Research Fellow, Project on the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School
RODART	SAMUEL	Visitor	In transition
SALIM	HAMID	MS Student, Computer Science, MIT	Independent Professional Web Sourcing, Boston MA
SECREST	MICHAEL	MPP Student, Associate, Explorations in Cyber International Relations, Harvard Belfer Center, Harvard Kennedy School	Vice President for Threat and Risk Management, State Street Corporation, Boston, MA

SHUKLA	AADYA	MIT Affiliate	Associate, Science, Project on Technology, Security, and Conflict in the Cyber Age, Harvard's Belfer Center
TESTART-PACHECO	CECILIA	MS MIT	Ph.D. MIT
VAISHNAV	CHINTAN	Postdoctoral Associate, Department of Political Science, Computer Science and Artificial Intelligence Laboratory, Sloan School of Management, MIT	Research Associate, Sloan School of Management, MIT
VALLE	EDWARD	MIT Student	MIT Student

10.2 The Record at Harvard University

STUDENT/POST-DOC LAST NAME	STUDENT/POST-DOC FIRST NAME	STATUS DURING THE VISIT	CURRENT AFFILIATION	TERM ON GRANT
Bates	Christopher	Graduate student		FY10
Denton	David	Graduate Student		FY10
Deyrup	Ivana	Graduate Student		FY10
Ellis	Ryan	STPP Post-doctoral fellow	STPP Post-doctoral fellow, Belfer Center, Harvard Kennedy School	FY13, FY14
Gaucherin	Benoit	Teaching Assistant, Cyber J-Term 2014	Deputy Chief Information Officer, Harvard University Information Technology	FY14
Gerver	Keith	Graduate Student		FY10
Haber	Jeremy	Graduate Student		FY10
Hill	Jonah	HKS Graduate Student		FY12
Joyce	Eric	HKS Graduate Student		FY10

Kello	Lucas	STPP Post-doctoral fellow	Senior Lecturer in International Relations, Director of the Cyber Studies Programme, Cyber Security, Oxford University	FY12, FY13, FY14
Lockshin	Zara	Graduate Student		FY10
Maurer	Timothy	Graduate Student		FY12
Mohan	Vivek	STPP Post-doctoral fellow	Attorney, Sidley Austin LLP's Privacy, Data Security, and Information Law practice group, Washington DC	FY12, FY13, FY14
Noyes	Matthew	Graduate Student		FY12
Sauter	Molly	Graduate Student		FY11
Shroegel	Philipp	Graduate Student		FY11
Sechrist	Michael	STPP Pre-doctoral fellow	VP, Threat and Risk Management, State Street Corporation	FY11, FY12
Shukla	Aadya	STPP Pre-doctoral fellow	Associate, Technology, Security, and Conflict in the Cyber Age, Harvard's Belfer Center	FY11, FY12, FY13
Toretta	Kristin	HKS Graduate student		FY11
Wall	Andru	Graduate student		FY10
Williams	Robert	Graduate student		FY10

11. SHARABLE RESOURCES, DATA, ANALYTICAL, METHODS and TOOLS

11.1 Cyber System for Strategy and Decision

Expansion of MIT's Global System for Sustainable Development to cover the Cyber domain (GSSD). Ontology-based and quality controlled knowledge data base consisting or tagged searchable abstracts with links to source. Content structure is based on the ECIR framework for integrating cyberspace and international relations. See gssd.mit.edu

11.2 Cybersecurity Wiki

Harvard's Berkman Center for Internet & Society—with contributions from the Science, Technology, and Public Policy Program's Explorations in Cyber International Relations—has developed a Cybersecurity Wiki that is designed to be a curated, comprehensive, evolving, and interactive collection of resources for researchers (not just legal researchers), technologists, policymakers, judges, students, and others interested in cybersecurity issues, broadly conceived. The general aim of the wiki is to collect in one place, and organize intelligently, important documents related to cybersecurity.

Designed to provide scholars, policymakers, IT professionals, and other stakeholders with a comprehensive set of data on national-level cyber security, information technology, and demographic data. The Dashboard allows stakeholders to observe chronological trends and multivariate correlations that can lead to insight into the current state, potential future trends, and approximate causes of global cyber security issues. (See http://coin.mit.edu:8080/Dashboard/).

11.3 Computational Taxonomy Generation Tool

The development of an automated system for content compilation, and comparisons designed to derive taxonomies or ontologies from large-scale database systems . (See ECIR website

11.4 Cybersecurity Model Curriculum

Harvard's Berkman Center's tool for instructors who plan to teach a cybersecurity class, providing them with resources arranged in a coherent, teachable fashion. Not for lay teachers. Provides a structured guide that is adaptable, yet rigorous, permitting professors to take various elements of the course plans and "drag and drop" to create their own customizable syllabi. Developed with

contributions from HKS and HLS faculty and fellows. Website:
http://h2o.law.harvard.edu/playlists/633

12. ECIR POLICY OUTREACH

During the ECIIC project period, two sustained initiatives were maintained throughout:

12.1 ECIR Workshops

Four Workshops were held during the Project period as mechanisms for outreach to the policy and business community. At each Workshop, students were encouraged to present posters for the Poster Session. The *Proceedings* are available on the ECIR Website.

See Appendix A-6 for Workshop titles, details, and co-sponsorship, as well as information about two Affiliated Workshops

12.2 Harvard – ECIR – Policy Seminar

Professor Joseph S. Nye chaired a bi-weekly seminar series on cyber policy and politics over the entire ECIR period. The seminar continues to date. See the ECIR website.

13. RELEVANCE TO THE MINERVA INITIATIVE

We illustrate the relevance of ECIR research for (a) the Minerva Program, and for (b) the US Department of Defense, in that order.

13.1 Relevance to the Minerva Program

Figure 13.1 below illustrates the convergence between the Minerva Program priority issues and the ECIR research themes and activities. This figure is to be read as follows:

The top segment refers to topics selected from the November 8, 2012 meeting at Harvard. The numbered items refer to the Minerva Program Priorities. The content of the box refers to the ECIR Research Agenda. The arrows indicate connections or relevance.

Figure 13.1 ECIR Contributions to the Minerva Program Priorities

13.2 Relevance to US Department of Defense

Based on the work and results so far, select results that contribute to DoD capabilities and implications for national defense and for the U.S. Grand Strategy are of three types: policy and strategy, (such as method to identify leverage points), (ii) new tools, modeling and methods (examples below); and (iii) new theory for the cyber age (i.e., 21st C.. international relations theory, alternative futures predicated on integration of cyberspace and international relations). *Some examples include:*

- The discovery through *control point analysis* of the full range of potential vulnerabilities and points of unwanted interventions or hidden "weaknesses" in the current structure of the Internet and the broader cyberspace context. This work, embedded in a broader international context, has never been done before, and if a medical analogy can be used, we can now determine the degree of robustness and resilience in the overall system, locate weaknesses, as well as those elements that we control versus those controlled by others.

- The development of *new tools* to support evolving capabilities for analysis and policy. These include customizable system dynamics models (for conflict dynamics), automated generation of new knowledge extracted from existing records (of scientific communities' or of adversaries' knowledge content), and work on automated identification of legal precedents

- The design of alternative *cyber futures* – based on the co-evolution of cyberspace and international relations – can serve as the basis for anticipating changes in distribution of power, emerging governance issues, and new contentions – all for a world that is increasingly diverse in its view of Internet "openness" or "closure.

- The construction of the *cyber-IR system* provides a common platform to for exploring potential power projections, developing "cross-domain" strategies, or the selection of "best" leverages and responses to emergent threats.

14. COLLABORATION with BUSINESS and INDUSTRY

14.1 (IC)³ Consortium

One specific product (or output) is the creation of the MIT *Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)³ Consortium.* As a result of the ECIR initiative, IC3 is filling a critical need for critical infrastructure. Security of conventional information systems is recognized as important, but is still not fully effective. The number and magnitude of recent cyber-attacks (Target, Home Depot, SONY, etc.) is growing weekly.

More important, but even less protected, is the security of our Cyber-Physical Infrastructure and IoT (Internet of Things). The computer controlled facilities that produce and deliver our electric power, oil and natural gas, chemicals, water, pharmaceuticals, food, manufactured goods, financial services, telecommunications, healthcare, emergency services, and the buildings that collectively form the infrastructure of a safe and secure world civilization are dangerously exposed to cyber-attacks.

While our critical infrastructure is even more important to secure than conventional information systems, much less research in cybersecurity for critical Infrastructure has been done. This is the research being done by (IC)³.

(IC)³ is focusing on the critical cybersecurity needs for critical infrastructure in the following significant ways:

(1) Justify top management attention & adoption
(2) Define actions that can be effective & measured
(3) Define a culture of Cyber-Safety
(4) Create a forum for CSO/CISO's to advance Cybersecurity

The MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity has already developed in basic research parameters and has launched a set of initial meetings,

See MIT-(IC)3 - Home

14.2 Co-Sponsors of ECIR Workshop

The ECIR Workshops were co-sponsored by (a) the *Business Executives for National Security*, a non-profit organization that provides business and nation security consulting services. The organization offers cyber security, threat finance, and disaster response consulting services; and (b) the *Council on Foreign Relations*, is an independent, nonpartisan membership organization, dedicated to being a resource for its members, namely, business leaders, journalists, educators and students, interested in international affairs.

END NOTE

The Final Report of the MIT – Harvard University Project on *Explorations in Cyber International Relations* highlights the major research results, the production of knowledge materials, the development of shared resources, the education of students, researchers, and policy analysts, as well as a range of related outputs.

The activities of the ECIR initiative did not generate one single result, rather a set of distinct multidisciplinary findings, jointly contributing to the overarching objectives outlined in the Research Agenda.

This Report is framed in summary form, with direct reference to the lead researcher(s). All source documents referred to in this Report are available on the ECIR web site.

Finally, by necessity this Report captures the most significant, but not all, of the results of ECIR to date. Our purpose here is to be as inclusive as possible, without claiming to be exhaustive.

The Appendix presents supporting materials and added information.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX

ECIR FINAL REPORT

This Appendix provides detailed information in issues presented in the Final Report. All is in the public domain, available on ECIR.mit.edu

Prepared by:

Professor Nazli Choucri, Principal Investigator - MIT

APPENDIX

A-1 PRODUCTION of NEW KNOWLEDE MATERIALS

- List of Publications, Papers, Research Results

A-2 BOOK PUBLISHED

CYBERPOLITICS in INTERNATIONAL RELATIONS

- Table of Contents

A-3 BOOK COMPLETED

ECIR STUDIES: CYBERSPACE and INTERNATIONAL RELATIONS

- Table of Contents
- Chapter Abstract

A-4 BOOK COMPLETED

THE CO-EVOLUTION DILEMMA: CYBERSPACE and INTERNATIONAL RELATIONS

- Table of Contents

A-5 Report on: PERSPECTIVES on CYBERSECURITY

- Annotated Table of Contents

A-6 ECIR WORKSHOPS

A-7 HARVARD POLICY SEMINAR

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX A-1

ECIR PUBLICATIONS and SCHOLARLY PRODUCTS

BOOKS

- Choucri, Nazli. 2012. *Cyberpolitics in International Relations.* Cambridge, MA: MIT Press.

