ECIR WORKSHOP ON  
Cyber Security & the Governance Gap:  
Complexity, Contention, Cooperation  
Co-Sponsored by  
Council on Foreign Relations  
and  
Business Executives for National Security  

January 6-7, 2014  
Marriott Hotel, Cambridge  
and  
MIT Media Laboratory  

Workshop Report  

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.
CONTENTS

INTRODUCTION

ISSUES in CONTEXT

CYBERSPACE & INTERNATIONAL RELATIONS – CO-EVOLUTION DILEMMA?
Nazli Choucri, Professor of Political Science, MIT; Principal Investigator, ECIR, MIT

CYBERSECURITY & CYBER GOVERNANCE
Joseph S. Nye, Jr., University Distinguished Service Professor, Harvard Kennedy School

FRAMING SESSION:
PERSPECTIVES ON GOVERNMENT & SECURITY

Venkatesh Narayanamurti, Moderator
Professor of Physics, Benjamin Peirce Professor of Technology and Public Policy, Harvard University; Principal Investigator, ECIR, Harvard

Presentation

CYBER GOVERNANCE – CHALLENGES & PERFORMANCE
Fadi Chehadé, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers (ICANN)

Panel

Melissa Hathaway, President, Hathaway Global Strategies LLC; Senior Advisor, Belfer Center, Harvard Kennedy School
Lynn St. Amour, President and Chief Executive Officer of the Internet Society (ISOC)
PANEL SESSIONS

PANEL I
DIMENSIONS of CYBER SECURITY

Michael Sulmeyer, Moderator
Senior Policy Advisor, Office of the Deputy Assistant Secretary of Defense for Cyber Policy

Presentation

MAJOR CHALLENGES TO GOVERNANCE OF CYBERSPACE
Tomas Lamanauskas, Head, Corporate Strategy Division, International Telecommunication Union (ITU)

Panel

Richard Bejtlich, Chief Security Officer, MANDIANT
Adam Segal, Maurice R. Greenberg Senior Fellow for China Studies, Council on Foreign Relations (CFR)

PANEL II
DILEMMAS OF CYBER GOVERNANCE

Melissa Hathaway, Moderator
President, Hathaway Global Strategies LLC; Senior Advisor, Belfer Center, Harvard Kennedy School

Panel

Xing Li, Professor, Electronic Engineering Department, Tsinghua University, Beijing, China; Deputy Director, China Education and Research Network (CERNET) Center
Milton Mueller, Professor, School of Information Studies, Syracuse University
Alexander Klimburg, Senior Advisor, Austrian Institute of International Affairs, Fellow (incoming) Harvard Kennedy School
PARALLEL PANELS

PANEL IIIa
CYBER SECURITY – EMERGENT ISSUES

Michael Siegel, Moderator
Principal Research Scientist, Sloan School of Management, MIT

Panel

Brandon Valeriano, Senior Lecturer, School of Social and Political Sciences, University of Glasgow
Tim Maurer, Policy Analyst, Open Technology Institute, New America Foundation
Katie Moussouris, Senior Security Strategist Lead, Microsoft
Urs Luterbacher, Honorary Professor, International Relations/Political Science, Graduate Institute, Geneva, Switzerland

PANEL IIIb
CYBER GOVERNANCE – BASICS FOR ACCORD

Joseph Kelly, Moderator
Senior Advisor for Cyber, Office of the Under Secretary of Defense for Intelligence

Panel

Kilnam Chon, Professor of Computer Science at the Korea Advanced Institute of Science and Technology (KAIST), Professor, Keio University
Jesse Sowell, Ph.D. Candidate, ESD, MIT
Greg Rattray, CEO and Founding Partner, Delta Risk, LLC
Scott Bradner, University Technology Officer, Harvard University
PANEL IV
PRIVATE-PUBLIC COLLABORATION – A CRITICAL IMPERATIVE?

Joel Brenner, Moderator
Legal and Security Consultant, Joel Brenner, LLC,

Panel

Jody Westby, CEO and Founder, Global Cyber Risk, LLC
Michael Sechrist, Vice President, Corporate Information Security, State Street Corporation
Charles Iheagwara, Managing Director, Unatek, Inc.

PANEL V
ALTERNATIVE FUTURES
COMPLEXITY, CONTENSION AND COLLABORATION

Michael Sulmeyer, Moderator
Senior Policy Advisor, Office of the Deputy Assistant Secretary of Defense for Cyber Policy

Panel

The Future of Cyberspace
David Clark, Senior Research Scientist, Computer Science and Artificial Laboratory (CSAIL), MIT

The Future of Cyber-Security
Herbert S. Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies

The Future of Cyber Governance
Nazli Choucri, Professor of Political Science, MIT; Principal Investigator, ECIR, MIT

END-NOTE

ACKNOWLEDGEMENT
POSTER SESSION

List of Posters
Individual Posters

ABOUT THE SPEAKERS

WORKSHOP PARTICIPANTS

ECIR PUBLICATIONS
INTRODUCTION

The Context

Of the many realities shaping the future of cyberspace and world politics, two distinctive and potentially powerful trends are among the most salient. One is the unrelenting growth and diversity of threats to cyber security. The other is the diversity of views and visions for governance of cyberspace. Each trend carries its own dynamics, supported by a wide range of actors and interests. Jointly they are central to the cyber arena and to world politics more broadly defined. The Workshop addresses these issues from different perspectives in order to highlight potential “gaps” in cyber governance and the management of security, and identify effective solutions.

The Workshop

We seek to stimulate a constructive discussion about the objectives and requirements for cyber governance by asking, “What sort of governance mechanisms and institutions can lead to effective oversight and management of threats to cyber security? What sort of decision-making, leadership, mandate and authority will be effective?” By the same token, we also ask: “What threats to cyber security can undermine the evolution of governance for cyberspace? Which classes of actors need to be involved in mitigating this process?” These issues are complex and contentious – but they also help highlight emergent forms of cooperation.

The Posters

The Poster Session includes contributions by researchers of the Joint MIT-Harvard ECIR Project as well as invited contributions by participants in this Workshop. Posters cover a wide range of topics related to the agenda, including technology developments, innovations, modeling initiatives, cyber conflicts, modes of collaboration and coordination, institutions of cyber governance, cyber operations of global entities, emergent norms, legal issues, cyber security, new ideas for regulation and management of cyberspace, among others.
Welcome to the Fourth Workshop of the Joint MIT-Harvard Project on Explorations in Cyber International Relations (ECIR). The ECIR Project is supported by a grant from the Minerva Program.

The first ECIR workshop was on substantive and organizational challenges. The second was on People, Power, and Cyber Politics. The third focused on the question of Who Controls Cyberspace?

The Council on Foreign Relations has been a co-sponsor early on. We are very pleased that the Business Executives for National Security (BENS) is joining us this time.

Much has happened -- in practice and in theory -- since the inception of ECIR. For a long time, the cyber domain and cyberspace and international relations were viewed as two distinct “parallel” areas—each with its distinctive properties. We now appreciate the interconnections, the mutual dependencies, and the limits in the portability of rules and regulations from one domain to the other. So where are we heading?

**Fourth Workshop**

This workshop is about the two powerful trends shaping the future of cyberspace and of international relations:

(a) Unrelenting growth and diversity of threats to cyber security more generally,
(b) Diversity of views and visions for governance of cyberspace.

We would like to ask:

What sort of governance mechanisms and institutions can lead to effective oversight and management of threats to cyber security? And, what sort of decision-making, leadership, mandate and authority will be effective?"

By the same token, we also ask:

What threats to cyber security can undermine the evolution of governance for cyberspace? And, which classes of actors need to be involved in mitigating this process?"

The comments that follow are contextual – based on the proposition that we are now at a point where we must recognize and manage the co-evolution of cyberspace and of international relations.

Co-Evolution

In this context, co-evolution refers to the interconnected developments of the cyber domain on the one hand, and of international politics, on the other. This co-evolution consists of, and forces us to deal with, cumulative effects over time created by new asymmetries, new actors, new conflicts. It is set by the old legacies and the new realities—as signaled in the slides.

At its origin, the Internet was in the realm of low politics, and the same with the expansion of the cyber domain. Constructed by computer scientists and varieties of technicians it was managed largely by the private sector. We have seen major changes in the configuration of the cyber domain over time, with changes in the distribution of internet users and internet usage by languages, for example, which have increased diversity in the cyber-ecosystem. This diversity highlights the variety of stakes and stakeholders.

In recent years, cyberspace evolved into the realm of high politics, characterized by having to do with power and influence, security and strategy, conflict and violence, leverage, pressure and so on. We have also recognized a set of "hidden feature" of the Internet. For example, at the physical layer are the undersea cables, with their vulnerability to environmental as well as human interventions or threats. At the logical and application layers there is the development of the anonymity networks.

Salient Cyber Features

Among the notable of the current cyber system are the following:

- New types of asymmetries -- notably the extent to which weaker actors can influence or even threaten stronger actors (such as press reports of anonymous penetration-incidences of the US government computer systems) -- has little precedence in world politics.
The creation of new actors—some with formal identities and others without—and their cyber empowerment, is altering the traditional international decision landscape in potentially significant ways.

The growing contestation of influence and control over cyber venues between the new institutions established to manage cyberspace (ICANN, IETF and others) and the traditional international institutions.

Various types of cyber conflicts (between and within states, of known as well as unknown identity and provenance) and security threats are becoming apparent, with the potentials for new modes and manifestations thereof.

Cyber collaboration in the effort to reduce uncertainty and introduce some measure of order in an “environment” that is increasingly perceived as “anarchic”.

There is a new cyber-based mobilization of civil society (the aggregations of individuals in their private capacity as well as organized elements of the private sector) and its potential empowerment across jurisdictions and in all parts of the world.

The intersection in spheres of influence – with the private sector managing order in cyberspace and sovereign authority managing order in the traditional domain worldwide – provided much of the rationale for organization of the first World Summit on the Information Society.

Given the co-evolution of cyberspace and international relations, do any of these features create a dilemma? As we move on, all of this leads us to consider the context for decision.

Decision and Dilemma

The context of decision includes the actors that are central to operation of the Internet and the overall cyber domain, the actors central to the state system, the private sector actors at the intersection of the cyber and state arenas and so forth. The net result is a high degree of density in the decision-making arena, at a level never seen before.

The number of actors increases the density of decision-entities -- each with new interests and new capabilities to pursue their interests -- and thus increased potentials for intersections in spheres of influence, with possibilities for new and different types of contention and possible conflict. In other words, the loads, threats, and pressures on the system are greater than the governance mechanisms can manage. This creates something of a dilemma.

If there is a dilemma it is that the threats to security are growing much faster than are the governance mechanisms. The governance mechanisms lack speed in comparison with rate
of changes in the cyber. Governance at this point concentrates more on process and routinization of interaction than on the security challenges.

Complexity of Security

If we put this dilemma in a broader context, we derive a three-dimensional security space (as shown in the accompanying attached slides):

- State based geospacial security of society
- Environmental security of life supporting properties, and
- Security and viability of cyberspace (with the Internet at its core).

The co-evolution of cyberspace and international relations is as much about the shaping of a dilemma as it is about managing fundamental realities of the cyber politics and the cyber era to date.
SLIDES
Cyberspace & International Relations
A Co-Evolution Dilemma?
Nazli Choucri
Professor of Political Science, MIT;

Workshop on
Cyber Security & the Governance Gap:
Complexity, Contention, Cooperation

Introduction:
Cyberspace & International Relations:
A Co-Evolution Dilemma?
Nazli Choucri, MIT
EOR Principal Investigator

Realities of the 21st Century

• Unexpected vulnerabilities & threats to security
• Changes in traditional power calculus
• Dominance of new private cyber actors
• Increased complexity of cyberspace
• Contentions over US-created cyber institutions
• Growth of cyber-conflicts & need for cyber-cooperation

RESULT
• Coupling of traditional and cyber domains
• Demand for governance & new policy response
  All of this is due to cyberspace

New Asymmetries – Emergent Claims

INTERNET USAGE BY LANGUAGE 2007 & GROWTH, 2000-2007

Denial of Service

3/6/2014
Co-Evolution: Density & Diversity for Decision

Cyberspace
- State Agencies
- Internet-Institutions
- Technical Operators
- Internet Service Providers
- International Institutions
- Informal Institutions
- Non-State Entities
- Exchange Point Managers
- Users
- Many others

International Relations


Conclusion
What does all this amount to?

- Increased coupling of "real" and cyber domains
- New vulnerabilities & challenges to national security
- Powerful asymmetries in traditional & cyber domains
- Wide range of new cyber-centered actors
- Growth in scale & scope of cyber-conflicts
- Contending models of cyber governance
- Growth in "hybrid" policies & responses
- Jointly these create new imperatives for governance

Notes:
- Joint Gains
- Domain: Cyber Security
- Threats to Security Trajectory & Intensity
- Geospatial Arena: The State = Traditional Domain
- Environment: Nature's Life Supports
- High
- Low
- New Arena: Cyber Security
- Reversing Arrows

3/6/2014
Introduction

Both cyber governance and cyber security can be quite ambiguous, as are many terms used in this subject (ex: cyberwar). Security is the absence or reduction of threat to key values; absolute security is impossible. The matter is really about managing trade-offs. Many lament that the makers of the Internet did not focus more on security when building it. However, even if they had we would still have a cybersecurity problem. Even the nicest technological fix will not fix our problems with cybersecurity: In other words, it is a challenge of creating a “narrower gap between the cat and the mouse.”

