Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

ECIR WORKSHOP ON

People, Power, and CyberPolitics

Co-Sponsored by

Council on Foreign Relations

December 7 and 8, 2011
MIT Faculty Club &
MIT Media Laboratory

Executive Summary
Poster Session
Participants

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.

EXECUTIVE SUMMARY

Introduction

For the first time in human history, a large number of people from all parts of the world participate in a new arena of information and communication of global scale and scope. Almost everyone everywhere has the opportunity to participate in cyberspace. Few states, if any, are able to control the flow of information via cyber venues that cross their boundaries. All states are recognizing, to one degree or another, that people matter – and sometimes they matter a lot.

The diffusion of social networking practices and growing use of mobile technologies – notably social media for personal or political uses – has further reinforced the potential power of entities other than the state. All of this affects the nature of the international system – structure, process, and participation – while shaping an emerging and rapidly growing global civil society that transcends traditional territoriality and sovereignty.

This Workshop focused on six questions:

- What has changed, if anything, for people power and global politics?
- How do we listen to messages?
- What are the new threats and opportunities for governance?
- What are the impacts of cyberpolitics on democracies?
- What can we learn from experience on social media and social action?
- Are there new visions for the future?

This *ECIR* workshop is the second in a series of sustained deliberations and explorations involving leading individuals in academia, government and business. The result of this workshop provides a baseline for an evolving understanding of people, power and cyberpolitics. The *ECIR* Project seeks to develop a new multidisciplinary field of scientific inquiry to provide the theories, tools, and modes of inquiry relevant to unprecedented, new, complex, and rapidly changing conditions created by the construction of cyberspace.

1. People Power & Global Politics: What has Changed?

The balance of power is shifting from the West to the East. The primacy of the Western powers is being challenged by a 'diffusion of power' over a variety of states (east/west, developing/developed) and to a variety of non-state actors (traditional and cyber) – all enabled by technologies which flatten hierarchies and create more network-like structures. Information Communication Technologies (ICT) and the lower barriers to access to these ICT tools for use in political action have caused a fundamental shift in the future of 'power' – and the study and analysis of it. The under-rated but very important impact of social media's ability to carry video messages is an example. The connections between those people who are on social media inside repressive

regimes and the diaspora community outside of the country are an important element in the role of social media in civic activities. There is a growing, central tension between transparency and accountability – as different ICT technologies and platforms are subjected to a variable degree of control.

Research priorities include a focus on the negative aspects of social media platforms and their impact on democracy, the potential misuses of technologies by states for surveillance, and the threat to the Internet by authoritarian governments. Communications through social media can move at an extraordinary speed to get the story out and coordinate action.

2. How do we Listen?

What happens when people get bad, irrelevant, or unimportant messages? There are large differences in rejection rates of partisan rumors by partisans, but not on non-partisan rumors. Direct contradiction works well in the short term, but people don't retain that, because of more familiarity with the myth than the counter-evidence.

People have been communicating all the time but the notion of privacy has changed. For example, social media posts have cut into email traffic and made it public. The young have a broadcasting capability, and the consequences are unknown.

Opinions of activists now number in the millions of political opinions spread globally by ICT on a daily basis. Various Social Language Processing techniques can be used in the strategic analysis of individual speeches or large collections of social media data. Three issues are relevant to "how we listen:" (a) The explosion of data – finding answers in the explosion of data is difficult, (b) Research methods – basic vs. rather abstract models with practical applicability are important, and (c) Quality of translation –different sets of methods can be applied to the original language or translated language; human language is incredibly subtle.

There are enormous, emerging social science opportunities ahead – representing a historical shift from studying to understanding and solving big societal issues and problems. Social scientists do not care about the needle in the haystack (individual document classification); they care about the haystack (category proportions).

3. What are Threats and Opportunities for Governance?

The fundamental difference of the Internet from other communication mediums is in *changing attitudes* and *getting people to act*. It is affecting the propensity of people to act during a coup or conflict. The source of credibility of the information and the fact that the sheer amount of information and images can sometimes quickly contradict one another can impede action.

There are two generic ways of conceptualizing the effect of communication on the individual: (a) through a change in attitude, and (b) through a propensity to act on your attitudes. The propensity to act on one's attitudes can be influenced by the low barriers to entry. Given the increasing transparency in our lives, both positive and negative, government is both a dis-intermediary and an

intermediary. The matter of publicity turns the conversation to the notion of information that is not necessarily hidden by a government, but information that a state actor is not anxious to make public.

4. What are the Impacts of Cyberpolitics on Democracies?

Four hypotheses help shape the discourse:

- *Analogical thinking hypothesis:* some of the thinking in the field of politics and technologies tries to draw the analogy between the experience of technology and the technological domain. There is a plausible reason why this hypothesis is wrong: a fundamental difference in demand.
- *Disintermediation hypothesis*: large organizations are less relevant because they reduce the organizational friction and coordination costs.
- *Public sphere hypothesis:* allows more people to communicate, reducing the domination of the public sphere by capital and capital equipment.
- *Transparency hypothesis*: make information more available, more credible and legitimate.
- *Organizational amplification hypothesis:* amplifies the functions of existing organizations gradually. Social media may allow for the sharing of this knowledge – which misses the fact that there are resources necessary for collective action *in addition to information*.

Methods are being developed for individuals to voice their dreams and articulate their ideas about how society should operate. The role of social media and its use by activists in relation to government control is important. However, it is one of the tools in political activity or used with the knowledge of being monitored. This means that communications are adaptive.

Two additional issues address broader processes: *(1) Social media mobilization theory*—the basic premise is that it just takes a click of a mouse to use a mobile phone is suspect because the ability of a government to shut down a system in the moment of political turmoil is unprecedented. (2) *Attention thesis*—Facebook is thoroughly monitored by state actors; and media is posted, translated and made available to media organizations by 'bridge bloggers' who then broadcast it; (i.e., Al-Jazeera).

5. What can we Learn from Experience?

We now know that the future is not just about technology – but about socio-technology. Authoritarian regimes have realized the power and danger of social media. As a result, censorship is being stepped up. The challenge ahead is that while we can generally agree with current causes taken up by those activists, we are arming with these subversive cyber tools: what happens when we don't agree with what they do?

The issues of risk (i.e., personal risk), relationships and the role of the Internet become salient. The Internet lowers the cost of communication and the ability to penetrate networks and increases the number of weak ties available to activists. Social media accelerates the spread of information and

its penetration of strong tie networks. In questioning why there is an assumption that the Internet creates only weak links, findings indicate that an activist will show up with his or her brother rather than someone he or she is friends with on Facebook.

The mainstream media enhanced the credibility of social media content because television broadcasts acted as quality control. For example, social media did not cause the Egyptian uprising, but it did impact the complex networks through which it occurred. New technologies are being developed to connect with the world of policy makers.

6. What will the "Next Generation" of Challenges Bring?

There is something very powerful about the Internet, even though the mainstream experience is trivial. At least three visions of the future can be identified:

Vision 1: The Future is one with more offense and defense

There are important fallacies in the study of cyberspace – namely, that the environment is reactive and that, in principle, a bordered Internet is in fact possible. The dominance of 'offensive postures' in cyberspace is largely true. Offense beats defense in cyberspace. If we cannot do good offense, we cannot do good deterrence – which leaves a circular state of affairs. There is a strong offensive orientation in governmental thinking. Despite the systemic difference between autocratic and democratic governments, both types of government are moving in the direction of being more suppressive.

Vision 2: The Future is created by us today

The more important question is this: *who* is driving the future of the Internet? The domain name system (DNS) is going to be a contentious area regarding control because of the ability to control the user's experience. In short, we must *buy the future we want*. Those who are funding the future are also heavily involved in the design process. We should be asking, "Who should be shaping the future Internet design?" In a mutual aid framework, it is a question of what granularity, how big the group is and whether the countries would be willing to pay.

Vision 3: The future depends on emerging technologies

The baseline design of the Internet was one of decentralization both from a technical point of view and from a political point of view. That baseline is rapidly changing, with the rise of centralized applications such as Twitter or Amazon. We must figure out how to take a politically charged matter and make it an engineering matter (or a technical problem). There is an abject need to focus on the 'future of technology' as well as the 'changes in society brought on by technology.' It is important to identify where the points of tectonic shifts are in the technology space.

End Note

This Executive Summary represents the general "state of the art" as seen by the Workshop participants. It also provides something of a baseline against which to track future developments. The discussion points new relevance of people in international relations, potential changes in

power distributions, and emergent complexities for cyberpolitics. As we move forward, we must address the following questions: Who controls cyberspace? What are emergent forms and uses of social media that influence—enable or impede— how people-power unfolds over time? What are the emergent contours of cyberpolitics? How will these affect power relations worldwide? There are many more questions, to be sure, however, these are among the most pressing.