- Choucri, Nazli, David Clark, Stuart Madnick *eds.* ECIR Studies on *Explorations in Cyberspace and International Relations.*

- Choucri, Nazli and David D. Clark**.** *The Co-Evolution Dilemma: International Relations in the Cyber Age***,** under consideration by MIT Press, in preparation.

- Ellis, Ryan. *The Politics of Critical Infrastructure Protection*, book ms submitted for review. Summer.

PUBLISHED CHAPTERS AND ARTICLES

- Chen, Jing and Silvio Micali. "Collusive Dominant-Strategy Truthfulness." *Journal of Economic Theory*. 147 (3) (2012): 1300-1312.

- Chen, Jing and Silvio Micali. "The Order Independence of Iterated Dominance in Extensive Games." *Theoretical Economics:* 8 (2013), 125–163.

- Chen, Jing, Silvio Micali, and Rafael Pass. "Tight Revenue Bounds with Possibilistic Beliefs and Level-k Rationality." *Econometrica* 0 (2015): 1-21.

- Choucri, Nazli and David Clark. "Who Controls Cyberspace?" *Bulletin of the Atomic Scientists*, September 1, 2013.

- Choucri, Nazli. "The Convergence of Cyberspace and Sustainability." *e-International Relations.* April 20, 2012. http://www.e-ir.info/2012/04/20/the-convergence-of-cyberspace-and-sustainability/.

- Choucri, Nazli. "Cyberpolitics in International Relations," in *The Oxford Companion to Theoretical Economics* (TE), ed. Joel Krieger, 2012: 267-271. New York: Oxford University Press.

- Choucri, Nazli, Stuart Madnick & Jeremy Ferwerda, *Information Technology for Development* (2013): Institutions for Cyber Security: International Responses and Global Imperatives, Information Technology for Development.

- Clark, David D. and Landau, Susan. "Untangling Attribution." *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, DC: The National Academies Press, 2010: 25-40 and *Harvard National Security Journal,* 2011. http://harvardnsj.org/2011/06/untangling-attribution/.

- Finlayson, Mark. "Report of the AAAI 2010 Fall Symposia: Computational Models of Narrative." *AI Magazine,* 32(1) (2011): 96-97.

- Finlayson, Mark (ed). *The Third Workshop on Computational Models of Narrative*. (CMN'12) May 2012.

- Hathaway, Melissa E. "Leadership and Responsibility for Cybersecurity." *Georgetown Journal of International Affairs* Special Issue (2012): 71-80.

- Hathaway, Melissa E. "Falling Prey to Cybercrime: Implications for Business and the Economy." Chap. 6 in *Securing Cyberspace: A New Domain for National Security*. Queenstown, Md.: Aspen Institute, February 2012.

- Hathaway, Melissa E. and Alexander Klimburg. "Preliminary Considerations: On National Cyber Security." Chap. 1 in *National Cyber Security Framework Manual*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, December 2012.

- Hathaway, Melissa. "NATO and the EU in Cyberspace: The Power of Both for the Good of All." *Security Europe*, November 2011.

- Henschel, Andreas. Erik Casagrande, Wei Lee Woon, Isam Janajreh, and Stuart Madnick. 2012. "A Unified Approach for Taxonomy-Based Technology Forecasting," in *Business Intelligence Applications and the Web: Models, Systems and Technologies*. eds. Marta E. Zorrilla, Jose-Norberto Mazón, Óscar Ferrández, Irene Garrigós, Florian Daniel and Juan Trujillot. IGI Global: 178-197.

- Hurwitz, Roger. "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly,* 6 (3) (Fall 2012): 20-45.

- Hurwitz, Roger. "The Disunity of Cyberspace," in J-F. Kremer & B. Muller, eds., *Cyber Space and International Relations: Theory, Prospects and Challenges*. (Springer Verlag, 2013).

- Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security.* Vol. 38, No. 2 (Fall 2013).

- Kello, Lucas. "Security," *The Oxford Companion to International Relations* (Oxford University Press, 2013).

- Li, Xitong, Yushun Fan, Stuart Madnick, Quan Z. Sheng. "A pattern-based approach to protocol mediation for web services composition." *Information and Software Technology* 52 (3) (2010): 304–323.

- Madnick, Stuart, Nazli Choucri, Steven Camina and Wei Lee Woon. "Towards Better Understanding Cybersecurity: or are 'Cyberspace' and 'Cyber Space' the same?" (2012) *pre-ICIS Workshop on Information Security and Privacy (SIGSEC)*. Paper 27. http://aisel.aisnet.org/wisp2012/27/.

- Mallery, John, Michael R. Nelson (Academic Co-chairs). "A Report from the Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD2)." TechAmerica Foundation. July 2011. http://www.techamericafoundation.org/cloud-commission.

- Mohan, Vivek and John Villasenor. "Decrypting the Fifth Amendment: The Limits of Self-Incrimination." *University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny* 15 (October 2012): 11-28. https://www.law.upenn.edu/journals/conlaw/heightened-scrutiny/.

- Nye, Jr., Joseph S. 2011. "Soft Power," in *The Future of Power*. New York: Public Affairs Press, 81-109.

- Nye, Jr., Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, 5, no. 4, (Winter 2011): 18-38.

- Nye, Joseph S. Jr. "The Twenty-First Century Will Not Be a 'Post-American' World." *International Studies Quarterly* 56, no. 1 (March 2012): 215-217.

- Nye, Joseph S. Jr. and Jack Landman Goldsmith. "The Future of Power." *Bulletin of the American Academy of Arts and Sciences*. Spring 2011.

- Shukla, Aadya. "Stance in Cyberspace: India and China." Submitted by invitation, *Foreign Policy.* Intended for publication, 2013.

- Vaishnav, Chintan, Nazli Choucri and David D. Clark. "Cyber International Relations as an Integrated System. *Environ Syst Decis* (2013) 33:561–576. Published online: 17 November 2013
  Springer Science Business Media New York, 2013.

- Winston, Patrick. "The Next 50 Years: A Personal View." *Biologically Inspired Cognitive Architectures.* 1 (July 2012): 92–99.

- Winston, Patrick H. "The Strong Story Hypothesis and the Directed Perception Hypothesis." In Pat Langely, ed., in *Technical Report FS-11-01, Papers from the AAAI Fall Symposium*, Menlo Park, CA (2011): 345-352.

- Winston, Patrick. "The Strong Story Hypothesis and the Directed Perception Hypothesis." *AAAI Fall Symposium Series* (2011): December 15, 2011 © 2011 Association for the Advancement of Artificial Intelligence.

- Winston, Patrick. "The Right Way." *Advances in Cognitive Systems* 1 (2012): 23–36.

- Woon, Wei Lee and Stuart Madnick. "Semantic distances for Technology Landscape Visualization." *Journal of Intelligent Information Systems* 39 (1) (2012): 29-58.

SCHEDULED PUBLICATIONS

- Basuchoudhary, Atin and Nazli Choucri, "The Evolution of Network Based Security Norms: An Analytical Narrative", IEEE IRI, 2014.

- Chen, Jing and Silvio Micali. "Mechanism Design with Set-Theoretic Beliefs." *Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science* (FOCS) 2011, 87–96. *Journal of Economic Theory*, 2013 (in press).

- Choucri, Nazli. "Emerging Trends in Cyberspace: Dimensions & Dilemmas. Prepared for the conference on Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition." The Matthew B. Ridgway Center for International Security Studies. University of Pittsburg. November 1-2, 2012. Chapter to appear in an edited volume by the *Strategic Studies Institute.*

- Hurwitz, Roger. "A New Normal? The Cultivation of Global Norms as Part of a Cyber Security Strategy," in *Cyber Power: The Quest for a Common Ground*, ed., P. Yannakogeorgos (Air University Press, forthcoming).

- Ellis, Ryan. "Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?" A review of the first set of mandatory cybersecurity regulations for the electric power industry. Forthcoming, 2014.

- Ellis, Ryan. "Threat Signatures, Intrusion Detection, and Intrusion Prevention: Risks and Opportunities," forthcoming, 2014.

- Ellis, Ryan. *Letters, Power Lines, and Other Dangerous Things: The Politics of Infrastructure Security.* Book manuscript to be submitted for review. (in progress).

- Kello, Lucas. "The State of European Cybersecurity: Shared Risks & Fragmented Defenses," in *Explorations in Cyber Politics for the Cyber Age,* edited volume.

- Mohan, Vivek and Jack Goldsmith. Botnet Remediation: "Legal Strategies and Options." (*Brookings Institute*, forthcoming 2013).

WORKING PAPERS in PROGRESS

- Ellis, Ryan. "Regulating Cybersecurity: A Review," forthcoming, 2013. A review of the first set of mandatory cybersecurity regulations for the electric power industry.

- Ellis, Ryan. "National Security, Telecommunications, and Regulation," forthcoming 2013. A consideration current cybersecurity efforts within the context of the long and well-documented intersection of national security, telecommunications, and regulatory policy.

- Ellis, Ryan. "A Public Service or a Commodity? Models of Vulnerability Disclosure." Harvard Kennedy School Case Study Program, forthcoming 2014. A teaching case devoted to vulnerability disclosure and zero-days.

- Mohan, Vivek. "Data and Information Security: Consent Decrees and the Private Sector," forthcoming, 2013.

RESEARCH PAPERS on ECIR WEBSITE

- Abbassi, Puji, Martin Kaul, Vivek Mohan, Yi Shen, Zev Winkelman. Securing the Net: Global Governance in the Digital Domain. Berlin, Beijing, and Washington, D.C.: Report for Global Governance 2022, September 2013.

- Belk, Robert and Matthew Noyes. "On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy." Paper, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, March 2012.

- Camiña, Steven, Stuart Madnick, Nazli Choucri and Wei Lee Woon. "Exploring Terms and Taxonomies Relating to the Cyber International Research Field: or are 'Cyberspace' and Cyber Space' the same?" ECIR Working Paper, August 2011.

- Chiesa, Alessandro, Silvio Micali and Zeyuan Allen Zhu. "Knightian Auctions." ECIR Working Paper, January 10, 2012.

- Cho, Yiseul. "Lessons for Cyber security international cooperation." ECIR Working Paper, July 2012.

- Choucri, Nazli. "Cyberpolitics in International Relations." *précis,* MIT Center for International Studies. Spring 2013. http://web.mit.edu/cis/precis/2013spring/cyberpolitics.html#.Ue_4ddLijh4.

- Clark, David D. "Three Views of Cyberspace." Version 3.1. ECIR Working Paper, January 5, 2011.

- Clark, David D. "Characterizing Cyberspace: Past, Present, and Future." ECIR Working Paper, March 12, 2010.

- Goldsmith, Daniel and Michael Siegel. "Systematic Approaches to Cyber Insecurity." ECIR Working Paper, January 2012.

- Goldsmith, Daniel and Michael Siegel. "Understanding Cyber Complexity: Systems Modeling and the Financial Services Sector." ECIR Working Paper, February, 2010.