Security

People value things other than security, such as privacy, freedom, etc. The analogy is to public health vs. quarantine. Post-9/11 period the pendulum between security and privacy; is it beginning to swing back towards privacy?

We mostly think about national security, but, there are many dimensions of security: personal, business, etc. It helps to be precise in discussion and to specify. Security against what or for what purposes? The Internet was not done with attention to embedded security. Even if it had, we would still have cyber security issues. No matter have good security is, it can always be breached.
Governance

There is governance in cyberspace (even given IDTF, ICANN, etc.) but no overarching guiding regime that sets hierarchical framework. Cyberspace is not alone in that respect. The same can be said about environment. Regime theory is complex: and it can be applied to cyber security.

What can we, interested in cyber governance, learn from governance of other fields around the world?

Time Frame

We can learn that organizing governance to provide security is a difficult and long process. We now know that it takes about two decades before international cooperation can develop in response to a disruptive technology (atomic energy used as an example). We are about at the 20-year mark right now with cyberspace. We have not gotten very far with cyber security because of the ambiguities discussed earlier.
FRAMING SESSION

Perspectives on Governance and Security

Moderator

Venkatesh Narayanamurti, Professor of Physics, Benjamin Peirce Professor of Technology and Public Policy, Harvard University; Principal Investigator, ECIR, Harvard

Presentation

Cyber Governance – Challenges & Performance

Fadi Chehadé, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers (ICANN)

Panel

Melissa Hathaway, President, Hathaway Global Strategies LLC; Senior Advisor, Belfer Center, Harvard Kennedy School

Lynn St. Amour, President and Chief Executive Officer of the Internet Society (ISOC)

This is an important time for ICANN. It marks its 20th year. We are in the midst of a particular period in Internet governance. “Cyberspace is pretty much dead” (as a distinct “space”). There is no aspect of our life that does not include the Internet; it has become
incredibly important to how the world works today. Heads of state do not have the depth of understanding to make informed decisions about governance. We are now asking the tough questions:

**Who Runs the Internet?**

There are two important aspects of this question.

**First:** The existing organizations created by the U.S. years ago (ICANN, IETF, ITU) are seen in the world as U.S.-centric institutions. It is very hard to infiltrate/discover these institutions. ICANN is now more open and global.

ICANN operations are split into 3: headquarters in Los Angeles, Singapore and Istanbul. It is a model similar to an embassy model. ICANN is starting to open centers of excellence around the world and expanding to touch the world. It also runs IANA: The pattern is to get permission from the U.S. Dept. of Commerce to do things with it and this is a sore point because people think that the U.S. has too much power/control. In this way, the role of the U.S. is not sustainable. ICANN is engaging; this is essential to making it a global organization/institution.

**Second:** The existing groups [ICANN, IETF, ITU] do not address open societal/cultural questions and issues, for example, privacy, cyberbullying and so on. These are broad and deep issues.

**ICANN Approach**

How do we address the above issues? What is the institutional construct to put this regime together? What is ICANN doing about this? Three key activities are necessary for ICANN to evolve:

**One:** There are three middle countries: the most middle country is Brazil. ICANN was able to shift president’s position to multi-stakeholder solution; will be calling the world to participate in a multi-stakeholder conference regarding Internet governance. This has the support of Rousseff (Brazil), Hollande (France) and Merkel (Germany) in co-sponsoring a major conference.

**Two:** ICANN assembled a commission to produce a report that will feed the Brazil conference. We must put all of the scholarly research together.

**Three:** ICANN launched a new dialogue area/movement called INet. It focuses on businesses, governments, etc. providing input into the evolution of the governance process.

Why are these steps taken?

**The Logic**

ICANN needs to offer the world the vision for how we are going to do this (govern the internet) together. The world is looking for this. This logic will not erase the nation-state mode, but we must find a way for all stakeholders to have a say in Internet governance.
There is a need for a level of thoughtful leadership in governments with regard to the issues. The U.S. government should better coordinate its opinions/stance on these issues.

Panel Perspectives

**Internet Society – St. Amour**

ISOC supports a decentralized system. There are growing new institutions/practices, and a continued integration of physical and cyber. We must stop and think about having one institution control a very important element of our lives. We cannot believe that one institution will solve all of our problems. It would be best to pull security matters apart. We expect that new solution paths will come up, but we must make sure we understand nuances. ISOC tried to identify some problems and solution paths.

**Political Analysis —Melissa Hathaway**

The U.S. government is fragmented. There is no leadership in (the area of Internet governance?) this area. The U.S. government has also lost a lot of its influence with regard to this area recently; therefore starting another organization is fraught with concern. The new initiatives with ICANN may be seen as competing with ITU (over matters of monetization). To continue with this perceived competition is not productive; we should work together on how to monetize the Internet. We must bring the argument back to its core; it is about the economy. There is a divide between ITU’s role and ICANN’s role.

**General Discussion**

It is ICANN’s belief that a single institution is not the answer. A new **model** is the solution. ICANN is not being defensive about ITU, it is being responsive. The one country, one vote mechanism and institution will not go away. Nevertheless, it is essential to bring
transparency to the nuances of all of the disputes occurring. These can then be broken down to find a common ground to move forward. Perhaps it is not correct to say that there is a rift, but ITU certainly has aspirations toward Internet governance. IANA’s functions are very complicated, even more so than ICANN itself.

We are at a point where the U.S.-centric argument must give way to a truly global organization.

The Russian government invited the ICANN President to visit the country. Russia believes that ICANN broke into a key country (Brazil) that would stand on the opposite side of the debate regarding the U.S. role in ICANN. Russia has a root server, but it wants a root service.

There is no technical reason why there cannot be more root services than the current limit allows. ICANN has a root service, and they replicate them all over the world. The argument that the limit was a technical one is no longer valid. So, how do we go about expanding root services?
PANEL SESSIONS

PANEL I
Dimensions of Cybersecurity

Moderator
Michael Sulmeyer, Senior Policy Advisor, Office of the Deputy Assistant Secretary of Defense for Cyber Policy

Presentation
Major Challenges to Governance of Cyberspace
Tomas Lamanauskas, Head, Corporate Strategy Division, International Telecommunication Union (ITU)

Panel
Richard Bejtlich, Chief Security Officer, MANDIANT
Adam Segal, Maurice R. Greenberg Senior Fellow for China Studies, Council on Foreign Relations (CFR)

Moderator
Michael Sulmeyer
Retaining the focus on gaps in governance and threats to cyber security, this session begins with a presentation on governance from a major institutional perspective, and then addresses questions pertaining to cyber security. These include:

- What are the tools & instruments that threaten cyber security?
- Security for whom? What, how and when?
- What is the broad “ecology” of cyber threat and insecurity?
- What are the ranges of motivations, expected gains thereof?
- Public sector (government and military), Private sector (national and international), and non-profit entities?
- What are the plausible scenarios for the immediate future?
- When is the next “cyber catastrophe”?

**Presentation**

Tomas Lamanauskas

The ITU is one of the most enduring U.N. agencies. Its current focus on telecommunications recognizes that this world is obviously changing. Headquartered in Geneva, it consists of three sectors: radio, communications and development.

**Protect vs. Provide**

The Internet is vital; we know we want some internet for everyone. But we are still at the stage at which we need to ensure that the ideal of the internet is available for everyone in the world (4.4 billion people are still offline).

How equitable is the internet? There is a great deal of variation in terms of ability to pay Internet access throughout the world.
Context for Cyber Security

Debates center on cyber war and cyber espionage. However, most people think of security as the ability to use the internet without facing threats. In fact, there are $500 billion USD annual losses to cybercrime and 1.5 million cybercrime victims each day. There is online abuse of the most vulnerable (children). The use of robots and implantable devices will turn cyber threats into physical threats, industry and business. Around 80% of cyber threats could be tackled by addressing the things we know how to address. Is everyone at the same stage in terms of protecting themselves? No.

Global Cyber Security Agenda

The ITU launched a global cybersecurity agenda based on 5 pillars: legal measures, technical measures, organizational measures, capacity building, and national and international cooperation. These five pillars are a framework to address cybersecurity issues. The ITU also supports countries around the world to help implement cybersecurity measures and provide assistance with policy development.

WCIT-12: set the ground for international cooperation on certain cybersecurity-related matters—notably Article 6, on security and the robustness of networks, and Article 7, on unsolicited bulk electronic communications. Some progress has been made, but there is much farther to go.

Other ITU Initiatives

Other major ITU initiatives include the Child Online Protection Initiative (since many parents have not used the Internet enough to be in the best position to teach their children how to use it), a continued standardization focus, work with the U.N. office for directing cybercrime, and helping countries to agree on common approaches to solving problems.

The Anti-Counterfeiting Trade Agreement, the International Telecommunication Regulations (2012), the Stop Online Piracy Act, and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property all involve heated debates about issues of frameworks.

Select ITU Key Principles

These include: the meaningful involvement of all stakeholders/countries on equal footing; collaboration of relevant organizations (UN and non-UN) and building on the achievements so far; pragmatism; concentration on real issues and avoiding unhelpful dichotomies.

The ITU will not be going into areas that are not in the mandate, but it is clear that it will be addressing areas that people do care about with regard to connectivity.
Panel Perspectives

Cyber Security – U.S. DoD

How does the U.S. Department of Defense think about its role in cybersecurity? The DoD has three missions:

- Defend U.S. DoD networks. Otherwise, it's difficult to help others do so.
- Prepare for contingency. This is basic standard military planning and operations; making sure that there is enough cyber support available for use in a crisis.
- "Defend the Nation": Provide a supporting role for Homeland Security and the FBI, such that there would not be any confusion in the event of a serious attack on the U.S. through cyberspace.

Going forward, there will be some reorganization and consolidation (due in part to sequestration). In the DoD policy office, cybersecurity is being consolidated with homeland defense. The DoD is getting better about crystalizing the mission, but with 20% head cuts, it needs even more focus on consolidation.

Cyber Security – Policies & Responses

Cybersecurity is a problem that both government and private companies have. We cannot think that governments do a better job with security than the private sector.

More access is better, but there will also be an increase in the number of victims of attack. It is becoming clear that cyber conflict follows physical conflict, but although a physical
event can precipitate a lot of cyber activity, in some cases it works the other way as well (Arab Spring, etc.).

What is the national strategy for the private sector? What is the individual strategy for companies to protect themselves? Most companies do not start thinking about this type of question until after they have had the breach. There is a small window in which you can introduce a strategy to a company to protect it. Can this window be made even smaller?

**Business View – BENS (Business Executives for National Security)**

The Business Executives for National Security is a nonprofit entity that started about 30 years ago with bit of a different business model than most. It pays its own way and does not look for grants, solicit donations, etc. It was originally focused around DoD as a way of bringing CEO recommendations to address answers to problems.

For example, the CEOs of the oil and gas industry looked at whether the DoD was purchasing fuel in a productive/efficient way. They put together group of CEOs from various parts of the economy, some with deep technical knowledge and some with good business background, and developed an awareness program that builds on the infrastructure and programs developed by other non-profits and some for profits.

Part of the project is to speak to the CEOs in a language that is not technical and intimidating. BENS spent a great deal of time developing checklists and lists of questions that are in “business language” instead of technical language, and would allow the CEOs to ask questions in a framework that makes more sense. So part of it is a risk assessment, part of it is comparative: how do you compare to other businesses in your industry, size group, etc.? How do you know what shifts to begin to make?

BENS does not really get at the issue of governance except in the area of the individual corporation: for the middle of the market that does not have the staff to do it themselves.

**The China View**

We often portray the Chinese as having a well thought out, top down strategy, but China sees itself as being outplayed by the U.S. and contained. To China, the idea that it is the main cyber threat in the world is an attempt to degrade China. It believes itself to be the primary victim and points to attacks by the U.S. The Chinese also see cyber conflict as accompanying physical conflict (for example, the China-Japan island dispute); these types of attacks can have more and more impact as Chinese society becomes more and more net-dependent.

The China view is: how do we reduce our dependence on the U.S. (and Japan)? How do we become technologically independent? The Interagency process is much worse in China than in the U.S. It is difficult to make agencies talk to each other to formulate strategies and responses.
Does the push for the establishment of cyber command serve as a deterrent? China believes it needs a much more offensive, aggressive strategy. But it does not have a cohesive message/agenda. At the same time, China is interested in maintaining regime power and domestic stability.

**Vulnerabilities & Disclosures**

While all of this is taking place, the level of hacking has not subsided (one unit took a short break to regroup and then came back). Europe has more robust disclosure requirements about the purchasing of vulnerabilities.

Coordinating vulnerabilities is a very complex issue; coordinating interactions between multiple vendors is especially complicated. The idea of having a single global coordination center sounds ideal, but it is unrealistic because of the complexity of the interactions (must attempt to coordinate up and down the supply chain). Are there an infinite number of vulnerabilities? Since human beings write software, yes. There are a finite number of exploitation techniques.

The distinction between *service* and *content* has a technical manifestation that is between network security and data-centric security. So far we have been living in a world where emphasis has been on network security. But now this will change for everyone. In addition, we have to separate network security from the security of people using the network. There is no such thing as Internet-crime, rather the people using the Internet are committing the crimes and this makes the Internet not secure. One is an issue for the network operators (not a government concern) and the other is something that governments need to be concerned with and have the infrastructure to deal with it.