POSTER SESSION: CONTENTS

Establishing the Baseline: A Framework for Organizing National Cybersecurity Initiatives

Shukla, Aadya, Fellow, Harvard Kennedy School

Finding Order in a Contentious Internet

Sowell, Jesse, PhD Candidate, ESD, MIT

Learning Legal Principles to Enable Law at Cyber Speeds

Finlayson, Mark A., PhD Candidate, EECS, MIT

Representing Cyberspace Using Taxonomies and Meta-data Analysis Cyber-enabled Loads & Capacities

Daw Elbait, Gihan, Postdoctoral Associate, MIT

Accountability at the Application Layer

Josephine Wolff, Technology & Policy Program

Start: September 2010
Research Group: Advanced Network Architecture Group in CSAIL; Explorations in Cyber International Relations, MIT-Harvard
Thesis Advisor: Dr. D. Clark, Senior Research Scientist

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

Malicious actors in cyberspace — be they computer-savvy teenagers or nation state-sponsored military forces — can be extremely difficult to identify definitively. This, in turn, can make it tricky to hold them accountable for their actions or take any kind of effective punitive or retaliatory measures. Many application-layer online identities do not have sufficiently strong accountability mechanisms embedded within them to deter misbehavior.

> "We need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable."
> — Mike McConnell,
> Former U.S. Director of National Intelligence

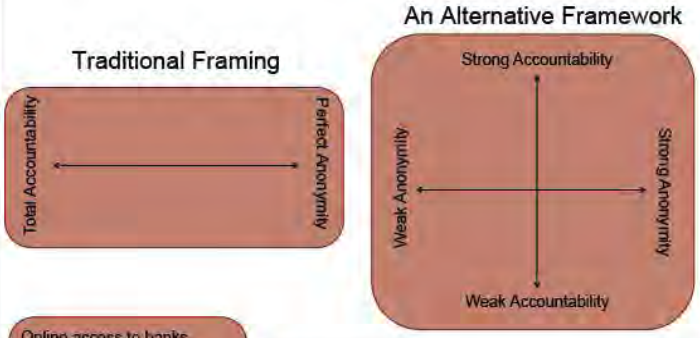
Participants in the ongoing debate over how accountable these online identities should be fall roughly into two opposing camps: those who believe we should be able to trace any online activity back to a specific user and those who believe we should protect Internet users' privacy and anonymity at all costs. Advocates on both sides of this debate often subscribe to the belief that there is a direct tradeoff between the accountability and anonymity of online identities, that to have more of one necessitates having less of the other.

Key Questions

- What are the implications of implementing accountability mechanisms at the application layer of the Internet, rather than the network layer?
- Are accountability and anonymity a zero-sum game for online identities, that is, must every effort to increase accountability necessarily decrease anonymity?
- If not, what is a more accurate way to characterize the space between perfect accountability and complete anonymity for Internet identity schemes?
- What types of identity schemes can be implemented to provide different combinations and kinds of anonymity and accountability suitable to various online contexts?

The Research

A New Framework for Accountability



Populating the Quadrants

Online access to banks, military networks, nuclear power plants, etc., often requires strong authentication systems that provide strong accountability but no anonymity.

Identities for applications like e-mail and Second Life may combine elements of anonymity and accountability to suit their needs and design since they derive benefits from both of these traits.

Malicious actors who are identified may still be difficult to hold accountable if they are located outside the aggrieved party's jurisdictional boundaries.

Services like Tor that provide users with very strong identity protection and virtually untraceable services but do not include a serious accountability component.

Preliminary Results

- **Accountability points of control in online applications**
  - Application designers (Linden Lab, Facebook, Blizzard)
  - Individual end-users
  - Legal regulations (CAN-SPAM Act, cyberbullying laws)
  - Intermediary control points:
    - Participatory governance structures (e.g. Wikipedia moderators and bureaucrats)
    - Email server administrators
    - Internet Service Providers
- **Creating costly identities**
  - The problem of "discardable identities" online stems from how cheap and easy it is to create new ones
  - In order to make these identities less discardable, we must find ways of imposing some type of cost on these identities, two broad possible types of costs include:
    - Financial costs (joining fees)
    - Time costs (reputation systems, initiation periods)
      - These costs can also serve as signals to other users about a person's investment in their identity
- **Trade-offs between investment in identity and privilege**
  - Firmer, better established identities can bypass costs of application action/privilege
  - Users with newer, or less well established identities are rate-limited in their actions, or must pay some fee for the same privileges
    - Allows users to decide on their own personal preferences for anonymity and tailor their online identities to these preferences
- **Conditional anonymity schemes**
  - Identity escrow (identity is provided to administrator/ central authority but kept secret at their discretion)
    - Trusted third-party identity management systems
  - Cryptographic identity protection

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

Comparative Analysis of Cybersecurity Metrics to Develop New Hypotheses

D. Fisher, S. Madnick, N. Choucri, X. Li, and J. Ferwerda, Massachusetts Institute of Technology

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Abstract

Few Internet security organizations provide
comprehensive, quantified, and reliable quantitative analysis,
especially in the international perspective
across multiple countries, multiple years, and multiple categories.

Organizations ask why they should spend valuable time and resources collecting and standardizing data. This report aims to provide an encouraging answer to this question by demonstrating the value that even limited metrics can provide in a comparative perspective.

We present some findings generated through the use of the Explorations in Cyber Internal Relations (ECIR) Data Dashboard. In essence, this dashboard consists of a simple graphing and analysis tool, coupled with a database consisting of data from disparate national-level cyber data sources provided by governments, Computer Emergency Response Teams (CERTs), and international organizations. Users of the dashboard can select relevant security variables, compare various countries, and scale information as needed.

In this paper, we present an example of observations concerning the fight against cybercrime, along with several hypotheses attempting to explain the findings.

We believe that these preliminary results suggest valuable ways in which such data could be used and we hope the research will help provide the incentives for organizations to increase the quality and quantity of standardized quantitative data available.

The Data Dashboard

The Data Dashboard consists of a simple graphing and analysis tool, coupled with a database consisting of data from disparate national-level cyber data sources provided by governments, Computer Emergency Response Teams (CERTs), and international organizations. The dashboard was developed to provide historical trend data and news to policymakers, academics, IT professionals and other stakeholders. By consulting the Dashboard, the user can compare trends in various categories in national-level cybersecurity threats and vulnerabilities among several countries and/or regions over time. The Dashboard provides data in five diverse categories:

- Demographic Data: Population, GDP (2000 US $), Electric Power Consumption, Software Piracy Losses, Tertiary School Enrollment
- IT Attributes: # Personal Computers, # Users with Internet Access, # Secure Internet Servers, # Hosts
- Political Attributes: Political Stability Index, Government Effectiveness Index, Rule of Law Index, Polity Index, Militarization Index
- Threat Attributes: Total CERT Reported Incidents, Virus/Worm/Malicious Code/Malware, Phishing/Personal Data Abuse, Scanning, DoS & Integrity Attacks
- Cyber Crime Attributes: Total Cyber Crime Cases, Cyber Crime Damage Dollar Loss, Cyber Crime Arrests, % Cyber Crimes Reported to Police

These data can be manipulated by the user through an online interface available to the general public, and can be manipulated to scale data sets by other attributes.

Case Study: Software Piracy Losses

The data available through the Data Dashboard system are particularly useful in cross-country metric comparisons. In Figure 1 below, the software piracy losses of seven countries are compared; at first sight, it appears that China and the United States have the highest piracy rates.

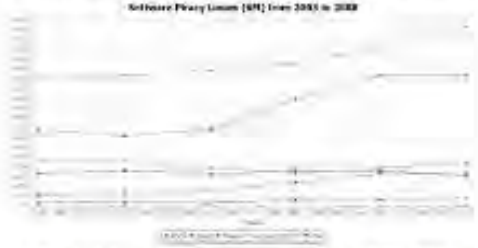


Figure 1: Software piracy losses of seven countries from 2003 to 2008.

The Data Dashboard also allows users to scale existing data by different metrics such as number of personal computers, number of users with Internet access, or other relevant data sets. In the case of software piracy, a more relevant data set may scale piracy losses by number of Internet users, as can be seen in Figure 2 below:

Figure 2: Piracy losses scaled by number of Internet users, 2003 to 2008.

