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

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.