Finally, we realize that we cannot really prevent risk, but we must focus on *resilience* and specifically on *infrastructure*. How do we shift culture from being risk-adverse to being resilient?
Major Challenges to Governance of Cyberspace

Tomas Lamanauskas
Head, Corporate Strategy Division, International Telecommunication Union (ITU)

Context: Major Challenges

Vision for the Internet

"Idyllic and utopian model of everyone being able to communicate with everyone else and do what they want to do"


How equitable is the Internet?

4.4 billion still offline
Putting Cybersecurity in the Context

Different Perspectives of Cybersecurity

It is first of all about trust and confidence necessary to derive benefits from the connectivity

What’s at Stake?

exchange information. Because the internet is unregulated, it has led to an escalation of the global sex trade and the commercial sexual exploitation of women and children.

It has rendered national borders meaningless and lawmakers and law enforcers worldwide have been left scrambling while organised criminal syndicates have used the internet to their advantage, displaying all forms of sexual exploitation and recruiting unsuspecting women.
Low Hanging Fruit Still Exists

“80% or more of currently successful attacks exploit weakness that can be avoided by following simple best practice, such as updating anti-malware software regularly”

The UK Cyber Security Strategy, 2011

Recognized Need for Action

“...We need to work together to bolster confidence in our networks, which are central to international commerce and governance.
- We need to strengthen national legislation ... push for international frameworks for collaboration ... and adopt the necessary measures to detect and defuse cyber threats.
- We need to plug loopholes to stop perpetrators of cybercrimes and bring them to justice.”

Ban Ki-moon, Seoul Conference on Cyberspace, October 17, 2013
Resolution 68/243 of the UN General Assembly on “Developments in the field of information and telecommunications in the context of international security” (2013)

- Calls upon Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information.

What is ITU Doing?

Global Cybersecurity Index

**Objective**

The Global Cybersecurity Index (GCI) aims to measure and rank each nation's level of cybersecurity development in five main areas:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- National and International Cooperation

**Goals**

- Promote cybersecurity strategies at a national level
- Drive implementation efforts across industries and sectors
- Integrate cybersecurity into the core of technological progress
- Foster a global culture of cybersecurity

Expected delivery of the full index - Q4 2014

WSIS+10 Review Process: Key Areas

From the discussion of the Action Line CS: Building confidence and security in the use of ICT

- Greater cooperation
- International frameworks
- International standards
- Computer Incident Response Teams
- "Culture of Cybersecurity"
- Protection of human rights, data and consumer rights
- Protection and empowerment of vulnerable online, especially children
- "Security by design"
- Management of critical infrastructure
- Assistance to developing and least developed countries
- Measurement
- Sovereignty

ITU Global Cybersecurity Agenda

Source: IMPACT
**Assistance for Policy Development and Implementation**

- HIPCAR (CARIBBEAN)
- ICB4PAC (PACIFIC)

**Regional and Special Support**
- ITU-IMPACT Arab Regional Cyber Security and Innovation Centre hosted by Oman CERT covering some 22 Arab countries.
- Memorandum of Understanding (MoU) with the Nigerian Communication Commission to set up a Regional Cybersecurity Centre in Nigeria (July 2013).
- ITU project for "Enhancing Cybersecurity in Least Developed Countries (LDCs)" following 3 main pillars:
  - Policy-level assistance
  - Capacity building efforts
  - Equipment and software distribution

---

**Child Online Protection Initiative**

- Key Objectives:
  - Identify risks and vulnerabilities to children in cyberspace
  - Create awareness
  - Develop practical tools to help minimize risk
  - Share knowledge and experience

- Partners:
  - 10 international organizations
  - 33 civil society organizations
  - 13 private sector organizations

---

**UN-wide Framework on Cybersecurity and Cybercrime**

- Endorsed by the United Nations System Chief Executives Board for Coordination (CEB) on 25 November 2013.
- Developed by ITU and UNODC along with 33 UN Agencies.
- Enables enhanced coordination among UN entities in their response to concerns of Member States regarding cybersecurity.

---

**Standardization**
- Conducted and coordinated by ITU-T Study Group 17 – Security
- Over 70 standards (ITU-T Recommendations) focusing on security
- Key areas of current work:
  - Cybersecurity
  - Child Online Protection
  - Security architectures and frameworks
  - Countering spam
  - Identity management
  - Security of applications and services for the Internet of Things, web services, social networks, cloud computing and Big Data

---

**Importance of Collaboration**

![Collaboration Logos]

---

3/6/2014
International Frameworks

UN Efforts on Various Aspects of Cybersecurity

- Resolution 68/167 of the UN General Assembly on “The Right to Privacy in the Digital Age” (2013)
- Resolution 57/239 of the UN General Assembly on “Creation of a global culture of cybersecurity” (2002)

Some progress is made – however, further work is needed towards a more comprehensive and inclusive framework... but...
Some Key Principles
Meaningful involvement of all stakeholders:
- In their respective roles as per outcomes of WSIS
- Potential requirements for the such involvement:
  - Transparent*
  - Balanced and Inclusive*
  - Accountable*
  - Legitimate
- ITU’s recent experience includes some models to consider:

*Adopted from Neelie Kroes
“Europe and the Internet in a global context: What future, what challenges ahead?”
(October 2013)

Importantly – Tensions are normal when looking for solutions to new challenges...

...What matters, is how we utilize and resolve such tensions
PANEL II
Dilemmas of Cyber Governance

Moderator
Melissa Hathaway, President, Hathaway Global Strategies LLC; Senior Advisor, Belfer Center, Harvard Kennedy School

Panel
Xing Li, Professor, Electronic Engineering Department, Tsinghua University, Beijing, China; Deputy China Education and Research Network (CERNET) Center
Milton Mueller, Professor, School of Information Studies, Syracuse University
Alexander Klimburg, Senior Advisor, Austrian Institute of International Affairs, Fellow Harvard Kennedy School

Confounding Cyber Security
Cybersecurity has been bundled into a single conversation. This includes political activism, organized crime, intellectual property theft, disruption of service, anything not 24/7 connectivity and so forth. There is no governance mechanism. This is a major gap. For example, if we consider cyber attacks, then we see potentials for Stuxnet variations (military-grade weapons) used against the U.S. and its allies.
How much more government should you have on the Internet? The US is behind Europe in regulation in many ways, notably data protection and surveillance. Going through big data to detect non-obvious relationships is complex.

Routers are insecure for a variety of reasons. The US is hosting many servers used for crime. We need to increase infrastructure hygiene, improve economic security, and lever control at critical points.

Government should enable private actors to do the right things. In practice, there is a lot of governance in areas like crime, but there are no overarching institutions.

**Internet Fragmentation**

What is fragmenting the Internet? How does this complicate governance (or not?). Firewalls protect and fragment all the time. A country cannot simply withdraw from the Internet. We also must consider national vs. global security. How does dividing the Internet into nation-state lines help security? Most of the work (e.g. for spam) is done by private actors.

States will intervene to protect their interest, even if that has negative consequences for them. We do not have transnational mechanisms to deal with this set of issues. Do we need any?

**Flexibility & Adaptation**

The Internet becomes more flexible as it adapts to government requests, as well as to user choices. China, with 120 million students, had to start IPv6 over IPv4. Translation is the way to go. More than 70% of young users know how to bypass the Green Dam.

**Institutions & Imperatives**

Many institutions are working on cybersecurity. For example, the Organization for Security and Cooperation in Europe is a good alternative to only-China or only-Russia organizations. At the same time, with intercontinental ballistic missiles, we know that accidental major conflicts are happening throughout cyberspace. Of the voluntary agreement, only two CBMs are practical.

Among the requirements for governance are the needs for transparency, agreement on a glossary of terms, the ability to escalate from CERT to CERT communications, and to national security communications.

The tendency is to leave “nasty” legislation to the European Union, to shield for national governments, introduce mandatory disclosure, and a requirement that applications providers must notify breaches to ENISA and national governments.
The bottom line is this:

There are “pockets” of governance in place. They differ by regions, issues, logics, implementation and enforcement. However, there are no explicit connections among pockets, nor a necessary tendency to generalize or expand models of practices in place.
PARALLEL PANELS

The parallel sessions are designed to “dig deeper” into the empirical, operational, and analytical basis that inform our views about emergent threats to cyber security. This panel considers actors, actions and outcomes. Different methods and operational strategies are presented.

Panel IIIa

Cyber Security – Emergent Issues

Moderator
Michael Siegel, Principal Research Scientist, Sloan School of Management, MIT

Panelists
Brandon Valeriano, Senior Lecturer, School of Social and Political Sciences, University of Glasgow
Tim Maurer, Policy Analyst, Open Technology Institute, New America Foundation
Katie Moussouris, Senior Security Strategist Lead, Microsoft
Urs Luterbacher, Honorary Professor, International Relations/Political Science, Graduate Institute, Geneva, Switzerland

Moderator
Michael Siegel
Introduction

In many ways the slides presented in this panel highlight emergent features of threats to cyber security – and diverse facets that are now taking shape. Among the salient issues are new cyber damage tools, markets for creative illegality, cyber conflicts, anonymity mechanisms, and new directions for state and non-state actors.

Key Questions

The main questions discussed are introduced via a system dynamics model (see slides). These include:

- How does the white market of exploits and vulnerabilities impact the black market demand?
- What is currently on offer in the white market?
- What is the life cycle of a cybercrime?
- What has been the influence of bug bounty programs on the supply of the vulnerabilities?
- How do state investments in cyber capabilities influence the foreign behavior?

Connecting Cyber & “Real” Conflicts

Many cyber-attacks have a very low severity and do not reach high level of severity. But can these be measured by type, intensity, and interactions?

Basic dispute *types* are vandalism, denial of service, intrusion, infiltrations, and their combinations. The *severity* of the dispute can be characterized in terms of:

- Minimal damage,
- Targeted attack on the critical infrastructure,
- Significant effect on a nation’s strategy,
- Dramatic effect on a nation and
- Escalated effect on a nation.

The interaction type of such cyber incidents that can be either probing, defensive or offensive acts and about the target types which can be private/non-state, state-military or state-non-military. Except for US and China, most of the cyber disputes are regional. For a summary table of around 125 publically acknowledged cyber conflicts between 2001 and 2011 between rival states, see: [http://dl.dropboxusercontent.com/u/5471522/Valeriano%20Maness%20Cyber%20Conflict%20JPR%20Final%20submission.pdf](http://dl.dropboxusercontent.com/u/5471522/Valeriano%20Maness%20Cyber%20Conflict%20JPR%20Final%20submission.pdf)

The Wassenaar Arrangement

Primary discussion was on the updating of the Wassenaar Arrangement. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control regime (MECR) with 41 participating states including many former COMECON (Warsaw Pact) countries: [http://www.wassenaar.org/](http://www.wassenaar.org/)
The Basic List is composed of Ten Categories based on increasing levels of sophistication:

- Category 1 – Special Materials and Related Equipment
- Category 2 – Materials Processing
- Category 3 – Electronics
- Category 4 – Computers
- Category 5 – Part 1 – Telecommunications
- Category 6 – Part 2 – "Information Security"
- Category 7 – Sensors and "Lasers"
- Category 8 – Navigation and Avionics
- Category 9 – Marine
- Category 10 – Aerospace and Propulsion

During the 2013 review, member states have agreed on new export controls were agreed in the areas of (a) surveillance and law enforcement/intelligence gathering tools, and (b) Internet Protocol (IP) network surveillance systems or equipment.

These changes do not include DRS and reverse engineering of the codes. Why were such changes made to the list? Was it due to the events like Arab Spring? Western Basic List has two nested subsections—Sensitive and Very Sensitive. Items of the Very Sensitive List include materials for stealth technology—i.e., equipment that could be used for submarine detection, advanced radar, and jet engine technologies.

The Munitions List has 22 categories which are not labeled. Are companies providing technologies that might be a help to the regimes? Or, under certain conditions, may be detrimental to international and regional security and stability? Further, what type of technologies are we actually talking about?

What is the time frame in which such changes can be actually implemented? This might even be part of a congressional effort on National Defense Authorization Acts to look into what technologies can be the part of the list.

**Microsoft Big Bounty Program**

Microsoft has been buying vulnerabilities and established a big bounty program whereby it paid up to $260,000 as reward money for information on vulnerabilities. Hackers shared the vulnerabilities due to:

1. **Compensation** through (a) selling vulnerabilities, (b) big bounty programs, and (c) penetration testing;
2. **Recognition**, such as snapchat vulnerability exposure, and
3. **Challenge** of solving complex problems.

The economy of exploit sales consists of three markets:

- **White Market** where a vendor offers a bounty for reporting vulnerability.
- **Grey Market** where brokers buy vulnerabilities and then sell them companies, states or (maybe) to organized crime.

3/6/2014
- Black Market where organized crime and government buy or take subscription of exploits for offensive activities.

No price data was shared apart from the money given away as prize money on Microsoft’s Bluehat prize (see http://www.microsoft.com/security/bluehatprize/).

After Microsoft introduced the big bounty program, the number of direct exploits submissions has increased by 74%. James Forshaw came up with a new exploitation technique to get the first ever $100,000 bounty.


