ECIR WORKSHOP ON

Who Controls Cyberspace?

Co-Sponsored by

Council on Foreign Relations

November 6 and 7, 2012
MIT Faculty Club &
MIT Media Laboratory

Workshop Report

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, views or conclusions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.
TABLE OF CONTENTS

FRAMING SESSIONS

FRAMING SESSION I
THE CHALLENGE, THE DILEMMAS AND THE AGENDA
Nazli Choucri, Professor of Political Science, MIT

FRAMING SESSION II
POWER IN CYBERSPACE – TODAY AND IN THE FUTURE
Joseph S. Nye, Jr., University Distinguished Service Professor, Harvard Kennedy School

FRAMING SESSION III
CONTROL OF THE INTERNET – THE CORE OF CYBERSPACE
David D. Clark, Senior Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT

PANEL SESSIONS

PANEL I
CONNECTIVITY, NETWORKS, AND INTERNET SERVICE PROVIDERS

David D. Clark, Chair
Senior Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT

Steve Whittaker, Principal Consultant, British Telecom; Research Affiliate, MIT Media Lab
Michael M. Afergan, Senior Vice President & General Manager, Site Division, Akamai
Barry Tishgart, Vice President, Network Services, Comcast Cable
INTERACTIVE PANEL
BARRIERS TO CONTROL: CERTAINTIES AND UNCERTAIN TIES

Herbert S. Lin, Chair
Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies

PANEL IIa
LOSING CONTROL IN CYBERSPACE

C. Lawrence Meador, Chair
Chairman, MGI Strategic Solutions

Dan Schutzer, President, Financial Services Technology Consortium, Financial Services Roundtable
Kevin O’Connell, President and CEO, Innovative Analytics and Training
David R. Martinez, Head of the Intelligence, Surveillance and Reconnaissance Systems and Technology Division, MIT Lincoln Laboratory

PANEL IIb
RESEARCH DIRECTIONS AND POLICY IMPERATIVES

Zachary Tumin, Chair
Special Assistant to the Director and Faculty Chair, Science, Technology, and Public Policy Program, Harvard Kennedy School

Lucas Kello, Research Fellow, Belfer Center for Science and International Affairs, Harvard Kennedy School
Vivek Mohan, Research Fellow, Belfer Center for Science and International Affairs, Harvard Kennedy School
Aadya Shukla, Research Fellow, Belfer Center for Science and International Affairs, Harvard Kennedy School
Shirley Hung, Postdoctoral Associate, Computer Science and Artificial Intelligence Laboratory, MIT
PANEL III
INFORMATION, DATA AND CONTENT

Joel Brenner, Chair
Of Counsel, Cooley LLP

Alan Davidson, Visiting Scholar, Engineering Systems Division, MIT; Former Director of Public Policy, Google
Jody R. Westby, CEO and Founder, Global Cyber Risk LLC
Ethan Zuckerman, Director, Center for Civic Media, MIT Media Lab
Howard Schrobe, Program Manager, Information Innovation Office, DARPA; Principal Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT

PANEL IV
GOVERNANCE, MANAGEMENT AND REGULATION

Melissa Hathaway, Chair
President, Hathaway Global Strategies LLC

Roger Hurwitz, Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT
Urs Luterbacher, Emeritus Professor, Institut universitaire de hautes études internationales, Geneva
Joseph Kelly, Chief of Cyber Intelligence, Office of the Under Secretary, U.S. Department of Defense

PANEL V
ALTERNATIVE FUTURES AND EMERGING CHALLENGES

Stuart Madnick, John Norris Maguire Professor of Information Technology, Sloan School of Management, MIT
Nazli Choucri, Professor of Political Science, Political Science Department, MIT

POSTER SESSION
List of Posters
Individual Posters (following the list)

PARTICIPANTS
Welcome to the Third Workshop of the Joint MIT-Harvard Project on Explorations in Cyber International Relations, sponsored by the U.S. Department of Defense Minerva Program. The question we shall examine – Who Controls Cyberspace? – appears to be simple, but it is challenge overall, with considerable complexity in scale and scope. We shall focus on international politics as our major area of concern. This framing session seeks to place the question in a context of power politics inherited from the 20th century, but focuses largely on the impacts created by the coupling of cyberspace and international politics.

Today the dual domains of interactions – cyber and physical – have become highly interactive and we can no longer treat them as distinctive or mutually exclusive “spaces.” In the vision of a Venn diagram, the intersections dominate the individual areas. At the same time, however, each domain has its distinctive properties that complicate efforts to examine them jointly.

This Introduction highlights some critical framing questions. First we “unbundle” the nature of the challenge. Consider these as something of a “checklist” of framing questions as we work our way through the agenda.

The Challenge

- **Why Control?**
  If control is important for theory, policy and planning purposes, are control and power identical? Is control driven by a question for efficiency? Security? Other?
- **How to control?**
  What are the instruments used, by whom, when and how?
○ *What to control?*
  This pertains to the target of control. Do we consider control of cyber-based infrastructure or the entire communication systems? What about jurisdiction?

○ *When to control?*
  Under what conditions do we actually want to control cyberspace? When there are threats to national security? When the pursuit of competitive advantage dictates? When international peace and stability is at stake? Other?

Of the many questions not covered above, one of the most important is the normative one, namely, *Who should control?* But even that question cannot be addressed without reference to *Who can control?* Which leaves us with yet another consideration: Are the normative issues considered devoid of pragmatic considerations?

Turning to the clear, persistent, and vexing dilemma:

**The Dilemma**

The dilemma is this: The increased complexity of international systems is greater than our ability to fully understand the implications of the changes, in addition to the “normal” problems in world politics.

Added uncertainties and new insecurities in international relations are due to characteristics, contentions, and configurations within, across, and surrounding cyberspace. All of this tends to obscure changes in power relations, intents of actors, relative capabilities and the like. In this framing session, we consider only the most obvious changes in the parameters of cyberspace. Four such parameters are important dimensions of the dilemma.

**New Cyber Dynamics and Cyber Demography**

○ Increased mobile-cellular subscription throughout the globe
  ● Developing world dominates pie chart of cellular signals

○ Growth of individual users

○ New bi-polarity?
  ● Internet users by country – primarily in U.S. and China
  ● Brazil, however, is a point of interest

○ Distribution of language on the Internet, change between 2000-2010
  ● English dominates but is not the only game in town

**New Asymmetries**

Missing is reference to the role of the state in normal discourse. With diversification comes the gap in the ease with which we can track what is going on.
New Activities and Threats to Security

In the past, we could divide activities into commercial or relating to national security. Now such categories are more obscured. Note, for example:

- Motivations for denial of service vary
- Patterns of intrusion differ
- Physical networks are vulnerable
- Undersea cables may provide new vulnerabilities
- Undersea cables as vulnerabilities?
- Alexandria incident: accident/other?

New Densities in Decision Spaces

If we exclude all entities and agencies involved in the actual working of the Internet and the operations essential for managing cyberspace, we can isolate the significant expansion in new actors, arenas, and instruments. For example, we see growth both in state and non-state actors. The growth in the number of states means diversity in the autonomous pursuit of interests. Then there are three key international institutions bearing on information matters – ICANN, ITU, and WTO – in addition to UN development agencies and private sector international cyber management organizations. To this must be added the non-state institutions and private entities such as Chambers of Commerce, businesses, NGOs, private sector standardization, regulatory practitioners, and civil society.

This simple “accounting” yields one important inference: the “space” becomes very crowded. If we consider all these factors individually or collectively, do they result in complicating, diversifying, or leveling of the playing field?

The Agenda

We now turn to the Agenda. But before doing that, let us focus for a moment on “cyberspace.” Cyberspace is a domain of human interaction. With the Internet as its core – constructed through the interconnection of millions of computers with standard setters and institutional managers – cyberspace is characterized by the interplay of a wide range of actors driven by an even larger range of incentives. The Agenda is informed by this new “reality.”

This Workshop is anchored in three Framing Sessions. These consist of a review of (a) the overall context, as an introduction, (b) the salience of power, as a central feature of the new reality, and (c) the presentation of control point analysis, an important anchor for ECIR as a whole.

The Framing Sessions are followed by organized Panels. The first Panel is on connectivity, networks and Internet Service Providers. The next is an interactive exchange with the
participants, focusing on barriers to control given the certain and the uncertain elements. Then come the two concurrent Panels. One is on research directions and policy imperatives, and the other on losing control in cyberspace. The third panel discusses information, data, and content while panel four focuses on governance, management and regulation. The final Panel Session signals alternative futures and emerging challenges.
Introduction – The Challenge, The Dilemmas and The Agenda
Nazli Choucri
Professor of Political Science, Political Science Department, MIT

ECIR Workshop on Who Controls Cyberspace?
Co-sponsored by the Council on Foreign Relations

Framing Session: Context The Challenge, the Dilemma & the Agenda
Nazli Choucri
Massachusetts Institute of Technology ECIR Principal Investigator
November 6-7, 2012

THE CONTEXT
New International Realities of the 21st Century
- Increased coupling of “real” and cyber domains
- New vulnerabilities & challenges to national security
- Powerful asymmetries in kinetic & cyber domains
- Wide range of new cyber-centered actors
- Increased complexity of cyber management
- Growth in scale and scope of cyber-conflicts
- Evolving cyber-cooperation and collaboration
- Growth in “hybrid” policies & responses

Jointly these create new imperatives for policy

Aspects of Complexity
Why control?
- Enhance efficiency
- Provide security
- Guarantee autonomy
- Maximize profits
- Maintain order
- Other?

What to control?
- Infrastructure construction
- Security of infrastructure
- Communication itself
- Content of communication
- Flow across jurisdiction
- Clearing exchange point?

How to control?
- Technical, institutional tools
- Regulatory mechanisms
- Unilateral approach
- Coordination strategies

When to Control
- Standards of operation
- Threats to national security
- Avoid global cyber instability
- Other? Never?

I. THE CHALLENGE
Capture the Complexities of Control

Are these matters of technology?
or network connections?
or regulation-in-place?
or politics, or power?
or international relations?

All, or none, of the above?

Framing Issues for Who Controls Cyberspace?
I. The Challenge: The Complexity of Control Many Facets – Many Interests

II. The Dilemma: Dynamics Shifts in Cyberspace & Crowding in Decision Domains

III. The Agenda: Diversity of Perspectives with Convergence & Divergence

Who Should Control?
Is this question relevant?
- Is it normative or pragmatic?
- What are the contentions?
- What are the necessities?
- How should it be addressed?
- How will it be addressed?

Why do we raise it here?
II. THE DILEMMA

Increase complexity of the international system is greater than our ability to fully understand the implications of the changes.

Major uncertainties and new insecurities in international relations are due to changes in cyberspace.

These changes obscure who counts politically, who is counted, and all aspect of control.

Dimensions of the Dilemma

New Cyber Dynamics & Demography
Changing user distributions
Language diversity

New Activities & Threats to Security
Shaping new power
Unexpected challenges to the state

New Density in Decision Spaces
New actors, arenas, instruments
Complicating or Leveling the Playing field?

Expansion of Mobile Cellular Signals
Percentage of the world’s population covered by a mobile cellular signal, 2011 compared to 2010

Expansion of Users
Global numbers of individuals using the Internet, total and per 100 inhabitants, 2001-2011

A New Bi-Polarity?
Internet User stats worldwide 2010

Internet users by country

USA
227m
74.7%
Internet users

China
298m
22.4%
Percentage of population

Japan
94m
72.5%

Brazil
68m
71%

Density in Decision Domain

Crowded decision-making:
- Technical Operators of Networks
- Traditional International Institutions
- New Cyber-focused institutions
- Informal Institutions & Entities
- Non-State Actors & Associations
- Many others

To Illustrate Density of Decision
For subset of cyber actors

Three Key International Institutions

<table>
<thead>
<tr>
<th>Development Assistance</th>
<th>Policy Coordination</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>WTO</td>
<td>ITU</td>
<td>ICANN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Law and Regulations</th>
<th>Scope of International ICT Decision Making</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrow</td>
<td>Bred.</td>
</tr>
<tr>
<td></td>
<td>Results of International ICT Decision Making</td>
</tr>
</tbody>
</table>
UN Development Agencies and Private Sector
International Cyber Management Organizations

Non-State Institutions and Private Entities

III. THE AGENDA

Framing Sessions
- Context
- Power
- Control Point Analysis

Panels on:
- Connectivity – Internet, Networks, ISP’s
- Content – Conflicts on information, data, materials
- Losing Control of Cyberspace – another set of issues
- Research Directions and Policy Imperatives
- Governance, Regulations and Management

The Integrative Session
- Alternative Futures & Emerging Challenges

THE END

Thank you
The information revolution is leading to a diffusion of power but it is not the first information revolution in human history, e.g., the invention of the printing press. The effect of the invention of the printing press was far reaching. Printing the Bible, with its wider accessibility led to the Protestant Reformation, the 30 Years’ War, the Westphalian peace, and the 1684 Westphalian concept of the sovereign state. The revolution played out in ways no one expected.

This current information revolution can date back to the 1960s – the beginning of Moore’s Law. This led to a reduction of costs and barriers to empower non-state actors while big states continue to control large amounts of resources enabling different capabilities, e.g., Stuxnet. When you empower state actors, everything is not suddenly equal. Instead of seeing the nation-state as obsolete, it crowds the stage in which the state operates. States as such, are not losing power but the stage on which they operate has become a lot more crowded.

Power Defined

Power is the ability to achieve a desired outcome; to get others to do what you want. This can be accomplished in three ways: (a) Threats and coercion – hard power, (b) Payments – hard power, and (c) Attraction and persuasion – soft power. Power resources must be distinguished from power behavior. In the cyber domain, we distinguish between: (a) the physical layer, where resources are scarce and costly, and where control of the physical layer can have both territorial and extraterritorial control over the virtual layer, and (b) the virtual layer, where economic network characteristics and political practices make jurisdiction control difficult but can affect the physical layers.

Cyber-based resources are much more limited but include anonymity, ease of entry and exit, etc. Generally, non-state actors have asymmetrical vulnerabilities compared to governments. As we assess the relative power resources, you can total the power resources of governments and companies and it will look as though the governments are ahead. However, individuals and lightly structured networks have less vulnerability.
We need to think of power as asymmetrical vulnerabilities in dependency of a relationship. On balance, the current trend is toward the reemergence of the Westphalian system in cyberspace (see article by Chris Demchak in *Strategic Studies Quarterly*). China’s control over the Internet is more nuanced than simply the Great Firewall, which is only one of three layers of control. It also includes self-censorship by companies active in China due to the passive threat of license of revocation and traditional police power. China is changing in strange ways. The Arab Spring is likely to be a decade of revolutions over time rather than a one-time occurrence.

**The Future of Power**

The lesson learned from Gutenberg’s invention of the printing press is that we don’t know how the future will play out and it will not be linear process.

