



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

Workshop Report

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ACKNOWLEDGEMENTS

INTRODUCTION

Nazli Choucri, Political Science Department, MIT

I. PEOPLE POWER & GLOBAL POLITICS: WHAT HAS CHANGED

Joseph S. Nye, Jr., Harvard Kennedy School

Gordon Smith, Centre for Global Studies, University of Victoria

Adam Segal, Council on Foreign Relations, Canada

Robin Staffin, Office of the Assistant Secretary of Defense for Research and Engineering

II. HOW DO WE LISTEN: NEW WAYS TO ANALYZE THE MESSAGES

Michael Siegel, Sloan School of Management, MIT

Gary King, Department of Government, Harvard University

David Beaver, Linguistics Department, University of Texas at Austin

Adam Berinsky, Political Science Department, MIT

III. PEOPLE, POWER & PRESSURES ON GOVERNANCE: THREATS & OPPORTUNITIES

Melissa Hathaway, Harvard Kennedy School

Joel Brenner, Cooley LLP

Roger Hurwitz, Computer Science and Artificial Intelligence Laboratory, MIT

Chappell Lawson, Political Science Department, MIT

IV. CYBERPOLITICS & DEMOCRACIES: WHERE ARE WE HEADED?

James Dougherty, Council on Foreign Relations

Archon Fung, Harvard Kennedy School

Peter Brecke, Political Science Department, Georgia Institute of Technology

Ethan Zuckerman, Media Laboratory, MIT

V. SOCIAL MEDIA & SOCIAL ACTION LEARNING FROM EXPERIENCE

Venkatesh "Venky" Narayanamurti, Harvard Kennedy School

Fergus Hanson, Lowy Institute, Sydney, Australia

Evann Smith, Department of Government, Harvard University

Robert Laubacher, Sloan School of Management, MIT

VI. THREE VISIONS: THE "NEXT GENERATION" OF CHALLENGES FOR PEOPLE, POWER, AND CYBERPOLITICS

Stuart Madnick, Sloan School of Management, MIT

Herb Lin, U.S. National Research Council of the National Academies

David Clark, Computer Science and Artificial Intelligence Laboratory, MIT

Jonathan Zittrain, Harvard Law School

VII. CLOSING COMMENTS: END NOTE

Nazli Choucri, Political Science Department, MIT

VIII. POSTER SESSIONS

Accountability at the Application Layer

Wolff, Josephine, SM Candidate, Technology & Policy Program, MIT

Comparative Analysis of Cybersecurity Metrics to Develop New Hypotheses

Fisher, Dara, SM Candidate, ESD, MIT

Control through the Layers in the Chinese Internet

Hung, Shirley, Postdoctoral Associate, MIT

Coordinates of Cyber International Relations

Vaishnav, Chintan, Postdoctoral Associate, MIT

Cost-benefit Analysis of CERT's International Cooperation Activities Focusing on Korean Case

Cho, Yiseul, SM Candidate, Technology & Policy Program, MIT

Cyber-enabled Loads & Capacities Methods

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

Cyber International Relations Theory: Assessing the State of Art

Reardon, Robert, Postdoctoral Associate, MIT

Cyberspace as Ungoverned Space Methods

Hoisington, Matthew, LLM Candidate, The Fletcher School of Law and Diplomacy

The Dynamics of Managing Undersea Cables Methods

Sechrist, Michael P., Project Manager, Harvard Kennedy School
Vaishnav, Chintan, Postdoctoral Associate, MIT

Escalation Management in Cyber Conflict: A Research Proposal

Reardon, Robert, Postdoctoral Associate, MIT

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, MIT

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

Daw Elbait, Gihan, Postdoctoral Associate, MIT

PARTICIPANTS

Poster Session and Workshop

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.

Acknowledgements

I would like to express my appreciation – and that of the entire ECIR Research Team – for the assistance and contributions of the following individuals in the preparation of the *Workshop Report*: Mark Finlayson, Shirley Hung, Jessica Malekos-Smith, Tim Maurer, Patricia McGarry, Vivek Mohan, Larry Pang, Daniel Pereira, Aadya Shukla, Michael Siegel, Jesse Sowell, and Chintan Vaishnav. Special thanks are due to Elizabeth Nigro for her contribution in the integration of the various parts of the Report into a final product.

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.

Nazli Choucri

INTRODUCTION

Nazli Choucri

Political Science Department, MIT

New Reality

For the first time in human history such a large number of people from all parts of the world participate in a new arena of information and communication of global scale and scope. Almost everyone everywhere has the opportunity to participate in cyberspace. Few states, if any, are able to control the flow of information via cyber venues that cross their boundaries. All states are recognizing, to one degree or another, that people matter – and sometimes they matter a lot. This reality is also influencing the changing power distribution in international relations. The “old” concentration of power in a bipolar cold war world has been replaced not by multipolarity but, more importantly, a “new” international structure characterized by the diffusion of power.