**Predicting Cyberspace Crises**

The AI tool *Globe Expert* seems, in the case of the cyberspace referential, to find the correct information about the absence of a black swan even though local breaking points are identified. Results show that the that US and China tend to overestimate governance and systemic problems at the expense of others such as the influence that other countries can exert on cyberspace and also technical problems due to hacking and big data clusters (mostly only for China). It is suggested that these perceptions should be corrected.

The detection of a black swan uniquely from the probability space associated with the set where it might nest is impossible. However, if information about it is contained within other segments then it might be possible to circumscribe very closely the whereabouts of a black swan. In general, the results so far show that as breaking points in cyberspace do exist they are for the moment localized.

These are mostly linked to big data cloud structures and centers and to some extent to the relations between the U.S. and China. However, a generalized crisis or breakdown (a so-called black swan) is unlikely in the next few years. *Global Expert* works well but some conceptual and error analysis problems have yet to be solved.
SLIDES
Cyber Security – Emergent Issues
Michael Siegel
Principal Research Scientist,
Sloan School of Management, MIT

CYBER SECURITY – EMERGENT ISSUES
Moderator
Michael Siegel
Principal Research Scientist, Sloan
School of Management, MIT
Panel
Brandon Valenzano
Senior Lecturer, School of Social and Political
Sciences, University of Edinburgh
Timmarsh
Policy Analyst, Open Technology
Institute, New America Foundation
Katie Moussouris
Senior Security Strategist Lead, Microsoft
Urs Luterbacher
Honorary Professor, International Relations/Political
Science, Graduate Institute, Geneva, Switzerland

Resolving Emergent Issues in Cyber Security:
Modeling and the Sum of the Parts
Michael Siegel
James Houghton
Sloan School of Management
MIT

How do white markets influence black market pricing?
An explicit price factor in both how widely the target
software is used as well as the difficulty of
cracking it.

How do bug bounty programs influence vulnerability supply?
Bounty Evaluation: $100,000 for New Mitigation Bypass Techniques Wanted
Dead or Alive

What is the lifecycle of cybercrime?
"We are setting aside a $200K budget
to purchase browser and browser plug-in vulnerabilities, which are
going to be used exclusively by us,
without being released to public."
— Paul @, Author of Blackhole, Apr ’13

How do white markets influence black market pricing?

How do bug bounty programs influence vulnerability supply?

Microsoft is announcing the first evolution of its bounty programs, first
announced in June of 2013. We are expanding the pool of talent who can
participate and submit novel mitigation bypass techniques and defensive ideas
to include responders of forensic expertise; not just active attacks in the wild."
How does State investment in cyber capability influence foreign behavior?

Pressure to Use Cyber Capability

Domestic Cyber Actions

Foreign Cyber Actions

Domestic Cyber Capability

Foreign Cyber Capability

Domestic Investment in Cyber

Foreign Investment in Cyber

“The Chinese are conducting espionage on a massive scale. [If we] ban sales of ... exploits to the U.S. and European allies ... the only possible outcome is that the Chinese will increase their internal production and skills and the... West will fall behind.”

- Gruppo, third party broker

CYBER SECURITY – EMERGENT ISSUES

Panel
Branko Valeriano  Senior Lecturer, School of Social and Political Sciences, University of Glasgow
Tim Maurer  Policy Analyst, Open Technology Institute, New America Foundation
Katie Minourou  Senior Security Strategist Lead, Microsoft
Urs Luterbacher  Honorary Professor, International Relations/Political Science, Graduate Institute, Geneva, Switzerland

3/6/2014
Empirical Cyber Conflict Studies

Brandon Valeriano
University of Glasgow

and

Ryan C. Maness
University of Illinois at Chicago

Low Rate of Usage for Cyber Tactics

Most Cyber Incidents are Regional

The Actions We Have Seen Have Been Low in Severity

There Has Been Little Reaction to the Cyber Operations, so far...
Katie Moussouris
Senior Security Strategist Lead, Microsoft

Security Researcher Motivations/Fulfillment

- Compensation
  - Financial incentives
  - Recognition of contributions
  - Personal growth

- Recognition
  - Public acknowledgment of work
  - Awards and honors

- Pursuit of Intellectual Happiness
  - Learning and innovation
  - Solving complex problems

Microsoft’s Bounty Programs

Over $128,000 PAID Strategic Impact

10+ Years of Researcher Engagement
Researchers are invaluable to our security strategy

The Vulnerability Economy

- White Market
  - Vulnerabilities with no financial reward

- Grey Market
  - Vulnerabilities with limited financial reward

- Black Market
  - Vulnerabilities with significant financial reward

Why Now?

Bounties are not one size fits all
Finding the right approach for our customers
Microsoft bounty programs

Mitigation Bypass Bounty
Microsoft will pay up to $100,000 USD for truly novel exploitation techniques against protections built into the latest version of our operating system (Windows 11 Preview).

BlueHat Bonus for Defense
Microsoft will pay up to $50,000 USD for defensive techniques that significantly improve our mitigation bypass defenses.

IE11 Preview Bug Bounty
Microsoft will pay up to $11,000 USD for critical-class vulnerabilities that affect IE11. IE11 Preview is now available for Windows 8.1 Preview, including bugs with privacy implications.

IE Preview Bug Bounty: All in the timing

Running a bounty program during the Preview (beta) period lets us address the greatest number of issues with the least impact to our customers.

Other bounty programs don't offer payment for products in beta, so we're pleased to address that gap in the marketplace in this pilot program.

Results: 23 submissions, 18 bulletin-class issues — 6 sandbox escapes

IE 11 Preview Bounty --> Reverses Reporting Trend

Change in Private/Bidirectional Bug Reports against Directly Reported (CVD) IE Bugs

Mitigation Bypass Bounty: $100,000
James and the Giant Check Presented 12/12/13

Pay to the order of James Forshaw $100,000
One Hundred Thousand and 00/100 Dollars USD
Memo: Mitigation Bypass Technique

Bounty Program Evolution

Mitigation Bypass Bounty – NOW OPEN TO ANYONE WHO TURNS IN A DISCOVERY FROM THE WILD

Stay tuned for further developments...

A Smart Security Strategy Has Layers

Researcher Engagement

Industry Collaboration

Establissh Vulnerability Response Processes

Build More Secure Products
Mitigation Bypass Bounty
Eligible Submissions

Eligible bypass submissions must demonstrate and describe an exploitation method that meets the following criteria:

- **Generic**: It must be applicable to one or more common memory corruption vulnerability classes.
- **Reliable**: It must have a low probability of failure.
- **Reasonable**: It must have reasonable requirements and prerequisites.
- **Impactful**: It must be applicable to high-risk application domains (browsers, document readers, etc).
- **User Mode**: It must be applicable to user mode applications.
- **Latest Version**: It must be applicable to the latest version of our product on the date the entry is submitted.
- **Novel**: It must be a novel and distinct method that is not known to Microsoft and has not been described in prior works.

APPENDIX

### IE11 Preview Bug Bounty
Payouts & Tiers

<table>
<thead>
<tr>
<th>Vulnerability Type</th>
<th>Code dump</th>
<th>Proof of concept</th>
<th>Exploiting exploit</th>
<th>WHIPS</th>
<th>Sandboxed escape</th>
<th>Raw payload Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCE vulnerability</td>
<td>not required</td>
<td>required</td>
<td>required</td>
<td>required</td>
<td>not required</td>
<td>Could exceed $11,000 USD*</td>
</tr>
<tr>
<td>Important or High-severity design flaws or vulnerabilities</td>
<td>not required</td>
<td>required</td>
<td>n/a</td>
<td>optional</td>
<td>not required</td>
<td>Tier 2: Minimum payment $1,000 USD</td>
</tr>
<tr>
<td>Security bug with Privacy Implications</td>
<td>not required</td>
<td>required</td>
<td>Proof of Concept is sufficient</td>
<td>optional</td>
<td>not required</td>
<td>Tier 3: Minimum payment $500 USD</td>
</tr>
<tr>
<td>Sandbox escape vulnerability</td>
<td>not required</td>
<td>optional</td>
<td>optional</td>
<td>optional</td>
<td>required</td>
<td>Tier 4: Minimum payment $250 USD</td>
</tr>
<tr>
<td>AA0 verification vulnerability</td>
<td>not required</td>
<td>required</td>
<td>n/a</td>
<td>optional</td>
<td>optional</td>
<td>Tier 5: Minimum payment $100 USD</td>
</tr>
</tbody>
</table>

*Maximum award for RCE vulnerabilities could exceed $11,000 USD.
Urs Luterbacher
Honorary Professor, International Relations/Political Science,
Graduate Institute, Geneva, Switzerland

Predicting The Likelihood of Cyberspace Crises With the Help of Information Theory: From breaking points to Black Swans
Urs Luterbacher, Thierry Lorho and Valerie Fert

This will be possible with the help of information theory
- Information theory was developed by Shannon (1948) in connection with the evolution of computer technology
- To understand it, start with the model of tossing a fair coin where each side has a probability of ½. 1 question with 1 answer will give the information about the result of the tossing heads or tail
- Entropy in this case will be maximal and worth 1 or 1 bit because only one question has to be asked with one answer
- Generalizing: if 3 questions with 3 answers necessary the entropy or information will be worth 3 bits

What about textual material?
- For a text made up with words similar principles are applied
- For each word and for each combination of words it is possible to determine a probability space
- By extension each document composed of texts and each set of documents can be represented in this way which will constitute an exact representation of the information structure contained in them
- The AI system used here works on the basis of dbacl, a digraphic Bayesian classifier for text documents which computes maximum (relative) entropy models for text corpora and can compute the Bayesian posterior distribution for a given document in terms of any number of previously computed models.

Entropy of a segment, Divergence, and, Cross Entropy between segments
- We will imagine three sets which we will call segments containing information a, b, and c. We can also define U the union of a, b, and c.
- All these segments can be represented by probability spaces. These segments are partially overlapping. One can measure the information shared by these three segments through indicators: Divergence, Cross-Entropy, and then Uncertainty, Information content, Predictability

Detecting Crises Information and “Black Swans”
- The detection of a black swan uniquely from the probability space associated with the set where it might nest is impossible
- However, if information about it are contained within other segments then it might be possible to circumscribe very closely the whereabouts of a black swan
- In order to obtain such informations, referentials in the form of a crude list and hierarchies of concepts have to be constructed by experts in the field. The AI system then starts its queries and gives results
- The results so far show that as breaking points in cyberspace do exist they are for the moment localized. These are mostly linked to big data cloud structures and centers and to some extent to the relations between the US and China. However a generalized crisis or breakdown (a so-called black swan) is unlikely in the next few years.

Cries or critical events are predicted by some people while most don’t
- So traditional doomsday sayer such as Peter Schiff, Mark Faber, and Nouriel Roubini and some seasoned economists such as Joseph Stiglitz, Robert Schiller and Martin Feldstein predicted an imminent financial crisis in 2007 or early 2008 but most others did not. Similar pronouncements are available for cyberspace problems
- This shows an ambiguity in the signals that can be picked up from various information sources
- Is it possible to do better? This is the purpose of the artificial intelligence system presented here
Results and Conclusions

- Our AI tool Globe Expert seems in the case of the cyberspace referential to find the correct information about the absence of a black swan even though local breaking points are identified.
- It shows that US and China tend to overestimate governance and systemic problems at the expense of others such as the influence that other countries can exert on cyberspace and also technical problems due to hacking and big data clusters (mostly only for China). It is suggested that these perceptions should be corrected.
- Significant threshold values for a black swan are not crossed (60% for all 3 indicators). These are justified by quantum information theory. For 100% indicator (interpreted them as a q-bit), there is more than 50% chance to have the event occurring.
- More needs to be done here and a type I and type II error analysis be undertaken to provide more validity.
- Techniques to harmonize referentials and their constructions have to be developed. Otherwise results could be perceived as artefacts of referentials.
- The AI tool therefore works well but some conceptual and error analysis problems have still to be solved.
PANEL IIIb
Cyber Governance – Basis for Accord

Moderator
Joseph Kelly, Senior Advisor for Cyber, Office of the Under Secretary of Defense for Intelligence

Panel
Kilnam Chon, Professor of Computer Science at the Korea Advanced Institute of Science and Technology (KAIST), Professor, Keio University
Jesse Sowell, Ph.D. Candidate, ESD, MIT
Greg Rattray, CEO and Founding Partner, Delta Risk, LLC
Scott Bradner, University Technology Officer, Harvard University

Many features of governance for cyberspace remain to be fully understood. Many of the contentions obscure some emergent trends. What are these features; what are the trends? What are the contentions? How does all this “fit together”? These include:

- Formal and informal mechanisms
- The role of the private sector
- Institutional and operational actors, structures and practices
- Perspectives from the RIR’s
- Barriers vs. facilitating factors
• Expected outcomes

Ubiquity & Control

The Internet is ubiquitous. However, the Internet challenges and even disrupts existing global regimes and systems: from the music and motion picture industries to global and individual security and privacy - and traditional versus electronic commerce. As the 2nd ECIR Workshop on *People, Power and Politics* addressed, the individual also has a stronger voice in this ecosystem. Control of the technical underpinnings translates into defining winners and losers, (in practice winners) or losers. From a technical perspective, the Internet works perfectly and ‘runs smoothly’; responsibilities are well assigned.