John Ruggie, of Harvard’s Kennedy School of Government, points out that in the feudal medieval system, the walls were not knocked down. Instead, outside the walls more and more trade would emerge requiring dispute settlement processes for these transactions. This gave rise to *lex mercatoria*, which upset the traditional feudal system by introducing new norms that are imported into feudal systems, and inside the walls, as traders were seeking safety of the castle.

This may be akin to what will take place in cyberspace, but with outcomes dependent on culture and region.
FRAMING SESSION III

Control of the Internet – The Core of Cyberspace

David D. Clark
Senior Research Scientist
Computer Science and
Artificial Intelligence Laboratory, MIT

Control point analysis is about how to identify the critical features in the traditional layers of the Internet model, who controls or manages them, and why. To illustrate, we will use a case study: how to view a web page.

The sequence of steps that must be taken is presented here in outline form. Please follow the text below with that understanding.

○ Get a running computer:
  ● Under the control of people who provide hardware and operating systems
  ● In high security environments translates into concern over supply chain
  ● Vulnerabilities
○ Run Dynamic Host Configuration Protocol (DHCP)
○ Access ISP
○ The potential interventions include the following:
  ● Malicious Domain Name Systems (DNS)
  ● Block virtual private networks (VPNs)
  ● Block remote DNS
  ● Lock download
○ Select browser
○ Provider of browser
○ Download software
○ Download mechanisms
○ Build a web page
○ Create a web page:
  ● Development tools
○ Server software
○ Activate a DNS name:
  ● DNS registrar
  ● DNS provider
○ Elect to use SSL
○ Obtain URL
○ Extract DNS:
  ● Convert DNS to IP address
  ● DNS server/system
Other steps:
- Retrieve certificates
- Verify certificate
- Accept verification
- Retrieve page – from a geek’s view, this is “the Internet”:
  - All ISPs along path
- Render page:
  - Browser

Some Conclusions

One:

Security technology *cannot* ensure that the network operates correctly. It can only turn arbitrary interventions into “clean” signals failure. The key discipline on the actors to behave in a trustworthy way seems to be loss of reputation.

Two:

If you want to change *cyberspace itself* you will have to take an action that impacts the relevant actors, those that control (right holders, standardization organizations, criminals). To illustrate control options for the U.S. Government, key actors are:
- U.S. ISPs
- U.S. government
- Rights holders – copyright holders
- Intervention by government: DMCA, lawful intercept, net neutrality
- Intervention by right holders: lobby for law, demand takedown

Three:

How can we pick good actions to achieve desired outcomes?

Lower layers (in traditional representation of the Internet) are more general. At the Transmission Control Protocol (TCP) layer, bits are just bits. So trying to solve a problem that arises at the higher information layer, or at the DNS layer, the filter is either too blunt.

If you have a problem at the information level, it needs to be solved at that level.
Control of the Internet – The Core of Cyberspace
David D. Clark
Senior Research Scientist, CSAIL, MIT

Control Point Analysis
David D. Clark
MIT CSAIL
November, 2012

In this talk
- Describe a different method for analysis of contention and control in cyberspace
  - Control Point Analysis.
- Compare with traditional layer model
- Diagram some case studies of different actors and their options for control.
  - Try for some general conclusions.

A traditional model
- The net
  - People: Individuals, groups, agents.
  - Information: Blogs, Youtube, Wikipedia, etc.
  - Application: Web, etc.
  - Services: DNS, TCP/IP
  - Internet: Ethernet, Optical fiber

Control point analysis
- Identify the critical features of the design by tracing the steps of a "simple" action and seeing who can control each step.
- An analysis that illustrates the dynamic operation of the system.
  - In contrast to the normal technical description, which tends to cover the static structure of layers and interfaces.
- Case study: how to view a web page.
Getting the page

Then what happens?

Some conclusions

- Security technology cannot ensure that the network operates correctly.
  - It plays a very specific role: turns arbitrary interventions into “clean” signals of failure.
- The key discipline on the actors seems to be loss of reputation.
  - For private sector, loss of business.
- Good behavior is defined by norms, not law or contract.

More conclusion

- Many of the strategies we have in getting the Internet to “work right” are not about means to achieve an agreed outcome, but about disagreements as to what outcome is desired and acceptable.
- The shape of the Internet is defined by a tussle among the stakeholders, not just technology.

Catalog the actors

Immediate control:
- ISPs
- DNS providers
- Hardware/OS providers
- Web hosting/software
- Web content providers
- Browser providers
- Certificate authorities
- Typical users

Indirect control:
- Equipment suppliers
- Standards bodies
- Internet governance organizations
- Rights holders
- Governments
- Criminals

Indirect control

- An actor that does not exercise direct control over the Internet must act indirectly by influencing the direct actors.
- The ability to exercise control depends on the power relationship among these actors.
  - This can differ from country to country.
Control options, U.S. ISP

Control options, U.S. Govt

Control options, Rights holders

The next step

- Control Point Analysis reveals the points where actors that directly influence the Internet exercise control.
  - Indirect action must influence these actors if it is to influence the Internet.
- Which actions are effective at dealing with which issues?
  - How can an actor such as private sector rights holders pick the best approach?
  - For this, need additional analysis derived from layer model.

Initial theory—layers

- Lower layers are more general.
- A remedy at a lower layer either is:
  - Over general. Blunt instrument.
  - Narrow target. Opponent can use generality to evade.
- So go up:
  - Try the people layer—lawsuits.
  - Don’t try the DNS (SOPA)
  - Don’t try to outlaw P2P protocols.

A traditional model
Summary

- There is no single approach to achieving an objective.
  - Match the method to the problem
- Control Point Analysis reveals the points where actors that directly influence the Internet exercise control.
  - Indirection action must influence these actors if it is to influences the Internet.
- We have other models that allow us to draw additional conclusions.
  - This is just a quick introduction.

Examples of issues

<table>
<thead>
<tr>
<th></th>
<th>Individual</th>
<th>State</th>
<th>International</th>
<th>Global</th>
<th>Non-profits</th>
<th>Profit-making</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Digital</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>Privacy;</td>
<td>Censorship</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Poor access;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Production</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>Privacy;</td>
<td>Censorship</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Poor access;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Production</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Blocking DNS</td>
<td></td>
<td>Authority</td>
<td></td>
<td></td>
<td>Control</td>
</tr>
<tr>
<td>Internet</td>
<td></td>
<td></td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
<td></td>
<td>Spectrum</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PANEL SESSIONS

PANEL I

Connectivity, Networks, and Internet Service Providers

Moderator
David D. Clark, Senior Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT

Panelists
Steve Whittaker, Principal Consultant, British Telecom; Research Affiliate, MIT Media Lab
Michael M. Afergan, Senior Vice President and General Manager, Site Division, Akamai
Barry Tishgart, Vice President Network Services, Comcast Cable

Presentations

Traditional political science focuses on state actors, but we must consider the private actors. This panel features those who build the lower layers and physical infrastructure. Power, for the most part, is in the hands of users – who wants to take this freedom? Cyberspace is becoming more social by connecting people. Privacy is a major concern: the network we are building is unprecedented in its scope, in its ability to know how a state is working and what its citizens are doing.

Who is in charge?

User’s freedom is a key principle; we are not convinced that any additional regulation or controls will contribute to greater freedom. Different trends are taking place. There are different economic dynamics at different levels of the layers.

Nobody is in charge; users are in control as economic-minded players creating highly complex systems that empower the individual. For example, Akamai is providing platforms around the world carrying 20-30% of the world’s Internet traffic. It is clear that we are seeing the consumerization of IT and challenging what control the corporation has over its employees in terms of security. A bring-your-own-device (BYOD) philosophy is spreading with users bringing their own devices to work with important implications for a company’s
control over content. The individual web experience of users is provided by several content providers simultaneously.

At the same time, the argument regarding an increasing return on scale is relevant. The Internet presses back – perhaps creating a truly global media market. However, there is legitimate pushback from nation states (the "Westphalianization" of cyberspace).

**How is presence in many countries with different jurisdictions managed?**

- Each individual country has its own telecom regulation. Each country has its own telecommunications laws. For example, Akamai does not provide content itself but enables its customers to provide content-raising. The additional question is where do Akamai’s rights and obligations start and end and where is its customer?

**To what extent does the playing field enable achieving the desired outcome, the outcome you want, both domestically and globally?**

- Infrastructure suppliers must build highly adaptable infrastructures that accommodate all sorts of streaming technologies, and to different devices. All of this brings new challenges to scale.
- Five years ago, there was heavy peer-to-peer traffic whereas today, most are streaming bits. We need to think about highly adapted infrastructure that includes covering new demands from streamlining, raising new questions of scale and changing user habits in the UK. The prevention to stream video resulted in built-up infrastructure capable of avoiding regulatory provisions. This is an example of the effect of regulation on infrastructure development.
- There are different ways of accessing the Internet with different devices at different locations.
- Anonymous attacks and hacktivism pose new challenges, as they are much harder to stop.
- Criminals are outsmarting the users, and governments can control where you can go, so as a user you are limited by dodging the criminals and being able to go to your destination by government.
- The bigger threat is not on connectivity, but an attack on the application.
- The most challenging issue in cybersecurity is the degree to which individual machines compromise the security of the network (botnets).
- ISPs are especially well-positioned to watch botnet traffic and identify it. Why do you (Comcast) not act upon that? Customers can download a sophisticated security suite that will alert users when a botnet attack is identified. It is argued that there is some reluctance to notify users, because
the question is what would the user do with this information? But if you see it before the customer sees it, why wait for the customer to call it in?

○ There is the need to balance privacy, to limit the assumptions ISPs can make about consumers’ activity.

○ There is an increased commoditization of content delivery, is this commoditization posing a threat for you to maintain a profit margin?

○ Cables are built by alliances of companies, not individual ISPs.

○ At the domestic level, you see ISPs fighting to control higher levels of economic activity, some will succeed and some will fail. Why do ISPs not notify customers of botnet infections?

○ There are various elements in place to help customers, for example, downloadable security packages. ISPs see it before customers see it, why wait for the customer and not block it directly? Some of that is taking place.

○ Privacy issues, such as ISPs notifying customers, require ISPs looking at customers’ machines.

Do you see commodization as a threat?

Commodization of your own traffic is a challenge emergence of isolated IP networks, non-public Internets for operations. Perhaps like the case of remote control of critical infrastructure, separation by industry begins to disappear. What does it mean to guarantee that a TV doesn’t behave like a laptop?

The latest attacks are on banks: the banks call the ISPs and say, shut it down, can you do it? The attack might still be going on, but the impact on what you care about can be mitigated by isolating it from leaving the country or network in which it originated, thus, protecting targets such as critical infrastructure.

To what degree are you actually able to monitor your network?

○ The DoD realized that it has no ability to gain situational awareness of its traffic because it runs over private networks.

○ Corporations operate on principle that a certain fraction of networks are failing any given day without knowing why and when part of the network will return and therefore resiliency is built into the system. On a daily basis today there are approximately two trillion requests across networks. There is no single solution but the need to combine different techniques, the need to embrace the notion of failure; and the need to assume that any system could fail.
Is the network doing what you want it to do and what is it being used for?

In 1988, Morris released a virus. A panelist received a phone call from a program manager at DARPA with “flames” coming out of the telephone. The panelist was asked what the program manager should tell his supervisors. He responded, “Tell them the network is doing exactly what it was designed to be doing and is delivering the virus as quickly as possible.” The Internet is transparent to success but opaque to failure. The layers have its strength and weaknesses, the latter arising from a need to ensure smooth interactions between the layers.

How does one value a generative ability of companies, the ability to use soft power capabilities, and the ability to block malicious activity? Who is going to control the next set of standards? If technology matures further, it will shift the points of control; the world is globalizing and new technology and powers are rising.

There is the question regarding using the Internet for critical infrastructure: is there a distinction between data relating to critical infrastructure?

In the recent attacks on banks, the banks went to the ISPs asking ISPs to stop the attacks. Can this be done?

Partly, it involves multiple ISPs, so is very complex. You cannot shut it down; you can only defend against it. In addition to banks and media, many other banks were also attacked but had measures in place to defend themselves. It is particularly complex if the attack is from various countries, therefore the ability to limit an attack to the originating country or network.

Is cooperative innovation possible?

It requires cooperation from actors that often do not have a fiscal relationship.

Role of the ITU and World Conference on International Telecommunication

The ITU is a treaty organization that played no role in the past in the regulation of the Internet. But they aim to renegotiate their position – what is at stake:

- Increase mechanisms by which one carries out censorship.
- Push from telecommunication companies to shift the neutral content model to one in which the sender pays for the delivery of content.
- Shift from the view that the Internet has worked well with the private negotiation of agreements.
- Most U.S. companies are aligned against this proposal.
- Commercial relationships are the way to go rather than antiquated settlement systems.
Going about fundamentally reworking the economic structure of the Internet is not feasible by an international body.

For decades, there has not been the ability to solve cybersecurity problems and an international organization would not have been useful. There is a mismatch between the existing architecture and the architecture they would feel comfortable with. The ITU is only the beginning; the state is not going away with the settlement issue; it is only being a small issue of a larger dynamic.

Open Discussion

The core question of the discussion is “Who is Responsible?” for the Internet? Activities are pursued from Internet freedom perspectives. “Who is in Charge?” is also a question of defining power of the consumer.

Cyber risk: Who is in control of criminals and governments’ power over criminals?

ISPs seem to have the most superior hand in control of criminal activity.

- This also raises anonymous attacks on criminals as a challenge; when compromised machines are used to attack malicious users, e.g., hacktivists.
- This presents serious coordination problems because of no fiscal connections between actors.

What about the ISPs? Why don’t ISPs take down botnets or notify users that they are vulnerable?

- There are different tools to achieve monitoring and different strategies.
- Users may be unsatisfied if they find out that ISPs are monitoring their computer’s activity.
- Users would not even know how to react if they are notified of their vulnerability to or infection with botnets.

To what extent are service providers able to monitor traffic? What about military communication through ISPs?

- Some activities will have to go regardless of how much ISPs monitor and control traffic.
- There is a cross-layer challenge to monitoring all activities, especially applications activities.
What about the ITU?

It has potential control points and treaty level meetings.

- The ITU is not going away.
- The State is not going away. Polarization is seen in the long run.

Who controls recognition and support of practices that provide best security?

- There is a feedback loop; a time element that influences the learning and shaping of best practices.

Since the premise of the panel is that users are main control actors, to what extent can governments enforce best practices? Can governments incent companies to implement best practices? How much caliber can the government afford to provide such incentives?
INTERACTIVE SESSION

Barriers to Control: Certainties and Uncertain Ties

Moderator
Herbert S. Lin
Chief Scientist
Computer Science and Telecommunications Board
National Research Council of the National Academies

Questions for Discussion

What is better for the U.S. – a completely unsecure or a completely secure world?