- Hill, Jonah Force. "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers." Paper, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2012.

- Hung, Shirley. "The Chinese Internet: Control Through the Layers." ECIR Working Paper, October 2012.

- Hurwitz, Roger and Patrick Winston. "Computational Representations of High Profile International Cyber Incidents." Paper presented to the panel Multi-Disciplinary Methods for Cyberspace Research at the Annual Meeting of the International Studies Association. Montreal, Quebec, Canada, March 2011.

- Hurwitz, Roger. "Taking Care: Four Takes on the Cyber Steward." Paper presented to CyberDialogue 2012: What is Stewardship in Cyberspace? Canada Centre for Global Security Studies at the Munk School of Global Affairs, Toronto, Ontario, Canada, March 2012.

- Hurwitz, Roger. "Trip report: The Budapest Cyberspace Conference on Cyberspace 2012," October 3 – 5, 2012.

- Madnick, Stuart, Nazli Choucri, Steven Camiña, Erik Fogg and Xitong Li. "Explorations in Cyber International Relations (ECIR) – Data Dashboard Report #1: CERT Data Sources and Prototype Dashboard System." ECIR Working Paper, August 2009.

- Madnick, Stuart, Wei Lee Woon, Andreas Henschel, Erik Casagrande, Ayse Firat, *et al.* "Technology Forecasting Using Data Mining and Semantics: Third & Final Annual Report." ECIR Working Paper CISL# 2011-01. May 2011.

- Mallery, John. "Trustworthy Cloud Computing: Risks, Challenges And Recommendations." Paper presented at the 2011 Workshop on Cyber Security and Global Affairs, Budapest, Hungary, May 31 – June 2, 2011.

- Maurer, Tim. "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-security." Discussion Paper 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School. September 2011.

- Maurer, Tim. “WikiLeaks 2010: A Glimpse of the Future? Discussion Paper 2011-12,” Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School. August 2011.

- Micali, Silvio, Jing Chen, and Avinatan Hassidim. “Resilient and Virtually Perfect Revenue from Perfectly Informed Players.” ECIR Working Paper. January 13, 2010.

- Mohan, Vivek. “The Electronic Communications Privacy Act (ECPA) & Need for Reform.” 2012.

- Mohan, Vivek. “Specialized Services Research and Summaries.” Briefing document prepared for the FCC’s Open Internet Advisory Committee (Jonathan Zittrain, Chair) 2012.

- Narayanamurti, Venkatesh, Tolu Odumosu, and Lee Vinsel. “The Discovery-Invention Cycle: Bridging the Basic/Applied Dichotomy.” Discussion Paper 2013-02, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2013.

- Nye, Joseph S. "Cyber Power." Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

- Ramtin, Amin. “Moving Forward on an International Convention for Cyberspace.” Project Minerva Working Paper Series. September 2010.

- Reardon, Robert and Nazli Choucri. “The Role of Cyberspace in International Relations: A View of the Literature.” Paper prepared for the 2012 ISA Annual Convention. San Diego, CA. April 1, 2012.

- Sechrist, Michael and Aki Peritz. “Protecting Cyberspace and the U.S. National Interest.” ECIR Working Paper. 2010.

- Sechrist, Michael. “Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership.” ECIR Working Paper. March 23, 2010.

- Sechrist, Michael. “New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems.” Discussion Paper 2012-03, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School. February 2012.

- Shukla, Aadya and Roger Hurwitz. "A Framework for Organizing Nati Security Strategies." Paper presented to the panel on Comparative Security Strategies at the International Studies Association Annual Meeting, San Diego, CA. April 4, 2012.

- Smith, James F. "Confronting Complex Cybersecurity Challenges." *Belfer Center Newsletter*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Summer 2013onal

- Siegel, Michael and Daniel Goldsmith. "Simulation Modeling for Cyber Resilience." ECIR Working Paper. October 2010.

- Sowell, Jesse H. "A View of Top-Down Governance." Paper presented to NANOG 55, Vancouver BC, June 4, 2012; Global Peering Forum (GPF7.0), New Orleans, LA, March 21, 2012; UKNOF23 , London, UK, October 9, 2012 and UKNOF24, London, UK, January 17, 2013.

- Sowell, Jesse H. "Mixed Context and Privacy." ECIR Working Paper. November 2010.

- Williams, Cindy. "Applications of ECIR Modeling Work to Cyber Policy Problems." ECIR Working Paper. March 10, 2010.

- Woon, Wei Lee, Andreas Henschel and Stuart Madnick. "A Framework for Technology Forecasting and Visualization." Working Paper CISL# 2009-11. September 2009.

- Young, William. "A System Safety Approach to Assuring Air Operations Against Cyberspace
  Disruptions." ECIR Working Paper, February 2013.

POSTED on SSRN

- Clark, David D. "Control Point Analysis." ECIR Working Paper, Version 2.2. September 10, 2012. 2012 TRPC Conference
  http://papers.ssrn.com/sol3/papers.cfm?abstract_id=203212.

- Choucri, Nazli and David D. Clark. "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma." November 2012. MIT Political Science Department Research Paper No. 2012-29
  http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2178586.

- Choucri, Nazli, Gihan Daw Elbait, and Stuart Madnick. "What is Cybersecurity? Explorations in Automated Knowledge Generation. " November 2012. MIT Political Science Department Research Paper No. 2012-30, November 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2178616.

- Madnick, Stuart, Xitong Li and Nazli Choucri. "Experiences and Challenges with using CERT Data to Analyze International Cyber Security." *Proceedings of the AIS SIGSEC Workshop on Information Security & Privacy* (WISP 2009) Phoenix, Arizona, December 2009: 6-16. [SWP #4759-09, CISL 2009-13, http://ssrn.com/abstract=1478206].

- Madnick, Stuart, Nazli Choucri, Steven Camiña, Erik Fogg, Xitong Li and Wei Fan. "Explorations in Cyber International Relations (ECIR) - Data Dashboard Report #1: CERT Data Sources and Prototype Dashboard System." September 2009. MIT Sloan Research Paper No. 4754-0 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1477618.

- Micali, Silvio, Nazli Choucri, Jing Chen, Cindy Williams. "Resilient Mechanism Design Foundations for Governance of Cyberspace: Exploration in Theory, Strategy, and Policy." MIT Political Science Department Research Paper No. 2013-30. August 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2317524.

- Rady, Mina. "Anonymity Networks: New Platforms for Conflict and Contention." MIT Political Science Department Research Paper No. 2013-5. March 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2241536.

- Woon, Wei Lee, Andreas Henschel and Stuart Madnick. "A Framework for Technology Forecasting and Visualization." September 2009. MIT Sloan Research Paper No. 4757-09. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478054.

WORKSHOP AND CONFERENCE PROCEEDINGS

- Azar, Pablo, Jing Chen, and Silvio Micali. "Crowdsourced Bayesian auctions." In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS 2012)*. ACM, New York, NY, USA, 236-248. DOI=10.1145/2090236.2090257 http://doi.acm.org/10.1145/2090236.2090257.

- Azar, Pablo and Silvio Micali. Rational proofs. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing (STOC 2012)*. ACM, New York, NY,

USA, 1017-1028. DOI=10.1145/2213977.2214069
http://doi.acm.org/10.1145/2213977.2214069.

- Clark, David D. and Landau, Susan. "The Problem Isn't Attribution; It's Multi-stage Attacks." *ReARCH '10 Proceedings of the Re-Architecting the Internet Workshop.* ACM New York, NY ©2010.

- Finlayson, Mark and Raquel Hervás. "The Prevalence of Descriptive Referring Expressions." *Proceedings of the ACL 2010 Conference Short Papers*. Uppsala, Sweden. July 11-16, 2010: 49–54.

- Finlayson, Mark and Nidhi Kulkarni. "jMWE: A Java Toolkit for Detecting Multi-Word Expressions. " *Proceedings of the 8th Workshop on Multiword Expressions: from Parsing and Generation to the Real World,* (MWE 2011) Portland, OR. June 23, 2011: 122-124.

- Finlayson, Mark. "Sets of Signals, Information Flow, and Folktales." *Proceedings of the Centennial Turing Conference, Special Session on Open Problems in the Philosophy of Information.* Cambridge, England. 2012.

- Finlayson, Mark. "The Story Workbench: An Extensible Semi-Automatic Text Annotation Tool." *Proceedings of the 4th Workshop on Intelligent Narrative Technologies*. Stanford, CA. November 2011: 21-24.

- Finlayson, Mark. "Corpus Annotation in Service of Intelligent Narrative Technologies." *Proceedings of the 4th Workshop on Intelligent Narrative Technologies*. Stanford, CA. November 2011: 17-20.

- Friedman, Allan, Tyler Moore, and Ariel D. Procaccia. "Would a 'Cyber Warrior' Protect Us? Exploring Trade-offs Between Attack and Defense of Information Systems." *Proceedings of the 2010 New Security Paradigms Workshop*. Concord, MA. September 2010: 85-94.

- Goldsmith, Daniel and Michael Siegel. "Cyber Politics: Understanding the use of Social Media for Dissident Movements in an Integrated State Stability Framework." *IEEE Proceedings of the 2012 International Conference on Advances in Social Network Analysis and Mining.* (ASONAM 2012). Istanbul, Turkey. August 201.2

- Houghton, James, Michael Siegel and Daniel Goldsmith. "Modeling the Influence of Narratives on Collective Behavior Case Study: Using social media to predict the

outbreak of violence in the 2011 London Riots." *Proceedings of The 31st International Conference of the System Dynamics Society*, Cambridge, MA. July 21 – July 25, 2013.

- Houghton, J., Siegel, M., Wirsch, A., Moulton, A., Madnick, S. , Goldsmith, D. "A Survey of Methods for Data Inclusion in System Dynamics Models." In the *Proceedings of the 32nd International Conference of the System Dynamics Society*. Delft, Netherlands, 2014.

- Houghton, J. Siegel, M. Vukovic, M. Towards a Model for Resource Allocation in API Value Networks. Paper presented at the *Intelligent Service Clouds Workshop 2014*.

- Krakauer, Caryn and Patrick Henry Winston. "Story Retrieval and Comparison using Concept Patterns." In Mark A. Finlayson, Pablo Gervas, Deniz Yuret, and Floris Bex, eds., in *Proceedings of the 3rd workshop on Computational Models of Narrative*, ELRA 3 (2012): 119-124.

- Madnick, Stuart, Nazli Choucri, Xitong Li and Jeremy Ferwerda. "Comparative Analysis of Cybersecurity Metrics to Develop New Hypotheses." *Proceedings of the Workshop on Information Security & Privacy* (WISP2011) (Jointly hosted by AIS SIGSEC and IFIP TC11.1) Shanghai, China. December 2011.

- Mallery, John. "International Data Exchange and A Trustworthy Host: Focal Areas For International Collaboration In Research And Education." *Proceedings of the BIC Annual Forum*, Brussels, Belgium. November 29, 2011.

- Micali, Silvio, Pablo Azar, and Jing Chen. "Crowdsourced Bayesian auctions." *Proceedings of the 3rd Innovations in Innovations in Theoretical Computer Science* (ITCS 2012) Cambridge, MA. January 2012: 236-248.

