Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

http://ecir.mit.edu/

A Research Collaboration of MIT and Harvard University

The Final Report

Version 1.2

Prepared by:

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

Cambridge, Mass. 2015

PART 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.

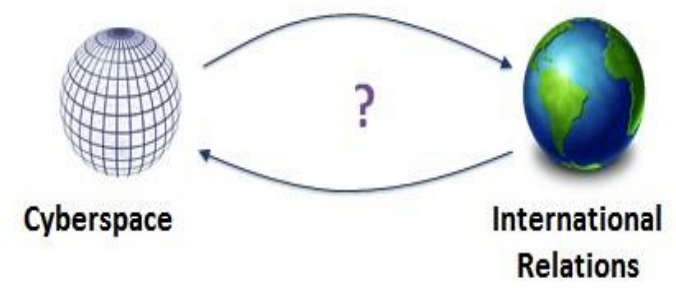

Figure 1.1 The Overarching question

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.