The terms of the question are unclear: You cannot make the world secure, only more secure. It is a matter of sliding scale.

What does security mean for different countries?

U.S. free speech is a protected right and corporate espionage is a crime. In some countries it is reversed. Some argue that if given the choice, countries would choose a completely unsecure environment because it has some stability and is easier to maintain than a uniformly more secure world.

Predicted consequences of the fundamental supremacy of the offense in information technology include:

- No good defense
- No good deterrence
- No good counterforce for damage limitation

Only offensive cyber operations for offensive purposes can provide the possibility of advantage

Possibly, if we can achieve a global harmonized legal framework to tackle cybercrime we can establish deterrence.
What is the value of delayed strike-back on deterrence if attribution to political actors is not possible?

What does deterrence want to achieve and what does strike-back mean? A delay which might allow an attacker to achieve the goal of time-limited operation before it will be stopped. The analogy is a mutual assured destruction that does not work because cyberspace is a different environment.

Why shouldn’t self-help be encouraged?

The legal environment matters. It is unclear what is meant if U.S. freedom of expression is a right and economic espionage is forbidden. In many parts of the world it is the other way around; the system can never be made fully secure. The optimal situation is to raise costs for the attacker which is in the U.S.’ interests because the U.S. has resources to still operate in a fairly secure environment and exploit remaining vulnerabilities, even at a high cost.

Finally, the analogy to nuclear era is stretched too far.
PANEL IIa
Losing Control in Cyberspace

Moderator
C. Lawrence Meador, Chairman, MGI Strategic Solutions

Panelists
Dan Schutzer, President, Financial Services Technology Consortium, Financial Services Roundtable
Kevin O’Connell, President and CEO, Innovative Analytics and Training
David R. Martinez, Head of the Intelligence, Surveillance and Reconnaissance Systems and Technology Division, MIT Lincoln Laboratory

Presentations

This panel is not interested in using cyber tools to attack, but finds that it’s not possible to learn about cyber defense without learning about cyber offence.

Some Threats to Cyberspace

- Hackery – “script kiddies”
- Cyber-theft of financial resources & intellectual property
- Cyber-espionage
- CAN, CNE - role of U.S. Cyber Command
- Financial Drain – Worldwide costs estimated at between half a trillion to a trillion dollars per year (e.g., McAfee).

Hackery varies in resources available and in the type of control that the hackers are looking for. Recently we have seen a substantial growth in theft of financial information and resources. There are no secure networks – assume that everything is compromised and that the type of compromise will vary according to the intention of the adversary.

For every company that discovers that it has been penetrated by an attack, there are likely to be about 100 others that do not discover that they have been hacked. We have been working to discover corporate and government best practices. There has been limited success, but progress is not impressive. Companies are not likely to disclose the fact that they have been hacked because they feel that it compromises their image.
Some companies will not share data with the government, because the government has Freedom of Information Act issues.

Some technologies that have been developed by the government to secure networks are classified and so cannot be shared with private enterprise.

**Recent History of Cyber Attacks as of this Year**

- Global cyber attacks this year’s “victims”: Visa, Google, Booz Allen Hamilton, AT&T, Sony, Mitsubishi, Nisan, DoD critical infrastructure systems.

**Major Cyber Attacks 2012**

- Stuxnet - Iranian nuclear program lost nearly a thousand centrifuges used for enriching uranium.
- Global DoS. Up 88% from the third quarter last year: Prolexic Attack Report, Q3-2012.

**Global Trends**

There is similar crowding that was noted in Framing Session I. In addition there are:

- Fragile economic future.
- Social media becoming the communication of choice.
- Many cyber actors: state and non-state actors, terrorists, criminals.
- Increase in cyber-espionage resulting in loss of IP.

The private sector is concerned about balance between revenue stream and how much is dedicated to cybersecurity, especially under pressure from stockholders.

There needs to be better ways to share information between parties – this goes to issues of strategy and policy. Without the ability to share information, it makes it difficult to defend systems.

Can we trust our routers? Global supply chain means that this may not be true. There are a lot of components that we don’t have control over because of the supply chain.

**National Challenges**

Several models frame the overall challenge: cybersecurity. This is patterned after the “kill chain.” What happens when criminals and bad actors are doing recon and staging an attack? There is a need to have good information sharing and good situational awareness.
The model is not just for defense, but also applies to the financial sector. It’s important for us to be able to act quickly, as the criminals will be moving quickly themselves.

Disaster, war and relief situations require them to share information with partner nations, which is something that no one does very well today.

We need to really assess if the things we are trying to implement are actually effective, which means we need quantitative metrics for determining quality.

There is a new potential for proposing a “DARPA grand challenge” including problems regarding cybersecurity. Better information sharing between federal and private sectors.

○ Global supply chain – can we really trust our routers? We have a lot of components present, but are they secure?
○ Need to increase the amount of cyber-crisis simulations to prepare for coming threats. Suggestion: red-blue military gaming exercises.
○ OODA Loop Comparison.
○ PROTECT – DETECT – REACT – SURVIVE.
○ The adversary’s TTPs evolve very quickly – our critical infrastructure and information systems must be resilient to fragile cyber environment.

**Defining Control**

The control of cyberspace will go increasingly to those who can understand development within it. Visualization is another key component of this model. As analysts get more and more detail, they continually are getting lost in the detail. How can we better synthesize the information presented to locate targets? Control of cyberspace will go to those who can understand developments in it, can convey that to others, and can anticipate and respond to developments, using human and machine response.

This is the perspective of working with analysts: people who have to look in detail at development on a daily basis.

It is unclear what the difference is between “normal” and “anomalies.” How can you use “anomalies” in the context of the intelligence community?

Visualization: As analysts get more data, they get lost in it. How do you use structure visual “breadcrumbs?” How do you describe “situational awareness in cyberspace” for analysts?

**Defining C3E**

Computational Cybersecurity in Compromised Environments’ (C3E) emphasis is on understanding developments in cyberspace, including methods for approaching them. C3E
brings in lots of different people who all deal with small bits of signals in large data sets: astronomers, fraud detectors, etc.

There are kinds of things you use to analyze cybersecurity problems that are the same as the problem of finding a guy with a virus who has to be found in thirty minutes. Using analogies such as this, they are able to look at different strategies for solving the problem.

**Infrastructure Dependencies**

What are the infrastructure dependencies in today’s banking systems? It used to be that you went to a bank where everything was controlled by the bank. Not anymore. Now we have everything delivered through third parties. There are some private networks, but for the customer facing problems these are all through the Internet on the customer’s own devices.

You can’t buy a generator to provide emergency communications like you can for power. Networks aren’t robust enough to depend on for reliability, but we don’t have backups.

**Possible Defenses**

Collaborate with others, so that you can share resources when necessary. Education of customers and employees is a good, but not foolproof strategy. Build additional vertical capabilities: emergency communication.

There are problems with active defense, but it is possible. This could become the digital equivalent of warfare. There is potential for misinforming and tampering with attacker communications:

- Can we trust our infrastructure to see us through hard times? Our biggest weakness is on our communication infrastructure – how can we bolster it? Can we trust the components even?
- Possible Defenses – measures include take down counter-attack, entrap and infect attacker sites, collect and exploit intelligence on attackers, misinformation and tamper with attackers’ communications, use decoys.
- Defining Active Defenses – the employment of limited offensive action and counter-attack to deny a contest area or position to the enemy.

**Costs of Cyber Attacks**

Panelists have not disclosed this methodology. Other opinions in the audience are that the numbers are not very good. Leon Panetta has discussed reacting in a forceful way against threats against critical infrastructure systems. As we all buy into cyber systems as critical infrastructure, it makes sense to include digital threats into that class of systems. One view is that DoD systems are not immune to the problems that have been discussed.
Open Discussion

Do you see any silver lining in the near future on any of the issues we have been talking about? Are there ways of reducing uncertainties?

You need a lot of talent to attack, and that is becoming an increasingly scarce commodity. Compensation for people with those skills becomes more attractive than the rewards of participating directly in criminal activity.

Also, even if you can’t stop the attack, you can often stop a real-world effect (often fraud) itself, because the digital component is just one layer of the path of attack. You can look for anomalous behavior on the other levels of the events.

We have moved away from the idea of perfect security – that’s appropriate. We can also share template responses to known problems. Also, the adversary is not a genius, and has not likely understood the problem more completely than all of the people working to secure the system.

The classical way to acquire weapons for the military takes a long time. We’re now realizing a need to respond quickly to the challenges of the adversary, meaning that six month timescales are becoming more the norm for that domain. Also, what will help in the cybersecurity domain are small businesses which are innovative and can come up with new ideas. These developments can provide parts of an integrated solution by adopting elements from the commercial sector.

Responses to cyber threats are going to be driven by the perception of current or predicted damage due to the problem. One silver lining is that the private sector is motivated to come up with solutions to these problems.

What about silent crimes: espionage, IP theft, credit card theft? How many perfect crimes go on at the moment?

IP theft is mostly about brand erosion and reputation. Theft related to trading data is often physically manifested as fraud, and there are external mechanisms for dealing with that. The amount of actual damage can be minimized using protections in domains other than cyber. Layered controls can help stop fraud.

We do not have a number with respect to actual damages. Private enterprise needs to maintain an element of profit, and they spend a lot of money in IP generation. It’s unclear how you solve the problem of attribution. You don’t know who is taking the information, which makes it difficult to get law enforcement involved.
How do you quantify the value of a lost secret? In lives lost, in dollars, etc? Are we looking at it from the wrong perspective? Instead of defending against attacks, can you just encrypt every data bit? Change the structure of the information flows to prevent attacks?

When you have data in motion, you absolutely need to encrypt. When you have data at rest, it is for someone to read. In that case, you need to look at other access to the data – are the people entitled to see the information compromised? You have to decrypt and use the data at some point. Encryption alone won’t solve the problem.

**TJ Maxx example:** had all the ‘other’ pieces in place. How do you get people to put the ‘other pieces’ in place in other industries? **It is the other (non-cyber) levels of protection that prevent fraud?**

Fraud is constantly happening: there are clear objectives and many opportunities for feedback and learning. Militaries have the same opportunities to learn through constant engagement. The problem with intellectual property theft is that you don’t often get the feedback of actual money transferred to give you the learning opportunities.
Losing Control in Cyberspace
C. Lawrence Meador
Chairman, MGI Strategic Solutions

Panel Agenda
- Key Themes
- Introduction of Speakers
- Threats to International Cyberspace Control
- Panel Speaker Session
- Questions and Answers
...and if we have time:
- Clouds?

“Losing Control” Panel Speakers
(No Offense Intended!)
- Dave Martinez, Principal Laboratory Researcher, Lincoln Laboratory, MIT
- Kevin O’Connell, President and CEO, Innovative Analytics and Training
- Dan Schutzer, Chief Technology Officer, BITS

 Threats to Control in International Cyberspace
- **Hackery**: From “script kiddies” to nation states
- **Cyber theft of financial resources** & information
- **Cyber theft of intellectual property** – BIG DEAL!
- **Cyber espionage** – BIG DEAL!
- **CNA, CNE**: Response -- US Cyber Command
- Malicious or overly zealous **government controls**
- World wide costs estimated at between half a trillion to a trillion dollars per year (McAfee)!

Recent History of Control Threats to Cyberspace
- **Global Cyber attacks this year** alone on Bank of America, Wells Fargo, Capital One, BB&T, Google, Booz Allen, Mitsubishi, Sony, AT&T, Nisan, Visa, MasterCard, Symantec, Ally Financial – and many others!
- **Cyber attacks against critical infrastructure systems**, DoD and the US Intelligence Community, Leon Panetta, US Secretary of Defense, Washington Post, 10/11/12

Some Recent Instructive Examples
- **Shamoon**: destroyed 30,000 Saudi computers, Leon Panetta speech to BENS, Washington Post, 8/15/12
- **Cyber Fighters of Izz ad-din Al Qassam**: bank attacks
- **Global DoS Attacks**: Up 88% from third quarter last year, Prolexic Attack Report, Q3 2012
- **Stuxnet**: Iranian nuclear program lost nearly a thousand centrifuges used for enriching uranium, NY Times, 6/1/12
- “We weren’t ready. And we suffered terribly….”, Leon Panetta, US Secretary of Defense, 10/11/12
Panel Speakers Session

Questions and (Maybe) Answers

Cloud Claims

- **Cost savings** from shared use of computing resources – pay only for what you use
- **Agile and elastic access** to massive processing and storage as needed – easy to scale up/down
- **Self service** startup and control
- **Potential Cybersecurity** enhancements/control
- Software, platform & infrastructure services
- International availability from **multiple vendors**: Amazon, Google, IBM, Microsoft.....

Cloud Issues

- “Private” vs. “Public” implementations
- Getting the long term economic benefits
- Rigorous or casual approach to Cybersecurity
- Investment required to transform to Clouds
- Software as a Service – SaaS
- Platform as a Service - PaaS
- Infrastructure as a Service - IaaS

Defense Science Board Task Force on Cyber-Security and Reliability in a Digital Cloud

December 2012 (hopefully!)

(Report Currently in Release Review by OSD)

Current and Future Cybersecurity R&D Opportunities

- Instrumentation and Metrics
- Authentication and Access Control
- Labeling, Isolation and Tracking
- Cyber Offense and Defense
- Streaming Statistical Analytics
- Hardware Provenance - TPMs
- Methods for Correctness
- Homomorphic Encryption

Attributes of a Strong Security Plan

- **Authentication**
  - Two-factor for generic authentication for users
  - **Authorization**
  - Supporter: Rights is a group of user’s access, ‘Supporter of Rights’ approach for some applications
  - **Access Control**
  - Compliant monitoring of network traffic and hops. Automated ‘hardening’ for external and internal threats
  - **User Access Control**
  - Rapid ability to disassociate an individual from a host system further
  - **Data Encryption**
  - Using encryption to protect and transit data. Key protection through formal Platform models (FPM) is required
  - **Data Collection**
  - Techniques for validating that software and data have not been modified
  - **Dependability Control**
  - Use of “Smart Algorithms” frequent monitoring of operation integrity and make adjustments
  - **IT Security Policy**
  - In network, automatic background checks and protection for IT resources
  - **Supply Chain Management**
  - **System Redundancy**
  - Parallel paths for data processing and storage
  - **Flexible Access**
  - Forward transfer of data, especially in event of damage/destroyed system
- **Advanced Techniques**
  - Implementation of stochastic and quantum operating systems and applications

Losing Control in Cyberspace
Dan Schutzer
President, Financial Services Technology Consortium, Financial Services Roundtable

Losing Control in Cyberspace
November 7, 2012
Dan Schutzer
CTO, The Financial Services
Roundtable/BITS

Infrastructure Dependencies
* Today we have back-up power what about back-up emergency communications?
* Are our networks robust enough and can we count on their assistance and survival?
  - Service denial attacks (block attack traffic, take down sites)
  - Attacks on the routing infrastructure
* Can we trust to be there uncompted
  - our third party suppliers?
  - The devices our customers use
  - GPS, weather satellites
  - The rest of our infrastructure

Possible Defenses
* Block, filter, drop and ignore traffic
* Slow down traffic – require extra validations
* Better techniques and challenges to distinguish between humans and malware
* Create moving target

* Active Defense (The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy)
  - Entrap and infect attacker sites
  - Take-down, counter-attack
  - Collect and exploit intelligence on attackers
  - Misinform and tamper with attackers communications
  - Create false targets, deflecting attackers resources
  - Use of decease
Losing Control in Cyberspace
Kevin O’Connell
President and CEO, Innovative Analytics and Training

Who Controls Cyberspace?
Panel on Losing Control in Cyberspace

Kevin O’Connell, President and CEO

November 2012

Premise of this Discussion
- Control of cyberspace will go, increasingly, to those who can understand developments within it ...
- Many definitions are vague or not commonly accepted
- Can convey that understanding to others ...
- In a commonly understood language
- And can anticipate and respond to developments, drawing upon the optimal combination of human and machine response

What Does “Normal” Mean in Cyberspace?
- The concept of “normal” is constantly evolving
  - Cold War era versus Cyber War era
  - Distinction between malicious and benign actors
- What is “normal” relates to how to convey important issues related to trust
- How do we even research this kind of issue?