- Raja, Anita, Catriona Kennedy and Roger Hurwitz. "Socially Intelligent Agents to support Ethical Decision-making." *Proceedings of AAMAS 2012 First International Workshop on Human-Agent Interaction Design and Models*. Valencia, Spain. June 2012: 123-130.

- Sechrist, Michael, Chintan Vaishnav, Daniel Goldsmith, and Nazli Choucri. "The Dynamics of Undersea Cables: Can the Old Modes of Governance Cope with New Demands of the Cyberspace?" *Proceedings of the 30th International Conference of the System Dynamics Society*, eds., Elke Husemann and David Lane. St. Gallen, Switzerland. July 22 – 26, 2012 .

- Sowell, Jesse H. "Mixed Context and Privacy." *Proceedings of the 38th Research Conference on Communication, Information and Internet Policy*, Telecommunications Policy Research Consortium, Farnham, VA. October 2010.

- Sowell, Jesse H. "Empirical Studies of Bottom-up Internet Governance." *Proceedings of the 40th Research Conference on Communication, Information and Internet Policy*. Telecommunications Policy Research Consortium, Arlington, VA. September 21–23, 2012.

ONLINE EDITORIALS

- Branscomb, Lewis and Ryan Ellis. "Dangerous Cargo: Action Needed on Hazardous Materials." *Power & Policy Blog*, June 13, 2013. http://www.powerandpolicy.com/2013/06/13/dangerous-cargo-action-needed-on-hazardous-materials/#more-2413.

- Ellis, Ryan. "Protecting US Critical Infrastructure: One Step Forward for Cybersecurity, One Back?" *Technology+Policy | Innovation@Work*, July 24, 2013 http://www.technologyandpolicy.org/2013/07/24/protecting-us-critical-infrastructure-one-step-forward-for-cybersecurity-one-back/#.Uflkx9Lijh6.

- Ellis, Ryan. "Cyber Security." Defense and Intelligence Projects Podcast. Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, March 5, 2013. http://belfercenter.ksg.harvard.edu/files/uploads/audio/Defense/Ellis.mp3.

- Kello, Lucas. "The Skeptics Misconstrue the Cyber Revolution: A Response to Commentators on ISSF/H-Diplo and Elsewhere." *H-Diplo/ISSF*, October 28, 2013 http://www.h-net.org/~diplo/ISSF/PDF/RE17.pdf.

- Mohan, Vivek. "Privacy Consciousness in the Big Data Era." *Hive*, May 15, 2013 http://hivedata.com/privacy-consciousness-in-the-big-data-era/.

- Mohan, Vivek. "Why the Government Matters: A Primer for Data-Minded Entrepreneurs." *Hive,* April 12, 2013 http://hivedata.com/why-the-government-matters-a-primer-for-data-minded-entrepreneurs/.

- Mohan, Vivek. "Scaling the Great Firewall." *The Indian Express*, March 2013 http://www.indianexpress.com/news/scaling-the-great-firewall/1084749/0.

- Mohan, Vivek. "Nothing to See Here." *The Indian Express*, December 2012 http://www.indianexpress.com/news/nothing-to-see-here/1041463/0.

- Odumosu, Tolu. "Technological Somnambulism Revisited: Sleeping through the New Invisible Surveillance Technologies." *Vignettes@STS.Next.20*, December 31, 2012 http://stsnext20.org/vignettes/2012/12/31/technological-somnambulism-revisited-sleeping-through-the-new-invisible-surveillance-technologies/.

- Tumin, Zachary and William Bratton. "Viral By Design: Teams in the Networked *World." Harvard Business Review*, April 2, 2012. http://blogs.hbr.org/2012/04/viral-by-design-teams-in-the-n/.

- Tumin, Zachary. "Running Al Qaeda." *Reuters Magazine*, June 2012 http://blogs.reuters.com/great-debate/2012/06/27/running-al-qaeda/.

THESES AND DISSERTATIONS

- Capen Low, Harold W. *Story Understanding in Genesis: Exploring Automatic Plot Construction through Commonsense Reasoning*. MS thesis, MIT (2011): Cambridge, MA.

- Fay, Matthew P. *Enabling Imagination through Story Alignment*. MS Thesis, MIT (2012): Cambridge, MA.

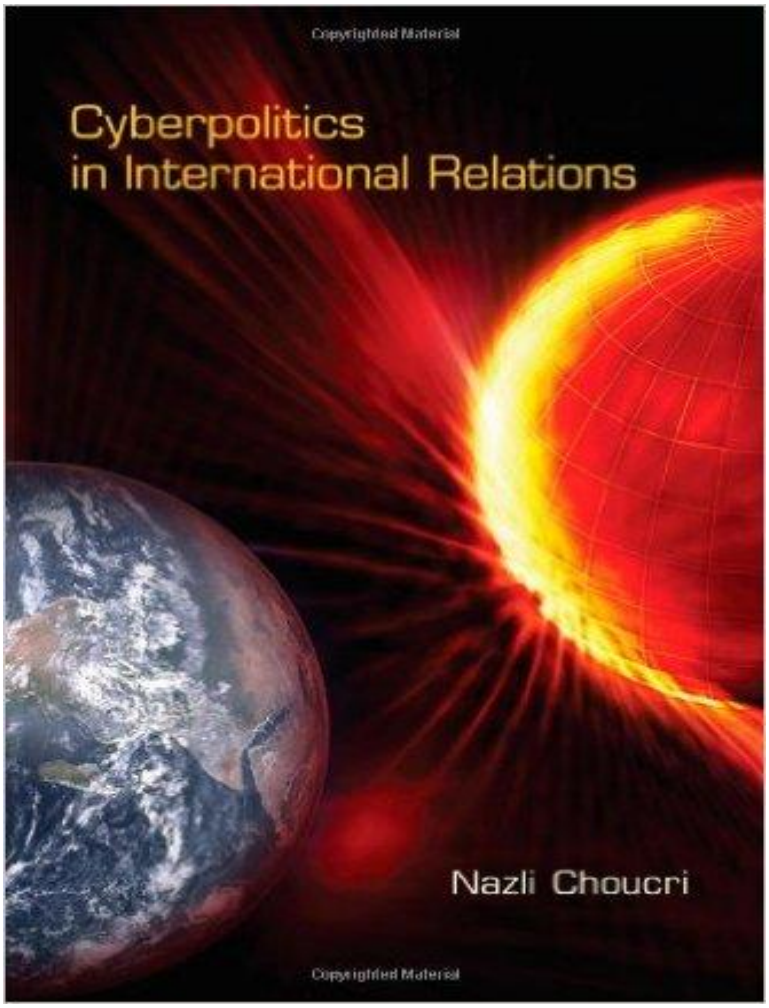
- Krakauer, Caryn. *Story Retrieval and Comparison Using Concept Patterns*. MS thesis (2012): Cambridge, MA.

- Nackoul, David. *Text to Text: Plot Unit Searches Generated from English*. MS thesis thesis, MIT(2010): Cambridge, MA

- Sewell, Jesse Horton. *Finding Order in a Contentious Internet* PhD thesis MIT, 2015

APPENDIX-2

Table of Contents for



CYBERPOLITICS IN INTERNATIONAL RELATIONS

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX A-3

Table of Contents

for

ECIR Explorations in Cyberspace and International Relations

Challenges, Investigations, Analysis, Results

Editors:

Nazli Choucri, David D. Clark, and Stuart Madnick

Table of Contents

Engineering Symposium. CESUN 2012, Delft University of Technology, 18-20 June 2012. MIT Political Science Department Research Paper No. 2012-16, SSRN

9. **Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda,** "Institutional Foundations for Cyber Security: Current Responses and Global Imperatives." *Information Technology for Development* (2013).

10. **Sowell, Jesse H.** "Empirical Studies of Bottom-Up Internet Governance." *Proceedings of the 40th Research Conference on Communication, Information and Internet Policy,* Telecommunications Policy Research Consortium. Arlington, VA. September 21–23, 2012

11. **Gamero-Garrido, Alexander.** "Cyber Conflicts in International Relations: Framework and Case Studies." ECIR Working Paper, March 2014

Part III
Methods, Modeling, & Simulation

12. **Houghton, James, Michael Siegel and Daniel Goldsmith.** "Modeling the Influence of Narratives on Collective Behavior Case Study: Using social media to predict the outbreak of violence in the 2011 London Riots." *Proceedings of the 31st International Conference of the System Dynamics Society*, Cambridge, MA. July 21 – July 25, 2013

13. **Hurwitz, Roger and Patrick Winston. "**Computational Representations of High Profile International Cyber Incidents." Paper presented to the panel, "Multi-Disciplinary Methods for Cyberspace Research," at the Annual Meeting of the International Studies Association, Montreal, Quebec, Canada, March 2011

14. **Patrick Winston "**The Right Way." *Advances in Cognitive Systems* 1 (2012): 23–36

15. **Goldsmith, Daniel and Michael Siegel.** "Cyber Politics: Understanding the use of Social Media for Dissident Movements in an Integrated State Stability Framework." *IEEE Proceedings of the 2012 International Conference on Advances in Social Network Analysis and Mining.* (ASONAM 2012) Istanbul, Turkey. August 2012.

16. **Woon, Wei Lee and Stuart Madnick**. "Semantic distances for Technology Landscape Visualization." *Journal of Intelligent Information Systems* 39 (1) (2012): 29-58

17. **Choucri Nazli, Gihan Daw Elbait and Stuart Madnick.** "What is Cybersecurity? Explorations in Automated Knowledge Generation." MIT Political Science Department Research Paper No. 2012-30, SSRN. November 2012

18. **Madnick, Stuart, Xitong Li and Nazli Choucri**. "Experiences and Challenges with using CERT Data to Analyze International Cyber Security." *Proceedings of the AIS SIGSEC Workshop on Information Security & Privacy* (WISP 2009) Phoenix, Arizona, December 2009: 6-16. [SWP #4759-09, CISL 2009-13

19. **Madnick, Stuart, Nazli Choucri, Xitong Li and Jeremy Ferwerda**. "Comparative Analysis of Cybersecurity Metrics to Develop New Hypotheses." *Proceedings of the Workshop on Information Security & Privacy* (WISP2011) (Jointly hosted by AIS SIGSEC and IFIP TC11.1) Shanghai, China. December 2011

Part IV
Policy and Policy Analysis

20. **Hurwitz, Roger. "**Taking Care: Four Takes on the Cyber Steward." Paper presented to Cyber Dialogue 2012: What is Stewardship in Cyberspace?." Munk School of Global Affairs, March 2012

21. **Hurwitz, Roger.** "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly.* 6 (3) (Fall 2012): 20-45

22. **Micali, Silvio, Nazli Choucri, Jing Chen and Cindy Williams. "**Resilient Mechanism Design Foundations for Governance of Cyberspace Exploration in Theory, Strategy, and Policy." ECIR Working Paper, August 2013

23. **Testart, Cecilia. "**Understanding ICANN's Complexity in a Growing and Changing Internet." ECIR Working Paper, March 2014

24. **Sechrist, Michael, Chintan Vaishnav, Daniel Goldsmith, and Nazli Choucri**. "The Dynamics Undersea Cables: Can the Old Modes of Governance Cope with New Demands of the Cyberspace?" *Proceedings of the 30th International*

*Conference of the System Dynamics Society***,** eds., Elke Husemann and David Lane. St. Gallen, Switzerland. July 22 – 26, 2012

25. **Nye, Jr., Joseph S.** 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5(4): 18-38.