We might expect that different nations would have different levels of enforcement vis-à-vis piracy that may affect the volume of illegal activity. One candidate method to measure this variation is the Rule of Law Index, compiled by the World Bank. Figure 3 makes use of the Data dashboard by utilizing three diverse types of information: software piracy losses, numbers of Internet users, and Rule of Law. Nations with higher Rule of Law should theoretically display lower rates of cyber crime versus countries with less developed legal systems.

Figure 3: Software piracy losses adjusted for Rule of Law per Internet user.

These results suggest that the absolute volume of software piracy has risen over the past decade, with the bulk of activity in a few nations such as the United States and China. The trends affecting piracy rates are more ambiguous, however, with different countries exhibiting different levels and trends. Surprisingly, a country's rate of piracy does not seem to be conditional on whether it is a developed or a less developed country. In almost all of the metrics examined here, Korea and Japan have outperformed, while the United States and Germany have exhibited less positive results. Although isolating the national events that lead to these different trends is difficult, this analysis suggests fruitful avenues for further research should data remain consistently available.

Next Steps

This analysis has sought to accomplish two distinct tasks. First, although Internet security data is scant and scattered across the Internet, we were nevertheless able to identify and illustrate several interesting trends from existing data that shed light on how different nations and organizations are coping with the global rise of cyber crime. Second, our results highlight several inconsistencies and ambiguities in data provided by different organizations, and we believe that relying on these published statistics without the benefit of a rigorous comparative analysis could lead to fundamentally misleading conclusions regarding the international efforts to improve cybersecurity and fight against cybercrime.

Although the data challenges may be interpreted as an argument against using such data sources, our research implies that the dilemmas could be ameliorated through careful analysis and by promoting a minimum level of standardization across Internet security statistics and the contexts within which they are collected. It is also clear through our analysis that an increase in data availability – be it from governments, CERTs, or international organizations – could yield positive effects in both supporting existing scholarship and the expansion into new fields of knowledge related to cyber crime. In spite of the identified shortcomings of the data, it is possible to learn and identify interesting trends using the Data Dashboard.

In the future, as part of the ECIR project, more data sources will be identified and incorporated to increase the effectiveness of the Dashboard project, so that further interesting international cybersecurity relations can be investigated.

Explorations in Cyber International Relations
Minerva Project at MIT & Harvard

This work is funded by the Office of Naval Research under award number N000140910597. 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.

Control through the Layers in the Chinese Internet

Shirley Hung, Postdoctoral Associate

Research Group: Explorations in Cyber International Relations, MIT-Harvard; Advanced Network Architecture Group, CSAIL

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Question

China is often cited as having the world's most advanced Internet censorship and surveillance regime. It garners much attention and sometimes fear in the media and among policymakers, yet most reports focus on specific incidents or capabilities, not the system as a whole. This project seeks to integrate knowledge of the Chinese political system and culture, social dynamics, and Internet technology to better understand how the control system commonly known as the Great Firewall operates. It also serves as a case study in a larger project on diversity of norms on the Internet around the world.

Methods and Sources

Owing to the interdisciplinary nature of the research, no single methodology applies. The bulk of the research is qualitative, combining institutional theory with an area-studies understanding of the Chinese political system, culture, and society. At present the technical research relies upon secondary sources, primarily computer scientists who attempt to reverse-engineer the Great Firewall.

Sources include Chinese government reports and statements, Chinese and Western media, NGOs, etc. Future research should include interviews with policymakers and those involved in implementation.

Preliminary Findings

Control exists at every layer of the Internet, growing more fine-grained at the top

- **Users**
  - Arrests and disappearances of bloggers and dissidents
  - Attacks on journalists and dissident email accounts
  - Online surveillance: "Big Mamas", 110 Cyber police, 50-cent gangs
- **Information**
  - List of "Approved Media News Sources"
  - Only state-owned outlets can post Internet video
  - Internal third-party monitoring
- **Application**
  - Consumer device controls: Green Dam, SIM chip registration, registration at Internet cafes
  - Most Web 2.0 applications blocked
  - Favor open source platforms
  - Promotion of domestic alternatives: Taobao, Alipay, QQ, Baidu, Weibo, Renren
- **Logical**
  - 8 ISPs with connections to foreign Internet backbone, most state-owned, e.g., China Telecom, China Unicom
- **Physical**
  - Access providers
    - State-owned infrastructure: 8.3M km of fiber
    - $830B spent from 1997-2009 on Internet infrastructure
  - Relationships with equipment providers: Huawei, Cisco, COTS DPI producers

The system reflects the political structure and government priority of social stability

- Three-part structure with overlapping jurisdictions and responsibilities
- Implementation responsibility delegated downward and outward to companies and society
- Internet control relies upon the panopticon effect and deterrence effect of high-profile cases

Future Research

This paper was originally intended only to gather existing research into a coherent primer on the control capabilities and mechanisms of the Chinese government. Further avenues for research include:

- Exploring the variety of views within the Chinese government on how to manage the Internet and international pressure to loosen censorship
- Understanding the role of social media within the Chinese Internet landscape. Preliminary discussions with Chinese policymakers suggest significant concern and little consensus on how to proceed.
- Mapping the technical landscape of China's extensive monitoring system. This will most likely require collaboration with computer scientists for their technical expertise.
- Conducting interviews with government officials, advisers, Track 2 policymakers, dissidents, bloggers and other social media figures, corporate figures including those with day-to-day experience with Internet control requirements, etc.

Acknowledgements

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.

The Coordinates of Cyber International Relations

Chintan Vaishnav, Post-doctoral Associate

Start: January 2011
Research Group: Explorations in Cyber International Relations, MIT
Advisors: Prof Nazli Choucri, Dr. David Clark

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

As the Internet and International Relations become increasingly interwoven, the properties of information goods such as information security, control, or freedom, or those of international activities such as trade, or diplomacy must be framed in the context of emergent behaviors of a system where the Cyberspace interacts with traditional IR. *The purpose of this research is to create a foundation for such understanding by conceptualizing the hitherto separate domains of Cyberspace and International Relations into an integrated system, to analyze the fundamental interdependencies between the two domains, using methods from systems analysis.*

Methods

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

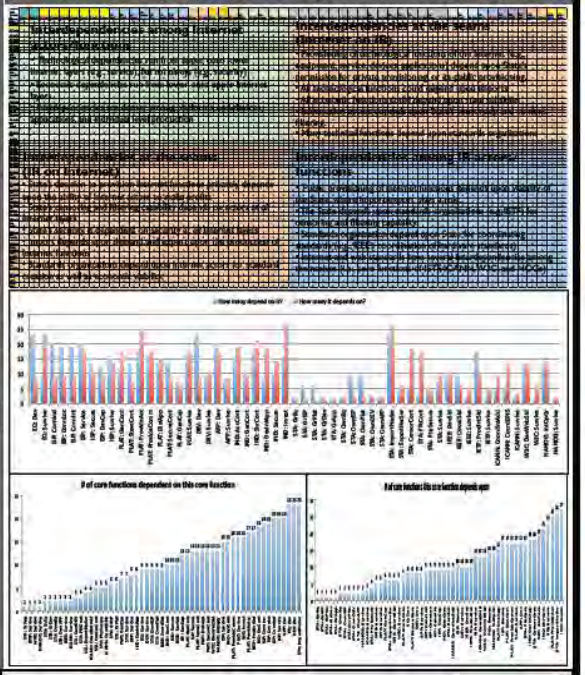
- Qualitative Matrix
- Binary Matrix
- Logical Matrix