Governance & Density

There are an ever-increasing number of actors involved in governance for some part of the Internet or its management – some of whom are becoming increasingly more organized. Currently there are 2.5 billion Internet users. The challenge is that at the end of this decade we will have 5 billion. Are we ready for this? If we are, then we can talk about governance. Take the Root server issue as an example: China and Russia want to have one. That is not that big a technical challenge. But do we have the governance structure to do it?

In the future, everyone will be online. In 2014, that everyone would mean 7.1 billion people. By 2050, UN estimates are between 8.3 and 10.9 billion people. From an institutional infrastructure perspective: are we ready? Only after this long-term readiness and preparedness are in place, *then* we can talk about network governance.

Past & Present

Early on governance of the Internet was not an issue. Operational integrity dominated. Early adopters and “geeks” structured Internet governance, in the early days of the late 1980’s and early 1990’s. Formal structures were late in coming. The Internet Engineering Task Force (IETF), for example, was founded as late as 1992. IETF had people from governments, but no official government representation. Government involvement in Internet standardization had started to emerge as early as 1977, with the Open Systems Interconnection (OSI) suite, which was started by the International Organization for Standardization (ISO).

The standard-setting bodies realized that the Internet is the future of all communications and tried to act accordingly. For example, in the area of Voice over Internet Protocol (VoIP): telephony companies tried to change protocols to improve it. Enter the role of disruption and innovation as it relates to standardization and governance (Skype proved the improved protocols unnecessary).

The Internet Corporation for Assigned Names and Numbers (ICANN) was setup to be the “Governor of the Internet.” In contrast, the International Telecommunications Union (ITU), founded in 1865, was setup to control the information communication of society, and goes beyond the functions of the Internet Assigned Numbers Authority (IANA).
In the 1970s and 1980, “there was just one Internet...is the goal to make it stay that way?” Reversing or addressing fragmentation is not the only way to approach the problem: the Internet is already fragmented. This is driven by technological as well as political factors. Future fragmentation, for example, includes the fact that internet traffic will be almost exclusively video and VoIP. Are we ready for that transition?

The Internet is going to be the communication network of the future. Nevertheless, implicit in that fact is also the reality that new pressures emerge. Basic infrastructure and growth challenges remain before there can be any realistic discussion of true governance: 5% of world economy is Internet. Will it grow to 10% or more?

**Governance & Security**

Overall, Internet governance is different from cyberspace governance: privacy, the economy, other major issues – there is no coordination at all to these cyberspace issues, which transcend ‘ordinary’ issues of Internet infrastructure and technical specifications. ICANN handles only domain-names - not the Internet as a critical infrastructure. In addition, ICANN proved that building even specific technical governance is difficult on a global level. (To date there are no institutions coordinating names on Google, Facebook, etc.) Beyond these technical issues, notions of governance are even more complex. Public policy isn’t exclusively in the realm of the government. Microsoft has a global cybersecurity team.

The private sector (Akamai, Comcast, etc.) know the network, but not the diplomacy. Policy-savvy engineers are not the norm. Yet, technical expertise is also a source of authority. How does this play out? External RIRs consultants are not public policy wonks, but resource allocation types. They look at the problem from a perspective of how to use and allocate resources. RIRs, Internet Exchange Points (IXPs), they want to make allocation policy (not public policy mandates).

Some argue that from a regional, geographic perspective, country-code top-level domains (ccTLD’s) are a waste of time. While Regional Internet Registries (RIR) and other self-governing entity have developed rules with an explicit absence of state governance, the past is not a predictor of the present or of the future.

The logic at the origin may not retain robustness over time.

Today, 10% of Internet users are American – a number that will recede to 5% or less. With that decrease, will the U.S. also rescind proportional control? Also, if there is a global institution UN type of organization at the top of the Internet governance, will it kill the innovative side of the Internet?

We also now have to consider the value of multi-stakeholders vs. the challenges of cybersecurity. In addition, there may be a “Stuxnet effect” that is, legitimizing attacks over the Internet. The gloves are off. DDoS attacks are not gone. It is all about protecting the Internet with the right governance model.
**Authority & Accountability**

The cybersecurity community in the financial systems and technology industries did not like what they saw as the implications, for them, of the “go-mobile era” – but it still happened. For example, the FBI recognizes it can’t stop all crime. Rattray also pointed out a general metric of success is that broad Distributed Denial-of-service (DDoS) attacks are “under control.” In principle, if there are regulations they must be forced ICANN, for example, was not created to manage all threats. Further, simple traffic functions like routing, and other critical functions, are an unattributed responsibility.

United Nations Group of Government Experts (UNGGE) and other mechanisms currently in place recognize that national governance requires accountability. Accountability issues remain rather dormant on the Internet, especially as related to security. Some argue that a narrowing down the working definition of security is needed to make it well-system. Others query whether this is a change of tone about security. Are we using DDoS attacks, or lack of success of these attacks and other incidents to justify government involvement?

In terms of political or policy-driven winners and losers: technical limitations determine what is feasible at the policy level. Prioritizations don’t work well, with requests that are not well understood. Not regulating something can actually help.

**Example**

Workshop participants offered recent changes at the Federal Communications Commission (FCC) as a further example. Internet environment is becoming more and more of a safety issue – and the FCC has historically been involved in safety.

A lot of what the Internet is doing is not undermining State authority. Not all non-State authority is competing with the State. Internet governance can be seen as a matter of resource management policy: Microsoft is getting involved in policy from a very resource-based perspective. It has proven itself a credible assessor, allowing them to suggest policy directions - without being obviously captured by interest groups (an important distinction).

**Bottom Line**

The bottom line is this: The era of no-government is (or is about to be) over. Governments are paying attention due to the big share of the economy, security matter, and the general shift in power relations worldwide.
While there are diverse perspectives – along with conflicts and contentions – over the nature and value of private public collaboration, almost everyone agrees that such collaboration is essential for the governance of cyberspace and the security of the cyber domain. Among the central issues are:

- Value in collaboration
- Innovation gains
- Costs, benefits and vulnerabilities
History Lessons

A lesson from history: when the Romans realized that their perimeter was indefensible, it was because internal lines of communication were almost nonexistent. Today, companies in the private sector represent the internal lines of defense. Often we see government and big companies trying to bundle smaller companies, which are a main source of innovation.

Private entities have a stake in cybersecurity. In the United States, the economy is run by small businesses with lateral and vertical networks. Some cases, such as Maryland National Cybersecurity Center, are built around big companies, with huge US investment ($13 bn). When that is the case, should it remain only big companies?

Collaboration for Talent

Partnership is needed not only for capital markets, even at the State level, or for public safety, but also for collaboration around the talent pool and for capturing the gains of innovative initiatives enabled by public-private partnerships. Small companies often are the source of solutions (notably authentication of identity). All things considered, some question whether the U.S. is retaining its leadership in the area of Internet security.

Hidden Vulnerability

One of the core principles of war is to disrupt the communication system of the adversary. The map of undersea cables shows pathways of potential vulnerability. Why have these not been disrupted? Is there a record of disruption incidents driven by intent? There is no tabulation of exploit events and the like. The federal government will probably mandate disclosure of incidents.
PANEL V

Alternate Features – Complexity, Contention, Collaboration

Moderator

Michael Sulmeyer, Senior Policy Advisor, Office of the Deputy Assistant Secretary of Defense for Cyber Policy

Presentations

The Future of Cyberspace
David Clark, Senior Research Scientist, Computer Science and Artificial Laboratory (CSAIL), MIT

The Future of Cyber Security
Herbert S. Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies

The Future of Cyber Governance
Nazli Choucri, Professor of Political Science, MIT; Principal Investigator, ECIR.

Throughout this Workshop we have come across enclaves in virtual relationships and trust. These are foundational. We have also identified components of governance that must be clarified. In many ways the elements are already in place, but there remain many “gaps in governance” – most significant of all are those related to the future of the political economy of Internet markets.
The Internet is technically defined, as a medium, at the packet carrier level. Conversely, when the users say “Internet” they mean the whole package -- including the application layer -- whereas the true technical specification of “Internet” only includes the packet carrier level. As a result Internet layer accountability is a bad idea.

Among the key design assumptions in the early stages of the Internet were that (a) you can separate people you trust and want to talk to from (b) people you don’t trust and don’t want to talk to.

Currently, there is a social engineering of the collective information of trust: Computer scientists are not the best people to engineer social interactions. From a computer science perspective, the long-term answer to network confidentiality has been encryption. It seems what we are really talking about is the further management of trust and confidence - the social engineering of trust – which ironically has to be a social experience because that is the way society creates trust.

On the other hand, we would like to have a secure and safe application level. But we cannot force application developers to do that. There must be an application level improvement of the user experience, while the private sector wants to make money. These two objectives are not necessarily the same thing. It is a choice to let only the private sector build applications.

The consumer is facing an Internet Protocol (IP) network that is not the Internet. Critical applications cannot migrate to other machines operating at an equal with the same type of network but not connected to the Internet. (A case in point is Comcast IP phones).
Nowadays, the Internet is causing globalization and cosmopolitanism at a reasonable rate. Different people use different applications. We have to accept the fact of diversity of these experiences and the fact that people’s sense of the internet experience will differ from person to person.

The Future of Cyber Security
Herbert S. Lin

Cybersecurity is an important issue but policy makers have not been involved in designing new policies. In many ways they react not initiate.

How can we use cyber forces to promote cybersecurity? Is it possible? If there is a critical issue, the question will be: “will they believe me in the hotline?”

Will security in the edge be resolved? How will market forces promote cybersecurity? Has it failed? Can they be manipulated?

Will there be a catastrophe? That would mean rapid action – an environment of “Russian panic”.

The whole point of a cyber operation is to exercise deception – what are the implications? What about offensive operations?

We know that passive defense plus law enforcement is seemingly insufficient. Intrusions to prepare you to handle harm. How does governance shape up to address these issues?

The Future of Cyber Governance
Nazli Choucri
The State

The State is a late comer to the cyber system. It does not fully understand all of the technical and policy complexities. But it will not withdraw from that arena. At the same time, the state is State is “hostage” to private sector decisions made early on. In general, the state is equilibrium-seeking in its mechanisms for managing and coordinating activities.

With the usual exceptions, states invite the participation of their constituencies in rule-making. Invariably states also seek a high degree of legitimacy. Under these conditions, the state is not very likely to involve use of force. But it will expand possibilities for improving its position or responding to intrusions. Already we see major states framing strategies for cross-domain responses, that is, responding to cyber intrusions with physical, diplomatic, force, or other traditional modes of activity.

The State is not the only entity with the capability or legitimacy to make demands for governance of the cyber domain or for the form of governance. Other entities are organized and mobilized to make demands and support their claims and interests.

Accountability

There is ambiguity about accountability. The very notion of governance implies some level of accountability, the specific type of which remains unclear. There is a two way relationship between those that govern and those that are governed. There are incentives, inducements, leverages, and penalties. However, the governed and those that govern can each be very diverse. The management of diversity is a major challenge of governance.

System-in-Place
The future of governance requires a basis for legitimacy and a mechanism for enforcement. The nuclear precedent provides some but limited insight. First, the nuclear case was about states dealing with states. Second, the number of states was relatively small; and third there is a serious scalability problem.

When all is said and done, the CERT system-in-place provides a major opportunity for connecting points-of-governance, where the points are located in different countries, and all are linked by some broad, agreed upon principles. But it is an under developed system. Nonetheless it is legitimate and in place.

The challenge is to reinforce the connections or linkages so as to create a more robust system-of-CERTS – a network of governance focused on metrics, measurement of cyber threats, to security. It highlights the critical features of cyberspace, namely demassification and deterritorialization, with particular emphasis on extending the potentials for security and sustainability.
Fourth ECIR Workshop

This Workshop contributes to the core goals of the ECIR research program. The program seeks to develop an approach 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 the cyber and the international relations domains, and create a body of knowledge that is theory-driven, empirically sound, and technically anchored such that it:

- clarifies threats and opportunities in cyberspace for national security, welfare, and influence;
- provides analytical tools for understanding and managing 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.

ECIR Research Themes

The research design is modular in its investigations of the cyberspace-international relations connections. It consists of a set of substantive issues with special attention to powerful cross-cutting factors, that is, concerns that cut across all substantive issues examined. Each theme is designed to highlight a “piece” of a complex “whole.” Jointly they are intended to improve our understanding of the reciprocal relationship between traditional international relations and the new domain of cyberspace.

Core themes of research are the following:

1. Framework and Foundations for Theory

   Constructing overarching frame and tools for analyzing interactions among the cyber and the kinetic arenas, and for clarifying how the “pieces” generate a view of the “whole”.

2. Cyber Power and Cyber Security: Control Point Analysis

   Exploring features of power and control, sources, and consequences of threats to security, and impacts of communication and social media on power relations.

3. Cyber Governance: Disciplined Behavior
Mapping and analyzing diverse modes of *private and public authority* in management of the cyber domain, emergent cyber norms, and *resilient mechanism design*.

4. **Alternative Futures: Contingent Developments**

Designing potential futures for cyberspace and international relations, with the underlying structure and processes.

**Cross-Cutting Themes**

In addition to relevance for the U.S. Department of Defense, two issues serve as cross-cutting themes:

- **Conflict and cooperation** - Highlighting *behavior-propensities* toward conflict, cooperation or a mix
- **Strategy and policy** - Exploring policy *response* i.e. actions to support goals

The remainder of this Report reflects different aspects of these overall initiatives.

