Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security

Nazli Choucri

Professor, Political Science Department
Massachusetts Institute of Technology

Daniel Goldsmith

PA Consulting Group

March 1, 2012

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security

Early in the twenty-first century, new, cyber-based threats to the well-being of individuals, economies, and societies added a new dimension to the well-understood threats of the twentieth century. For the first time in human history, advances in information and communications technologies are potentially accessible to much of the world's population. These Internet based advances allow almost anyone to disseminate messages, meaning that a wide range of actors, state and nonstate, have the potential to disrupt networks and commerce with relatively little fear of discovery. In cyberspace, it is hard to know with certainty what is behind a particular action—and actions in one place can have effects around the world.

A powerful example of how advances in cyberspace have changed the national security environment is the deployment of Stuxnet, a complex piece of malicious software that reportedly damaged the uranium enrichment facilities of Iran's nuclear program (Broad and Sanger, 2010). Both Israel and the United States have been blamed as creators of the virus, but in part because of the nature of cyberspace, the origin of the software remains in dispute.[1] Another apparent case of international relations conducted in cyberspace were the 2007 cyber attacks that overwhelmed the websites of prominent Estonian organizations, including public-sector agencies, banks, and media firms. Some Estonian officials blamed Russia for the attacks, but responsibility was never proved. Similarly, in 2010 Google announced that it and a variety of high-tech, security, and defense firms had been targeted in an attempt, apparently originating in China, to gain access to and steal valuable digitized information. The episode resulted in a temporary shutdown of Google's China site.

This new, cyber dimension of international affairs presents great challenges to deterrence, a cornerstone of national security policy since the end of World War II. In the traditional, pre-Internet deterrence context of the twentieth century, the United States and the Soviet Union—state actors with symmetrical capabilities, known identities, and shared aversions to the escalation of tensions—presided over a bipolar international system. International relations in the twenty-first century, by contrast, involve a large number of new states created at the end of the Cold War, as well as a wide range of non-state actors that inhabit a complex environment characterized by asymmetries, obscured identities, few shared aversions, and diverse, often unknown goals and objectives (Choucri, forthcoming).

Cyber threats are serious, growing, and destabilizing. The deterrence theories and strategies created and employed during the Cold War are not easily portable to the cyber domain. Some prominent research groups are attempting to understand the cyber revolution in international

affairs, and governments have made a few efforts to cooperate in cyber matters, notably in the area of Internet-based crime and the creation of Computer Emergency Response Teams (CERT). In general, though, policy responses lag far behind developments in the virtual realm. In large part because of the evolving characteristics of cyberspace, the full range and effects of cyber interactions and the potential scale and scope of cyber threats simply are not well understood. A relatively new joint effort of Harvard and MIT—the Explorations in Cyber International Relations project—aims to create a new research discipline that integrates cyberspace into the fabric of international affairs, in all of its manifestations, such as to eliminate the current tendency to consider cyberspace and international affairs as two distinct parallel arenas or areas of interaction. This new initiative seeks to provide the theories, data, and analytic tools tailored to the complexities of the twenty-first century and necessary for governments to make sense of, and successfully manage, their international relations in the cyber era.

Emerging Attention to Cyber Governance

In his recent book on cyberwar, Richard Clarke, the former US counterterrorism czar, concludes that the international community should develop cooperative strategies for dealing with the new state of international cyber affairs (Clarke and Knacke, 2010). While he highlights treaty making, the broader issues are of bringing order into the chaotic cyber environment. Cyber governance at national and international levels consists of mechanisms designed to institutionalize support for stable and robust cyberspace and cyber-based interactions, to enhance cyber security, to minimize cyber disruption and damage, and to deploy cyber venues that enhance human well-being.

The Convention on Cybercrime, adopted by the Council of Europe on November 8, 2001, stands out as a formal initiative in this arena. The convention focused on copyright infringement, violations of network security, and Internet espionage (Council of Europe, 2001) and tried to foster international cooperation by harmonizing criminal laws and investigative and prosecutorial procedures around the world. By 2012, 32 states had ratified the convention—including the United States, where the convention went into effect in 2007—and another 15 countries had signed but not yet ratified the accord. Importantly, though, China, Russia, and many Eastern European countries have not signed. Despite its incomplete membership, the convention does represent a level of formal cooperation on cyber crime that had not previously existed.