New Complexity

In the “new” world people also matter in a particularly unprecedented way. The age distribution of the global population is skewed toward the young age groups. And everywhere it is the young people that dominate participation in cyberspace. More and more, the diffusion of social networking practices and growing use of mobile technologies – notably social media for personal or political uses – has reinforced the 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

New Challenge

A critical challenge at this time is that the organized fields of knowledge do not provide a sufficiently robust basis for analyzing, anticipating, and responding a new way of understanding power, politics, the state, and institutions of governance: nationally and internationally. The goal of the *ECIR* Project is 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.


Workshop

This workshop is the second in a series of sustained deliberations and explorations involving leading individuals in academia, government and business. The outcome of this workshop will provide a baseline for evolving understanding of people, power and cyberpolitics.

Introduction: People, Power, and CyberPolitics

Nazli Choucri

Massachusetts Institute of Technology, Department of Political Science

 <p>Explorations in Cyber International Relations Massachusetts Institute of Technology Harvard University</p> <p>Workshop on People, Power, and CyberPolitics Co-Sponsored by Council on Foreign Relations</p> <h3>Introduction</h3> <p>Nazli Choucri Massachusetts Institute of Technology</p> <p>December 7 and 8, 2011 1</p>	<h3>Explorations in Cyber International Relations</h3> <p>A multi-disciplinary collaborative research project of MIT and Harvard to create a new cyber-inclusive field of international relations to:</p> <ul style="list-style-type: none">• Provide theoretical frames and methodologies to analyze new international cyber-centered realities• Attract and educate a new generation of researchers, scholars, and analysts• Clarify threats and opportunities in for national security and international well-being• Contribute to policy discourse and deliberations <p>2</p>
<h3>People, Power, and CyberPolitics</h3> <ul style="list-style-type: none">• People Almost anyone can participate in the new domain Everywhere young people dominate cyber access & participation Explosion of social media reinforces power of people People are acting, challenging the state• Power The state is faced with new and unexpected pressures Changes are happening faster than the ability to fully track Emerging and growing influence of civil society• CyberPolitics Changing demography of cyberspace Use of power in traditional venues to influence cyber domains Use of power in cyber venues to influence traditional domains The added power of anonymity <p>3</p>	<h3>The Workshop</h3> <ul style="list-style-type: none">• Participants with diverse background, training, interests, and perspectives• Agenda focused around a set of initial questions – to bring out differences of views• Few assumptions, but framed around overarching issues, such as:<ul style="list-style-type: none">• Are the new realities transient or transformative?• What do we know? what do we not know? what should we know?• What are major research and policy imperatives? <p>4</p>
<h3>At the End of the Day</h3> <ul style="list-style-type: none">• Better understanding of how, when, and why people, power and cyberpolitics shape realities on the ground• Baseline of issues, contentions in theory and practice• Assessment of what we might be missing• Priorities for research and policy – nationally and internationally• Potential networks of Workshop participants with shared interests• Illustrations of the next generation research <p>5</p>	<h3>People, Power, and CyberPolitics</h3> <p>Expect the Unexpected</p> <p>6</p>

I. People, Power and Global Politics: What has Changed?

Framing Questions

How do people matter in international relations?

How does context matter? How does social media matter?

What are the impacts on the development of the 21st C. world order?

How are these issues relevant to foreign policy and national security?

What are major research challenges?

Panel

Moderator

Joseph S. Nye, Jr., *Harvard Kennedy School*

Panelists

Robin Staffin, *Office of the Assistant Secretary of Defense for Research and Engineering*

Gordon Smith, *Centre for Global Studies, University of Victoria, Canada*

Adam Segal, *Council on Foreign Relations, New York*

Presentations

Joseph S. Nye, Jr.

Traditionally, political science views the state as the central node of policy and decision-making. As a result, the state has become the primary analytical unit of the political scientist. This has led to less of an analytical focus on civic engagement and/or political action by 'the people.' Information Communication Technologies (ICT) and the lower barriers 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.

A few forces have contributed to this shift. For one, the balance of power is shifting from

the West to the East (see Adam Segal's books *Advantage: How American Innovation Can Overcome the Asian Challenge* and *Digital Dragon: High-technology Enterprises in China* as vital works for gaining an understanding of how China specifically adopted a wide array of policies designed to raise its technological capability and foster industrial growth). Secondly, 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.

Technology as the driver for a power shift is not a new phenomenon. It is how this change is currently manifesting which needs to be looked at differently. For example, Johannes Gutenberg's printing presses led to numerous cultural changes, including the Protestant Reformation. This may not be the appropriate analogy, however, for the power shifts that we are currently witnessing. The new patterns of civilization we are seeing, including the creation of new values in the market economy and political action in the public sphere, are more analogous to changes that occurred around the feudal state in the Middle Ages.