The Poster Session shows the MIT-Harvard activities as well as those of a broader range of researchers. In many ways, this session points to some important future imperatives for research. These, along with the results covered in the List of Publications are also part of this Report and illustrate the scale and scope of ECIR research to date.
ACKNOWLEDGEMENT

The assistance, contributions, and management skills of Patricia McGarry are gratefully acknowledged, as is the assistance of Elizabeth Nigro. Sarah Stillman managed the entire production of the Report. Thanks are due to the MIT Industrial Liaison Office of the Office of Corporate Relations throughout the Workshop.
POSTER SESSION

List of Posters
*by title of poster

Bridging the Cyber Security Governance Gap: A Realistic Agenda for Multi-Track Diplomacy
Marco Mayer, Adjunct Professor, Cyber Space and International Relations, PhD Programmes, SSSUP, Pisa
Fabio Rugge, Italian Ministry of Foreign Affairs, Adjunct Professor, Security Studies, Florence University
In Cooperation with the Centro Universitario di Studi Strategici, Internazionali e imprenditoriali (CSSII)

Complexity of ICANN: Structure, functions, and resources

Critical Infrastructure: Does ICT Make it More Vulnerable?
John C. Hoag, Ph.D. Ohio University ITS School, Case Western Reserve University EECS Department

Cyber Conflict History: Assessing State Responsibility and Other Major Trends

Cyberconflict and Understanding the Geography of the Internet
Danilo Delia, PhD Candidate
Alix Desforges, PhD Candidate
Affiliation: Castex Chair of Cyberstrategy and French Institute of Geopolitics, University of Paris 8

Cyberplaces and the Politics of Disruption
Renee Marlin-Bennett, Professor of Political Science
Kavi Abraham, PhD Candidate
Affiliation: Johns Hopkins University

Data Initiatives: ECIR Data Dashboard
Stuart Madnick, Nazli Choucri, Steven Camina, Yiseal Cho, Gihan Dawelbait, Jeremy Ferwerda, Dara Fisher, Erik Fogg, Xitong Li, Hamid Salim,
Aadya Shukla and Fan Wei  
Research Affiliation: Explorations in Cyber International relations, MIT-Harvard and the MIT Sloan School of Management

**Defense-in-Depth in Practice**  
Josephine Wolff, PhD Candidate  
Research Group: Advanced Network Architecture Group  
Thesis Advisor: Dr. D. Clark, Senior Research Scientist

**Design of Action and Alliance Strategy in Defense against Anonymous Cyber Threats**  
Mina Rady, MIT Affiliate  
Research Group: Political Science, MIT  
Supervisor: Dr. Nazli Choucri

**Do We Care About Surveillance? Edward Snowden’s Impact and Policy Implications**  
Evan Marshall, 4th Year MIT Undergraduate and Mechanical Engineering Candidate

**Framing the Value of IX Participation**  
Jesse Sowell, ESD PhD Candidate, MIT Group: Advanced Network Architecture Group, CSAIL  
Thesis Advisor: Dr. D. Clark Committee: Prof. K. Oye (chair); Prof. C. Fine; Prof. N. Choucri; Dr. F. Field

**International Conflicts in Cyberspace**  
Alex Gamero-Garrido, MS Candidate in Technology and Policy, Engineering Systems Division, Research Group: Explorations in Cyber International Relations (ECIR), MIT-Harvard.  
Advisor: Prof. Nazli Choucri, MIT Political Science  
Co-Advisor: Dr. David Clark, MIT CSAIL

**The Meaning of the Cyber Revolution: Perils to Theory and Statecraft**  
Lucas Kello, Postdoctoral Research Fellow, Harvard Kennedy School  
This poster is based on an article by the same title published in International Security, Vol. 38, No. 2 (Fall 2013), pp. 7-40; www.mitpressjournals.org/loi/isec

**Mental Models in the Cyber Domain**  
James Houghton, Research Associate, MIT Sloan School  
Michael Siegel, MIT Center for Digital Business

**Resilience Metrics for Cyber Systems**  
Igor Linkov¹, Daniel A. Eisenberg², Kenton Plourde¹, Thomas P. Seager², Julia Allen³, Alex Kott⁴  
Research Affiliations: ¹ US Army Engineer Research & Development Center, ² Arizona State University, ³ Carnegie Mellon Software Engineering Institute, ⁴ Army Research Laboratory

---

3/6/2014
   Arash Nourian, MIT Sloan School of Management

Strategic Level Assessment of Cyber Vulnerability Organizational and Global
   Kathleen M. Carley, Ph.D., Carnegie Mellon University
   Research Affiliation: Carnegie Mellon, Center for Computational Analysis of Social
   and Organizational Systems (CASOS)

Sustainability and Cyber Sustainability: complexity models in a GSSD* perspective
   Jean-François Mascari, National Research Council, Italy
   in collaboration with Nazli Choucri, Political Science, MIT
   *Global System for Sustainable Development (see gssd.mit.edu)

What Do We Know about Cyber Conflict? Scope, Impact, and restraint in Cyberspace
   Brandon Valeriano, University of Glasgow
   Ryan C. Maness, University of Illinois at Chicago

Who Controls Anonymity?: Control Point Analysis of The Onion Routing Anonymity
   Network (TOR)
   Mina Rady, MIT AffiliateResearch Group: Political Science, MIT
   Supervisor: Dr. Nazli Choucri
ABOUT THE SPEAKERS

Richard Bejtlich is Mandiant’s Chief Security Officer. He has more than 15 years of experience in enterprise level intrusion detection and incident response working with the federal government, defense industrial base and Fortune 100 companies. Prior to joining Mandiant, Richard was the Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Before his work at GE, he operated TaoSecurity LLC as an independent consultant, protected national security interests for ManTech Corporation’s Computer Forensics and Intrusion Analysis division, investigated intrusions as part of Foundstone’s incident response team and monitored client networks for Ball Corporation. He began his digital security career as a military intelligence officer at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC) and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. He wrote The Tao of Network Security Monitoring, Extrusion Detection, co-authored Real Digital Forensics, and most recently The Practice of Network Security Monitoring. He currently writes for his blog (taosecurity.blogspot.com) and teaches for Black Hat.

Alfred Rives Berkeley, III is a Member of Technology Advisory Board at Safeguard Sciences, Inc. He is the Chairman at Princeton Capital Management, Inc., since January 2013 and an Analyst. He previously served as the Chairman at Princeton from 1996 to 2006. Mr. Berkeley is a Trustee of the Johns Hopkins University and the Nature Conservancy. He serves on the National Infrastructure Assurance Council, a post to which George W. Bush appointed him. He is a Trustee of the Mathematical Sciences Research Institute and is also a Member of the Board of Director of WebEx Communication, Inc. Previously, Mr. Berkeley served as the Chief Investment Officer and Software Analyst at Alex. Brown & Sons. Previously, in 1996, Mr. Berkeley was named President at the NASDAQ Stock Market, Inc. until 2000 and then as Vice-Chairman until 2003. He has served as an officer in the US Air Force and the US Air Force Reserve. He has served as a Director of a number of public and private companies, institutions, and non-profit organizations, including the President’s National Infrastructure Advisory Council and Monetary Authority of Singapore’s International Advisory Council. Mr. Berkeley earned his M.B.A. from the Wharton School and a bachelor’s degree from the University of Virginia.
Scott Bradner is the University Technology Security Officer at Harvard University. He has been involved in the design, operation and use of data networks at Harvard University since the early days of the ARPANET. He was involved in the design of the original Harvard data networks, the Longwood Medical Area network (LMAnet) and New England Academic and Research Network (NEARnet). He was founding chair of the technical committees of LMAnet, NEARnet and the Corporation for Research and Enterprise Network (CoREN). Mr. Bradner served in a number of roles in the IETF. He was the co-director of the Operational Requirements Area (1993-1997), IPng Area (1993-1996), Transport Area (1997-2003) and Sub-IP Area (2001-2003). He was a member of the IESG (1993-2003) and was an elected trustee of the Internet Society (1993-1999), where he currently serves as the Secretary to the Board of Trustees. Scott is also a member of the IETF Administrative Support Activity (IASA) as well as a trustee of the IETF Trust. Mr. Bradner is a Senior Technical Consultant in the Office of the Harvard University CTO. He founded the Harvard Network Device Test Lab, is a frequent speaker at technical conferences, a weekly columnist for Network World, and does a bit of independent consulting on the side.

Joel F. Brenner is legal and security consultant at Joel Brenner, LLC. He specializes in cyber and physical security, data protection and privacy, intelligence law, the administration of classified information and facilities, and the regulation of sensitive cross-border transactions. He has represented companies and individuals in a wide variety of transactions and proceedings including sensitive foreign acquisitions involving the Committee on Foreign Investment in the U.S. (CFIUS), the law governing network operations, the liability of foreign governments, export controls, and internal corporate and government investigations. Mr. Brenner was Senior Counsel at the National Security Agency, advising Agency leadership on the public-private effort to create better security for the Internet. From 2006 until mid-2009, he was the head of U.S. counterintelligence under the Director of National Intelligence and was responsible for integrating the counterintelligence activities of the 17 departments and agencies with intelligence authorities, including the FBI and CIA and elements of the Departments of Defense, Energy, and Homeland Security. He holds a JD from the Harvard Law School, a PhD from the London School of Economics, and a BA from the University of Wisconsin – Madison. Mr. Brenner was awarded the Intelligence Community Achievement Medal in July 2009. Mr. Brenner is the author of AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME AND WARFARE (Penguin Press, 2011). Mr. Brenner is admitted to practice in Washington, DC, Virginia, Maryland, and New York.
Fadi Chehadé is the President and CEO of ICANN. His career has been defined by building consensus and promoting collaborative technologies and practices. He has more than 25 years of experience in building and leading progressive Internet enterprises, leveraging relationships with senior executives and government officials across Asia, Europe, the Middle East and the United States. He speaks fluent Arabic, English, French, and Italian. Most recently he served as Chief Executive Officer of Vocado LLC, a U.S. firm that is a provider of cloud-based software for the administration of educational institutions. Prior to Vocado, Chehadé was CEO of CoreObjects Software, Inc., a leader in new product software development services for both large and growing companies. He oversaw the expansion of the company to include more than 400 engineers and its successful acquisition by Symphony Services. Chehadé served as the General Manager of IBM’s Global Technology Services in the Middle East and North Africa. Based in Dubai, he has founded and led three companies since 1987: Viacore, RosettaNet and Nett Information Products.

Kilnam Chon is a Professor at Keio University. He also teaches at KAIST. Chon holds a Ph.D and a M.Sc. in Computer Science from the University of California, Los Angeles and a B.Sc. in Engineering Science from Osaka University. He started working as a System Engineer at Rockwell in the late sixties. From 1976 to 1980, he worked in the Technical Team of Jet Propulsion Laboratory. He then joined ETRI (formerly KIET) as a Principal Investigator. Since 1982, Chon has been teaching at KAIST. In 2008, he taught at the Tsinghua University in Beijing as a Visiting Professor. Since the early 80's, he has been working with network systems and the Internet. He has actively participated in groups like APNG, APAN and APTLD. Currently he Co-chairs the Coordination Committee of Intercontinental Research Networking. He is the developer of the first Internet in Asia, which was called SDN. In 2000, he founded Networking, Inc.

Nazli Choucri is Professor of Political Science at MIT. She works on sources and consequences of international transformations and change, with a focus on propensities for international conflict and imperatives for cooperation. She is the architect and director of the Global System for Sustainable Development (GSSD), a multi-lingual knowledge networking system in Arabic, Chinese, English, and the recent addition of Spanish (http://gssd.mit.edu). She has authored or co-authored ten books and over 130 articles, notably, Cyberpolitics in International Relations, MIT Press (2012). Professor Choucri is Principal Investigator of a multi-year, multi-disciplinary collaborative research project of MIT and Harvard University on Explorations in Cyber International Relations (http://ecir.mit.edu/). In this context, she is drawing on the GSSD experience to design and implement the Cyber System for Strategy and Decision. She is the founding Editor of the MIT
Press Series on *Global Environmental Accord* and the former General Editor of the *International Political Science Reviews*. Professor Choucri has been involved in research or advisory work with national and international agencies, and in diverse countries—notably, Abu Dhabi, Algeria, Canada, Colombia, Egypt, France, Germany, Greece, Honduras, Japan, Kuwait, Mexico, North Yemen, Pakistan, Qatar, Sudan, Switzerland, Syria, Tunisia, and Turkey.

**David D. Clark** is a Senior Research Scientist at MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL). Clark was Chief Protocol Architect of the Internet (1981 – 1989), a chairman of the Computer Science and Telecommunications Board of the National Academies, and is currently co-director of the MIT Communications Futures Program. His current research looks at re-definition of the architectural underpinnings of the Internet and the relation of technology and architecture to economic, societal and policy considerations.

**Melissa Hathaway** is President of Hathaway Global Strategies LLC and a Senior Advisor at Harvard Kennedy School’s Belfer Center. Ms. Hathaway served in the Obama Administration as Acting Senior Director for Cyberspace at the National Security Council and led the Cyberspace Policy Review. During the last two years of the administration of George W. Bush, Ms. Hathaway served as Cyber Coordination Executive and Director of the Joint Interagency Cyber Task Force in the Office of the Director of National Intelligence where she led the development of the Comprehensive National Cybersecurity Initiative (CNCI).