At the same time, however, rivalry among the major powers and contentions over the principles that should govern cyber-based interactions prevent the development of worldwide governance structures for managing cyber crime, as well as many other deleterious activities. For example, China and Russia recently offered the Shanghai Cooperation Organization as a replacement for the Convention on Cybercrime. Founded in 2001, the organization's membership consists of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan (Scheineson, 2009); on many diplomatic and strategic issues, the organization is more closely aligned to China and Russia than to the United States, Europe, and Japan. But it would be futile to look for internal

consistency on all matters of politics—national or international—or to expect consensus on the definition of the problems or on agreement over the priorities for global action. Russia, for example, has a formal policy to focus on the "information war"—defined as actions by a state to undermine another state's "political, economic, and social systems"—and not on agreements to stop cyber crime. In the United States, there has been increased talk on the need for a policy to deal with international cyber threats. In 2009, the US government completed a review of its cyber-security policy and created the high-profile Cyber Command, which unifies the Army, Air Force, Navy, and Marines. The Obama administration subsequently appointed Howard Schmidt as the White House cyber-security coordinator, and, in 2011, the US Defense Department developed its own cyber strategy (Department of Defense, 2011).

The public version of this strategy document emphasized five strategic initiatives: treating cyberspace as an operational military domain, employing new defense operating concepts, partnering with other US government agencies and the private sector, building relationships with allies and partners to strengthen collective cyber security, and leveraging the nation's workforce for technological innovation. Nonetheless, some observers have argued that the strategy is insufficient, because it lacks a unified approach, specific details and timetables, and funding sources (Clarke, 2011; Nakashima, 2011).

At the international level, new institutional mechanisms were designed to support global cyber security, most notably the CERT. Originally developed by the US Defense Advanced Research Projects Agency, the CERT Coordination Center was established at Carnegie Mellon University in November 1988. Since then, the CERT system has expanded worldwide, with more than 250 organizations that deal with Internet security problems.[2] The core functions of the teams—as defined by the coordination center—involve response to security emergencies, promotion of valid security technology, and protection of network continuity. The usual problems of coordination persist, most notably in the collection of data on cyber threats where there is little agreement on definition or measurement practices. Effective coordination will evolve over time, probably at a slower rate than actual threat incidents.

There is widespread recognition of the rapidly changing nature of cyber interactions, the diversity of cyber threats, and the growing potential for response strategies. Existing research initiatives that focus on global cyber security include the NATO Cooperative Cyber Defense Center of Excellence in Estonia and the Information Warfare Monitor, a public-private venture between the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and the SecDev Group, an Ottawa-based think tank. The Information Warfare Monitor recently issued reports on cyber espionage—the theft of national and corporate information from networks—and Chinese cyber-surveillance activities. The NATO Cooperative Cyber Defense Center, established in response to the 2007 Estonia cyber attacks, focuses on expanding capability, cooperation, and information sharing among NATO countries.

A New Cyber Initiative

The above-mentioned organizations are venues in which some cooperation and research can occur, but there are no programs that have a central mission to provide a theoretical framework as well as the data and analytical tools for understanding and responding to the international cyber reality of the twenty-first century. The joint MIT and Harvard Explorations in Cyber International Relations (ECIR) project, launched in 2009, hopes to change that by creating an integrated view of cyber and "real" international relations.[3] It is designed to realign the foundations of international relations theory and policy with the new realities of cyberspace by establishing a new multidisciplinary field of study. To educate a new generation of researchers, scholars, and analysts and to equip them with the necessary tools for this century, the project aims to clarify threats and opportunities in cyberspace in regard to national security, national welfare, and national influence and to provide analytical tools that can help governments understand and manage the cyber domain as it evolves over time.

Housed at MIT, the joint project consists of 15 faculty members and senior researchers (political science, business and management, and computer science) at MIT and at Harvard University's Kennedy School of Government and its Law School. There are currently 13 post-doctoral associates or fellows, as well as graduate researchers and undergraduate students. The project activities consist of research, educational initiatives, and outreach initiatives—in addition to the usual scholarly production of publications, policy briefs, and advisory activities, nationally and internationally.

From a theory perspective, the project seeks to understand the opportunities and vulnerabilities created as nations and non-state actors interact in cyberspace—where, how, and with what effects. This interaction is clear in the real world, but there is very little systematic knowledge about this in the cyber world. For example, it is unknown who or what holds the reins of power in the cyber world—that is, exactly what entities, and under what mandate, enable the flow of information (and how they enable this flow at various points in the process). This information must be garnered if basic features of the cyber domain are to be understood.