26. **Rady, Mina.** Anonymity Networks: New Platforms for Conflict and Contention, ECIR Working Paper, 2013.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX A-3

Abstracts of Chapters

for

ECIR Explorations in Cyberspace and International Relations

Challenges, Investigations, Analysis, Results

Editors:

Nazli Choucri, David D. Clark, and Stuart Madnick

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.

Abstract of Chapters

1. **Choucri, Nazli, David D. Clark, and Stuart Madnick "**Introduction to ECIR Volume".

Cyber International Relations, refers to the conjunction of two domains or realities—those pertaining to emergent trends in international relations and those enabled by a constructed domain (cyber) as a new arena of human interaction with its own modalities, realities, and contentions. This chapter introduces the features of cyberspace that are creating powerful challenges in international relations theory, actions, methods, and policy. It introduces the three parts of the book and their respective content.

Part I: Challenges of the Cyber Age

2. **Reardon, Robert and Nazli Choucri**. "The Role of Cyberspace in International Relations: A View of the Literature." Paper prepared for the 2012 ISA Annual Convention. San Diego, CA. April 1, 2012.

This paper reviews the literature on cyber international relations of the previous decade. The review covers all journal articles on the role of cyberspace and information technology that appeared in 26 major policy, scholarly IR, and political science journals between the years 2001-2010. The search yielded 49 articles, mostly from policy journals. The articles are sorted into five distinct issue areas: global civil society, governance, economic development, the effects on authoritarian regimes, and security. The review identifies, and discusses the significance of three unifying themes throughout all of the articles: efforts to define the relevant subject of analysis; cyberspace's qualitatively transformative effects on international politics, particularly the empowerment of previously marginalized actors; and, at the highest analytic level, efforts to theoretically capture the mutually embedded relationship between technology and politics. These themes can help guide future research on cyber international relations, and focus attention on ways that debates within each of the five distinct issue areas are interconnected, and can be usefully approached using a unified conceptual framework.

3. **Choucri, Nazli.** "Emerging Trends in Cyberspace: Dimensions & Dilemmas." Prepared for the conference on Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition. The Matthew B. Ridgway Center for International Security Studies. University of Pittsburg. November 1-2, 2012. Chapter to appear in an edited volume by the *Strategic Studies Institute*.

Almost everyone everywhere recognizes that cyberspace is a fact of daily life. Created by human ingenuity with the Internet at its core, cyberspace has become a fundamental feature of the 21st century. Almost overnight, interactions in this virtual domain have catapulted to the realm of high politics and are at the forefront of almost all major issues in international relations. Today, this domain has become a source of vulnerability – posing potential threats to national security and a disturbance of the familiar international order – and a major arena of unlimited opportunity for power and potential across various forms of value. The rapidly shifting configurations of interactions in this virtual domain – with expanding actors and actions with diverse causes and consequences – continue to create major disturbances in the traditional system, a major legacy of the 20th century.

The vocabulary of world politics has already accommodated these new realities by signaling references to cyber conflict, cyber power, cyber intrusion, cyber cooperation, cyber security, to name only a few. The early concepts were put forth in hyphenated terms (such as cyber-security); now these are increasingly framed in one word (notably, cybersecurity). At first glance, such differences might seem trivial, but the shifts points to an explicit recognition of a new phenomenon, one that is no longer captured by the hyphenated concepts imported from the familiar politics of 20th century international relations.

4. **Clark, David D. and Susan Landau** "Untangling Attribution." *Proceedings of a Workshop on Deterring Cyberattacks: Information Strategies and Developing Options for U.S. Policy*, Washington, DC: The National Academies Press, 2010, 25-40 and Harvard National Security Journal, 2011

   As a result of increasing Internet insecurity — DDoS attacks, spam, cybercrime, and data theft — there have been calls for an Internet architecture that would link people to packets (the fundamental communications unit used in the Internet). The notion is that this technical "fix" would enable better investigations and thus deterrence of attacks. However, in the context in which the most serious national-security cybersecurity threat the US faces is data exfiltration from corporate and government sites by other jurisdictions, such a solution would be a mistake.

5. **Clark, David D**. "Control Point Analysis." ECIR Working Paper, Version 2.2 of September 10, 2012. 2012 TRPC Conference, SSRN**.**

As the Internet becomes more and more embedded in every sector of society, more and more actors have become concerned with its character, now and in the future. The private sector actors, such as Internet Service Providers or ISPs, are motivated by profits as they shape and evolve the Internet. The public sector is driven by a range of objectives: access and uptake, competition policy, regime stability, policies with regard to controlling access to classes of content, and the like. The range of actions open to governments to shape the Internet are

traditional and well-understood, including law and regulation, procurement, investment in research and development, participation in the standards process and more diffuse forms of leadership. But these actions do not directly shape the Internet.

6. **Clark, David D. "**Characterizing Cyberspace: Past, Present, and Future." ECIR Working Paper, March 12, 2010

In general terms, most practitioners share a working concept of cyberspace—it is the collection of computing devices connected by networks in which electronic information is stored and *utilized, and communication takes place. Another way to understand the nature of cyberspace is* to articulate its purpose, which I will describe as the processing, manipulation and exploitation of information, the facilitation and augmentation of communication among people, and the interaction of people and information. Both information and people are central to the power of cyberspace. If we seek a better understanding of what cyberspace might be, one approach is to identify its salient characteristics: a catalog of its characteristics may be more useful than a list of competing definitions.

Part II: Foundations for Cyber-IR Theory

7. **Choucri, Nazli and David D. Clark**. **"**Integrating Cyberspace and International Relations: The Co-Evolution Dilemma**."** MIT Political Science Department Research Paper No. 2012-29, November 2012, SSRN

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

8. **Vaishnav, Chintan, Nazli Choucri and David D. Clark "**Cyber International Relations as an Integrated System." Paper presented at the Third International Engineering Symposium. CESUN 2012, Delft University of Technology, 18-20 June 2012. MIT Political Science Department Research Paper No. 2012-16, SSRN

The purpose of this paper is to develop coordinates of the milieu where the activities and spheres of influence of those who use and provision the Internet intersect and possibly compete with each other, and how they come in contact with the activities of the State and other international actors. Our focus is not on understanding the venues in the Internet infrastructure where such interactions occur, but is on the core activities of the various actors that brings them together.

The Internet domain is contingent on the activities of multiple actors who are interdependent in various ways, and who are highly heterogeneous in their roles and capabilities, each often trying to gain advantage and expand its influence. International relations can also be characterized in those terms. This work is fundamental to any systematic understanding of how the two domains—jointly called Cyber International Relations—interconnect. Its goal is to provide a baseline upon which could be built the understanding of the nature of the heterogeneous influences of the various actors, and the various outcomes that could result from it.

9. **Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda,** "Institutional Foundations for Cyber Security: Current Responses and Global Imperatives." *Information Technology for Development* (2013).

Almost everyone recognizes the salience of cyberspace as a fact of daily life. Given its ubiquity, scale, and scope, cyberspace 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 increasingly for people in the developing world. This paper seeks to provide an initial baseline, for representing and tracking institutional responses to a rapidly changing international landscape, real as well as virtual. We shall argue that the current institutional landscape managing security issues in the cyber domain has developed in major ways, but that it is still "under construction." We also expect institutions for cyber security to support and reinforce the contributions of information technology to the development process. We begin with (a) highlights of international institutional theory and an empirical "census" of the institutions-in-place for cyber security, and then turn to (b) key imperatives of information technology-development linkages and the various cyber processes that enhance developmental processes, (c) major institutional responses to cyber threats and cyber crime as well as select international and national policy postures so critical for industrial countries and increasingly for developing states as well, and (d) the salience of new mechanisms designed specifically in response to cyber threats.

10. **Sowell**, **Jesse H.** "Empirical Studies of Bottom-Up Internet Governance." *Proceedings of the 40th Research Conference on Communication, Information and Internet Policy,* Telecommunications Policy Research Consortium. Arlington, VA. September 21–23, 2012

The notion of bottom-up governance in the Internet is not new, but the precise underlying mechanisms have received little primary, empirical study. The majority of Internet governance literature is couched in contrasting familiar top-down modes of governance with the design of and subsequent critique of governance institutions such as ICANN or the WSIS processes that created the Internet Governance Forum (IGF). This paper reports on dissertation work collecting and analyzing empirical evidence of how bottom-up governance mechanisms operate in situ. Methodologically, participant-observer ethnographies are supplemented by text mining and social network analysis—the combination facilitates analysis of community-generated artifacts cross-validated against semi-structured interviews. This paper reports on ethnographic studies

thus far, drawing on early interviews and private conversations. Scoping the domain, this work evaluates organizational modes at the intersection of Internet operations and security. Three categories of non-state organizational modes contribute evidence: network operator groups (NOGs) and RIRs; Internet eXchange Points (IXPs); anti-abuse organizations and communities such as the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), Spamhaus, and the Anti-Phishing Working Group (APWG). As of this writing, the anti-abuse study is the least developed study and will be addressed comparatively. The author engages as a participant-observer in forums from each category, developing relationships and engaging in semi-structured interviews with participants and organizers.

11. **Gamero-Garrido, Alexander. "**Cyber Conflicts in International Relations: Framework and Case Studies." ECIR Working Paper, March 2014

Twenty years ago, the possibility of having an international conflict extend into the cyber domain was distant. Since then much has changed. Today cyber conflict is not considered particularly unusual. But considerable uncertainties remain about the nature, scale, scope and other features of such conflicts. This paper addresses these issues using a re-analysis of the case studies presented in A Fierce Domain recently published by the Atlantic Council. In addition, we draw upon other materials (academic and media) to expand our understanding of each case, and add several cases to the original collection resulting in a data set of 17 cyber conflict, spanning almost three decades (1985-2013). Cuckoo's Egg, Morris Worm, Solar Sunrise, EDT, ILOVEYOU, Chinese Espionage, Estonia, Russo-Georgian war, Conficker, NSA-Snowden, WikiLeaks and Stuxnet are some of the major cases included. This study presents each case in terms of (a) its socio-political context, (b) technical features, (c) the outcome and inferences drawn in the sources examined. The profile of each case includes the actors, their actions, tools they used and power relationships, and the outcomes with inferences or observations. Emphasis is placed on characteristics of cyberspace visible on conflicts. Findings include: Distributed Denial of Service is the most common offensive action; accountability is difficult in cyberspace, particularly with international conflicts; outcomes of each instance have been variable, and economic impact is hard to estimate; the private sector has been a key player in cybersecurity; size of an actor, and countries' ICT infrastructure, influence the nature of the cyber conflicts.