The Research

Internet Actor	Abbreviation	Core Function
Equipment Providers	EQ: Dev	Design and Develop Network Equipment
	EQ: Survive	Generate funds to survive
ISPs	ISP: ConnInd	Connect with Individuals, Businesses, and Platforms
	ISP: ConnLoc	Connect with domestic ISPs
	ISP: ConnInt	Connect with the International backbone ISPs
	ISP: Service	Provide Internet service
	ISP: Secure	Secure links and servers
	ISP: DevCap	Develop capacity to meet demand
	ISP: Survive	Generate funds to survive
Information/ Communications/ Applications Platforms	PLAT: GenCont	Generate content
	PLAT: StoreCont	Store content
	PLAT: ProvideAcc	Provide access to content
	PLAT: ProvideComm	Provide communications platform
	PLAT: DistApp	Distribute Applications
	PLAT: SecureCont	Secure Content
	PLAT: GenCap	Develop capacity to meet demand
	PLAT: Survive	Generate funds to survive
Device Makers	DEV: Dev	Design and develop end devices for communications
	DEV: Survive	Generate funds to survive
Application Providers	APP: Dev	Design and Develop Internet Applications
	APP: Survive	Generate funds to survive
Individuals	IND: AccCont	Access Content
	IND: GenCont	Generate Content
	IND: ShrCont	Share Content
	IND: DevIntApp	Develop Internet Applications
	IND: Secure	Secure Links/Content
	IND: Invest	Invest in Internet Technologies
International Relations Actor	**Abbreviation**	**Core Functions**
State	STA: GrEq	Grant private equipment providers
	STA: GrISP	Grant private ISPs
	STA: GrPlat	Grant grant Information/Communications Applications Platform
	STA: GrDev	Grant private device makers
	STA: GrApp	Grant private application providers
	STA: OwnEq	Own and operate network equipment manufacturing
	STA: OwnISP	Own and operate ISP functions
	STA: OwnPlat	Own and operate Information/Communications/Applications Platforms
	STA: OwnDEV	Own and operate device manufacturing and maintenance
	STA: OwnAPP	Own and operate application development
	STA: ImportHwSw	Import hardware/software products
	STA: ExportHwSw	Export hardware/software products
	STA: CensorCont	Censor content
	STA: FiltCont	Filter content
	STA: PhySecure	Physically secure Internet access, services, and information flows
	STA: Survive	Generate funds to survive
IEEE	IEEE: DevStd	Develop Hardware Standards
	IEEE: CoordStd	Coordinate Hardware Standards
	IEEE: Survive	Generate funds to survive
IETF	IETF: ProdIntStd	Produce Internet Standards
	IETF: Survive	Generate funds to survive
ICANN	ICANN: CoordIntAdd	Coordinate Internet Addresses
	ICANN: CoordDNS	Coordinate the DNS
	ICANN: Survive	Generate funds to survive
W3C	W3C: DevWebStd	Develop Web Standards
	W3C: Survive	Generate funds to survive
NANOG	NANOG: IntOpGr	Identify and Solve Problems of Internet Operations and Growth

Preliminary Results

Matrix of Interdependencies in Cyber International Systems



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.

Cyber-enabled Loads & Capacities

William E. Young, Jr (LtCol, USAF), PhD Student

Start: October 2011
Research Group: Cyber Security; Explorations in Cyber International Relations, MIT-Harvard
Advisor: Prof Stuart Madnick

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

Understanding Cyber Loads on State Resilience

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.

Methods

Qualitative & Quantitative System Dynamics Modeling

- Expand the limits of the Goldsmith, et al Pre-Conflict Anticipation and Shaping (PCAS) model to include cyber load and capacity effects on state resilience

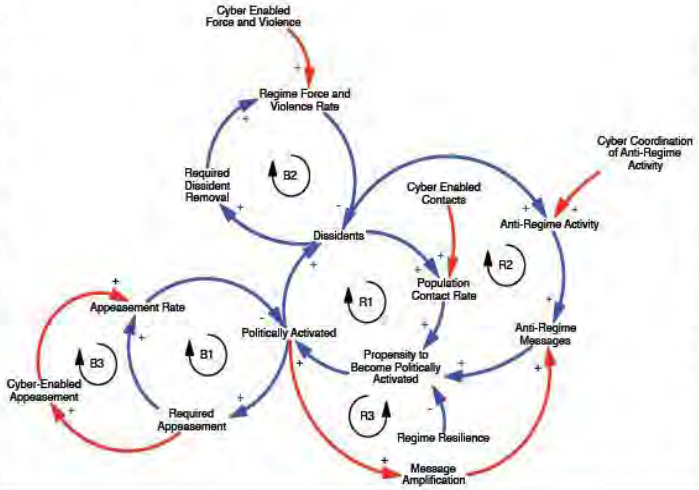
-Use emerging literature to refine the feedback structure in both dissident and state high-level cyber activity to include aspects of:

- message amplification
- appeasement
- coordination of anti-regime activity
- cyber enabled force & violence

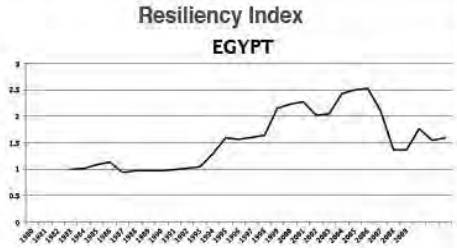
The Research

Loads versus Capacities

High-Level Causal Loop Diagram



Preliminary Results



Methodology: Choucri et al, 2006

Remaining Research

- Test basic model structure against various case studies against broader set of narratives to ensure model still captures the key cyber dynamics
- Model "cyber" loop effects using a suitable proxy with quantitative data to better understand dynamic behavior of loop

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.

This research builds on the outstanding model and research from: Nazli Choucri, Christi Electris, Daniel Goldsmith, Dinsha Mistree, Stuart E. Madnick, J. Bradley Morrison, Michael D. Siegel and Margaret Sweitzer-Hamilton.

Cyber International Relations Theory: Assessing the State of the Art

Robert Reardon and Nazli Choucri, Political Science, MIT

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Objectives

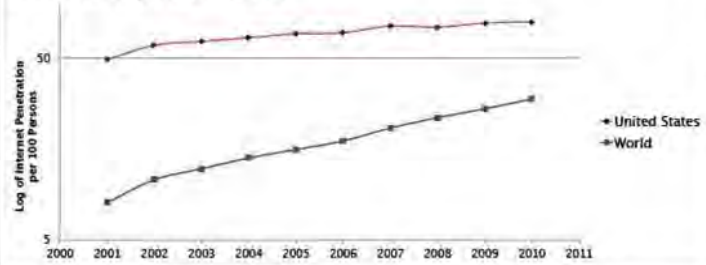
- Outline the scope of the International Relations literature on cyber-related issues with relevance to IR theory
- Frame this literature in terms of its contribution to theory building, theory testing, and issue area
- Assess the strengths and weaknesses of the literature
- Identify gaps and possible avenues for future research

Methods

- Conduct an exhaustive search of the 40 most significant academic and policy-oriented IR journals for articles related to cyber politics
- Limit search to 10-year period 2001-2010, and to journal articles
- Sort articles according to major IR theoretical paradigm, level of analysis, and issue area (where applicable)
- Paradigms: realism, liberalism, institutionalism, constructivism
- Levels of analysis: system level, state level, sub-state level, individual level
- Principal issue areas: cyber security, development, global civil society and the changing role of the state, domestic political change and democratization
- Relevant books, chapters, working papers brought into analysis where appropriate

Why Should IR Theorists Be Interested in Cyber?

Over the past 10 years, Internet use has become an increasingly *international* phenomenon:



A number of recent events have highlighted the significance of cyber in international politics:

- The Stuxnet attack on Iran's centrifuge program
- The use of social media by the Green Movement in Iran, and across the Middle East in the Arab Spring
- Wikileaks
- The rapid development of China's cyber infrastructure, and China's efforts to control access to the Web
- The increasing use of cyberspace as a platform for state surveillance
- The rapid development and spread of mobile communication technologies, and the rise of novel network architectures

Yet surprisingly little scholarship has addressed these issues:

- Between 2001-2010, out of the top 40 academic IR and policy journals, only 10 have published one or more articles related to cyber issues.
- The problem is worst in academia: only 5 academic journals have published articles on cyber.
- The search yielded a total of 27 articles from the 40 journals during the entire decade. 20 of the 27 appeared in policy journals. None appeared in the major political science journals such as APSR.
- Only 6 articles presented research explicitly aimed at building and/or testing new theory to understand cyber politics.
- If the problem is that new theory is not needed to understand cyber politics, then where are articles to advance this claim?

Key Characteristics of the Literature

- Particularly with respect to political organization and domestic political change, findings tend to be unjustifiably sanguine, teleological. For instance, cyber innovation and diffusion is frequently linked to democratization, the development of a liberal civil society, and increased civil and political liberties, without attention to how the same technologies can be used by regimes to restrict freedoms and enhance their control. The best research has sought to show how the two are interlinked.
- Work on cyber security, on the other hand, tends to be unjustifiably alarmist. Cases such as Stuxnet and the cyber attacks on Estonia and Georgia are held up as evidence of the potency of cyber conflict, even as the facts of these cases do not support such claims. The more cautious research has questioned the potential for cyber to be used as a strategic weapons.
- Much of the existing literature seeks to use Internet governance and other cyber issues to rehash debates over globalization and the decline of state authority in international politics. As a result, some promising avenues of research have been under-explored. For example, little has been written on why particular forms of governance or organization in cyberspace has been adopted, or which forces shape these choices.
- Although most treatments of cyber issues adopt either neorealist or liberalist assumptions about international relations, there is a growing body of constructivist research on cyber issues. Overall, this has been a positive development, as constructivism is well suited to examine the role that the content of information in cyberspace might play in international relations.
- Little work has been done on institutionalist approaches to cyber politics. This is remarkable, considering the increasing attention that cyber issues have received in multilateral fora, and the growing efforts being put into crafting international institutions that deal with cyber issues.
- Perhaps because of the small number of articles and the diversity of topics and approaches, there is little cumulativity in the literature.
- No studies engage across issue areas. This is problematic, as there are relevant policy tradeoffs that are poorly understood, such as between promoting civil liberties and cyber security.