From a technological perspective, the project explores, for example, the extent to which existing methodologies in analysis of international relations are portable to the cyber arena, and to adjust these as needed, or, alternatively, to customize methods to the cyber domain. There are several key questions that must be answered. Among them: Who will steer the technological evolution of the cyber domain and how? Is the Internet today a model for the future? Is it changing? If so, how? If not, why not? The policy challenge is to render the toolkit of policy responses more consistent with the complexities of cyber realities. So far, cyberspace has been an open arena. But this is changing. In the United States, lawmakers are struggling with how to manage competing interests, currently illustrated by the 2012 proposed anti-piracy bill. Almost everywhere, there are contentions over regimes for regulating interactions in the cyber domain. China and like-minded states focus on uses of the state-based International Telecommunications Union (ITU) and the IGF

(Internet Governance Forum), for example, while the United States and other like-minded states prefer to rely on the private-sector arrangements customized to the cyber domain, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF), among others. From a diplomatic perspective, the challenge is to frame new modes and instruments of negotiation to manage the interactions of the real world and cyberspace. Internationally, the World Summit on Information Society (Geneva, 2003; Tunis, 2005) and other similar projects seek to formulate common principles, practices, and priorities for the cyber domain. And the 2011 London Conference on Cyberspace launched—with little apparent success—an international inclusive dialogue to help guide the behavior in cyberspace.

New Research Initiative

If ECIR is to achieve its mission—notably to improve the understanding and management of cyber interactions, reduce conflict, and enhance efforts to contain or prevent the deployment of cyber weapons of large-scale destruction and large-scale, cyber-driven disruption—it must effectively reduce, if not entirely eliminate, three critical disconnects or gaps in current understandings and practices.

The Cyber-theory Gap

There is an enormous disconnect between the cyber realities of today and the theories of the twentieth century, which continue to guide national policy and international relations. For example, the emphasis on the state-based system of international relations is increasingly tested more by a wide range of new actors—from Wikileaks' Julian Assange to the jihadist webmasters of Al Qaeda—with new cyber-enabled modes of interaction. To close the cyber-theory gap, the collaboration between one of the authors of this article, political scientist Nazli Choucri, and computer scientist David D. Clark, who in the 1980s led development of the Internet's architecture, created a framework for integrating cyberspace into the fabric of twenty-first-century international relations. One of the most significant insights gained so far from this mapping effort involves the large degree to which the entire cyber system is run and controlled by the private sector in a world where state-based international institutions are seeking to extend sovereign authority over the cyber domain.

The Empirical-data Gap

Well-recognized, there is a powerful disconnect between cyber activities on the one hand and the quality, integration, and consistency of the data about these activities on the other. To close these gaps, ECIR set out to identify, collect, and reconcile (where possible) existing data sets relevant to cyber international relations and propose new uses and integration of data into theory and policy.

It must also find ways of facilitating analysis of large-scale data—such as statistics on cyber access by country—from diverse perspectives and for different purposes.

An example of research to close the empirical-data gap is the construction of the cyber-data dashboard—developed by the ECIR team and led by MIT computer scientist Stuart Madnick—to harness and, to the extent possible, reconcile diverse cyber-data sources, including CERT data. The dashboard functions as a simple, easy-to-use source for global and nation-level data, with specific emphasis on cyber-security threat data and high-profile events. Its first version focuses on the data generated by CERT to provide a coherent overview of cyber-threat incidents worldwide.

The Policy-analysis Gap

This disconnect is between traditional modes of policy analysis and the realities that focus largely on states and threats through the cyber domain that involve non-state actors, isolated individuals, or groups whose identity is not known, for example. Generally, national leaders turn to past policies—based on past realities—when responding to new challenges. In some arenas, this can be a wise practice, and one supported by institutional and bureaucratic logic, but there are no precedents for cyberspace as a domain of international interaction.

Closing the policy-analysis gap is perhaps best illustrated by one of ECIR's research activities. It involves modeling the cyber politics surrounding the Arab Spring, which highlighted the fragility of regimes worldwide and the ability of coordinated dissidents to challenge or topple governments with the help of cyber organizing tools. Political revolts in seven countries were triggered by the events in Tunisia in December 2010, followed by a similar but more far-reaching initiative in Egypt. A modeling effort led by Daniel Goldsmith and Michael Siegel, both at the MIT Sloan School of Management, is a dynamic simulation project that investigates how cyber venues are used in the pursuit of regime change. The analysis shows how cyber interventions both enable dissidents, via faster and more widespread messaging capability, and enable regimes, via the ability to block content on, block access to, and gather intelligence through the Internet. The nature of the race between them was powerfully influenced by the dissidents' use of social networks and, when the Internet was shut down, the use of traditional phone lines.