Part III: Methods, Modeling, & Simulation

12. **Houghton, James, Michael Siegel and Daniel Goldsmith**. "Modeling the Influence of Narratives on Collective Behavior Case Study: Using social media to predict the outbreak of violence in the 2011 London Riots." *Proceedings of the 31st International Conference of the System Dynamics Society*, Cambridge, MA. July 21 – July 25, 2013

This paper considers the problem of understanding the influences of narratives or stories on individual and group behavior. Narrative theory describes how stories help people make sense of the world, and is being used to explain behavior in domains such as security, health care, and consumer behavior. We are interested in using narrative theory to develop better predictions of behavior and have developed a multi-methodology approach to combine narrative influence with system dynamics modeling of group behavior. Our model quantifies how individuals use narratives to understand current events and make decisions. We model the time-varying strength of cultural narratives as a degree of belief in the narrative's explanatory power, updated heuristically in response to observations about similarity between cultural narratives and current events. We use Twitter posts to measure narrative-significant observations in the real world. Using this approach, we investigate a case study of the violent riots in London in 2011 and demonstrate how relevant narratives can be identified, monitored, and included in behavior models to predict violent activity.

13. **Hurwitz, Roger and Patrick Winston. "**Computational Representations of High Profile International Cyber Incidents." Paper presented to the panel, "Multi-Disciplinary Methods for Cyberspace Research," at the Annual Meeting of the International Studies Association, Montreal, Quebec, Canada, March 2011

Several high profile incidents have shaped both popular and government understanding of international cyber conflicts. One of the most iconic is the distributed denial of service attack (DDoS) on Estonian government, media and financial sites in April-May, 2007. The attack by "hacktivists" in Russia, perhaps supported by the Russian government, was a response to symbolic and legal moves by the Estonian government to expunge traces of Estonia's subjugation to the Soviet Union.

14. Patrick Winston "The Right Way." *Advances in Cognitive Systems* 1 (2012): 23–36
I ask why humans are smarter than other primates, and I hypothesize that an important part of the answer lies in the Inner Language Hypothesis, a prerequisite to what I call the Strong Story Hypothesis, which holds that storytelling and understanding have a central role in human intelligence. Next, I introduce the Directed Perception Hypothesis, which holds that we derive much of our common sense, including the common sense required in story understanding, by deploying our perceptual apparatus on real and imagined events. Both the Strong Story Hypothesis and the Directed Perception Hypothesis become more valuable in light of our social nature, an idea captured in the Social Animal Hypothesis.

15. **Goldsmith, Daniel and Michael Siegel.** "Cyber Politics: Understanding the use of Social Media for Dissident Movements in an Integrated State Stability Framework." *IEEE Proceedings of the 2012 International Conference on Advances in Social Network Analysis and Mining.* (ASONAM 2012) Istanbul, Turkey. August 2012

Recent events in North Africa and the Gulf States have highlighted both the fragility of states worldwide and the ability of coordinated dissidents to challenge or topple regimes. The common processes of 'loads' generated by dissident activities and the core features of state resilience and its 'capacity' to withstand these 'loads' have been explored in the traditional "real world" view. More recently, however, there has been increased attention to the "cyber world"—the role of cyber technologies in coordinating and amplifying dissident messages, as well as in aiding regimes in suppressing anti-regime dissidents. As of yet, these two views (real and cyber) have not been integrated into a common framework that seeks to explain overall changes in regime stability over time. Further, emerging uses of social media technologies, such as Twitter have not fully been examined within an overall framework of state stability that represents the nature and dynamics of 'loads' generated by dissident activities in the real (i.e. protests) and cyber (i.e., planning and coordination via cyber venues) domains.

16. **Woon, Wei Lee and Stuart Madnick**. "Semantic distances for Technology Landscape Visualization." *Journal of Intelligent Information Systems* 39 (1) (2012): 29-58

This paper presents a novel approach to the visualization of research domains in science and technology. The proposed methodology is based on the use of bibliometrics; i.e., analysis is conducted using information regarding trends and patterns of publication rather than the actual content. In particular, we explore the use of term co-occurrence frequencies as an indicator of semantic closeness between pairs of terms. To demonstrate the utility of this approach, a number of visualizations are generated for a collection of renewable energy related keywords.As these keywords are regarded as manifestations of the associated research topics, we contend that the proposed visualizations can be interpreted as representations of the underlying technology landscape.

17. **Choucri Nazli, Gihan Daw Elbait and Stuart Madnick** "What is Cybersecurity? Explorations in Automated Knowledge Generation." MIT Political Science Department Research Paper No. 2012-30, SSRN. November 2012

This paper addresses a serious impediment to theory and policy for cybersecurity: Trivial as it might appear on the surface, there is no agreed upon understanding of the issue, no formal definition, and not even a consensus on the mere spelling of the terms — so that efforts to develop policies and postures, or capture relevant knowledge are seriously hampered. In this context, we present a "proof of concept" for a new research strategy based on a close examination of a large corpus of scholarly knowledge, and the extent to which it enables us to generate new knowledge about cybersecurity of relevance to international relations and to national security relevant to the nation's security and to international relations. Given the new cyber realities, this paper is also a "proof" of how to create new knowledge through automated investigations of the record to date.

18. **Madnick, Stuart, Xitong Li and Nazli Choucri**. "Experiences and Challenges with using CERT Data to Analyze International Cyber Security." *Proceedings of the AIS SIGSEC Workshop on Information Security & Privacy* (WISP 2009) Phoenix, Arizona, December 2009: 6-16. [SWP #4759-09, CISL 2009-13

With the increasing interconnection of computer networks and sophistication of cyber attacks, it is important to understand the dynamics of such situations, especially in regards to cyber international relations. The Explorations in Cyber International Relations (ECIR) Data Dashboard Project is an initiative to gather worldwide cybersecurity data publicly provided by nation-level Computer Emergency Response Teams (CERTs) and to provide a set of tools to analyze the cybersecurity data. The unique contributions of this paper are: (1) an evaluation of the current state of the diverse nation-level CERT cybersecurity data sources, (2) a description of the Data Dashboard tool developed and some interesting analyses from using our tool, and (3) a summary of some challenges with the CERT data availability and usability uncovered in our research.

19. **Madnick, Stuart, Nazli Choucri, Xitong Li and Jeremy Ferwerda**. "Comparative Analysis of Cybersecurity Metrics to Develop New Hypotheses." *Proceedings of the Workshop on Information Security & Privacy* (WISP2011) (Jointly hosted by AIS SIGSEC and IFIP TC11.1) Shanghai, China. December 2011

Few Internet security organizations provide comprehensive, detailed, and reliable quantitative metrics, especially in the international perspective across multiple countries, multiple years, and multiple categories. As common refrain to justify this situation, organizations ask why they should spend valuable time and resources collecting and standardizing data.

We seek to provide an encouraging answer to this question by demonstrating the value that even limited metrics can provide in a comparative perspective. We present some findings generated through the use of a research tool, the Explorations in Cyber Internet Relations (ECIR) Data Dashboard. In essence, this dashboard consists of a simple graphing and analysis tool, coupled with a database consisting of data from disparate national-level cyber data sources provided by governments, Computer Emergency Response Teams (CERTs), and international organizations. Users of the dashboard can select relevant security variables, compare various countries, and scale information as needed.

In this paper, using this tool, we present an example of observations concerning the fight against cybercrime, along with several hypotheses attempting to explain the findings. We believe that these preliminary results suggest valuable ways in which such data could be used and we hope this research will help provide the incentives for organizations to increase the quality and quantity of standardized quantitative data available.

Part IV: Policy and Policy Analysis

20. Hurwitz, Roger. "Taking Care: Four Takes on the Cyber Steward." Paper presented to Cyber Dialogue 2012: What is Stewardship in Cyberspace?, Munk School of Global Affairs, March 2012

Stewardship denotes a custodial, non-proprietary relationship to a resource or domain. The notion of a "cyber steward" resonates with those of us who regard cyberspace as a commons or domain that belongs to no one, and yet we sense some duty to protect or manage it. This essay explores possible job descriptions of "cyber steward" and what might motivate a person or organization to take the job. The job description can vary with one's view of the commons. The motivations towards this stewardship usually involves more than the self-interested, prudential concern for future use of the commons, which drives self-organization to preserve natural resource commons. It can also involve more than a desire to reciprocate for the benefits now being enjoyed, as in the gift culture that marked the early days of the Internet. The "sense of duty" might answer to the interdependence of being in cyberspace, respond to a fear for the loss of its freedom, or harbour a utopian vision of a global society enabled by cyber networks. But it can also be a self-serving pretext to shield a ruling elite from criticism or to preserve some technological advantage over others.

21. Hurwitz, Roger "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly*. 6 (3) (Fall 2012): 20-45

Policymakers increasingly recognize the need for agreements to regulate cyber behaviors at the international level. In 2010, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security recommended "dialogue among States to discuss. Since then, the United States, Russia, China, and several other cyber powers have proposed norms for discussion, and in November 2011, the United Kingdom convened an intergovernmental conference to discuss cyber "rules of the road." These activities are a positive change from the first decade of this century, when the United States and Russia could not agree on what should be discussed and the one existing international agreement for cyberspace—the Budapest Convention on Cybercrime—gained little traction. Nevertheless, the search for agreement has a long way to go. Homeland Security secretary Janet Napolitano noted in summer 2011 that efforts for "a comprehensive international framework" to govern cyber behaviors are still at "a nascent stage." That search may well be disappointing. Council on Foreign Relations fellows Adam Segal and Matthew Waxman caution that "the idea of ultimately negotiating a worldwide, comprehensive cybersecurity treaty is a pipe dream." In their views, differences in ideologies and strategic priorities will keep the United States, Russia, and China from reaching meaningful agreements: "With the United States and European democracies at one end and China and Russia at another,

states disagree sharply over such issues as whether international laws of war and self-defense should apply to cyber attacks, the right to block information from citizens, and the roles that private or quasi-private actors should play in Internet governance."

22. **Micali, Silvio, Nazli Choucri, Jing Chen and Cindy Williams. "**Resilient Mechanism Design Foundations for Governance of Cyberspace Exploration in Theory, Strategy, and Policy." ECIR Working Paper, August 2013

Three related trends in world politics – shifting in power relations, increased diversity of actors and entities, and the growing mobilization and politicization of global constituencies are contributing to a global "tussle" which threatens to erupt in a full-fledged international confrontation. Such contests may well reinforce the potentially powerful cleavages, such as those that became evident before, during, and after the World Conference on Information Technology, WCIT-2012. If present trends continue, it is unlikely that WCIT-2013 will reduce the cleavages and resolve the contentions.