About the Authors

Robert Reardon is ECIR Postdoctoral Associate in the Political Science Department at MIT. Nazli Choucri is Professor of Political Science at MIT, and is the MIT Principal Investigator for ECIR.

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 alone and do not necessarily reflect the views of the Office of Naval Research or any other organization.

Cyberspace as Ungoverned Space

Matthew Hoisington, LLM Candidate (2012)

Research Group: The Fletcher School of Law and Diplomacy, Tufts University

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

Identify the governance structures of cyberspace and determine whether they are sufficient to enable regulation. In addition, analyze whether reasonable limits exist on the activities undertaken by governments.

Methods

Split the issue up into two sub-issues: governance of cyberspace; and governance through cyberspace.

The Research

Governance of Cyberspace: Cybersecurity

To what extent are governments able to regulate in cyberspace? In cases where they are unable or unwilling to regulate, what informal forms of governance (driven by the private sector, individuals, etc.) step into the void to close the governance gaps? How does this happen and is it successful and/or sufficient?

Governance through Cyberspace: Surveillance and Monitoring

What limits are set on the activities of governments in cyberspace? Are governments able to regulate in new and innovative ways by operationalizing the cyber domain to their advantage? To the extent that cyberspace enables regulation, are the rights of the regulated being protected?

Preliminary Results/Results

While it serves as a useful tool for individuals and groups, cyberspace enables much more regulation than is commonly thought. On balance the space may actually serve the interests of governments more than that of individuals or groups because of the increased surveillance and monitoring capabilities that it presents.

Remaining Research/Follow-up

What governance gaps remain? Will we see increased government control of cyberspace in the future? How will illicit groups evolve in cyberspace?

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.

The Dynamics of Managing Undersea Cables

Michael P. Sechrist, MPP; Chintan Vaishnav, PhD; Daniel Goldsmith, MBA

Start: May 2011
Research Group: Cyber Security; Explorations in Cyber International Relations, MIT-Harvard
Advisor: Prof Nazli Choucri

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

Can the Old Modes of Governance Meet the New Demands of the Internet?

The exponential growth of the Internet may soon demand that undersea cable deployment happen as quickly as possible. Legacy institutional barriers may need to be streamlined to the point of near instantaneous approval. Staying ahead of the exponential Internet growth rate is key to implementing a resilient, redundant, accessible Internet in the U.S. and around the world.

Methods

Qualitative & Quantitative System Dynamics Modeling

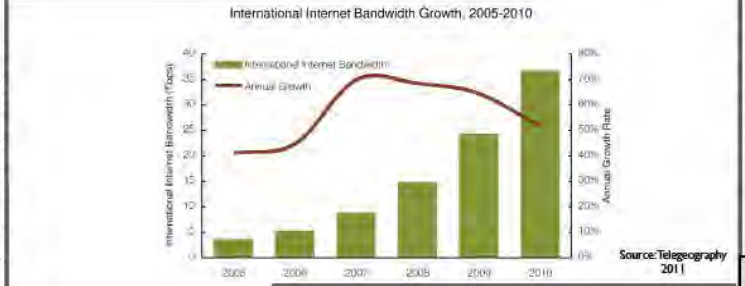
- Use a system dynamics model to identify and analyze the causal structures responsible for the above problem.

- Use emerging literature to refine the feedback structure in both dissident and state high-level cyber activity (message amplification, appeasement, coordination of anti-regime activity, force & violence, contact).

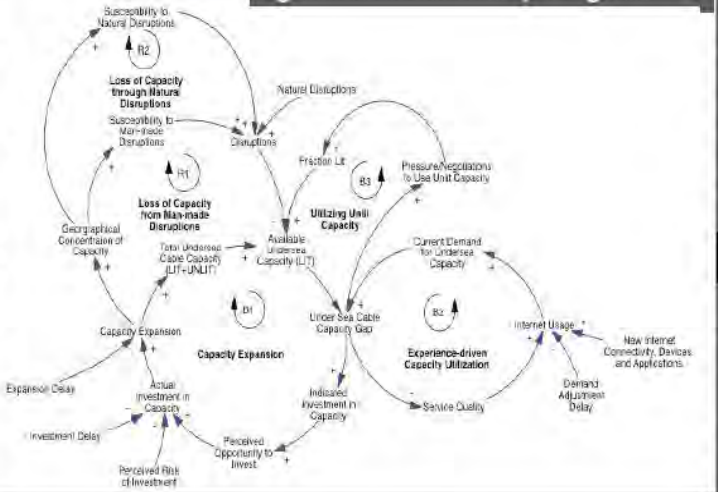
- Perform policy analysis of the model to propose solutions.

The Research

Internet Growth Doubles Yearly



High-Level Causal Loop Diagram



Preliminary Results

With an Internet growing by a factor of 1000 over the next 20 years, the physical layer of the Internet needs to grow and expand; the current open-ended, ill-defined and opaque cable permitting processes, in the form of Team Telecom in the United States and other agencies in other states around the world, adds unnecessary risk to making this Internet growth a reality.

Remaining Research

- Test basic model structure against various cable deployments and outages to ensure model captures important cyber dynamics
- Model U.S. and international governance structures for cable permitting and deployment; add this research to system dynamics model

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.

Escalation Management in Cyber Conflict: A Research Proposal

Robert Reardon, ECIR Postdoctoral Associate, Political Science, MIT

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Research Questions

- *Under what conditions is cyber conflict most likely to lead to uncontrolled escalation?*
- *Under what conditions is cyber conflict likely to lead to escalation in other domains (conventional, nuclear)?*
- *What steps are most affective at the reducing the risks of escalation?*
- *How relevant are existing theories of deterrence and escalation management to cyber conflict?*

Relevant Attributes of Cyber

- Constant background of attacks
- Diversity of actors (state and non-state)
- Diverse motives for attacks
- Difficult to identify attacker
- Difficult to identify the source, purpose of attack.

Implications

- Avoid framing cyber defense in military terms, and avoid defining threshold for cyber "act of war."
- Declaratory policies should remain ambiguous (could perversely encourage other parties, create credibility trap)
- Efforts to deter through retaliation are likely to be self-defeating.
- Important role for international coordination and foreign capacity building.
- Strengthen lines of communication and promote international dialogue.
- Deterrence by denial has limited utility, and can risk unacceptable or self-defeating costs.

Analytic Framework

- Most Analyses Have Looked to Theories Developed for Cold-War Nuclear Deterrence as Model to Understand Escalation in Cyber
- A Number of Characteristics of Cyber Conflict Suggest Irregular Warfare May be a Better Framework for Analysis:
  - *Combatants are extremely difficult to deter*
  - *Many have no interest in managing conflict intensity.*
  - *Asymmetries of information, interest, and capabilities are present.*
  - *Escalation management is set in a context of overlapping and simultaneous conflicts.*

Escalation Management in Different Forms of Conflict

	Nuclear (Cold War)	Irregular Warfare	Cyber
Paths to Escalation	Few	Many, Diverse, Multiple Conflicts Exist Simultaneously	Many, Diverse, Multiple Conflicts Exist Simultaneously
Relevant Actors	Small Number of States, Global Interests	Many, Diverse, Often with Regional or Local Interests	Many, Diverse, Often with Regional or Local Interests
Knowledge of Other Actors' Intentions and Capabilities	High, Signals Relatively Easy to Send, Receive, and Interpret	Low, Signal-to-Noise Problem	Low, Signal-to-Noise Problem
Ability to Accurately Attribute Attacks	High	Low	Low
Risk of Deliberate Escalation	Low	High	Unknown
Risk of Proxy Attacks	Low	High	High
Frequency of Attacks	None	High	Constant
Damage from Attack	Extremely High, Symmetric Vulnerability	Variable, Asymmetric Vulnerability	Extremely Variable, Typically Low, Asymmetric Vulnerability

Research Plan

- Explore existing literature on deterrence and escalation management in irregular warfare.
- Identify key areas of similarity /difference between cyber and other forms of irregular warfare.
- Develop comparative case-study analysis, drawing from four different types of conflict: irregular warfare, nuclear, conventional, and cyber.