Objectives of C3E
- C3E = Computational Cybersecurity in Compromised Environments, or “How Will We Succeed in Bad Cyber Neighborhoods?”
- Emphasis is on understanding developments in cyberspace, including methods for approaching them
- Purpose, consistent with C3E #9, is to help develop research ideas for novel cybersecurity solutions
- Drawing on emerging scientific and technical concepts
- Also to foster creation of a diverse community of interest focused on the analysis of cybersecurity threat and response
- For C3E 2012
  - to assess decision-making and risk management issues in cyberspace
  - to assess visualization in cyberspace and its link to perception
- Emphasis on the practitioner: how do you make it real?

What is C3E?
- C3E gatherings and their emphasis
  - 2009 (Santa Fe, NM) to understand how adversaries have insinuated themselves into our systems and networks, and the extent to which computational and other analytic approaches could be leveraged to mitigate their influence
  - 2010 (Santa Barbara, CA) to understand state-of-the-art models and data practices could inform strategy and tactics for the practitioner
  - 2012 (Keystone, CO) to discuss predictive analytics and the role of intersecting anomalies and emergent behavior in supporting them
- All three reports now publicly available; summary report in draft for IEEE 2013

The Identity Challenge Problem
- Starting Point: Our “Friend with Deadly Virus” and the Challenge to Find Him in 30 Minutes
  + Combination of analytic methods and visualization techniques to attack problem within approximately 40k nodes
- Value and Lessons Learned
  - Importance of a “real” problem being provided to outsiders
  - Value of competition in content development
  - Success of C3E as a diverse Community of Interest
  - Value of the analytic methods and visualization techniques to Cybersecurity
Role of the Practitioner
- C3E has always kept the practitioner - ops center chief, analyst, industry IT manager - in mind, but this year decided to try and be more explicit about practical issues.
- Three presentations emphasized the challenges for the practitioner:
  - “Cyber Red/Blue” Lincoln Labs simulation walked the group through the tradeoffs associated with multiple attacks for a corporate manager
  - Presentation on understanding resilience in command and control resilience
  - LANL presentation on day to day activities and realities

Decision-making/Risk management
- What obstacles to DM/RM are particularly relevant to cyber?
- What methods and practices can help overcome them?
- What technologies can support those methods and practices?
- How can we measure the effectiveness of tools and techniques?
- What issues affect user acceptance of tools and techniques?

Decision-making/Risk Management
- Challenges
  - Situational Unawareness caused by Human Irrationality
  - Fear of Consequences
  - Too Much Transparency
  - Bounded Rationality
  - Social Issues
  - Lack of knowledge of ourselves

Decision-making/Risk management
- Methods and Technologies
  - Expand Sensory Awareness
  - Facilitate person-person collaboration
  - Facilitate person-machine collaboration
  - Context awareness
  - Communication across different parts of the organization
  - Predictive techniques

From Visualization to Perception
- What are the emerging “best practices” in visualization for the analyst?
  - How can they orient, assess, and move around large data sets efficiently and effectively?
  - How can visualization provide a tool for the analyst to navigate easily through large data sets to explore potential relationships and to develop or validate hypotheses?
- What is the role of streaming analytics and other techniques in enhancing perception of cyberspace threats?
- What is our current scientific understanding of the relationship between visualization and perception in both the human and machine-learning worlds?
- How can we distinguish between anomalies recognized by machines—often the result of incomplete data or computational errors—and anomalies that merit further investigation or immediate response?

Additional Questions
- How can the accuracy/validity of a visualization be assessed?
- What confidence/uncertainty can be assigned to a visualization? What descriptors or classifiers of uncertainty are there?
- What are the sources of data used for visualization? Are some better than others? Why?
- What should we learn from the Identity Challenge problem?
  - In particular, regarding cyber security from this type of analysis, visualization, and interaction?
Creating Situational Awareness of Cyberspace

- Mitigate Bias
- Understanding the big picture
- Prioritize network events and anomalies
- Immediate Representation vs. detailed analysis

A Comprehensive View of Cyber Power

Enabling Exploration of Cyberspace
- Capitalizing on our Tree-like thought process
- Investigation of "what if" scenarios
- Exploring what is "normal"

Empowering Humans to make Decisions
- Mitigating biases to improve the human cognitive process:
  - Perception
  - Comprehension
  - Projection

Final Thoughts
- Our understanding of developments in cyberspace underlies much of our ability to respond ... and exercise control
- If you cannot warn, you must anticipate!
- Non-traditional approaches to understanding cyberspace are essential to success
  - Including analyst-data-technology divides
  - Emerging analytic methods and visualization
Losing Control in Cyberspace
David R. Martinez
Head of the Intelligence, Surveillance & Reconnaissance Systems & Technology Division, MIT Lincoln Laboratory

Global Trends and National Challenges

Global Trends
- Cybersecurity demands international collaboration
- Fragile economic future
- Heavy dependence on critical infrastructure and information systems
- Increase in cyber espionage resulting in loss of IP
- Many cyber actors: state and non-state actors, terrorists, criminals,......
- Social media becoming the communication of choice
- Information technologies are commodities available worldwide

National Challenges
- Sharing of cyber information among federal and private sectors
- Attribution (who, what, when and how)
- Cyber strategy and accountable policies
- Cyber exploitation and offenses
- Global supply chains
- Modeling and simulation including red/blue exercises (grand challenges)
- Education-training and equipping

* Challenges relative to Cybersecurity

Keeping Pace with Adversary Tactics-Techniques and Procedures

- Adversary TTP's evolve very quickly – Our critical infrastructure and information systems must be resilient to fragile cyber environment
This panel seeks to gain insight to what we know and don’t know about cyberspace in specific fields. Existing techniques are not sufficient to know cyberspace. A set of questions is directed to the panelists. We begin with:

**What are the Challenges of Cyberspace in your field?**

**International Relations**

As Thomas Kuhn stated, social sciences are too messy. Even today what he said is right. There is no single dominant paradigm. Rather, there are a few competing ones. Paradigms exist in a sense that Kuhn attributed the notion of paradigm. They have a deep commitment to assumptions; on the basis of what Kuhn called social science. In international relations (IR) theoretical paradigms have two important components:

1. Make use of broad concepts like anarchy, power, system, etc. which guide the design of research questions.
2. Paradigms involve questions that play an important role that guide falsifiability.

The key paradigms are: neoliberalism, neorealism and liberalism. There is not much debate on cyber analysis in our field. The paradigm shift involves a presence of crisis in the field. It also involves a variance in theoretical assumptions which is so large that the scientific
community questions existing axioms. We don’t really have a paradigm shift since IR exists in a state of crisis. We try to make sense of cyber rivalry and existent situations.

Cyberspace may diminish state policy relevance. This does not mean the field of IR is experiencing a loss of relevance. What aspects of the cyber question might plunge IR into a state of crisis? The most important problem is state-centric formalism, which defines most dominant IR approaches. The information revolution is intensifying globalization and blurring the lines of society. This is corrosive of our basic theories:

1. It strains our broad conceptualization of anarchy and order. Distribution of power between states.
2. Agent diversity and preference pool pollution is bringing into question a fundamental IR assumption: actors in IR are homogeneous in their purposes and goals. Anarchy of cyberspace allows actors to form into units. Anonymity and asymmetry of cyberspace empowers non-traditional actors and exacerbates tensions. Non-traditional actors act in a strategically significant way that could damage national security. They do so for non-traditional motives and subversive aims. This brings into question that actors pursue the same purposes and have the same concerns of security.

Any statements about potential cyber crisis in IR are both limited and provisional: they are limited in scope because the international community is still beyond the reach of cyberspace; provisional in validity because new phenomena and new technology are still in their infancy.

**Law and Jurisprudence**

Regarding jurisprudence and interpretation of the Constitution, depending on whose theories you subscribe to there are six modalities, each of which thinks about the cases at hand differently. A judge may analyze these issues and apply different modalities. It is hard to say if there is a paradigm shift in law, or whether there should be one. Judges don’t understand technology that well. If cyber is expressed through paradigm shifts, scholars would abandon constitutional interpretation and use other methods of interpreting and applying laws. There is no paradigm shift in law and it is unclear whether one is needed.

**Computer Science**

From a computer science perspective, a fundamental change with respect to technology has caused a paradigm shift, not just a cosmetic change. The social network era is a paradigm shift, a fundamental change because it has a vital impact on users, providers, and the nature of services. Given the nature of technology, a paradigm shift is already happening on three levels. Where are the control points? How relevant is who controls cyberspace?
1. Transmission of information
2. Storage
3. End point usage of information

These three levels are relevant for who controls cyberspace. Change is a challenge for the physical layers of cyberspace. This can change the business model. IT can also change the politics and the policies.

The end point usage of information: Cloud technology is a challenge for policy makers. Cloud service providers have the problem of the “dirty disk.” This is one of the issues of the shift in the technology paradigm, centralized to virtual platform change. How technology is changing and how policy should address these changes are important questions.

How adequate are the concepts in your field?

International Relations

Power is a substitute word for control. As IR scholars, we think of these things in terms of power not control, but there is a difference. Most IR theory is based on a state system. Actors are states. We don’t really recognize little extra groups or other wielders of power. But cyberspace is a space for these little groups to gain more power, and to challenge state-based systems. They are not on the same level as states, but they are more powerful than before. Anybody who knows coding and has computers can make a computer network and can start wielding power, which can make them challenging or problematic for a state. Non-state actors are becoming an issue in IR theory, particularly terrorists. If they were not enough of a threat in IR theory, then why are people with computers a threat? Cyberspace is a challenge to the idea of anarchy and order. Cyberspace makes anarchy worse— it challenges order.

Cyber-realities and virtues of non-traditional actors are not just affecting our understanding of anarchy, but are taking our views to pre-anarchy. Anarchy is not just about power and its distribution. It also underpins society and common understanding, norms and principles of behavior. As for interstate cyber-domain concern, some of our traditional views are under influence. Take these two cases for example:

Case A: The U.S. decided not to use cyber-weapons against other states, for example, the Libya 2003 case. If impartial stories we know are true, those decisions are based on collateral damage concern and potentially destructive power of cyber instruments. When you include patriotic hackers and groups like Anonymous then you contaminate the preference pool. The basic social fabric of anarchy adds measure of expectancy and regularity even in absence of central authority, potentially destabilizing dealings of states.
Case B: The 2007 Estonia case involving non-state hackers. Consequential to the security of Estonia, it caused the government to adopt NATO Article 5 and get into a major crisis with Russia.

Law and Jurisprudence

What are five or six things we need to agree to do in order to protect critical infrastructure, and provide safe harbor? What are things that will provide enduring governance structure? Email vs. regular post is an analogy. Analogy is in transmission, mail in the cloud that is over six months old is considered not needed and government can read it without a warrant. Spam can be read by governments without a warrant. Crafting governance structure for the long term is very difficult. We don’t want to be wrong.

What about State and Non-State Actors?

There is asymmetry in terms of power for non-state actors. All that is needed is someone with some nodes and servers to launch an attack. An important question to consider is what policies would be considered to target attackers and to punish them. Which policy acts as a deterrent in the future is an important question. Non-state actors have different motivations to pull them together; state actors have different concerns and obstacles. State actors have fewer motives to get together and collaborate, but non-state actors find it easier to get together. We have to think in terms of asymmetry and collaboration.

China has a reputation concerning its patriotic actors, who could constitute non-state actors because they act independently. Some are controlled by the state. For example, the People’s Liberation Army (PLA) was tracked by IP addresses. Some groups are based in universities. They have attacked American companies, FBI sites, and the DoD. If you can attribute action to the state, then you can retaliate. What if your citizen does something that you could not control—are you still responsible? It is unclear whether this is diminishment of state control or not. At the end of day, there is still no single authority in charge.

One difference between state and non-state actors is with respect to de-packet inspection. If the government does de-packet inspection of civilian data it causes legal concerns. However, if a private sector company does it just requires a change in terms of service. Compare to state wiretap law. The ladder of power is changing; presenting an interesting dichotomy of issues that includes the speed with which cybersecurity issues are handled. We are moving too quickly for law to keep up as it was designed to move in a slow and deliberate manner.
The Role of Technological Change

The way technology works is the end user is the ultimate consumer of technology. By default, we fall back to structure. Context is the king and you have to provide useable service to consumers. Whether you make standards or not, certain standards creep in and when a paradigm shift happens, they just happen gradually. How will information sharing and context become relevant in IR? We really need a proper cyber 9/11, which will do us a lot of good.

Twenty percent is controlling 80% of the issues. One solution is to empower small to medium size companies to produce needed tools, and to lobby the government. Instead of blaming them, we have to help them, and provide big solutions. Technology entrepreneurs that have influence on creating lobbies can interfere with government and try to change things slowly—even overnight.

There are important concepts and objects we should be focusing on and start thinking about. Simplification is essential to theory, particularly explanatory theory. Without simplification—the main purpose of paradigms—we confront reality with complexity that overwhelms us. These conceptual simplifications can serve as a blinder to reality. Knowing what to discern and what needs explanation is essential. The problem is of flaws and incentives within academic perception. What would have happened to Newton after his law of motion?

In social and political science and in IR, people who have been wrong consistently for decades get higher positions. Mearsheimer predicted that the EU would return to multipolar rivalry and antagonism and he is still influential.

Open Discussion

In predicting outcome of world politics, simplification may not be a virtue.