23. **Testart, Cecilia. "**Understanding ICANN's Complexity in a Growing and Changing Internet." ECIR Working Paper, March 2014

The ever-increasing relevance of the Internet in all aspects of our lives has significantly raised the interest of cyberspace in the political, economical and international spheres. Internet governance and its future design are now relevant to many different stakeholders eager to influence and engage in the decision and policy-making processes. The Internet Corporations for Assigned Names and Numbers (ICANN) is recognized as the central institution involved in the governance of the global Internet. Specifically, it is in charge of the allocation, coordination and development of policy relating to the critical Internet resources –Internet Protocol addresses, Domain Names System and parameter numbers. It was created in 1998, when the Internet had less than 10% of the current Internet users and the World Wide Web potential was just emerging, and was expected to have a technical mandate. Over time, ICANN structure has evolved, resulting in a large and complex institution, with several internal bodies intermingled with its functions. Nonetheless, a very limited number of Internet users know what ICANN is or what ICANN does, because the Internet has always "just worked". This paper contributes to the understanding of who participates in ICANN's decision-making and policy-development processes and how. It first examines in details the internal structure of the organization, and then its structural and financial evolution and change since its early stage. The study is based on an in-depth analysis of the legal, financial and public documents of ICANN, as well as the information published directly by ICANN's internal bodies. The paper reveals the substantial expansion in scale and scope of ICANN mandate and activities since its creation. ICANN recurring changes leading to the current complex structure and processes for policy development, allowed it to cope with and adapt to growth, evolution and change in the Internet and its usages. Additionally, these processes constitute an outreach mechanism for ICANN to its constituencies. However, the permanent internal restructuring, deter and hinder the follow up by external interested parties such as governments and international organizations, which are now requesting more involvement in policy-development processes concerning the Internet.

24. Nye, Jr., Joseph S. 2011. Nuclear Lessons for Cyber Security? Strategic Studies Quarterly 5(4): 18-38.

The explosive growth of cyberspace is the most recent "revolution in military affairs" that promises to have a profound effect on international relations. The commercial World Wide Web is less than two decades old, and it has exploded from a few million users in 1990s to some two billion users today. The Internet's emergence has created great opportunities and great vulnerabilities for states, but policymakers have yet to fully comprehend its function and implications. As a former director of the CIA has noted, "Rarely has something been so important and so talked about with less clarity and less apparent understanding [than cyber security]." If history is any guide, learning to navigate this new domain will take time. The United States and the Soviet Union took decades to adapt and respond to nuclear technology. As we try to make sense of our halting responses to the current cyber revolution, are there any lessons we can learn from our responses to the nuclear transformation? Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy. This article provides a short overview of the problem of cyber security and suggests several lessons that can be learned from the nuclear experience. While the two technologies are vastly different, there are nonetheless useful comparisons one can make of the ways in which governments learn to respond to technological revolutions.

25. Sechrist, Michael, Chintan Vaishnav, Daniel Goldsmith, and Nazli Choucri. "The Dynamics of Undersea Cables: Can the Old Modes of Governance Cope with New Demands of the Cyberspace?" *Proceedings of the 30th International Conference of the System Dynamics Society,* eds., Elke Husemann and David Lane. St. Gallen, Switzerland. July 22 – 26, 2012

Cyberspace is built on physical foundations that support the "virtual" manifestations we know of and use in everyday computing. Physical infrastructure can include wired, fiber optic, satellite and microwave links, as well as routing equipment. An often overlooked but critical part of the Internet infrastructure is undersea communication cable links. Undersea cables are the technology of choice to move large amounts of data around the world quickly. In the U.S., approximately 95% of all international Internet and phone traffic travel via undersea cables. Nearly all government traffic, including sensitive diplomatic and military orders, travels these cables to reach officials in the field. The problem, however, is that the undersea cable infrastructure is susceptible to several types of vulnerability, including: rising capacity constraints, increased exposure to disruption from both natural and mad-made sources, and emerging security risks from cable concentration in dense geographical networks (such as New York and New Jersey, and places like Egypt/Suez Canal.) Moreover, even under normal working conditions, there is a concern whether governance-as-usual can keep up with the future growth of Internet traffic. In this paper, we explore the impact of these problems on the dynamics of managing undersea cable infrastructure.

26. Rady, Mina. "Anonymity Networks: New Platforms for Conflict and Contention" ECIR Working Paper 2013.

Access to information is critical during population uprisings against repressive regimes. As a venue for information and data exchange, cyberspace offers many powerful social platforms for exchange of information. But the infrastructure of the Internet allows government to block or censor such platforms. In turn, anonymity networks emerged as conventional mechanisms for Internet users to circumvent government censorship. In this paper we show that anonymity networks became "terrains" for government-population conflict as they enable citizens to overpower governments' conventional control mechanisms over cyber-information exchanges. We delineate escalations of this cyber-conflict by studying two notable cases: Egypt, a simple case, and Iran, a more complex case. We take Tor network as the anonymity network that is subject of investigation. We highlight the range of actions that each actor can take to retaliate via anonymity networks. We conclude that design specifications and protocols of anonymous communication determine the strategies of escalation. Finally, we lay out the foundation for monitoring and analyzing dynamics and control point analysis of anonymous networks.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX A-4

Table of Contents

for

The Co-Evolution Dilemma: Cyberspace and International Relations

Authors

Nazli Choucri and David D. Clark

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.

TABLE of CONTENTS

for

The Co-Evolution Dilemma:

Cyberspace and International Relations

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX A-5

Report on

PERSPECTIVES on CYBERSECURITY

Annotated Table of Contents

Report on

PERSPECTIVES on CYBERSECURITY

`

Annotated of Table of Contents

1 Cybersecurity – Problems, Premises, Perspectives

Nazli Choucri and Chrisma Jackson

An introduction and comparative views of cyberspace

2 An Abbreviated Technical Perspective on Cybersecurity

Ben Z. Yan

Chapter 2 focuses on key technical issues. The purpose is to provide a "platform" that serves as foundations for understanding the technical functionalities essential for Internet operations and, by extensions, the potential targets for threat or damage. None of this issues addressed are contingent on a definition broader than the strictly technical features. Whatever is the definition of cybersecurity that assumed canonical status, it will most surely incorporate technical features.

3 The Conceptual Underpinning of Cyber Security Studies

Liu Yangyue

Chapter 3 introduces conceptual issues that will, increasingly, feature into the cybersecurity debates. It is about the conceptual underpinnings of cybersecurity from the perspective of security studies. Today it is near-impossible to talk of national security without reference to threats in and of the cyber domain. This condition, driven by today's imperatives, requires conceptual and analytical underpinnings if it is to assume a position of credibility in policy analysis or in broader theoretical contexts. Such is the challenge addressed in this chapter.

4 Cyberspace as the Domain of Content

Lyla Fisher

Chapter 4 focuses on cyberspace as a domain of content. By way of orientation, it differentiates between the ends and means of cyberspace so that policymakers can focus on the ends and experts can specialize in the means. This perspective has implications for emergent conceptions of cybersecurity given that it is the security of content that dominates

The next two chapters can be viewed as parallel analyses.

5 DoD Perspective on Cybersecurity

Glen Voltz

6 China's Perspective on Cyber Security

Liu Yangyue

.Chapter 5 is on cybersecurity seen by the US Department of Defense. Chapter 6 is on the China case. It is fair to say that these are far from mirror images of each other. Each reflects distinctive concerns. If there is a simple way of characterizing the US and the China perspective, it may be this: the US focuses on matters of process. China concentrates on features of structure. However unsatisfactory this distinction most surely is, nonetheless it captures some features of the differences between the two countries' conceptions of imperatives for cybersecurity.

The next two chapters can be viewed in parallel.

7 Pursuing Deterrence Internationally in Cyberspace

Chrisma Jackson

8 Is Deterrence Possible in Cyber Warfare?

Brooke Gier

Chapter 7 and Chapter 8 each take on the issue of deterrence in the cyber context. Is there a place for deterrence conventionally understood in the context of cybersecurity? Chapter 7 provides an initial mapping of the issues at hand. Labelled as a "discussion" of deterrence in the cyber era, this chapter outlines some of the major features or perhaps fault lines in debates and deliberations. Chapter 8 simply asks: "Is deterrence possible in cyber warfare?"

9 A Theoretical Framework for Analyzing Interactions between Contemporary Transnational Activism and Digital Communication

Vivian Peron

Chapter 9 provides a major shift in focus, idiom, orientation, methodology, and inference space. Puts forth a theoretical framework for analyzing interactions between transitional activism and digital communication. While the connection to cybersecurity may not be immediately obvious from this statement of focus, the fact remains that any cross border source of cyber threat is, by definition, transitional in the strict sense of the term. At the same time, transitional activism refers to a form of political activity that is organized across borders without reliance on the role of direction of the state

system. Inevitably, this chapter reminds us that, however tempting it might be, we cannot ascribe all incidents of cyber intrusion to state actors. But the motivations are multiple. Threats to cybersecurity in business and industry are likely come as much from other states than from competitors in the marketplace. But the responses by the state are different from those by business, private or public. The fact remains, however, the data are inconclusive about sources, motivations and so forth. What we are more confident about is the nature of the intrusion and, more often than not, the immediate impacts on the target.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

APPENDIX A-6

ECIR Workshops

Appendix A-6 presents only a brief note on the Workshop topics.

Details on Agenda, Workshop Report, list of attendees, and related information are on the ECIR website.

A-6.1 ECIR WORKSHOP SPONSORS

Council on Foreign Relations (CFR)

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR takes no institutional positions on matters of policy.

Business Executives for National Security (BENS)

Business Executives for National Security is a non-profit organization that provides business and nation security consulting services. The organization offers cyber security, threat finance, and disaster response consulting services. Business Executives for National Security was founded in 1982 and is headquartered in Washington, District of Columbia with additional offices in Kansas City, Missouri; Atlanta, Georgia; New York, New York; Duncanville, Texas; and California.

A-6.2 ECIR Workshops

Workshop 1

Cyber International Relations: Emergent Realities of Conflict and Cooperation

In international relations, the traditional approaches to theory, research, practice and policy were derived from experiences in the 18th and 19th centuries, refined further in the 20th century. But cyberspace has created new conditions—problems and opportunities—-for which there are no clear precedents. As an environment for communication, a venue for social interaction and an enabler of new mechanisms for power and leverage, cyberspace calls for new perspectives, policies and practices.

An event of the MIT-Harvard multidisciplinary Minerva Project on "Explorations in Cyber International Relations" (ECIR), this conference seeks to adjust traditional views to the cyber realities of the 21st century. Of the many questions shaping world politics today, few are as daunting as Who Controls Cyberspace? Clear as it might appear, this question is deceptively simple, even elusive. It obscures other hidden or implicit aspects, namely, who can control cyberspace, who will control, and who should control cyberspace. However framed, the issue of control is closely tied to matters of scale and scope as well as authority and legitimacy – and most certainly intent and capacity.

Our vision is to create new understandings of these realities that help: Highlight alternative perspectives and policies as well as institutional requirements; Clarify threats and opportunities in cyberspace for national security, welfare, and influence; Provide analytical tools for understanding and managing transformation and change; and Attract and educate a new generation of researchers, scholars, and analysts. We hope to develop an integrated approach to international relations and help frame cyber theory and practice for the 21st century. Most important of all, we seek to provide foundations for an integrated view of international relations.

Workshop 2

People, Power, and CyberPolitics

The People, Power, and CyberPolitics Conference is a joint project of MIT and Harvard University on Explorations in Cyber International Relations (ECIR). Co-sponsored by the Council on Foreign Relations, this workshop is the second in a series of sustained deliberations and explorations involving leading individuals in academia, government and business. The outcome of the workshop will be a new

understanding of emergent dimensions of cyberpolitics with respect to (i) the evolving pressures on policy and theory, and (ii) the methods and techniques of exploring current conditions and understanding the contours of potential futures.