Author and Affiliation

Robert Reardon is a postdoctoral associate with the ECIR project at MIT. He received his PhD in political science from MIT in 2010, and spent the 2010-2011 academic year as a Stanton Nuclear Security Fellow at RAND, where he continues to work as an adjunct political scientist.

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 alone and do not necessarily reflect the views of the Office of Naval Research or any other organization.

Establishing the Baseline: A Framework for Organizing National Cybersecurity Initiatives

Aadya Shukla, Science, Technology and Public Policy Fellow

Research Group: Harvard University, Kennedy School of Government

Explorations in Cyber International Relations

Workshop on People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

1.BACKGROUND

Policy making needs Interoperation

A clear understanding and communication of stakeholders' concerns across both domestic and international boundaries is a must.

Multiplicity of standards, guidelines and frameworks makes Interoperation difficult.

- The OECD issued *Guidelines for the Security of Information Systems* (1992).
- The UN issues resolution (55/63) on combating criminal misuse of Information Technologies (2000).
- Council of Europe Draft on Cybersecurity (1999)
- ENISA (European Network and Information Security Agency) Guidelines on Incident Management (2010)
- Comprehensive Guidelines to combat cyber challenge from Organization of American States (OAS), 2004.
- UK / US guidelines on Cybersecurity (2009 onwards)

2. PROBLEM STATEMENT

An Integrated framework to characterize various strategies embodied in various national and international strategies is missing from the domain.

Therefore, It is hard to answer the following questions:

1. **What are the specific and generic concerns of the stakeholders in cyberspace?**
2. **How do nation states balance their domestic priorities against need to comply with international guidelines?**
3. **How successful a particular initiative is against a specific type of cyber concern?**
4. **How does a national strategy scale up with change in cyber priorities?**
5. **What can be learned from other national initiatives?**

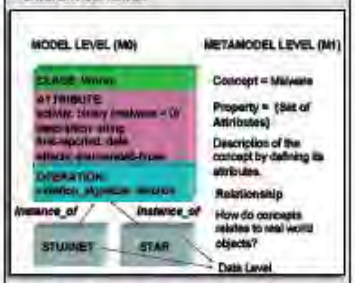
3. APPROACH

Apply Metamodeling technique (used in Software Engineering and AI) to design the required Integrated Framework.

What is:

Metamodel: Model of models.

Metamodeling: Higher level abstraction to represent observed or expected behavior of a real world phenomenon constrained by different contexts.



If the task were to characterize the phenomenon of Malware, then we can use meta level constructs (*Concept, Property and Relationship*), to have a model of models for all malware types.

4. SOLUTION

A light weight metamodel as an integrated framework for cyber strategies to establish the baseline:

Separate models for different types of cyber strategies (i.e., Standard, Guideline, Regulation)

Model component Classes :

'Actor' roles and categories of stakeholders (for example: ENISA is an instance of an Actor in a role 'policy-owner').

'Scope' class defines boundaries of relevance: Geographical (national, regional, international); Application (Crime, Security, Commerce, Society); Technical (hardware, software, network)

'Priority' defines weight of different cyber concerns per cyber strategy.

Protocol defines processes, documents and nodes (human & machine) required to deploy a given cyber strategy.

5. UTILITY OF SOLUTION

National (Dutch, German and British) and regional cyber strategy (EU) were analyzed to enable better characterization of these initiatives.

Comparison of the EU Model with the rest demonstrates that evolution of regional strategy and national strategies of the members of the regional alliance happens at different scales.

Comparison of national initiatives highlights further categories required for Interoperation and improvements among nation states.

A clean way to separate the generic and specific cyber concerns of nation states.

Metamodel can be used to aggregate initiatives by cyber concerns to identify partners and allies in cyberspace.

Helps to decipher cyber strategy initiatives in a technology independent manner.

6. CONCLUSIONS

1. UNDERSTANDING YOUR OWN TURF IS NOT ENOUGH

Fluid international boundaries and asymmetric nature of threat in cyberspace, requires policy level interoperation in a wider context. Our metamodelling approach allows a collective, consistent, dynamic and systematic understanding by adding new models to the Framework.

2. PRACTICAL APPLICATION

Metamodel will be used in building a feature-based online tool to assist new researcher& policymakers interested in understanding the domain.

ACKNOWLEDGEMENT

- Prof. V. Narayanmurti & Prof. N. Choucri,
- ECIR Consortium (Explorations of Cyber International Relations - A Joint Harvard-MIT Project funded by the Department of Defense),
- STPP Programme, Harvard Kennedy School,

Question & Comments at: aadya_shukla@ksg.harvard.edu

Minerva Research Project at MIT & Harvard Explorations in Cyber International Relations

This work is funded by the Office of Naval Research under award number N00014091059. Any opinions, findings, and conclusions or recommendations expressed here are those of the author and do not necessarily reflect the views of the Office of Naval Research.

MIT ESD engineering management social sciences

Finding Order in a Contentious Internet

Jesse Sowell, ESD PhD Candidate

Start: **September 2009**
Research Group: **Advanced Network Architecture Group, CSAIL**
Thesis Advisor: **Dr. D. Clark** Committee: **Prof. K. Oye (chair); Prof. C. Fine; Prof. N. Choucri; Dr. F. Field**

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

In 1998 an attempt to remove an offensive video blocked YouTube for most of the Internet...network operators resolved the issue in three hours. Spamhaus disseminates authoritative spam blocking lists, performing a vetting function while distributing monitoring and enforcement effort. Non-state collectives are increasingly playing function-specific Internet governance roles, often competing with conventional governance modes. Despite demonstrated operational and decisional capacity, little is known about how this capacity develops or how it is maintained. This research is an empirical, comparative analysis of governance arrangements and the implications for the ongoing design and operations of the Internet.

Key Questions

- Why do actors in these governance arrangements (institutions) cooperate?
- What elements of structure and process reinforce cooperation and contribute to operational capacity?
- Are these patterns durable, not simply one-off events?
- How contingent are patterns on the public, private, or hybrid character of the organization modes in which they are embedded?
- What factors contribute to dynamic efficiency?
- How do these governance arrangements interact with conventional modes of governance? How do they compare?
- What contributes to legitimacy, authority, and accountability in these arrangements?

Methodology

Social Network Analysis (*structure*)
- Attendee lists (figure to right)
- E-mail speakers
- Policy co-authors

Text Mining (*structure, process*)
- Concept clusters in documents
- Actors related by common interests

Cases and Interviews (*process, mechanisms*)
- Identify policy and issue communities
- Observation of the community
- Surface causal mechanisms

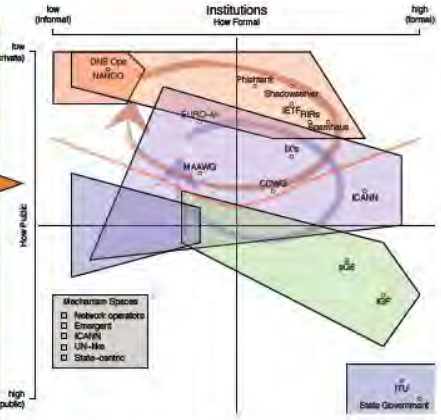
Filter and sort corpi

Validate structure, processes, mechanisms

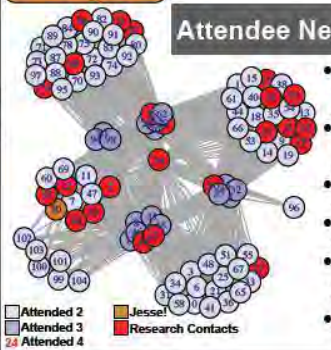
The Research

Institution Landscape and Boundaries

Two simple dimensions of institutions are (1) formality and (2) the mix and influence of public and private actors. This space illustrates the variety of organizational modes at play. Institutions are placed approximately: polygons represent the sets of governance mechanisms used by organizations and, importantly, the overlap. The red line represents the boundary, and interface, between bottom-up and top-down arrangements.