**Charles Iheagwara** is the Director of Cyber security practice of Unatek, Inc. a US government Information Technology contractor located in Bethesda, Maryland. He also serves as a Subject Matter Expert to Grant Thornton, LLP. Previously, he was the CTO of Unatek, Inc., Lead Consultant at KPMG, Lead Consultant at Lockheed Martin and District of Columbia government Computer Emergency Response Coordinator. A Licensed Professional Engineer, Charles received a Master of Science (SM) degree in Management and Engineering from the Massachusetts Institute of Technology (MIT), a Ph.D. in Computer Science from the University of Glamorgan, Wales, M.S degree in Minerals Engineering from the University of Minnesota, a Certificate in Environmental Management from George Washington University, and B.Sc./M.Sc. degrees in Metallurgical Engineering from the National University of Science and Technology, Moscow, Russia. He also attended
Harvard Business School where he completed several MBA courses in satisfaction of the MIT degree requirements.

**Joseph Kelly** is Senior Advisor for Cyber for the Under Secretary of Defense for Intelligence. He has 20 years of experience in the defense industry and first joined the IO Division in 1997 as a contractor. He has been involved with many of the IO division’s central efforts to define and promote IO, such as the development of the 2006 version of DoDD 3600.01 and its subordinate policies, support to the 2000 and 2006 IO program reviews and the implementation of the 2003 IO Roadmap. He has also been intimately involved with the IO division’s work on cyberspace operations and the establishment of U.S. Cyberspace Command. During his 19 years as a contractor, he has supported clients on projects ranging from strategic planning to policy analysis and from critical infrastructure protection to solutions for global communications and identity management. Mr. Kelly holds a Master’s degree from Johns Hopkins University’s School of Advanced International Studies and a bachelor’s degree from Georgetown University.

**Alexander Klimburg** is a Research Fellow with the Science, Technology, and Public Policy Program at the Belfer Center for Science and International Affairs at the Harvard Kennedy School. He has been a senior adviser at the Austrian Institute for International Affairs since 2006 and has acted as an adviser to a number of governments and international organizations on issues within international cyber security, critical infrastructure protection, and internet governance. He has participated in international and intergovernmental discussions within the European Union (EU) and the Organization for Security and Co-operation in Europe, and has been a member of various national, international and EU policy and working groups, as well as track 1/1.5 diplomatic initiatives and technical research groups (including on nation-wide IDS/IPS deployments). He is the principle author of a 2011 European Parliament study, *Cyberpower and Cybersecurity*, the editor of the NATO-funded *National Cybersecurity Framework Manual*, as well as a number of other publications. Previously, Klimburg worked on ICT strategy issues in corporate finance and IT/strategy consulting in Europe and Asia. He holds degrees from the School of Oriental and African Studies and the London School of Economics and Political Science and is a D.Phil. candidate at the University of Vienna.

**Tomas Lamanauskas** heads the Corporate Strategy Division at the International Telecommunication Union (ITU). His extensive ICT policy and regulatory experience includes positions of Deputy General Director, Board Member and CEO of telecommunications regulators in the Caribbean, Middle East and Europe. He also acted as Government Advisor on ICT policies in the Pacific. Tomas Lamanauskas has master’s degrees in Public Administration (Harvard University), Law (Vilnius University) and
Telecommunications Regulation and Policy (the University of the West Indies). He has delivered more than 70 presentations, published 18 articles (papers) and co-authored 3 books in the field of ICT. He is also a member of the Editorial Board of the “Telecommunications Policy” journal.

Xing Li is currently a Professor in the Electronic Engineering Department at Tsinghua University, Beijing, China. His research activities and interests include statistical signal processing, multimedia communication and computer networks. He has published more than 120 papers in his research areas. Since 1993, Dr. Li became one of the pioneers of the China Education and Research Network (CERNET, http://www.edu.cn) and is chief architect. He is a member of Technical Board of the China Education and Research Network Project and deputy director of China Education and Research Network (CERNET) Center. He set up the first IP v6 network in China and has been very active for the Internet development in Asia Pacific region and participating in APNG, APIA, APRICOT and APAN since 1994. He has been serving in the executive council of APNIC since 1996 and is currently a member of IAB. Xing Li received his B. S. degree in radio electronics from Tsinghua University, China in 1982, and his M. S. and Ph. D. degrees in electrical engineering from Drexel University, USA in 1985 and 1989, respectively.

Herbert S. Lin is Chief Scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy, a 1991 study on the future of computer science, a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence, a 2000 study on workforce issues in high-technology, a 2002 study on protecting kids from Internet pornography and sexual exploitation, a 2004 study on aspects of the FBI's information technology modernization program, a 2005 study on electronic voting, a 2005 study on computational biology, a 2007 study on privacy and information technology, a 2007 study on cybersecurity research, a 2009 study on healthcare informatics, a 2009 study on offensive information warfare, and a 2010 study on cyber deterrence.

Urs Luterbacher is Honorary Professor, International Relations/Political Science at the Graduate Institute, Geneva. He was Professor of Political Science at the Graduate Institute of International from 1973-2010. He has done work on problems of international conflict and cooperation and international environmental problems using formal models and game
Stuart Madnick has been an MIT faculty member since 1972. He served as the head of MIT’s Information Technologies Group in the Sloan School of Management for more than twenty years. Dr. Madnick is the author or co-author of over 250 books, articles, or reports including the classic textbook on Operating Systems. His current research interests include information integration technologies, semantic connectivity among disparate distributed information systems, database technology, software project management, internet applications, and the strategic use of information technology.

Tim Maurer is a Policy Analyst focusing on Internet policy and international affairs at the New America Foundation’s Open Technology Institute including cyber-security, human rights policy, and Internet governance. Tim’s research has been published by Harvard University, Foreign Policy, and Slate among others. In October 2013, he spoke at the United Nations and has been an expert to the Organization for Security and Cooperation in Europe. He speaks frequently at national and international conferences and has been featured by print, radio, and television media including the Kojo Nnamdi show, PRI’s The World, Greek Public Television, the LA Times, the Russian Kommersant, the German Die Zeit and other media outlets. He conducts his academic research as a non-resident research fellow at the Citizen Lab. Prior to joining New America, Tim was part of the Technology and Public Policy Program at the Center for Strategic and International Studies where he wrote a study analyzing the institutional structures of critical infrastructure protection in the U.S. and international cyber-security. Tim holds a Master in Public Policy concentrating on international and global affairs from the Harvard Kennedy School. His thesis was a research project on transnational organized crime conducted for the White House National Security Council. He received his B.A. in political science from the Freie Universität Berlin.

Katie Moussouris is the Senior Security Strategist Lead at Microsoft. Her team’s work encompasses industry-leading programs such as Microsoft’s Bounty programs (www.microsoft.com/bountyprograms), the BlueHat conference, security researcher outreach and Microsoft’s Vulnerability Disclosure Policies. Moussouris also founded Microsoft Vulnerability Research, which is responsible for Microsoft’s research and reporting of vulnerabilities in 3rd party software. She was the editor of a new ISO standard.
on Vulnerability Handling Processes, following her work over the past 5 years as the lead expert in the U.S. National Body on an ISO draft standard on Vulnerability Disclosure.

Milton L. Mueller is Professor at the Syracuse University School of Information Studies. His research and teaching explore the political economy of communication and information. For the past 15 years his research, teaching and public service have concentrated on problems related to global Internet governance. His books Networks and States: The global politics of Internet governance (MIT Press, 2010) and Ruling the Root: Internet Governance and the Taming of Cyberspace (MIT Press, 2002) are acclaimed scholarly accounts of the global governance regime emerging around the Internet. His commentary and analysis of current events can be found on the Internet Governance Project blog.

Venkatesh “Venky” Narayanamurti is the Director of the Science, Technology and Public Policy Program at the Belfer Center for Science and International Affairs at the Harvard Kennedy School (HKS). He is also the Benjamin Peirce Professor of Technology and Public Policy and a Professor of Physics at Harvard. He was formerly the John L. Armstrong Professor and Dean of the School of Engineering and Applied Sciences and Dean of Physical Sciences at Harvard. Previously he served as the Richard A. Auhll Professor and Dean of Engineering at the University of California at Santa Barbara. Prior to that he was Vice President of Research at Sandia National Laboratories and Director of Solid State Electronics Research at Bell Labs. He obtained his PhD in Physics from Cornell University and has an Honorary Doctorate from Tohoku University. He is an elected member of the American Academy of Arts and Sciences, the National Academy of Engineering and the Royal Swedish Academy of Engineering Sciences, and a Fellow of the American Physical Society, the American Association for the Advancement of Science, the IEEE, and the Indian Academy of Sciences. He is the author of more than 200 scientific papers in different areas of condensed matter and applied physics.

Gregory Rattray is a founding partner at Delta Risk LLC. During his 23 year Air Force career, he served as the director for cyber security on the National Security Council staff in the White House where he was a key contributor to the President’s National Strategy to Secure Cyberspace, helped initiate the first national cyber security exercise program involving government and the private sector, and served as a senior security advisor on foreign investments for the US government regarding corporate acquisitions and outsourcing concerns in the telecommunications and information technology sector. Dr. Rattray also commanded the Operations Group of the AF Information Warfare Center. In this role, he was responsible for collaboration with defense industrial base partners related to advanced persistent cyber threats. He also served from 2007-2010 as the chief security advisor to Internet Corporation for Assigned Names and Numbers (ICANN) establishing strategies for ICANN’s role in enhancing security and resiliency of the domain name system. He was the driving force in the establishment of the Cyber Conflict Studies Association (CCSA) to ensure US national efforts were guided by a deeper well of intellectual capital involving private industry, think tanks, government, and academia. He received his Bachelor’s Degree in Political Science and Military History from the U.S. Air Force Academy; a Master of Public Policy from the John F. Kennedy School of Government, Harvard University; and his Doctor of Philosophy in International Affairs from the Fletcher School of Law and Diplomacy, Tufts University. He is the author of Strategic Warfare in Cyberspace.

Michael Sechrist is Vice President for Corporate Information Security at State Street Corporation. He was the former project manager of ECIR at the Belfer Center's Science, Technology, and Public Policy Program. Mr. Sechrist is an expert on undersea communication cable security policies and economic models and is the author of "Cyberspace in Deep Water: Protecting Undersea Communications Cables", a policy paper presented to the Department of Homeland Security in spring 2010. He has presented these findings to the Pacific Telecommunications Council and the International Cable Protection Committee (ICPC) and has helped the ICPC develop the first international public-private partnership to protect undersea cables.

Before coming to CFR, Dr. Segal was an arms control analyst for the China Project at the Union of Concerned Scientists. There, he wrote about missile defense, nuclear weapons, and Asian security issues. He has been a visiting scholar at the Massachusetts Institute of Technology's Center for International Studies, the Shanghai Academy of Social Sciences, and Tsinghua University in Beijing. He has taught at Vassar College and Columbia University. Dr. Segal is the author of *Digital Dragon: High-Technology Enterprises in China* (Cornell University Press, 2003), as well as several articles and book chapters on Chinese technology policy. His work has appeared in the *Financial Times, The Economist, Foreign Policy, The Wall Street Journal*, and *Foreign Affairs*, among others. Dr. Segal has a BA and PhD in government from Cornell University, and an MA in international relations from the Fletcher School of Law and Diplomacy, Tufts University.

**Michael Siegel** is a Principal Research Scientist at the MIT Sloan School of Management. He is currently the Director of the Interdependence of Security and the Extended Enterprise (I-SEE) Special Interest Group at the MIT Center for Digital Business and Co-Director of the PROductivity from Information Technology (PROFIT) Project. Dr. Siegel’s research interests include the use of information technology in financial risk management and global financial systems, applications of computation social science to analyzing state stability, eBusiness and financial services, global eBusiness opportunities, financial account aggregation, ROI analysis for online financial applications, heterogeneous database systems, managing data semantics, query optimization, intelligent database systems, and learning in database systems.

**Jesse Sowell** is PhD Candidate in the Engineering Systems Division of the Advanced Network Architecture Group of the Computer Science and Artificial Intelligence Laboratory at MIT. He is investigating Internet jurisdiction conflicts and the ongoing changes in power relationships among online and offline stakeholders. He is interested in understanding the types of rules and collaborative stakeholder relationships that reduce Internet jurisdiction conflicts and the role of intentional architectural design that facilitates multistakeholder collaboration.

**Lynn St. Amour** is President/CEO of the Internet Society (ISOC). She joined ISOC in 1998 as Executive Director of its Europe, Middle East, and Africa (EMEA) division, and has been responsible for ISOC’s international expansion. She became ISOC’s global Executive Director and COO in 1999 and held that position until her appointment as President and CEO in February of 2001. St. Amour’s background includes positions at the highest levels in
international sales and marketing, strategic planning, partner management and manufacturing. Prior to joining ISOC, she was director of Business Development and Joint Venture Operations for AT&T’s Europe, Middle East and Africa division. She led the negotiation and development of several telecommunications joint ventures with leading European companies. She was responsible for managing the AT&T Unisource Communications Services joint venture - an alliance between AT&T, and the Swiss, Swedish and Dutch PTT’s - to ensure alignment of strategic goals and achievement of operating targets. A graduate of the University of Vermont, St. Amour began her career in information technology with the General Electric Corporation.