For the first time in human history such a large number of people from all parts of the world participate in a new arena of information and communication of global scale and scope. Almost everyone everywhere has the opportunity to participate in cyberspace. Few states, if any, are able to control the flow of information via cyber venues that cross their boundaries. All states are recognizing, to one degree or another, that people matter – and sometimes they matter a lot.

This reality is also influencing the changing power distribution in international relations. The "old" concentration of power in a bipolar cold war world has been replaced not by multi-polarity but, more importantly, a "new" international structure characterized by the diffusion of power. All of this affects the nature of the international system – structure, process, and participation – while shaping an emerging and rapidly growing global civil society that transcends traditional territoriality and sovereignty. In the "new" world people matter more in politics in developed and developing nations, sometimes in similar ways and sometimes not.

People also matter in a particularly unprecedented way. The age distribution of the global population is skewed toward the young age groups. And everywhere it is the young people that dominate participation in cyberspace. More and more, the diffusion of social networking practices and growing use of mobile technologies – notably social media for personal or political uses – has reinforced the power of people.

Especially relevant in this context is that the organized fields of knowledge –their scientific foundations – do not provide a sufficiently robust basis for analyzing, anticipating, and responding a new way of understanding power, politics, the state, and institutions of governance: nationally and internationally. The ECIR Project seeks to develop a new multidisciplinary field of scientific inquiry to provide the theories, tools, and modes of inquiry relevant to unprecedented, new, complex, and rapidly changing conditions created by the construction of cyberspace. This workshop is the second in a series of sustained deliberations and explorations involving leading individuals in academia, government and business. The outcome of this workshop will be a new understanding for why, how and when people, power, and cyberpolitics shape the future

Workshop 3

Who Controls Cyberspace? A Puzzle for National Security and International Relations

The Question

Of the many questions shaping world politics today, few are as daunting as Who Controls Cyberspace? Clear as it might appear, this question is deceptively simple, even elusive. It obscures other hidden or implicit aspects, namely, who can control cyberspace, who will control, and who should control cyberspace. However framed, the issue of control is closely tied to matters of scale and scope as well as authority and legitimacy – and most certainly intent and capacity.

The Purpose

The purpose of this Workshop is to examine the control issue – of the Internet and of cyberspace – while also taking into account the operational (who can control), the pragmatic (who will control) and the normative aspects (who should control)? Invariably, these issues are framed by the current context of the Internet we know and cyberspace that we believe we understand. Less clear, are the priorities, capabilities, intents, and preferences of critical actors, as well as the context within which they operate. It goes without saying that, however framed or understood, control is about power and politics, conflict and contention, and "tussles" over alternative arrangements. At the same time, the ubiquity of cyberspace with its pervasive features and fluidity, all but assures that everyone, everywhere is affected by the controls in place as well as all issues surrounding future possibilities and contingencies.

The Complexities

As a question, "Who controls cyberspace?" harbors various complexities. At a minimum it calls for a derivative framing: who controls what, when, how, and why? And we need to consider the Internet as well as the broader cyberspace. The tools and instruments of control, the technological foundations and attendant implications cannot be ignored. Then, too, the actors and the decision contexts are varied and diverse. The usual types include public and private actors, state and non-state, national and international, legal and illegal, and a few others. But there are new actors whose functions, capabilities, preferences and priorities may also matter. And are there any impacts for national security and for the conduct of international relations?

The Workshop

This Workshop proceeds from the assumption that we have as yet no overarching and complete accounting of who controls what, when, and how, nor do we fully understand what are the precise points of control, where they are currently located and where the future ones might be placed. Accordingly, the Workshop is based on first principles, namely, cyber-ecosystems, power in "real" and cyber contexts, and introduce control point analysis. Then it turns to specific control features from four different perspectives: (a) people as users; (b) business and industry; (c) states and governments; and (d) the international community, private and public – across different regions of the world.

Given the complexity of cyberspace and its scale and scope, we shall introduce control point analysis in order to anchor the discussion in matters of structure and process in their most basic and inescapable form, and then focus on control issues for: (a) essentials of connectivity; (b) matters of content; and (c) international cyber norms, law, and governance. Given that cyberspace is one of several global issues (or domain of human activity) where effective control is central to overall operations, we shall then turn to two other areas that share some common features. One is international banking and finance, also dispersed, fluid, and ever changing but with a long record of operational control, with relatively robust structure and process; the other is a set of examples reflecting the frontier of knowledge where the quest for control remains an ongoing activity, with little formal structure and limited operational process. What can we learn from each case?

The Workshop concludes with a session on the Future of Control in Cyberspace. This session seeks to provide some inferential contributions by drawing out the "what if…" or, alternatively, "if…, then…" for key issues and potential consequences. Since the Workshop considers different perspectives (or lenses) across various aspects (or features) of cyberspace we should be able to address much of the complexity of cyberspace. At the very least we would have developed a mapping of the control points, leverages, interests, assets, actions and potential outcomes that shape our world today and for the decades to come

Workshop 4

Cyber Security & the Governance Gap: Complexity. Contention, Cooperation

Of the many realities shaping world politics, two contending trends in cyberpolitics are among the most salient. On the one hand are the continued growth and diversity of threats to cyber security; on the other are the many features of international negotiations and national politics that both shape and impede the development of governance for cyberspace. This workshop focuses on the dynamics shaping these dual features—cyber threats and cyber governance—while also taking into account *operational, pragmatic,* and *normative* aspects, as well as potential *policy* responses. At the core is "nature of the gap" between the two—all from different perspectives: people as users; business and industry; states and governments; and the international community, private and public—everywhere. The question is which trend will dominate: threats to cyber security or the expansion of cyber governance? Does that matter? If so how? If not, why not?

A-6.3 AFFILIATED WORKSHOPS

Harvard-MIT-University of Toronto

Cyber Norms Workshop I 2011

The Cyber Norms workshop was a response to the growing awareness at the international level of the need for such norms to stabilize behavior in cyberspace. The need was recognized in a 2010 report by the UN Group of Governmental Experts on Information Security, which included representatives of the United States, Russia, China and twelve other countries. Since then, the US and other major states have also called for international discussions on cyber norms and a major intergovernmental conference on cyber "rules of the road," met in London, Nov. 1 -2, 2011.

Harvard-MIT-University of Toronto,

Cyber Norms Workshop II 2012

A workshop on international cyber norms met for the second time at the Massachusetts Institute of Technology (MIT) in Cambridge, MA, from September 12 to 14, 2012. In the last few years, there has been growing recognition that widely accepted, articulated norms can support the beneficial development of global cyberspace and reduce the likelihood of conflicts there. One objective of our workshops is to identify norms which could fill such a role, explore their groundings in law and technology, and estimate the feasibility of their acceptance, given current political and economic contexts.

A-7

HARVARD POLICY SEMINAR

Meeting bi-weekly, below is the list of speakers for the Harvard Policy Seminar

Spring 2012

- Ari Juels, Chief Scientist at RSA Labs
- Herb Lin, Chief scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies
- Dr. Sandro Gaycken, Institute of Computer Science, Free University Berlin
- Susan Landau, Visiting Scholar, Harvard University
- Melissa Hathaway, President, Hathaway Global Consulting, LLC
- Adam Segal, Council on Foreign Relations
- Dr. Chris Demchack, Professor, Strategic Research Department, US Naval War College Lucas Kello, HKS STPP Research Fellow; Aadya Shukla, HKS STPP Research Fellow

Fall 2012

- Alexander Klimburg, Fellow & Senior Advisor, Austrian Institute for International Affairs
- Tim Maurer, Research Associate, Center for Strategic and International Studies
- Scott O. Bradner, Senior Technology Consultant, Office of the CTO, Harvard University
- General Keith Alexander, Director, NSA, Commander, US Cyber Command
- Tim Junio, Research Fellow, Center for International Security and Cooperation, Stanford Unviersity
- Brian Kahin, Fellow, MIT Sloan School Center for Digital Business

- Jack Goldsmith, Henry L. Shattuck Professor of Law, Harvard Law School
- Jonathan Zittrain, Professor – (of Law) HLS, (of Law) HKS, and (of Computer Science) SEAS

Spring 2013

- Vaibhav Garg, Postdoctoral Research Scientist, Drexel University Computer Science Department
- Professor Nazli Choucri & David Clark, MIT
- Herb Lin, Chief Scientist, Computer Science and Telecommunications Board, National Academies
- Col William Churchwell & CW5 Todd Boudreau, US Army Signal Center of Excellence
- Aadya Shukla, Fellow, Belfer Center for Science and International Affairsa
- David Sanger, Chief Washington Correspondent, NYT, and Adjunct Lecturer in Public Policy, Harvard Kennedy School
- Susan Landau, Guggenheim Fellow

Fall 2013

- Bruce Schneier (Fellow, Berkman Center for Internet and Society, Harvard University)
- Ron Deibert (Professor of Political Science, and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto)
- Scott O. Bradner (Senior Technology Consultant, Harvard University)
- Roger Hurwitz (CSAIL, MIT)
- General Michael Hayden (Former Director, National Security Agency and Central Intelligence Agency)
- Katie Moussouris (Head of Security Community Outreach and Strategy, Microsoft)

Winter/Spring 2014

- Chris Demchak (Professor, Naval War College)
- David Sanger (Chief Washington Correspondent, The New York Times; Senior Fellow and Adjunct Lecturer, Harvard Kennedy School)
- Christopher Painter (Coordinator for Cyber Issues, U.S. Department of State) and Alexander Klimburg (Fellow, Harvard Kennedy School)
- Simson Garfinkel (Professor, Naval Postgraduate School)
- Nazli Choucri (Professor of Political Science, MIT)
- Melissa Hathaway (Senior Advisor, Project on Technology, Security, and Conflict in the Cyber Age, Belfer Center)

Fall 2014

- Jim Waldo (Gordon McKay Professor of the Practice of Computer Science and Chief Technology Officer, Harvard University)
- Susan Landau (Professor of Cybersecurity Policy, Department of Social Science and Policy Studies, Worcester Polytechnic Institute)
- Bruce Schneier (Fellow, Berkman Center for Internet and Society, Harvard University)
- John Mallery (Research Scientist, MIT CSAIL)
- Joel Brenner (Joel Brenner LLC)
- Scott O. Bradner (Senior Technology Consultant, Harvard University)

Winter/Spring 2015

- David Sanger (Chief Washington Correspondent, The New York Times; Senior Fellow and Adjunct Lecturer, Harvard Kennedy School
- Cameron Kerry (Senior Counsel, Sidley Austin)
- Hon. Richard Danzig (Director, Center for a New American Security)
- Susan Landau (Professor of Cybersecurity Policy, Department of Social Science and Policy Studies, Worcester Polytechnic Institute)

- Melissa Hathaway (Senior Advisor, Project on Technology, Security, and Conflict in the Cyber Age, Belfer Center)