Attendee Network



- Comprises 105 actors that attended at least two of four major governance-related conferences
- Illustrates overlap between network operator community and IP resource management community
- Relation metric: number of conferences attended together
- Clusters are permutations of subsets of the four conferences
- Three "layers": attended two, attended three, core attendee (24) was at all four
- Red nodes are research contacts from recent fieldwork

Preliminary Results

Emergent governance arrangements == private regimes
- Regime components
  - NOGs serve as informal information exchanges, reducing community uncertainty
  - RIRs engage in monitoring and some enforcement
- Evidence of a broad, pluralistic marketplace of governance arrangements
  - Variety of accountability mechanisms
  - Confirmation of client-constituent spectrum
- Interface with top-down arrangements
  - Active collaboration with states and IGO's
  - Collaborating organizational modes are not isomorphic

Remaining Research

Theory Building
- Preliminary results provide sufficient evidence to develop an expanded theory of private authority (chapter 3)
- Develop criteria for testing theory

Analysis
- Social network metric development
- Identify and extract issue and community clusters from documents
- Evaluate social networks and communities over time

Social network analysis and idiographic studies proceed in tandem. Analysis provides initial structure to interviews. Subsequent cases analysis provides validation of indicators and insights into hidden variables. Two more iterations, incorporating community data collection, are expected between now and Fall 2012.

Idiographic Studies
- Function-specific organizations
- Asia-Pacific region communities
- Revisit North America and EU
- ICANN and IGF?
- Africa and Latin America/South America?

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

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.

Learning Legal Principles to Enable Law at Cyber Speeds

Mark A. Finlayson, PhD Candidate

Started Program: Fall 2003; Defended: Oct 2011
Research Group: Genesis Group, MIT CSAIL
Thesis Advisor: Patrick Winston, EECS Committee: Whitman Richards, BCS; Peter Szolovits, EECS & HST; Josh Tenenbaum, BCS

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Goal: Law at Cyber Speeds

If we are to enable the creation of **Automatic Cyber Targeting Systems** to respond in network time to cyberattacks, we must be able to do legal analyses at network speeds.

Problem: Automatically Identifying Legal Principles

Identification of and reasoning from case precedents relies on legal principles; computers currently have no ability to extract legal principles in an automatic and dynamic way.

Step 1: Assemble Corpus of Appellate Cases

Test Domain: Probable Cause

Example Legal Case:

US v Mays 466 F.3d 335 (2006)

Police officers conducted two controlled purchases of "crack" cocaine from an address in Shreveport, Louisiana. For the first transaction, a confidential informant allegedly purchased 0.3 grams of "crack" cocaine for $20 from a black male named "Melvin." For the second transaction, the same informant purchased 0.3 grams of "crack" cocaine for $20 from a black female whom the informant identified as "Melvin's mother." Officer Bo Lummus of the Shreveport Police Department prepared an affidavit to apply for a search warrant. The magistrate judge found probable cause and issued the warrant.

Police found and seized approximately 25 grams of powder cocaine and 72 grams of "crack" cocaine, as well as firearms, ammunition, a bulletproof vest, three digital scales, and a measuring cup in a duffel bag identified as belonging to Melvin Lee Mays. Mays was arrested. He filed a motion to suppress, alleging that the search warrant was not supported by probable cause. He also filed an objection to the notice filed by the Government alleging two prior felony narcotics convictions and one prior felony conviction for aggravated battery. Mays further filed a motion to sever the felon-in-possession charges from the remaining charges and post-verdict motions for a new trial and judgment of acquittal. Finally, Mays objected to an enhancement in his pre-sentence report based on a narcotics conviction he received when he was 17 years old but tried as an adult.

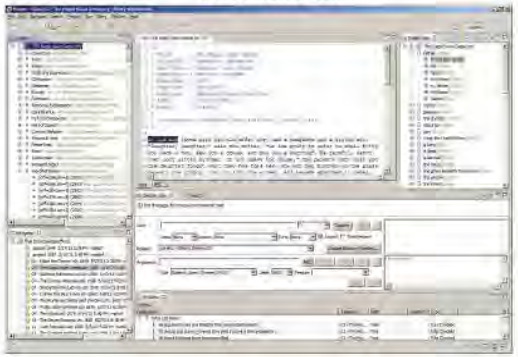
The district court denied all of Mays's motions and objections. Mays was convicted and sentenced.

Mays timely appealed.

We affirm the conviction and sentence.

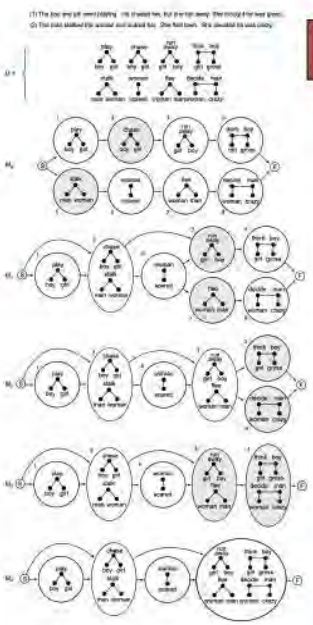
Step 2: Semantic Annotation

(Finlayson 2008, 2011)

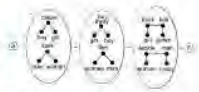


Step 3: Run Analogical Story Merging (ASM)

(Finlayson 2009, 2011)



Result: Extracted Legal Principles



Evaluation: Compare with Legal Principles explicitly identified in the case review

Capabilities Enabled

- Automatic identification of relevant legal precedents
- Automatic discovery of emerging legal frameworks
- Automatic Cyber Targeting systems to respond in network time to cyberattacks

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 alone and do not necessarily reflect the views of the Office of Naval Research or any other organization.

Representing Cyberspace using taxonomies and Meta-data analysis

Gihan Daw Elbait, PhD

Research Group: Explorations in Cyber International Relations, MIT-Harvard;
Political Science/Sloan School of Management Prof. N. Choucri and Prof. S. Madnick and S. Camina

Explorations in Cyber International Relations

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Problem

- **Modeling and mapping** the landscapes of emerging research fields, such as cyberspace.
- Most research fields are composed of many **subfields which are related in intricate ways,** therefore **structural organization** of these subfields could be of great use.
- Acquiring and analyzing such knowledge is hampered by the **vast amount of data** available in publications.
- The need of **database integration** to enable the mapping of relevant component of the topic in hand (e.g. Cyberspace and International Relations).

Research Goals

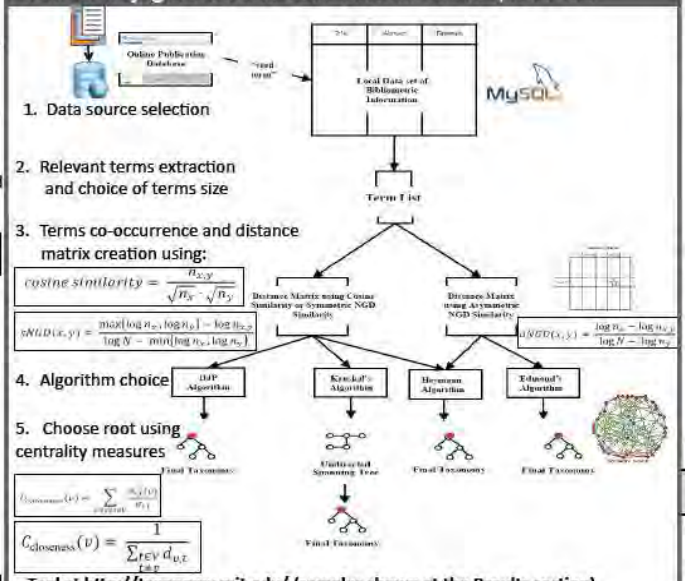
- To develop automated, publication database-independent methods for generating **taxonomies.**
- Advancing the algorithms in the sub-field of **bibliometrics**
- Applying these tools in **support of the Explorations in Cyber International Relations (ECIR) research effort.**
- **Integration of databases** of technology and social sciences to capture the whole landscape of cyberspace
- To generate ways **of visually representing** the data in a manner that is easily usable and understandable for end users.

Current Activities

- Providing a tool that generates and visualizes taxonomies (e.g. Cyberspace taxonomy).
- Meta data analysis to explore and compare the data of different topics (e.g. publication volume, authors affiliations,..)
- Choice and integration of relevant databases sources (e.g. identified the gap between using engineering/computer science vs. social science as the pool of publications for the purpose of the cyberspace taxonomy generation

Methods

Taxonomy generation and visualization process:



Tool at http://taxonomy.mit.edu/ (samples shown at the Results section)

Meta data analysis:

Social Science Databases	cyberspace	cyber security	social media
Science Direct	2979	259	638
Microsoft Academic Research beta	506	24	38
JSTOR	7817	143	265
SSRN	608	85	209
SSRC	1	1	0
Engineering Databases	**cyberspace**	**cyber security**	**social media**
Science Direct	3433	1005	1165
Engineering Village	4920	2501	2136
Microsoft Academic Research beta	2127	435	1170

Table. 1 Shows # of records for each of the search queries "cyberspace", "cyber security", "social media" in social science vs. engineering/computer databases.