There is value in static approaches. When arguing about crisis, recent events like Iran and Stuxnet, for example, aren’t states more important than we are predicting? Maybe it is pretty simple like the traditional IR theory.

Cyberspace may not completely change IR theory, but it changes some of the actors. Cyberspace is the first to do that; IR theory more or less explains what it was designed to explain. Discipline can stand some challenge. Some conditions should be relaxed; cyberspace has not changed the whole thing.
New realities and questions of influence are disrupting our traditional theories and views on the world. It is provisional and limited.

There are important aspects of national and international security. Nuclear weapons and others systems are not reachable by cyberspace. There are fundamental differences between natural and political science. Natural order is unchanging because it is compiled of material entities, material facts and laws that do not change.

However, laws have to change as we progress. Realities and laws of behavior can and do change over time. Some predict a return to multi-polarity in Europe, but this does not apply to Europe today—they have other problems.

We still have to see how this technology change will work itself out. Will it be less disruptive than atomic bomb explosions? We are still at a very early stage and we need caution for anything we say.
PANEL III
Information, Data, and Content

Moderator
Joel Brenner, Of Counsel, Cooley LLP

Panelists
Alan Davidson, Visiting Scholar, Engineering Systems Division, MIT; Former Director of Public Policy, Google
Jody R. Westby, CEO and Founder, Global Cyber Risk LLC
Ethan Zuckerman, Director, Center for Civic Media, MIT Media Lab
Howard Schrobe, Program Manager, Information Innovation Office, DARPA; Principal Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT

Statements & Presentations

This panel positions information, data, and content within the overall “mix” of influences that shapes who “Who Controls Cyberspace?” Multiple views are presented, along with potential contentions and disagreements.

Alternative Perspectives

Academic View

There is more state control today, but we are also over-focusing on state control. The independent journalists and activists often labeled by their governments as terrorists seek protection. Our main problems in terms of control are:

- DDoS – can’t easily trace back to state
- Site hijacking with alternative content
- Targeted espionage
- Intermediary censorship

Responses to these problems are generally prioritized according to what we can have an impact on:

- Lawful intercept – legitimate companies selling tools to counter crypto in societies where you know this is.
- Addressing companies directly when intermediary censorship occurs.
- We should focus on the type of control that we can influence.
**DARPA’s View**

DARPA is focusing on the control issue from the standpoint of how best to protect the war fighter. They are working on technologies that will guarantee people the right not to be attributed by the state as a “good” actor or “bad” actor.

Technology is dual-edged and the line between offense and defense is not fixed. This is evident in the battle for control over cyberspace.

**Corporate View**

From a corporate perspective, there is a growing amount of concern over the state’s control of the Internet. The Internet interprets censorship as damage and works around it. There are changes in the government administrative units. The old dogma was you that you can’t control the Internet. The new dogma of the state is that we can control the Internet, just watch us. We are in a world where there are many flashpoints – it is a very dynamic model right now. What is the role of international regulators going to be?

**Specific Questions**

**What is the best tool to address companies selling our adversaries’ routers for nefarious purposes?**

Routers can be used for both legal and illegal purposes. But the companies should care about the welfare of their shareholders and if there are ways to do this without involving the state, then all the better. For consulting companies this is more of an individual human rights issue. Companies are not thinking about this very much, unless it is those (such as Yahoo) that have struggled with state demands to limit content. Companies are mostly concerned with economic espionage. One can see the rise of state regulation and control network authoritarianism.

The government should think about this in an export control way. If a U.S.-based company is supporting undemocratic principles, the U.S. government can provide them with a “cover,” an imposed limitation so that they can avoid doing that without being accountable to shareholders who expect tapping that market.

While there is a focus on single-use technology, some dual-use technology is exported for a single-use purpose of surveillance.
Should we propose to limit – not just based on the country – but based on intended technological use? Via public pressure? Should we more than just look at surveillance technology?

The choices that corporations make have impact on more users than most decisions taken by nation-states. Why can't a company invest in making its service unblockable affirmatively (e.g., video streaming service)? What would make such a company go down that path? What is the cost of regulation? The problem is that the dialogue has not even begun. There could be companies that the board takes a position without an export control for the ideological/marketing image merit of it.

Google and Facebook have huge problems with the EU, how do we feel about the new EU directive?

These are good examples of how there is a rise of state action, particularly in the consumer protection space. Companies like Google, though they have a lot of power, are still susceptible to state regulation. We focus on Iran and China but there are many democracies who do not view the Internet the same way it is viewed in the United States. What will happen when the state tries to control Google?

This is what is happening with Google. They do not disclose any information and have been difficult when it comes to cooperation — for example, information about their cloud server. Furthermore, they have refused to negotiate on anything regarding where data goes around the world.

How is Europe handling this with the newly implemented regulation?

Europe has a very different approach to governing the Internet. The non-state actors of the world, like Google, are very powerful as well. It is very easy to characterize the concern of the users who are living under totalitarian regimes. It is also surprising that some democracies, like Brazil, have begun to change their tone by exercising greater regulation and control. The cost of regulation is an open question. The EU is developing new policies that are a concern to American companies. Google is not transparent and does not provide information, for example, regarding how it complies with the EU privacy directive.
Open Discussion

Are states “thoughtful intruders”?

The reason the Great Firewall is working so well is because it was developed in parallel with social media tools that are easier to use for Chinese users. There are surprisingly open critical discussions taking place on Chinese social media, therefore establishing control and a certain amount of openness. Tunisia did not shut down Facebook because that would create intense backlash. Instead, the Tunisian government hacked into Facebook to collect intelligence.

What are red lines and overarching international norms around human rights and free expression that go beyond? For example, Google Street View blurring faces, licenses in Germany, and YouTube videos critical of the monarchy in Thailand not being available?

Companies have a very strong free speech bias and high threshold to remove content.

“The Rise of the Hyper Giants”

This is a new situation which developed very quickly. We have no precedents for that type of speed.

What do we know of the content control situation in Saudi Arabia?

The principle premise is that the governments are exerting greater control. The governments that have the resources to control Internet content are endeavoring to exercise more network monitoring for security. However, there is always a high risk of mission creep. There is an allusion that end-to-end networks are decentralized, but this is no longer the case.

How is the culture on governing cyberspace changing?

We all naturally have groups that we trust more to protect our rights than others. Some companies are more sensitive to the political climate of their customers. The question to ask is when and where do you push back on this? Can free speech still be protected? There is a normative value in this that companies want to promote free speech and a decentralized network is perhaps better.

Can we measure the degrees of control in cyberspace? Is it useful to try?

Freedom House publishes a great report each year that assesses freedom of speech exercised on the Internet. Another good source on this is the Google transparency report – available on Bing.
The problem of self-censorship to avoid problems arises in every culture. More work is being done on state control (e.g., the Freedom House annual report) and companies’ own transparency reports.

**When is it Google’s job to collect information on how often a term is being searched? For example, can it help spot an epidemic earlier if a lot of people are Googling “flu symptoms?”**

No, Google should not have the responsibility to monitor and report on this. But other panelists were split.

Google did publish flu trends. It runs a Health Track application but will restrict some information from being released for some liability issues. Companies need to be sensitive to local demands, but all companies have a predisposition to free content when it comes to taking down content.

**Companies have capacities to track informational trends can have value for state priorities such as public health, when is it their responsibility to relinquish their control and share it with other concerned agencies?**

They do not have that responsibility. Google has put out such information in the past (e.g., flu symptoms). Such information sharing gets tricky when a scientist at Twitter tells the Kuwait government that they should expect protests tomorrow. There is no need for regulation of these predictive capacities yet there are other incentives for companies to publish such data.

**On protection of sensitive technologies by export control lists:**

Should we sell that technology to India and not to China? There is no guarantee that there won’t be reselling of technology. The way export control works means you cannot allow reselling to a country that is on the export control list. As a concept, the dialogue could be very productive.

**Do we agree that we are discussing knowledge control?**

Whether it’s in the form of privacy regulation, or the release of interesting aggregated information: this is an extremely dynamic environment. The reason EU citizens are more comfortable with governments holding data is that there are privacy protections in place. All those things are very fluid with the political situation.

This is not an issue the government is ready to deal with or one the public is informed about. There is probably more noise about it than allows for building a popular movement around it.
Who are the U.S.’ natural allies in this context?

Views on this depend on who you think you have influence over; control comes with a price. Corporations are not united over this.

End Note

There are upcoming conferences in India and Dubai to discuss the transnational laws regarding Internet freedom and copyright laws. It will be interesting to see how this plays out. Who are our allies in cyberspace? What about the BRICS? What is the UN’s role, if any in this governance game?
PANEL IV
Governance, Management, and Regulation

Moderator
Melissa Hathaway, President, Hathaway Global Strategies LLC

Panelists
Roger Hurwitz, Research Scientist, Computer Science and Artificial Intelligence Laboratory, MIT
Urs Luterbacher, Emeritus Professor, Institut universitaire de hautes études internationales, Geneva
Joseph Kelly, Chief of Cyber Intelligence, Office of the Under Secretary, U.S. Department of Defense

Framing Questions and Presentations

What is the role of the state?

There are remarkable differences in the role of the state in cyberspace discussions. Three points of difference between the countries that will be represented in WCIT:

1. Proposals dealing with the reduction of anonymity.
2. Proposals dealing with reduction of Internet freedom.
3. Economic question – roaming charges. Cyber has become a hot topic compared to only a few years ago. The number of people with access to the Internet will grow further from 2 billion.

The Internet has contributed to economic growth but the role of the state and regulation remains an open question: WCIT Internet traffic routing, some proposal still based on telephony POTS notion, Internet freedom including content control, and economic dimension and the question of charges, for example international roaming. States are using different venues to push their proposals, the ITU being one of them. Some states are attempting to extend their national borders into cyberspace.

Some findings and data-based predictions on the likelihood of changes to Internet structure are as follows: it is optimal to redistribute and should be obvious that less developed countries should get cheap and easy access to the Internet as it is beneficial to everyone. Most EU countries will not change their positions in the next ten years. Opponents to change have mobilized some in the form of parties. Eastern Europe is the one exception –
attempting to extract more from the Internet, but even there the probability for not changing is still high.

The Internet is a public good based on a decentralized architecture. Providing cheap and affordable access to developing countries is in everyone’s interest. Global experts’ analysis of documents is available online, analyzing four million documents using data to develop probabilistic findings and predicting that no EU country will change its position in next ten years. The exception is governments in Eastern Europe that are more dependent on gaining additional revenue.

The Internet evolved as an open ecosystem, with governments being envious of ‘knowledge control’ companies such as Google. Governments want their systems to be secure. China is an example where you have control and economic growth; the difference between companies is monetizing content and companies monetizing connectivity.

Openness is good for economic development. However, it plays out between the haves – those who can make full use of an open environment, and the have-nots – those who want to increase their share of the pie. A walled-garden experience allows governments to Google-like data collection capabilities. The danger occurs when it is technologically feasible to give governments the level of control they want.

**Are we at a point where we can afford to treat the network as a commodity? Or, do we need to treat it as a national strategic asset if it is tied to GDP growth, and a provision of essential citizen services?**

The Internet is a public good, not a commodity. There is a need to increase subsidies to the Global South to enhance their access so they have a stake in the system. The Internet is this ICT infrastructure that underpins all aspects of our society, therefore it is a very interesting platform to project power and influence national security outcomes.

More than twenty different international policy organizations, including the United Nations, NATO, the EU, ASEAN, and OAS are playing a role in governance and believe they should help direct future developments. These organizations, along with another 20+, are looking at technology and discussing policy. It is difficult for the U.S. to participate in all of these forums. The lines are spread thin and therefore, the U.S.’ message is inconsistent.
What about WCIT?

The ITU is a Specialized Agency of the UN. The 2010 Plenitary decided to hold WCIT timed after U.S. elections, a change of Chinese leadership, and the end of Secretary-General Toure’s term. Whereas the U.S. government’s position is that International Telecommunication Regulations (ITRs) are limited to telecommunications, is not that of many other countries. There is a need to avoid harm to facilities and services due to the Morris worm that occurred the same month. Developing countries lack the resources to build up their national infrastructures.

ITU’s mission is to sustain the growth of communication networks and to facilitate universal access. Measuring information society is important because there is a belief that this information society is the path for growth, innovation, and education. WCIT is set to update ITRs, which define regulations for telephone networks. The view from the U.S. is this is about Telcos, but that is not the view from all other countries. This ITR was signed in 1988—after the Morris worm was launched—so it includes concerns for cybersecurity. Traffic revenue generation has diminished and thus, no one can afford the bandwidth. How do you bring these infrastructures into a legal framework and allow for compensation?

There is an added view that the Internet is a different animal than telecommunications. Therefore, there is the belief that ITRs do not apply to the Internet. The U.S. and the EU have been blocking power and if they agree, they can stop any other attempt by Russia, China, or Latin American countries to amend the ITU treaty.

What about ICANN?

ICANN promised greater participation to G77 countries if they withdrew proposals against ICANN’s role in Internet governance. The agreement that subsidies to Global South should be increased which was part of discussion in Europe but the level of resources falls short of providing adequate investment. The approach is a nation-statist model in which each state pursues individual self-interest and in light of financial crisis focuses on national priorities inhibiting international cooperation.

The multi-stakeholder model for ICANN, recently opposed by China, Russia, Latin America, and 77 developed countries, was altered by ICANN’s suggestion to include greater representation. Otherwise development will continue to languish. It is in the developed countries’ interest to invest in their own country’s infrastructure. Government is bad at talking to industry. The decision about appropriate compensation will come down to how much the government is willing to ensure it.
We are on a slide towards the death of anonymity because it becomes easier to live in Apple’s walled-garden, or because you do not trust corporations, or from the standpoint of authoritarian regimes.

**How do Russia and China and Brazil and India, and swing states, such as South Africa, and Sweden think about the Internet as a sphere of control?**

Russian and Chinese positions are based on the principle from the 1648 Peace of Westphalia: *cuius rego eius religio* and domestic sovereignty. However, the Internet was developed at a time when the U.S. was the uncontested hegemon in the world.

**How has Stuxnet changed the dynamic and what should be response? What would be your response to the U.S. government creating a positive narrative when other governments call into question? The U.S. government’s involvement in controlling cyberspace through e.g., ICANN**

There seems to be a growing sense in the world of civilian infrastructure being off-limits, and that this should be a global norm. The U.S. government can restore credibility by supporting that point. However, it is not yet a norm, and has very limited influence over ICANN. While the U.S. government is supporting the application of Law of Armed Conflict (LOAC) to cyberspace, it has not gone as far as saying that the critical infrastructure IANA contract has been transferred from Department of Commerce over to non-governmental actors.