Conclusion

If the ECIR mission is to be successful, it must integrate the real and the cyber into a unified framework to help steer policy makers and practitioners through the twenty-first century—and, of course, provide a new generation with a relevant education buttressed by methods of inquiry, educational capabilities, and tools of analysis for current realities.

The remarkable growth of cyber access worldwide has brought with it an increasing diversity of actors and entities. English—long the dominant language on the Internet—is now used by less than 30 percent of the Internet population. All countries, and a large fraction of the world's population, are engaged in the cyber domain. And these shifts in the cyber demography and ecology have real-world ramifications that have few precedents if any.

Time is most certainly of the essence: What we see, know, and understand today in the cyber domain may not be the same realities of tomorrow.

Funding

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.

Notes

1. Stuxnet infects Windows systems in its search for industrial control systems, called supervisory control and data acquisition (SCADA) systems. The target systems include code that automates industrial machinery (Falliere, 2010). A majority of the infected computers worldwide were located in Iran, with uranium enrichment factories as the supposed target of the Stuxnet worm (Fildes, 2010). Stuxnet was first observed and spread in early 2010, but the roots were traced back roughly to June 2009. The Russian cyber-security company Kaspersky Lab claimed that the attack could only be conducted with nation-state support (Fildes, 2010). The most likely origin of the virus seems to be either Israel or the United States, though the origin remains disputed (Keizer, 2010). Israeli officials have hinted that their country may be involved (Broad et al., 2011). Iran's top nuclear negotiator blamed the United States and claimed that an investigation found that the United States was the source of the attack.
2. These programs use CERT or a similar name http://www.us-cert.gov/aboutus.html.
3. The project is rooted in the Minerva Initiative, a Defense Department-sponsored, university-based, social science research program. Former Defense Secretary Robert Gates launched Minerva in 2008 with the goal of improving the department's "basic understanding of the social, cultural, behavioral, and political forces that shape regions of the world of strategic importance" to the United States (Department of Defense, 2008).

References

Broad WJ and Sanger DE (2010) Worm was perfect for sabotaging centrifuges. New York Times, November 18, p. A1.

Broad WJ, Markoff J, and Sanger DE (2011) Israel tests on worm called crucial in Iran nuclear delay. New York Times, January 15, p. A1.

Choucri N (forthcoming) Cyberpolitics in International Relations. Cambridge, MA: MIT Press.

Clarke R (2011) The coming cyber wars: Obama's cyber strategy is missing the point. Boston Globe, July 31, Op-Ed.

Clarke R and Knacke R (2010) Cyberwar: The Next Threat to National Security and What to Do About It. New York: Ecco.

Council of Europe (2001) Convention on Cybercrime. Available at: conventions.coe.int/Treaty/en/Treaties/html/185.htm.

Department of Defense (2008) The Minerva Initiative. Available at: http://minerva.dtic.mil/index.html.

Department of Defense (2011) Department of Defense Strategy for Operating in Cyberspace. July. Available at: http://www.defense.gov/news/ d20110714cyber.pdf.

Falliere N (2010) Stuxnet introduces the first known rootkit for industrial control systems. Symantec blog, August 19. Available at: http://www.symantec.com/connect/blogs/stuxnet-introduces-firstknown-rootkit-scada-devices.

Fildes J (2010) Stuxnet worm 'targeted high-value Iranian assets.' BBC News, September 23. Available at: http://www.bbc.co.uk/news/technology-11388018.

Keizer G (2010) Is Stuxnet the 'best' malware ever? Infoworld, September 16. Available at: http://www.infoworld.com/print/137598.

Nakashima E (2011) US cyber approach 'too predictable' for one top general. Washington Post, July 14. Available at: http://www.washingtonpost.com/ national/national-security/us-cyber-approachtoo-predictable-for-one-top-general/2011/07/14/ gIQAYJC6EI_story.html.

Scheineson A (2009) The Shanghai Cooperation Organization. Council on Foreign Relations, March 24. Available at: www.cfr.org/international-peace-and-security/shanghai-cooperationorganization/p10883.

Author Biographies

Nazli Choucri is professor of political science at MIT and principal investigator for the Project on Explorations in Cyber International Relations (ECIR) of the Minerva Program.

Daniel Goldsmith is an affiliated researcher at the MIT Sloan School of Management and a principal consultant at the PA Consulting Group.