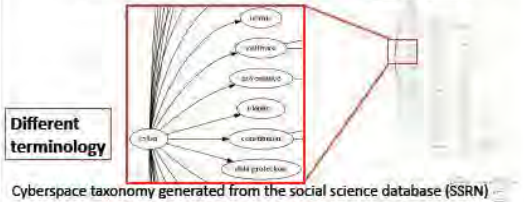
- In Table 1. the upper part shows results from the social media databases while the lower part shows data from engineering/computer databases. The numbers suggests that the social science databases are lagging behind In terms of numbers of articles on the cyber security and social media fields.
- We further use meta data from bibliographic categories including Database, Author Affiliation, Year, Country, language, etc.. for a high level exploration and comparison of different topics. (see upper part of the results section for examples)

Results

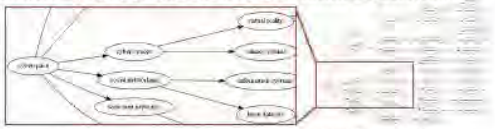
"Cyber security" publication size trend

"Social media" publication size trend

Different Publication source



Cyberspace taxonomy generated from the social science database (SSRN)



Cyberspace taxonomy generated from the engineering village database

Summary

1. Taxonomies for scientific research bodies facilitate the organization of knowledge.
2. Size of **cyber related publications** in social science is lagging behind those from engineering/computer sciences and they contain different terminology (see Results section).
3. The integration of the relevant databases is essential (e.g. social sciences and engineering/computer) in order to cover all concepts of the field when modeling/mapping a cyber International Relation field.
4. Standardization of the quality of the meta data provided by online databases is necessary for data analysis.

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(s)and do not necessarily reflect the views of the Office of Naval Research.

PARTICIPANTS

Poster Session and Workshop

Bruce Bakis
Principal Cyber Security Engineer
MITRE Corporation

David Beaver
Associate Professor
Linguistics Department
University of Texas at Austin

Adam Berinsky
Associate Professor of Political Science
Director, Political Experiments Research Lab
Massachusetts Institute of Technology

Marjory Blumenthal
Associate Provost
Georgetown University

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

José Campos
Director
Microsoft Corporation

James Caulfield
Director
Operational Intelligence, Internet and Directory Services Group
Federal Reserve Bank of Boston

Kevin Cavanaugh
Vice President, Messaging and Collaboration
IBM Software Group

Yiseul Cho
Masters Candidate
Technology Policy Program
School of Engineering
Massachusetts Institute of Technology

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

Claudio Cioffi-Revilla
Professor of Computational Social Science
George Mason University

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

Charles Cogan
Associate
International Security Program,
Belfer Center for Science & International Affairs
Harvard Kennedy School

Gihan Daw Elbait
Postdoctoral Associate
Department of Political Science
Massachusetts Institute of Technology

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

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

Mark Edington
Executive Director
Harvard Decision Science Laboratory
Harvard University

Scott Farr
Commander, United States Navy
National Security Fellow
Harvard Kennedy School

Mark Finlayson
PhD Candidate
Electrical Engineering and Computer Science
Massachusetts Institute of Technology

Dara Fisher
Graduate Student
Technology and Policy Program
School of Engineering
Massachusetts Institute of Technology

Jane Fountain
Professor of Political Science and Public Policy
Adjunct Professor of Computer Science
University of Massachusetts Amherst

Archon Fung
Ford Foundation Professor of Diplomacy and Citizenship
Harvard Kennedy School of Government

Dan Geer
Chief Information Security Officer
In-Q-Tel

Firas Glaiel
Graduate Student
Engineering Systems Division
Massachusetts Institute of Technology
Principal Software Engineer
Raytheon Network Centric Systems

Michael Glennon
Professor of International Law
The Fletcher School of Law and Diplomacy

Daniel Goldsmith
Principal Consultant
PA Consulting

Phillip Hallam-Baker
Internet Security Protocol Architect
Comodo

Fergus Hanson
Research Fellow and Deputy Editor
The Interpreter
Lowy Institute/Georgetown University

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

Matthew Hoisington
LL.M. Student
Fletcher School of Law and Diplomacy

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

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

Lucas Kello
Research Fellow
Belfer Center for Science & International Affairs
Harvard Kennedy School

Gary King
Albert J. Weatherhead III University Professor
Department of Government
Harvard University

Gary Kollmorgen
President/CEO
GSK Inc.
Contractor Support
Office of Naval Research

Robert Laubacher
Research Scientist
Associate Director, Center for Collective Intelligence
Massachusetts Institute of Technology

Chappell Lawson
Associate Professor of Political Science
Director of the MIT International Science and Technology Initiatives (MISTI)
Secretary of the Faculty
Massachusetts Institute of Technology

Herb Lin
Chief Scientist
Computer Science and Telecommunications Board, National Research Council of the National Academies

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

Tim Maurer
Non-resident Fellow
Global Public Policy Institute

William McClane
National Security Fellow
Harvard Kennedy School

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

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

Venkatesh "Venky" Narayanamurti
Director, Science, Technology and Public Policy Program, Belfer Center for Science and International Affairs
Benjamin Peirce Professor of Technology and Public Policy
Harvard Kennedy School
Professor of Physics
Harvard University

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

Olumide Longe
Fellow
MISTI Initiatives
Massachusetts Institute of Technology

Taylor Owen
Banting Postdoctoral Fellow
Liu Institute for Global Issues
University of British Columbia

Robert Pavelko
Commander, 21st Space Operations Squadron, Vandenberg Air Force Base, California
United States Air Force Academy

David Palés
Fellow, Advanced Study Program
Massachusetts Institute of Technology

Larry Pang
Undergraduate Student
Sloan School of Management
Massachusetts Institute of Technology

Thomas Quinn
Senior Vice President and Chief
Information Security Officer
State Street

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

Noah Rayman
Undergraduate Student
Harvard University

Robert Reardon
Postdoctoral Associate
Explorations in Cyber International
Relations
Massachusetts Institute of Technology

David Robinson
Knight Law & Media Scholar
Information Society Project
Yale Law School

David Sacko
Professor of Political Science
US Air Force Academy

Masroor Sajid
Fellow, Advanced Study Program
Science, Technology and Society
Massachusetts Institute of Technology

Harvey Sapolsky
Professor of Public Policy and
Organization, Emeritus
Massachusetts Institute of Technology

Mark Schonfeld, Esq.
Partner
Burns & Levinson LLP

Michael Sechrist
Program Manager
Explorations in Cyber International
Relations
Belfer Center's Science, Technology, and
Public Policy Program
Harvard Kennedy School

Adam Segal
Ira A. Lipman Senior Fellow
Counterterrorism and National Security
Studies Council on Foreign Relations

Eugene Skolnikoff
Professor of Political Science Emeritus
Massachusetts Institute of Technology

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

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

Evann Smith
Doctoral Candidate
Department of Government
Harvard University

Gordon Smith
Executive Director, Centre for Global Studies, Adjunct Professor of Political Science
University of Victoria

Jesse Sowell
Doctoral Candidate
Engineering System Division; Advanced Network Architecture Group, Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

Robin Staffin
Director for Basic Research, Office of the Assistant Secretary of Defense, Research and Engineering
U.S. Department of Defense

Jessica Stern
Writer
Faculty Affiliate
Belfer Center for Science and International Affairs
Harvard University

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

Chintan Vaishnav
Postdoctoral Associate
Department of Political Science
Massachusetts Institute of Technology

Mitzi Wertheim
Professor of Practice for Sustainability, Enterprises & Social Networks
Cebrowski Institute
Naval Postgraduate School
Director
The Energy Conversation

Richard Wang
Director, MIT Information Quality Program
Co-director, Total Data Quality Management Program at MIT
University Professor, University of Arkansas at Little Rock

Josephine Wolff
Graduate Student
Technology & Policy Program
Massachusetts Institute of Technology

William Young
PhD Student
School of Engineering
Massachusetts Institute of Technology
Lieutenant Colonel, USAF

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

Jonathan Zittrain
Professor of Law
Harvard Law School and Harvard Kennedy School
Professor of Computer Science
Harvard School of Engineering and Applied Sciences
Co-Founder and Faculty Co-Director
Berkman Center for Internet and Society

Ethan Zuckerman
Principal Research Scientist
Media Laboratory
Massachusetts Institute of Technology