China is seen as giving power to dissidents both inside and outside the country. It would also like to use any move towards an international treaty as an opportunity for furthering arms control. Both Russia and China believe that the U.S. has an advantage in the developments of cyber weapons demonstrated by Stuxnet.

China would like to reapply the Westphalian ideas of no intervention in internal affairs of one state by other states. Western states are underestimating the resentment associated with control of ICT by western societies, as it is perceived as a form of colonization. China is pursuing changing default settings by pressuring the manufacturers in Korea. China has made a lot of investments in its own internal supply chain. Any frontal attacks against the current Internet structure are doomed to failure because of the blocking power of the U.S. and the European Union.

The issue of loss over control and potential greater danger in the future is important. Other countries can develop and implement rival standards – with the analogy to cell phone industry and standards – especially at the device level.
Open Discussion

Revenues Matter

Local advertising is important to create revenue streams. However, there is not enough revenue in advertising for infrastructure providers to utilize to subsidize broadband access. If you put a price on settlement, you have set the minimum value of content coming into a particular country, which will basically put a content tax on delivery.

There has been an international flow of hard money, especially out of the U.S., that did not go into investment in infrastructure. This has dried up with the introduction of services such as Skype. On the developing world side, this is an attempt to regain some of the lost inflow of money. But taxing the content would be detrimental to developing countries.

None of the custodians seem to be technologically capable to make the decisions about what ICT infrastructure should be developed.

Universal Service Fund

The concept of the universal service fund in the U.S. has been proliferating around the world.

It is a service fee that is exacted from the carriers based on the size of their infrastructure. In the United States, the Universal Service Fund was meant to develop the rural economy. Instead, it was spent on education and as such, has been abused by carriers, even though it is allocated in clearly designated accounts and earmarked for infrastructure development.

Standards

What is the interplay between the development of indigenous standards and global standards? What are the advantages and disadvantages of developing indigenous standards?

A standard that breaks interoperability is not going to succeed.
This session is the End Note for the Workshop. It highlights some of the key issues and positions expressed, as well as the contentions and continued uncertainties.

**Who Controls Cyberspace? Some answers heard today:**

- The users – if you don’t like something there are ways around it
- Many actors working together
- Many actors working separately
- Nothing is inevitable and it will take a long time to play out
- Criminals and hacktivists are taking over
- Different cultures in different countries
- If U.S. unilaterally constrains its companies, will other countries fill the void?

**Can we predict the future of control over cyberspace?**

It's hard to predict the future. For example, will social media undermine or support governments? There are a lot of dual-use technologies that can be used for good or for evil, and we won’t know until things play out. We have some ideas, and some predictions, but the reality is that the use of technology in the future is going to be a surprise.

**Bottom line: Who controls cyberspace?**

- We do. Sometimes.
- There are many actors each with control over different parts of the puzzle, but we sometimes have trouble getting those pieces to fit together.
Internet layering might be its own worst enemy

Layering of cyber technologies makes it hard to know what is going on in the cyber world, which is a strength and a weakness. It makes it difficult to stop specific behavior, or to attribute behavior to specific individuals.

Democratization of Cyber Technologies

Of the many changes going on, a compelling example seems to be a democratization of cyber technologies as they go out to the masses. How far will this democratization go? Will there be more Facebook accounts than people on Earth?

Dual-Use Technologies

How dual-use technologies will be used is gradually taking shape. We must distinguish between dual-use technologies and dual-categorization of users (freedom fighter v. terrorist).

Complexity Matters

There are complex interdependencies on technologies and their interactions. It is hard to predict the future of control on cyberspace – in pieces and parts or overall. We know that some solutions to problems that we do know often create new problems that we do not know of yet.

Since we are dealing with a highly complex, interdependent world, we must address the terrible and complex degree of interdependence in world technology.

Protection against Threats

- Why assume that perfect protection is possible now? It never existed before.
- Cybercrime rising:
  - Including both money, IP, and espionage
  - Not always reported
- Some espouse ideas that the criminals are taking over. There are a lot of different threats out there. There are signs that the cyber-crime world is becoming increasingly complex and integrated. Not all strategies for dealing with this reality are easy, and some are not possible.

All information security eventually relies on physical violence. The trouble is being able to find the right targets to apply violence to.
Governance and Protection

○ Governments might pass requirements that are really not technically feasible.
○ Results of Index Cards Poll at the Workshop show that the greatest threats are to:
  ● Critical infrastructure ~ 34% of the Workshop respondents
  ● Lack of public awareness/users ~ 22% of Workshop respondents
○ Needed is a greater focus on public policy, laws, and education.
○ Perfect protection does not exist in any venue, and therefore it is unrealistic to think that we should be able to accomplish complete security in cyberspace. Cyber-crime can be perpetrated by both non-state and governmental actors mimicking non-state actors for public relations purposes.

Diversity of Norms

○ It is difficult to get agreements and develop norms. Norms can change, but not always easily, quickly, or in the direction you want.
○ There are some things that you can legislate, but in some cases, this just means that regulated activity moves to different parts of the world – to governments with different legislation or regulations.
○ One man’s terrorist is another man’s freedom fighter. How do you provide [anonymity, etc.] technologies to one group that won’t be misused or used against our interests by another?
○ It’s great to be able to make a law – but that doesn’t mean the law can be implemented in an effective manner.

What Next?

Some possibilities can be framed by the combination of two critical conditions:

a. Control – Private or Public?
   ○ Think of a future that is entirely privately governed, or
   ○ Imagine a cybersphere that is absolutely controlled by governments
b. Politics – Conflict or Collaboration?
   ○ One future is the international system dominated by war
   ○ Another future is a peaceful environment

A combination of control (private vs. public) and international politics (dominated by conflict vs. dominated by cooperation) helps us frame the boundary conditions we should consider seriously.
Alternative Futures and Emerging Challenges
Stuart Madnick
John Norris Maguire Professor of Information Technology, Sloan School of Management, MIT

Alternative Futures and Emerging Challenges
-- What have we heard today
Stuart Madnick
John Norris Maguire Professor of Information Technology, MIT Sloan School of Management
& Professor of Engineering Systems
MIT School of Engineering

Changes
• Many changes ... “democratization” of cyber technologies
  – Cell phones
  – Satellite images
  – Global communication
  – At what point will there be more Facebook accounts
    than people on Earth?
• Dependency of our societies on multiple technologies can make us more vulnerable
  – After Hurricane Sandy, getting power to gas stations in NJ not enough ... unless also telephone service
to process credit cards!
  – Many different technologies and providers to just display a web page (note: interdependencies)

… and the solutions can be part of the problem ...

Complex Interactions
• Predicting Future of Control of Cyberspace?
  (E.g., Does social media undermine government
  ... or support government?)
  – Hard to predict, especially about the future ...
  – Future might be an “emergent” phenomenon ...
    over a long period of time

Who controls Cyberspace?
Some answers heard ...
• The users ...
  – At least in USA. If you don’t like something, there are
    ways around [Comcast]
• Many actors
  – ... working together, but not all controlled [Akamai]
• Nothing is inevitable ...
  – will take time to “play out” [BT]
• Criminals (and hacktivists) are taking over ...
  – Elaborate infrastructure is emerging
• Some proposed changes will be very hard
  – Probably practically impossible (changes to business models)

Internet Layering might be its own worse enemy
• Layering makes it hard to really know what is going on ...
• The lower layers don’t really know what the upper layers are doing (and the reverse)
• Hard to “shut bad things down”
• Attribution, especially prompt attribution, can be difficult ...
### Some requirements
- To understand cyber defense, you need to really understand cyber offense!

### Threats
- Never had perfect protection before, why assume possible now.
- Cybercrime rising
  - including both money and IP and espionage
  - Not always reported (maybe rarely reported)
  - Increasing cybercrime ecosystem
- Some “attacks” are fairly obvious (e.g., DOS)
- But, some (esp., IP and espionage) might go unnoticed for a long time (maybe forever)
  - T.J. Max credit card syphoning went on for years
- How many “perfect crimes” are out there?

### Control
- Different actions in different countries
  - Different cultures in different countries
- If US unilaterally constrains its companies
  - Will other countries fill the void?
- Dual-use technologies and saying: “one person’s ‘freedom fighter’ is another person’s ‘terrorist’.”
  - Anonymous networks help ‘freedom fighters’ to avoid detection by their government
  - But it also helps ‘terrorists,’ child porn, etc.

### Governance
- Governments might pass requirements that are really not technically feasible
- Ability to be anonymous is rapidly disappearing

### Threats in Cyberspace

<table>
<thead>
<tr>
<th>What is the greatest threat in cyberspace?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Infrastructure</td>
</tr>
<tr>
<td>Users &amp; User Education</td>
</tr>
<tr>
<td>Lack of Public Awareness</td>
</tr>
<tr>
<td>Policy/Legal Intervention</td>
</tr>
<tr>
<td>Attribution</td>
</tr>
<tr>
<td>Concentration of Control</td>
</tr>
<tr>
<td>Insecure Systems</td>
</tr>
<tr>
<td>State Threats</td>
</tr>
</tbody>
</table>

---

**Who Controls Cyberspace?**

**Results of “Index Cards” Poll**

ECIR Workshop  
November 7, 2012  
MIT Media Lab
**Threats in Cyberspace**

*What is the greatest threat in cyberspace?*

- Critical Infrastructure: 17 votes
- Policy/Legal Intervention: 4 votes
- Users & User Education: 6 votes
- State Threats: 3 votes
- Lack of Public Awareness: 3 votes
- Concentration of Control: 2 votes
- Attribution: 5 votes
- Insurance Systems: 8 votes

**Controlling Cyberspace**

*What form of control would help to reduce that threat?*

- Public Policy & Laws: 13 votes (26%)
- Public Information Campaigns: 8 votes (16%)
- Public-Private Partnerships: 5 votes (10%)
- Re-architecture of the Internet: 5 votes (10%)
- Norms & Culture: 5 votes (10%)
- International Agreements: 4 votes (8%)
- Decentralization: 4 votes (8%)
- Other: 6 votes (12%)

---

**Controlling Cyberspace**

*What form of control would help to reduce that threat?*

- “Other” considerations:
  - “Put Dave Clark in charge”
  - “This is not a problem that can be addressed through control”
  - “Let me know when you find out”
  - “Nothing foreseen”

---

**Finding a Solution**

**Top Threats:**

- Critical Infrastructure
- Users & User Education
- Policy/Legal Intervention
- Attribution

**Top Controls:**

- Public Policy & Laws
- Public Information Campaigns

---

**Finding a Solution**

**Challenge at the Intersection:**

How to balance the threats and implement controls

**Important example**

- User education raised as both an issue and a solution
- But how do we accomplish this?
- The fact that we are meeting at a university is at least one good starting point ...
- Lets all work on that together ...
POSTER SESSION
List of Posters

Explorations in Cyber International Relations
Nazli Choucri, Principal Investigator, ECIR; Professor of Political Science, MIT
Venky Naraynamurti, Co-Principal Investigator, ECIR; Director of the Science, Technology and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School

The Coordinates of Cyber International Relations
Chintan Vaishnav, Research Associate, Sloan School of Management, MIT

Cyber Defense Resources and Vulnerabilities
Josephine Wolff, PhD Candidate, Engineering Systems Division, MIT

Cyber-enabled Loads & Capabilities Methods
William E. Young, Jr. (Col, USAF), PhD candidate, Engineering Systems Division, MIT

Diversity of Use Experience and Alternative Future Internets
David D. Clark, Computer Science and Artificial Intelligence Laboratory, MIT
Shirley Hung, Postdoctoral Associate, Computer Science and Artificial Intelligence Laboratory, MIT

The Dynamics of Managing Undersea Cables: When the Solution is the Problem
Michael P. Sechrist, MPP; Chintan Vaishnav, PhD; Daniel Goldsmith, MBA

Establishing the Baseline: A Framework for Organizing National Cybersecurity Initiatives
Aadya Shukla, Science, Technology and Public Policy Fellow, Belfer Center for Science and International Affairs Harvard Kennedy School

Integrating Anonymity Networks as Platforms for Emerging Cyber International Conflict
Mina Rady, Visiting Student, Department of Political Science, MIT
When Virtual Issues Become Real World Applications
James Houghton, Research Associate, Sloan School of Management, MIT

Who Controls Cyber Anonymity: Control Point Analysis of Cyber Anonymous Activity
Mina Rady, Visiting Student, Department of Political Science, MIT
**ECIR is a joint interdisciplinary research project**
exploring cyber space & international relations, including implications for power and politics, conflict and competition, and violence and war – focusing on new methods for theory development, empirical data & policy analysis – with education of new generations of researchers & analysts.

See [ecir.mit.edu](http://ecir.mit.edu)

### Problem
Distinct features of cyberspace—such as time, scope, space, permeation, ubiquity, participation, attribution—challenge traditional modes of inquiry in international relations & limits their utility.

The solution lies with better theory and new methods that respond to the new conditions.

### ECIR Vision
To create an integrated theory driven, multidisciplinary empirically-based knowledge domain that:

(a) clarifies cyber threats and opportunities for national security;
(b) provides new analytical tools; and
(c) educates a new generation of researchers, scholars, and analysts.

### Methods
The research design consists of:
- Domain Integration of Cyberspace International Relations
- Data development & Empirical Analysis
- Dynamic Modeling, Simulation, & Policy Analysis

---

### The Research

**Examples:**

**Managing Vulnerabilities Undersea Cables**
Cyberspace is built on physical foundations. The undersea cable infrastructure is susceptible to several types of vulnerability.

The challenge is to reduce the vulnerability & build resilience by modeling technology & policy, & by building private public partnerships.

**Cyber-enabled Loads & Capacities**
Cyberspace produces new feedback channels that have real and tangible effects (loads) on state resilience (capacity). In some cases, this feedback amplifies dissident influence on the state. However in other cases, cyberspace allows the state to exert a greater level of control on its populace than previously available.

---

### Initial Results

- **Initial results include:**
  1. Constructed empirically based alignment mechanism to jointly define cyberspace and international relations;
  2. Demonstrated the value of control point analysis;
  3. Provided comparative empirical patterns of how different actors control the Internet;
  4. Enabled the power of partnerships for reducing vulnerabilities; and
  5. Generated empirical evidence about the salience of private authority in the management of cyberspace.

---

### Political Impact on DoD Capabilities & Implications for National Defense

This project seeks to provide specific methods for (a) anticipating, tracking and clarifying threats and opportunities in cyberspace for national security, welfare and influence; (b) providing analytical tools for understanding and managing worldwide cyber transformation and change; (c) constructing methods with real “hands on” use; and (d) attracting and educating a new generation of researchers, scholars and analysts.

---

### Acknowledgement
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.
The Coordinates of Cyber International Relations
Chintan Vaishnav
Pest-doctoral Associate

Problem
This work conceptualizes the hitherto separate domains of Cyberspace and International Relations into an integrated socio-technical system to identify and analyze its emergent properties, utilizing the methods of engineering systems. The work is an exploration in both theory and methodology.

