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

MINERVA INITIATIVE
DEPARTMENT OF DEFENSE

Cambridge, Mass. 2015

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

Part I
Challenges of the Cyber Age

Part II
Foundations for Cyber-IR Theory

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.