**Michael Sulmeyer** was a predoctoral fellow and Honors Seminar TA at CISAC for 2010-2011. He is a law student at Stanford Law School where he co-chairs the Stanford National Security Law Society and is a member of the Afghanistan Legal Education Project. He is also completing a DPhil in Politics for Oxford University about the termination of major weapons systems. As a Marshall Scholar, he received his Masters in War Studies with Distinction from King’s College, London in 2005. From 2003-2004, Michael served as Special Assistant to the Principal Deputy Under Secretary of Defense for Policy. Before that, he was a Research Assistant at the Center for Strategic and International Studies.

**Brandon Valeriano** (Ph.D. Vanderbilt University) is a Lecturer at the University of Glasgow in the School of Social and Political Sciences (also in the area of Global Security). Dr. Valeriano’s main research interests include investigations of the causes of conflict and peace in the international system, as well as the study race/ethnicity from the international perspective. He has published over two dozen articles and book chapters in such outlets as the *Journal of Politics, International Studies Quarterly, International Interactions, Third World Quarterly, and Foreign Affairs*. He has just completed a book on the origins of rivalry (*Becoming Rivals*, Routledge 2013) and a book on *Hollywood’s Representations of the Sino-Tibetan Conflict* (Palgrave, 2012).

**Jody R. Westby** provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, cybercrime, breach management, and IT governance. She also serves as Adjunct Professor to the Georgia Institute of Technology’s School of Computer Science and is Adjunct Distinguished Fellow to Carnegie Mellon CyLab. Ms. Westby is a member of the bars of the District of Columbia, Pennsylvania, and Colorado and serves as chair of the American Bar Association’s Privacy and Computer Crime Committee. She co-chairs the World Federation of Scientists’ (WFS) Permanent Monitoring
Panel on Information Security and served on the ITU Secretary-General’s High Level Experts Group on Cybersecurity. Ms. Westby led the development of *the International Toolkit on Cybercrime Legislation* and is an editor and co-author of the 2010 WFS-ITU publication, *The Quest for Cyber Peace*. Ms. Westby is co-author and editor of four books on privacy, security, cybercrime, and enterprise security programs and author of two books on legal issues associated with cybersecurity research. Ms. Westby practiced law at Shearman & Sterling and Paul, Weiss, Rifkind, Wharton & Garrison. B.A., summa cum laude, University of Tulsa; J.D., magna cum laude, Georgetown University Law Center; Order of the Coif.
PARTICIPANTS

Gaurav Agarwal
Supply Chain Consultant
Bayer A.G.; MIT Affiliate

Bruce Bakis
Principal Scientist
MITRE Corporation

Samiah E. Baroni
Department Chair
Information Operations and Cyber and
Geostrategic Resource Intelligence
Concentrations
National Intelligence University

Joel Brenner
Legal and Security Consultant
Joel Brenner, LLC

Richard Bejtlich
Chief Security Officer
Mandiant

Elena Belinkaia
Software Engineer

Alfred Berkeley
Chairman, Princeton Capitol Management, Inc. Lead, Cyber Effort, Business Executives for National Security (BENS)

Bob Boynton
Professor, New Media & Politics
University of Iowa

Scott Bradner
University Technology Officer
Harvard University

Lt. Col. Jon Brickley
Army Cyber Command Fellow, West Point

Dragos Calitoiu
Adjunct Professor, School of Mathematics and Statistics, Carelton University

José Campos
Director
Microsoft Corporation

Fadi Chehadé
President and CEO
ICANN

Sinead Cheung
Student
Wellesley College

Kilnam Chon
Professor of Computer Science
Korea Advanced Institute of Science and Technology (KAIST)
Professor
Keio University

Nazli Choucri
Professor of Political Science
Associate Director, Technology and Development Program
Principal Investigator, Explorations in Cyber International Relations (ECIR)
Massachusetts Institute of Technology

David D. Clark
Senior Research Scientist
Computer Science and Artificial Intelligence Laboratory (CSAIL)
Massachusetts Institute of Technology

3/6/2014
Colin Connor  
Military Fellow  
Security Studies Program  
Massachusetts Institute of Technology

Curt Dalton  
Vice President  
Chief Information Security Officer  
Sapient

Danilo Delia  
Ph.D. Candidate  
Chiare Castex de CyberStratégie

Joseph DeMarco  
Partner, DeVore & Demarco, LLP

Chris Demchak  
Professor  
Strategic Research Department  
U.S. Naval War College

Alix Desforges  
Ph.D. Candidate  
French Insitute of Geopolitics  
University of Paris  
Researcher  
Chiare Castex de CyberStratégie

Dina El-Damak  
Ph.D. Candidate  
Electrical Engineering and Computer Science  
Massachusetts Institute of Technology

Ryan Ellis  
Postdoctoral Research Fellow  
Science, Technology, and Public Policy Program/Project on Technology, Security, and Conflict in the Cyber Age  
Harvard Kennedy School

Wafik Farag  
Private Consultant

Erin Fitzgerald  
Director  
Minerva Research Initiative  
Basic Research Office  
Office of the Assistant Secretary of Defense for Research and Engineering

Alexander Gamero-Garrido  
Research Assistant  
Explorations in Cyber International Relations (ECIR)  
Massachusetts Institute of Technology

Dan Geer  
Security Researcher and Columnist  
In-Q-Tel

Scott Gerber  
Graduate Student of Political Science  
Johns Hopkins University  
Fellow  
Army’s Strategic Plans and Policy Program

Michael Glennon  
Professor of International Law  
Fletcher School, Tufts University

Daniel Goldsmith  
Director, Business Development  
Eduventures

Karl Grindal  
Associate  
Delta Risk LLC

John Hagen  
Assistant Professor of International Relations  
West Point

Major Scott Handler  
Executive Officer  
782nd Military Intelligence (Cyber) Battalion  
United States Army
Melissa Hathaway
President
Hathaway Global Strategies, LLC
Senior Advisor
Belfer Center for Science and
International Affairs, Harvard Kennedy
School

Jonah Hill
Consultant
Monitor 360

John Hoag
Associate Professor
McClure School of Information and
Telecommunication Systems
Ohio University; Adjunct, Visiting
Associate Professor, Electrical
Engineering and Computer Science
Case Western Reserve University

David Hoffmaster
Lead, Cyber Support Team
782nd Military Intelligence (Cyber)
Battalion
United States Army

James Houghton
Research Associate
Sloan School of Management
Massachusetts Institute of Technology

Cerintha Jai Yi Hui
Student, Chemical Engineering
Massachusetts Institute of Technology

Charles Iheagwara
Managing Director
Unatek, Inc.
Founder and CEO
IntrusionOnline Corporation

Lucas Kello
Postdoctoral Research Fellow
International Security Program/Science,
Technology, and Public Policy
Program/Project on Technology, Security,
and Conflict in the Cyber Age
Harvard Kennedy School

Joseph Kelly
Senior Advisor for Cyber
Office of the Under Secretary of Defense
U.S. Department of Defense

Alexander Klimburg
Senior Advisor
Austrian Institute of International Affairs
Fellow, Harvard Kennedy School

Tomas Lamanauskas
Head, Corporate Strategy Division
International Telecommunication Union
(ITU)

Kwan Lee
Industrial Liaison Program
Massachusetts Institute of Technology

Xing Li
Professor, Electronic Engineering
Tsinghua University, Beijing, China
Deputy Director
China Education and Research Network
Center (CERNET)

Herbert S. Lin
Chief Scientist
Computer Science and
Telecommunications Board, National
Research Council of the National
Academies
Igor Linkov
Risk and Decision Science Focus Area
Lead, US Army Corps of Engineers
Adjunct Professor of Engineering and
Public Policy, Carnegie Mellon University

Cory Lofdahl
Senior Scientist
Charles River Analytics

Urs Luterbacher
Emeritus Professor of Political Science
Graduate Institute of International and
Developmental Studies, Geneva, Switzerland

Eric Markowsky
Industrial Liaison Program
Massachusetts Institute of Technology

Renee Marlin-Bennett
Professor of Political Science
Johns Hopkins University

Tim Maurer
Policy Analyst
Open Technology Institute
The New America Foundation

Marco Mayer
Adjunct Professor
University of Florence, Italy

Bruce McConnell
Senior Vice President
EastWest Institute

Michael Siegel
Principal Research Scientist
Sloan School of Management
Massachusetts Institute of Technology

Andrew Miller
Ph.D Candidate, Political Science
Massachusetts Institute of Technology

Stuart Miniman
Researcher and Analyst
Wikibon

Vivek Mohan
Associate, Sidney Austin LLP
Associate, Belfer Center for Science and International Affairs
Harvard Kennedy School

Mark Morrison
Senior Vice President
Chief Information Security Officer
State Street Corporation

Allen Moulton
Research Scientist
Sociotechnical Systems Research Center (SSRC)
Massachusetts Institute of Technology

Katie Moussouris
Senior Security Strategist Lead
Microsoft

Milton Mueller
Professor
School of Information Studies
Syracuse University

Venkatesh “Venky” Narayananamurti
Benjamin Peirce Professor of Technology and Public Policy and Professor of Physics
Harvard University, Co-Principal Investigator Explorations in Cyber International Relations (ECIR), Harvard Kennedy School

Joseph S. Nye, Jr.
Harvard University Distinguished Service Professor, Kennedy School of Government

David O’Brien
Project Manager and Researcher,
Berkman Center for Internet & Society
Harvard University
William Parsons
Maximal Image

Denise Peake
Chief, Community Leadership Office
Information Assurance Directorate
National Security Agency
U.S. Department of Defense

Mina Rady
Consultant
Global System for Sustainable
Development and Cyber System for
Strategy and Decision (GSSD)
Massachusetts Institute of Technology

Greg Rattray
CEO and Founding Partner
Delta Risk, LLC

Chip Register
Executive Vice President
Sapient Corporation
Managing Director
Sapient Global Market

Fabio Rugge
Diplomat
Italian Ministry of Foreign Affairs

David Saul
Senior Vice President; Chief Scientist
State Street Corporation

Michael Sechrist
Vice President
Threat and Vulnerability Management
Corporate Information Security Office
State Street Corporation

Adam Segal
Maurice R Greenberg Senior Fellow in
China Studies
Director, Program on Digital and
Cyberspace Policy

Charles Sennott
Editor-at-large; Co-founder
Global Post

Enrique Shadah
Senior Industrial Liasion Officer
Office of Corporate Relations Industrial
Liasion Program
Massachusetts Institute of Technology

Michael Siegel
Principal Research Scientist
Sloan School of Management
Massachusetts Institute of Technology

Jesse Sowell
Ph.D. Candidate
Engineering Systems Division (ESD)
Massachusetts Institute of Technology

Michael Specter
Graduate Student
Technology and Policy Program
Massachusetts Institute of Technology

Lynn St. Amour
President & Chief Executive Officer
Internet Society

Amr Suleiman
Ph.D. Candidate
Electrical Engineering & Computer
Science
Massachusetts Institute of Technology

Michael Sulmeyer
Senior Policy Advisor for Cyber Policy
U.S. Department of Defense

Theresa Swineheart
Senior Advisor to the President on
Strategy
ICANN
Keng Meng Tan
SM Candidate
Department of Political Science
Massachusetts Institute of Technology

Cecilia Testart
SM Candidate
Technology and Policy Program
Massachusetts Institute of Technology

Nevine Tewfik
Head of the Research, Studies and Policies Bureau
International Relations Division
Ministry of Communications and Information Technology (MCIT)

Connie Uthoff
Assistant Director
Masters of Strategic Cyber Operations and Information Technology Management Program
George Washington University

Brandon Valeriano
Senior Lecturer
Department of Politics and Global Security
University of Glasgow

Mitzi Wertheim
Professor of Practice for Sustainability Enterprises & Social Networks
Cebrowski Institute
Naval Postgraduate School

Jody R. Westby
CEO and Founder
Global Cyber Risk, LLC

Steve Whittaker
Chief Researcher
BT Exact Technologies Research Affiliate
MIT Media Laboratory

Josephine Wolff
Ph.D. Candidate
Engineering Systems Division
Massachusetts Institute of Technology

Dorothy Zinberg
Lecturer in Public Policy and Faculty Associate
Belfer Center for Science and International Affairs
Harvard Kennedy School of Government
ECIR PUBLICATIONS*

*This list includes almost all of the materials published or in preparation by the ECIR Team. It is updated periodically to include recent materials. At this point it is not necessarily all-inclusive.

ECIR PUBLICATIONS

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

2009-2013

ORGANIZED as FOLLOWS:

I. BOOKS

II. PUBLISHED ARTICLES and CHAPTERS

III. WORKING PAPERS and REPORTS on ECIR WEBSITE or SSRN

IV. PROCEEDINGS of CONFERENCES and WORKSHOPS
I. BOOKS


*In Preparation*


II. PUBLISHED ARTICLES and CHAPTERS


• Li, Xitong, Yushun Fan, Stuart Madnick, Quan Z. Sheng. 2010. A Pattern-based Approach to Protocol Mediation for Web Services Composition. *Information and Software Technology* 52 (3), 304–323z.


III. WORKING PAPERS and REPORTS on ECIR WEBSITE or SSRN


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


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


• Sowell, Jesse H. “A View of Top-Down Governance.” Paper presented to NANOG 55, Vancouver BC, June 4, 2012; Global Peering Forum (GPF7.0), New Orleans, LA, March

3/6/2014


### IV. PROCEEDINGS of CONFERENCES and WORKSHOPS