We first identify important actors and their core functions in the two domains to disambiguate the important questions of system boundary. We then create a domain structure matrix (DSM) of the interdependencies among the core functions of the various actors. We then examine the DSM in two ways: (a) by qualitatively analyzing to show that Cyber-IR is characterized by the activities of multiple actors who are interdependent in various ways, and who are highly heterogeneous in their roles and capabilities, and (b) by quantitative analysis using matrix-based techniques to illustrate how certain core functions are more important than others, and why attributes such as geographical location, economic status, etc., of the actors shape their influence in Cyber-IR. This work forms a baseline for further understanding of the nature of the heterogeneous influences of the various actors, and the various outcomes that could result from it.

Methodology
Step 1: Identify important actors in Internet and International Relations
Step 2: Identify core functions performed by the actors
Step 3: Identify interdependencies among core functions
Step 4: Code and Analyze the Structure of Interdependencies
  - Qualitative Matrix
  - Binary Matrix

Applying Methodology
Internet Actors and Core Functions
- Equipment Providers
- Infrastructure/Broadband Internet Services
- Content/Platform Providers
- Service Providers

IR Actors and Core Functions
- Great powers/strategic decision-makers
- Global player/BUS/IGOs
- Internet and open-source
- Global state actors

Analysis and Results
Q1: Are some Cyber-IR actors/functions more important than others? Yes!
Q2: What dependencies are critical for the Internet, IR, and the relationship of the two?
Lessons on Dependencies within the Internet
First: Technological dependencies are very important. Some dependencies are critical, others are not.
Lessons on Dependencies within IR
Second: Standard organizations depend upon technology providers for not just standard creation but also the economic viability.

Lessons on Dependencies across the Internet
Third: Public provisioning of Internet functions occurs when depending upon the State is the only economically viable option. Such States heavily depend upon import of technology.

Lessons on Dependencies between the two
Fourth: While there is evidence currently of whether ITU depends upon the activities of WTO, they will likely become increasingly important.

Lessons on Dependencies at the seams (of the Internet on IR)
Fifth: In many cases, provision of technological functions of the Internet still depend upon State’s permission.
Sixth: For poorer states, dependence heavily on imports and subsidies for provisioning the Internet. Technologically advanced states depend heavily upon a complex web of dependencies on global supply chains for provisioning the Internet.
Seventh: Information access depends upon State’s censorship and content filtering.
Eighth: Standard organizations such as IETF, ICAAN increasingly depend upon the balance of State vs. non-State interests, enduring high coordination costs.
Ninth: States’ supporting organizations and standards organizations, many of whom are non-State, private actors.
Tenth: Security of a State’s cyber infrastructure depends upon security at all layers of the Internet with many Internet actors outside of State’s jurisdiction.
Cyber Defense Resources & Vulnerabilities

Josephine Wolff, PhD Candidate

Investment in security is aimed at reducing losses due to security breaches and typically determined by calculating annualized loss expectancy (ALE) metrics. However, in the cybersecurity space there is inadequate data on the frequency of breaches, the costs associated with those breaches, and the effectiveness of countermeasures, for organizations to be able to perform meaningful ALE calculations. With rising rates of both IT security spending and online attacks, surveys indicate that many business and government executives are unsure of how to allocate resources for defense and whether their investments in security measures are making any.

Key Questions
- How do private and public organizations make decisions about allocating resources for defense against cyber attacks, malware and online abuse and how do they assess whether those decisions were worthwhile or successful?
- Where do private organizations and government agencies ultimately end up allocating these resources?
- How can a deeper understanding of the different factors that contribute to defense decisions map onto a new understanding of different categories of attacks and vulnerabilities?

Methods
Comparative Case Studies & Interviews:
- Case studies of defense resources allocated by private companies in different sectors and government agencies, including U.S. Cyber Command and the Department of Homeland Security

Process Tracing:
- Analysis of decision-making processes for implementing defense measures

Document Analysis:
- Assessment of formal documents used for outlining defense strategies and metrics

Proposed Research
Investment in Cyber Defense Measures

Expected Contributions
- Comparative analysis of the processes by which different private companies and government agencies decide how to allocate resources for defense against cyber attacks and information security breaches and methods used to assess the effectiveness of these allocations
- Characterization of the different elements involved in defense against cyber attacks
- Assessment of where and how different types of organizations ultimately end up spending their resources for defense
- Mapping of defense resource allocations onto a taxonomy for distinguishing between different types of attacks by understanding how well they have been defended against

Literature Review
Gordon & Loeb (2006) found that less than 25% of firms reported using economic analysis to inform investments in information security, while an earlier survey found that many firms employ a "wait-and-see" approach, deferring investments in online security until after their systems are breached (Gordon et al., 2003). Rowe & Gallagher (2006) identified several factors driving firms' investment in information security, but little work has been done to understand how these decisions are made or characterize the resulting cyber defense landscape.

Funding Acknowledgment
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 and do not necessarily reflect the views of the Office of Naval Research.

Defense-Based Taxonomy of Attacks
Cyber attacks have been classified according to a variety of different elements, including:
- Motivation
- Technique
- Target

However, a crucial determinant of an attack's success is the extent to which it has been anticipated and protected against, factors that are not incorporated into most existing attack taxonomies.
Cyber Mission Assurance using STPA

William E. Young, Jr (Col, USAF), PhD Student,
Advisor: Prof Nancy Leveson

Problem
From Cyber Security to Mission Assurance
Improving Campaign Mission Assurance
How can we complete campaign mission across a wide range of degradations?

Current gaps:
1) Emergent system properties ignored
2) Assurance restricted to tactical level
3) Ignores Operational (campaign) Design

Solution:
1) Use systems thinking
2) Leverage safety-guided design

Method
System-Theoretic Process Analysis—
(STPA)
- Identify system goals, accidents & hazards
- Create control structure
- Create process model
- Identify unsafe control actions:
  - providing causes hazard
  - not providing causes hazard
- Identify critical threat scenarios
- Redesign system & iterate

The Research
STPA Operationalizes USAF Cyber Construct

Preliminary Results

Remaining Research
- Finish STPA of representative campaign design (& modifying STPA for military context)
- Conduct pilot experiments
- Prepare materials for training workshops
- Conduct experiments on design groups (STPA, control) in cyber-focused exercises measuring “faults” (potential degrades mission cannot survive)

Thank You!
This research is partially funded by MIT Lincoln Laboratory’s Cyber System Assessment Group. Any opinions, findings, & conclusions or recommendations expressed are those of the author and do not necessarily reflect the views of MIT Lincoln Labs or the USAF. Also, I extend my deepest appreciation to the many members of the Complex Systems Research Lab, Lincoln Labs Divisions 1, 6 & 19 & Group 69, Prof Nancy Leveson, Prof Stuart Macnich and Alen Moulton
Diversity of User Experience and Alternative Future Internets

David D. Clark, Senior Research Scientist, CSAIL
Shirley Hung, Postdoctoral Associate, CSAIL

Objective

One of the primary objectives of the ECIR project is to understand what forms the future Internet may take. This requires identification of the levers, constraints, and conditions under which each scenario may evolve.

Current visualizations

Technologists have mapped the Internet by connectivity, traffic, and even physical fiber. Each method provides different insights into physical and economic structure: who the players are, their relationships, and the depth and frequency of connections. But they do not reveal the wide variation in how people actually experience the Internet.

Diversity of user experience

User experience of the Internet varies greatly globally, and to a lesser extent even domestically. For example, the user map of Facebook looks nothing like the global traffic map due to blocking of Facebook in China and Russia:

Thinking about variation in user experiences requires consideration of language, culture, society, laws and regulations, not just packets, fibers, and dollars.

Each layer of the Internet can impact users in different ways, with increasing specificity moving up through the layers:

- Internet
- Application
- Information
- Social
- Physical

Assumptions of homogeneity

There is often an assumption that the Internet experience should be the same globally. John Perry Barlow’s “A Declaration of the Independence of Cyberspace” denied physical world government had any authority over the domain and declared cyberspace its own domain with its own “culture... ethics... [and] unwritten codes”. Yet we know from looking around the world that this is not true. Demanding a homogenious global Internet that achieves the “open” ideals of the West is unrealistic. Demanding homogeneity without the “open” caveat requires compromise that would by definition force us to give up some of our cherished values. (e.g. Yahoo! France, Gutmans/ WSJ Australia, Chinese censorship impact on Hollywood movies) It also risks alienating others to the point of disconnecting altogether, as Iran has threatened.

A heterogeneous future

The other possible outcome is a heterogeneous world in which we preserve our values but must tolerate differences we find objectionable in others. This future Internet would take on a core-periphery shape, with dense interconnection between “open” core states, and a spectrum of more or less interconnection in the periphery. It is possible that clusters will form, with greater interconnection within these clusters than to other clusters, and with some countries becoming their own, largely isolated network.

Future research: What is the future Internet we want?

We should think pragmatically about what a future Internet that would best achieve U.S. interests would look like, and how we can shape the evolution of the current Internet to achieve those goals. This requires asking what our aspirations for a future Internet are, which are achievable alone, and which require international or global cooperation. It also necessitates recognition of inherent tensions in goals (e.g. security-liberty) and discussion of acceptable tradeoffs. [ongoing work]

Acknowledgements

This work is funded by the Office of Naval Research under award number N00014-09-1-0557. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the view of the Office of Naval Research.
The Dynamics of Managing Undersea Cables When Solution Becomes The Problem

Michael Sechrest (Harvard), Chintan Vaishnav (MIT), Daniel Goldsmith (MIT), Nazli Choucri (MIT)

Problem

In the U.S., approximately 95% of all international Internet and phone traffic travels via undersea cables. Nearly all government traffic, including sensitive diplomatic and military orders, travels these cables to reach officials in the field. The problem, however, is that the undersea cable infrastructure is susceptible to several types of vulnerability, including rising capacity constraints, increased exposure to disruption from both natural and man-made sources, and emerging security risks from cable concentration in dense geographical networks (such as New York and New Jersey, and places like Egypt/Suez Canal). Moreover, even under normal working conditions, there is a concern whether governance-as-usual can keep up with the future growth of Internet traffic. In this work, we explore the impact of these problems on the dynamics of managing undersea cable infrastructure.

Analysis and Results

Analysis of Steady State Error (SSE)

\[ \text{Investment } a \times (\text{Desired Margin} - \text{Actual Margin}) = \text{Steady State Error} \]

Dynamic Complexities Complicating Decision Making

1. Utilization is rising exponentially
2. Time to investment varies with stakeholders

Conclusions

Policy Lessons
1. Counter to conventional wisdom, it may be more efficient to have fewer than a certain number investors in the undersea infrastructure where possible, to limit investment delays and ensures quick response when there are disruptions.
2. When large number of investors are necessary, public private partnership, being explored by International Cable Protection Committee, may work only when (a) partners participate not just in responding to disruptions but also in capacity planning, and (b) current values of parameters that cause the steady state error (i.e., additional capacity required, time to invest in and build undersea cables) are monitored and socialized with the partners, and efficient action is mandated accordingly.

Policy Alternative
Nations that are connected at their borders via roadways and railways ought to lay fiber connectivity when new road and railway infrastructure is built, to reduce load on undersea cable infrastructure, and improve response to disruptions.
Understanding “Cyber Conflict”

Aadya Shukla (Fellow, STPP & Harvard-MIT Minerva Project)

Belfer Center of Science and Technology, Kennedy School of Government, Harvard University
Advisors: Prof. V. Narayanmurti, Prof. J. Nye, Prof. N. Choucri, Dr Roger Hurwitz, Prof. S. Madnick

1. Motivation

“Oxford English Dictionary defines Control as “a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system”. It is important to understand what processes, risks and relationships influence the degree of control and conflict when interests of multiple stakeholders dominate.

2. Problem

Emergence of cyber as the new arena for conflict raises three basic questions:

a) What qualifies as a Cyber Conflict? (multiple definitions exist).

b) Does intervention of cyber in conflict life-cycle requires new models to decipher control points in cyberspace?

c) What is different between conflicts in kinetic and cyberspace?

3. Solution

Application of USE CASE ANALYSIS to understand the mechanics of cyber conflict to arrive at a model of cyber conflict in a data driven manner (analysis of events since 2001). In Software Engineering domain use case analysis is used as an established tool to define processes and roles a stakeholder employs to interact with a system, and system’s response to the user stimulus.

4. Building The Model

Hypothesis: For a conflict to qualify as cyber conflict layers of cyberspace must act as a major control points for its introduction, adaptation, horizontal escalation and containment.

5. Initial Findings and Value

a. Cyber conflict uses all layers of cyberspace in order to qualify as a valid instance of cyber conflict.

b. Confusing “cyber conflict” with the “conflict using cyber” can be misleading.

c. In cyber conflict the dynamics of interaction among conflict stages does not always follow the stages as understood in the kinetic space.

d. The model helps to define the relationship between actors and layers of cyberspace as control points to suggest mitigation approach.

Thank You!

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.

Also, I extend my deepest appreciation to the many members of the Internet community that have contributed their time, interest, and feedback to this research. This work would not be possible without their help and support.
Anonymity Networks: Platforms For Emerging Cyber International Conflict.

MIT Political Science Department
Advisor: Dr. Nazli Choucri
Mina Rady, Visiting Student

Conflict dynamics between governments and their populations have amplified across the last decade. With the emergence of cyberspace, these dynamics have transported from the physical realm to take place across the cyber domain. Anonymity Networks became a playground for such conflicts as they enabled citizens to overpower the classical methods of law enforcement on the cyberspace. Therefore, they witnessed actions and reactions between Governments, Populations and Computer Security researchers. In this paper we delineate escalations of this cyberconflict by studying two famous cases of such conflict, simple case: Egypt and more sophisticated case: Iran. We take Tor network as the anonymity network that is subject of investigation due to its pervasiveness. We conclude with cataloging the range of actions that each actor can take to retaliate via anonymity networks. We, then, lay out the foundation for future work that delineates the International Relations aspect of Anonymity Networks.

Research Organization

Part 1:
- Basic background on operation mechanisms of Anonymity Networks.
- We describe the operational mechanism and components of “Tor Network.”
- Then we introduce our data sources (Tor Network different statistics and Google Trends) and we show Tor’s access rates correlate demographically with states level of censorship.

Parts 2 and 3:
- We track the exportation of political tension in Egypt and Iran from the physical realm to the Cyber-anonymity realm. We trace the development

Part 4: General Observations of actions/reaction and Conclusions.

1. Basic Proxy Technology: Intermediate Proxy Server is used to anonymize traffic from both sides of the connection.

A Network of Volunteering Proxy Servers

Client IP Address 1

Proxy Server IP Address 3

Server IP Address 2

Client IP Address 2

Server IP Address 3

Data packets travel across three proxy servers to mask IP address of the source and of the destination.

Application: Overcome censorship that is based on IP addresses of destination web sites (Most common form of ISP based censorship)

2. Simple Case: Egypt

Egypt-specific statistics of directly connecting users to Tor network (From: January-February 2011)

3. Complex Case: Iran

4. General Conclusion*

*(More elaborate Conclusion in Paper)

Reconfiguration of Roles:
1- Individuals: are granting power to overcome state censorship.
2- Individuals: are granting power to preserve anonymity by donating bandwidth and proxies worldwide.
3- Governments: are enforcing authority of censorship, attribution and retribution on anonymous Networks, mostly with collateral damage.
4- Non-Profit Org: Produce and Support Anonymous Networks with high degree of scalability and decentralization.

This work was funded by the Office of Naval Research under award number N00014-09-1-1059. 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. I also extend my deepest appreciation to the many members of the Internet community that have contributed their time, interest, and feedback to this research. This work would not be possible without their help and support.
When Virtual Issues Become Real World Actions
Case Study: The Influence of Social Media Narrative Building on the 2011 London Riots

James Houghton, Research Associate, MIT Sloan School of Management

Social media messaging builds narratives

Models show how decisions shape real world events

Narratives compete to influence decisions

Integrating rich social media data can predict outcomes

Special Thanks To:
Who Controls Anonymity: Control Point Analysis of The Onion Routing Anonymity Network (Tor) [Working]

MIT Political Science Department
Advisor: Dr. Nazli Choucri
Mina Rady, Visiting Student

Explorations in Cyber International Relations 
Massachusetts Institute of Technology
Harvard University

Workshop on People, Power, and Cyber Politics 
November 6 and 7, 2012 
MIT Media Lab

Anonymity networks have played major roles in both good and bad ways. By offering a way to use the Internet that shields the cyberer from their target, they become well defined targets of surveillance, cybercrime, and cyber terrorism. The defending who can be seen in to undermine the integrity of such networks in the coming are critical in what we maintain integrity. The former, an election that acts as a disruptive concern for art and artists, and art, which is a key to undermining the potential of our future. This is in order. In this paper, we introduce our major new model in this problem: we decompose the operation of a major anonymity network (Tor) across internet layers. Then we deploy control points that are the core of our work. We develop a method for tracking and investigating different layers that can be taken at each layer with actors who are previously unknown to the existing and newly identified organizations and actors. We use Tor network model as the subject of our investigation due to its destructive potential. This work is based on nation technical and non-technical papers surveyed. The network is in terms of their technical evolution and known vulnerabilities.

Research Organizations:
1. We visualize the network necessary to establish the routing connection and the level of monitoring in common as follows:
2. By surveying numerous papers and national policies on "anonymization" of Tor network, we examined our analysis with two types of control capacities:
   A. Network Survivability Control (i.e. actions that can be taken to the existence of the network)
   B. Anonymity Threatening Control (i.e. actions that can be taken to undermine the purpose of the network).
3. Then we map actors that already fit or potential can exploit each network layer in the table provided in the right to avoid the control action and outcome.

Conclusions (Working):
Last layer seems to be significant. However, most anti-control actions have been taken solely by China. For the rest of the world, it is very expensive to impose such actions without collateral damage to network integrity (e.g. an Iranian attempt to block SSL packets).
- Control actions of individuals can be very influential if taken collectively by groups of proxy operators. The larger the group, the greater the influence.
- No control action so far was an explicit collective action by Tor users.
- Collective action by individuals can overpower a single state's control actions.

Future Research:
1. Map the actions within the Internet Layers Framework of Cybersecurity Levels of Analysis and Internet Layers (CICLICLIC)
2. Investigate lateral penetration mechanisms to global distributions of network (CICLICLIC)
3. Investigate territorial boundaries of various anonymity networks

Internet Exchange Level Traffic Analysis
**Traffic Analysis:**

- Port: 80
- IP: 192.168.0.1

*This work is funded by the Office of the Director of National Intelligence under award number 2013-19-0192. No official endorsement should be inferred. Omissions of those who do not necessarily reflect the views of the Office of the Director of National Intelligence.
PARTICIPANTS
Poster Session and Workshop

Michael M. Afergan
Senior Vice President & General Manager
Site Division
Akamai

Gaurav Agarwal
Supply Chain Consultant
Bayer A.G.

Mattias Bagge
Manager for Research and Technology
FMV Representative
Swedish Armed Forces Research and Technology Group
Swedish Defence Materiel Administration

Samiah E. Baroni
Faculty
School of Science & Technology
Intelligence
National Intelligence University

Colonel Atin Basu Choudhary
Professor of Economics and Business
Virginia Military Institute

Peter Brecke
Assistant Dean for Information Technology
Ivan Allen College of Liberal Arts
Associate Professor
Sam Nunn School of International Affairs, Georgia Institute of Technology

Joel Brenner
Of Counsel
Cooley LLP

Marijke Breuning
Professor of Political Science
University of North Texas

Jarod Bullock
Analyst
U.S. Department of Defense

Blaise Calandro
Software Technology Planning Manager
Missiles and Fire Control
Lockheed Martin

José Campos
Director
Microsoft Corporation

Jessica Choi
Undergraduate Student
Wellesley College

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

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

Susana Cordeiro Guerra
PhD student
Department of Political Science
Massachusetts Institute of Technology
Alan Davidson  
Visiting Scholar  
Engineering Systems Division  
Massachusetts Institute of Technology  
formerly of Google  

Rodrigo Davies  
Research Assistant  
Center for Civic Media  
Massachusetts Institute of Technology  

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

Thomas Dillingham  
National Security Fellow  
Harvard Kennedy School  

Jiordan Diorio  
Cyber Security Strategy  
U.S. Department of Defense  

James Dougherty  
Adjunct Senior Fellow for Business and Foreign Policy  
Council on Foreign Relations  

Captain Dave Duffie (ret.)  
Vice President and Manager  
Ametek  

Ryan Ellis  
Postdoctoral Research Fellow  
Science, Technology, Public Policy Program  
Information and Telecommunications Public Policy Project  
Harvard Kennedy School  

CW2 Judy Esquibel, U.S. Army  
Bravo Company, 781st Military Intelligence (MI) Battalion  

Dighton Fiddner  
Assistant Professor  
Department of Political Science  
Indiana University of Pennsylvania  

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

Allan Friedman  
Fellow in Governance Studies  
Research Director, Center for Technology Innovation  
Brookings Institute  

Connie Frizzell  
National Security Fellow  
Harvard Kennedy School  

Wendy Garrity  
National Security Fellow  
Harvard Kennedy School  

Fabio Ghironi  
Associate Professor of Economics  
Boston College  

Daniel Goldsmith  
Principal Consultant  
PA Consulting  

Joshua Haines  
Assistant Group Leader  
Cyber Systems and Technology Group  
MIT Lincoln Laboratory  

Major Scott Handler, U.S. Army  
Assistant Professor of International Relations  
U.S. Military Academy  

80
Melissa Hathaway  
Senior Advisor  
Explorations in Cyber International Relations  
Belfer Center for Science and International Affairs  
Harvard Kennedy School  
President, Hathaway Global Strategies LLC

Robert Herklotz  
Program Manager  
AFOSR/RSL  
Air Force Office of Scientific Research

Jonah Hill  
Consultant  
Monitor 360

Matthew Hoisington  
Office of Legal Affairs  
United Nations

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

Shirley Hung  
Postdoctoral Associate  
Computer Science and Artificial Intelligence Laboratory  
Massachusetts Institute of Technology

Roger Hurwitz  
Research Scientist  
Computer Science and Artificial Intelligence Laboratory  
Massachusetts Institute of Technology

Lieutenant Colonel Deron R. Jackson, U.S. Air Force  
Assistant Professor  
Deputy Department Head, Department of Political Science  
U.S. Air Force Academy

Joseph Kelly  
Chief, Cyber Intelligence  
Office of the Under Secretary of Defense  
U.S. Department of Defense

Lucas Kello  
Research Fellow in Science, Technology and Public Policy Program  
Belfer Center for Science and International Affairs  
Harvard Kennedy School

Gabriel Koehler-Derrick  
Associate  
Combating Terrorism Center  
U.S. Military Academy

Susan Landau  
Independent Scholar  
Privacyink.org

Irving Lachow  
Research Director  
Center for Information Assurance  
Information  
National Defense University

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

Daniel Lincoln  
Visiting Scholar  
Center for International Higher Education  
Boston College

Igor Linkov  
Risk and Decision Science Area Lead  
US Army Corps of Engineers  
Adjunct Professor of Engineering and Public Policy  
Carnegie Mellon University
Cory Lofdahl  
Senior Scientist  
Charles River Analytics

Olumide Babatope Longe  
Fulbright Fellow  
International Center for Information Technology & Development, College of Business  
Southern University  
Faculty  
Department of Computer Science  
University of Ibadan, Nigeria

Urs Luterbacher  
Emeritus Professor  
International Relations/Political Science  
Institut universitaire de hautes études internationales

Stuart Madnick  
John Norris Maguire Professor of Information Technology, Sloan School of Management  
Professor of Engineering Systems, School of Engineering  
Massachusetts Institute of Technology

Jessica Malekos-Smith  
Undergraduate Student  
Wellesley College  
Cadet, U.S. Air Force Reserve Officer  
Training Corps, Massachusetts Institute of Technology

John Mallery  
Research Scientist  
Computer Science & Artificial Intelligence Laboratory  
Massachusetts Institute of Technology

Cheri Markt  
Engineering Excellence Project Manager  
Lockheed Martin

David Martinez  
Principal Staff  
Communication Systems and Cyber Security Division  
MIT Lincoln Laboratory

Tim Maurer  
Program Associate  
Open Technology Institute  
The New America Foundation

Colonel Tom McCarthy, U.S. Air Force  
Deputy Chair  
Professor  
International Security Studies  
Air War College: Air University

C. Lawrence Meador  
Chairman  
MGI Strategic Solutions

Toufic Mezher  
Professor  
Engineering and Systems Management  
Masdar Institute

Mike Mock  
Emerging Technology SME  
Defense Intelligence Agency

Vivek Mohan  
Research Fellow in Information and Communications Technology Public Policy  
Belfer Center for Science and International Affairs  
Harvard Kennedy School

Michael Morales  
Software Lead  
Intelligent Microgrid Programs  
Missiles and Fire Control  
Lockheed Martin
Clay Morgan
Senior Acquisition Editor for
Environmental Sciences, Political Science
and Bioethics
The MIT Press

Allen Moulton
Research Scientist
Center for Technology, Policy, and
Industrial Development
Massachusetts Institute of Technology

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

Kevin O’Connell
President and CEO
Innovative Analytics & Training

Taylor Owen
Research Director
Tow Center for Digital Journalism
Columbia School of Journalism

David Palés
Fellow, Advanced Study Program
Massachusetts Institute of Technology

Mina Rady
Visiting Student
Department of Political Science
Massachusetts Institute of Technology

John Randell
Program Officer for Science Policy
Associate Director for Science Policy
Initiatives
American Academy of Arts and Sciences

David Robinson
Visiting Fellow
Information Society Project
Yale Law School

Masroor Sajid
Information Security/Process
Management Consultant
Massachusetts Institute of Technology

Vic Salemme
Vice President SQA
State Street Corporation

Harvey Sapolsky
Former Director, MIT Security Studies
Program
Professor of Public Policy and
Organization, Emeritus
Massachusetts Institute of Technology

David Saul
Senior Vice President; Chief Scientist
State Street Corporation

Molly Sauter
Research Assistant
Center for Civic Media
Massachusetts Institute of Technology

Mikael Schönström
Project Manager for Command, Control &
Communication Systems
Swedish Defence Materiel Administration

Lieutenant Colonel Robert Schubert,
U.S. Marine Corps
Defense Intelligence Agency

Dan Schutzer
President
Financial Services Technology
Consortium
The Financial Services Roundtable

Michael Sechrist
Vice President, Corporate Information
Security
State Street Corporation
Enrique Shadah  
Senior Industrial Liaison Officer  
Office of Corporate Relations Industrial Liaison Program  
Massachusetts Institute of Technology  

Captain Benjamin Shearn, U.S. Air Force  
Instructor  
U.S. Air Force Academy  

Howard Schrobe  
Principal Research Scientist  
Computer Science and Artificial Intelligence Laboratory, MIT  
Program Manager  
Information Innovation Office  
DARPA  

Aadya Shukla  
Research Fellow in Science, Technology and Public Policy Program  
Belfer Center for Science and International Affairs  
Harvard Kennedy School  

Stuart Shulman  
Assistant Professor  
Department of Political Science  
University of Massachusetts Amherst  

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

Jeffrey Silverman  
Chief Investment Strategist  
Co-founder and Chairman  
Agman Partners  

Eugene Skolnikoff  
Professor of Political Science Emeritus  
Massachusetts Institute of Technology  

Evann Smith  
Doctoral Candidate  
Department of Government  
Harvard University  

Michael Specter  
Associate Staff  
MIT Lincoln Laboratory  

David Talbot  
Senior Editor  
MIT Technology Review  

Major General Tatsuhiro Tanaka (ret.)  
Japan Ground Self Defense Force Fellow  
Harvard University Asia Center  

Wayne Thornton  
Senior Scientist  
Charles River Analytics  

Tim Tobiasz  
National Security Fellow  
Harvard Kennedy School  

Zachary Tumin  
Special Project Assistant, Science, Technology and Public Policy Program Director  
Belfer Center for Science and International Affairs  
Harvard Kennedy School  

Chintan Vaishnav  
Research Associate  
Sloan School of Management  
Massachusetts Institute of Technology  

Gili Vadin  
Undergraduate Student  
Harvard College  
Research Assistant  
Berkman Center for Internet & Society  
Harvard University
Takashi Watanabe  
Associate  
The Weatherhead Center  
Harvard University

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

Linton Wells  
Director  
Center for Technology and National Security Policy  
National Defense University

Jody R. Westby  
CEO and Founder  
Global Cyber Risk LLC

Steve Whittaker  
Principal Consultant  
BT Exact Technologies  
Research Affiliate, MIT Media Laboratory

Josephine Wolff  
PhD Student  
Engineering Systems Division  
Massachusetts Institute of Technology

Randall Wright  
Senior Industrial Liaison Officer  
Massachusetts Institute of Technology

Yifan Wu  
Undergraduate Student  
Harvard College

Colonel William Young, Jr., U.S. Air Force  
PhD Student  
Engineering Systems Division  
Massachusetts Institute of Technology

Dorothy Zinberg  
Lecturer in Public Policy/Senior Research Associate  
Belfer Center for Science and International Affairs  
Harvard Kennedy School

Ethan Zuckerman  
Principal Research Scientist  
Media Laboratory  
Massachusetts Institute of Technology