Medieval merchants developed the '*Lex Mercatoria*' (Merchant Law) to go about their business without replacing the feudal state laws in Italy. The feudal system was not replaced overnight. Rather, it was transformed slowly by a constant flow of accretions, additions and new systematic and structural layers. The *Lex Mercatoria* did not displace the medieval castle but grew *around* the castle. What are the ways the contemporary power shift will manifest in similar additive, subtractive and layered process?

It would be a mistake to view the situation as binary. The non-state actors are not supplanting the State. Instead, the stage on which actors vie for power is becoming more crowded with a plethora of organizations and individuals. Individuals are now able to play new roles (i.e., – new third actor in Egyptian Politics via the civic force displayed in the public square).

The dynamics of actor-actor interaction are also changing. Controlling anonymous groups of non-state actors, backed by technology, is fast becoming a dilemma for the state actors. The number of transnational actors is also increasing. Non-state actors (hackers or large corporations) are defining their own set of norms outside the control of state actors to conduct their business. New international political structures are emerging, structures that are no longer simply comprised of two parties but various three or multi-party equations are emerging.

The MIT/Harvard ECIR research community must address the following two questions. First: *What is the impact of these power shifts?* And, secondly; *How do various stakeholders speculate about this change?*

Robin Staffin

"I know why you're here, Neo...I know what you've been doing, why you hardly sleep... It's the question that brought you here. You know the question, just as I did." ...The Matrix

We are brought here to this panel discussion by the question, "what is the changing nature of Cyberspace and of Internet itself." It is a fitting question to address at the institution that played such a major intellectual role in development of cyberspace. It is also significant in the context of the joint MIT-Harvard project, "Explorations in Cyber International Relations (ECIR)," which is cosponsoring this symposium. ECIR is a major project under DoD's Minerva Program.

Initiated by the Department of Defense in 2008, the Minerva program seeks a deeper understanding of the social, cultural, and political dynamics that shape regions of the world of strategic interest, and their impact and interaction with modern technology. It is a gigantic challenge getting one's arms around such a broad set of forces and trends, but it is important that we attempt to do so, since societal and cultural environments define much of the context of our national security posture.

It is also not easy in this particular case to see this challenge of cyber with clarity because of the varying world views and perspectives on cyberspace. Cyberspace challenges are highly interdisciplinary, and this is another reason why we are all here.

A cautionary tale from the early years of the World Wide Web that relates to the wide reach of internet communication: High energy physicists are generally credited with the creation and early development of the Web, driven by collaboration needs for rapid, global communication of data and analyses. Well, it so happened that an enthusiastic few would on occasion communicate their 'take' on fresh scientific data by personal blog. They didn't realize that scientific reporters also read their blogs and would use this as source material, giving them an early window into possible major discoveries, such as for the search for the long-sought Higgs boson. The irony here was that it was this same scientific community, the early inventors and developers of the web and its tools, would also be one of its earliest victims. What are the implications of such public/private sector data, collaboration and data issues moving forward?

Gordon Smith

Given that the distribution of power is being diffused, there is a need to focus research on new forms of civic engagement and new media - especially the role of social media platforms like Facebook and Twitter to support the "uprisings" in the Middle East.

The noted role of social media in these uprisings should not be overestimated. Some people are exaggerating the role of Twitter and Facebook, while others falsely dismiss their influence. It is important to focus on one pivotal question: *Which social media platform*

played what role and how?

The insights of work by MIT Researcher Ethan Zuckerman are important, specifically the recent interrogation of what caused the self-immolation video of the vegetable seller from Tunisia to be spread so instantaneously – and what were the mechanisms behind its rapid spread across the globe?¹ The self-immolation by the man in Tunisia was not the first such act. Key to its spread was its accessibility to people outside Tunisia and their ability to take further action.² Social media can move at an extraordinary speed to get the story out and in terms of coordinating action. The under-rated but very important impact of social media's ability to carry video messages – especially if the video URL is embedded in Twitter is an example.

Social media has now created a perception and/or proven that “the people” can bring down even the worst tyrants. As Marc Lynch noted, the ‘wall of fear’ has been shattered.³ The challenge now is for research in the area of how social media can contribute to the implementation phase or the building phase of a democracy. The role of diaspora communities in responding through Internet activity to events or political actions in other countries is important. 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 (such as repackaging reportage for pick-up by traditional media) is very vital. The role of the curators of social media is becoming increasingly important.

The following proposition must be tested: how important is social media going to be in this building process?

Huge quantitative social science research opportunities exist. These include smart phone penetration metrics, for example, with their capacity to bear witness through video on smartphones. Or we can look at the Tahrir Square's tweets as a percentage or share of votes for the Muslim Brotherhood and Salafists.

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 must be studied. Governments can also use social media to monitor its people and misrepresent the facts. A remark from the audience drew attention to the fact that with the social media it is impossible to hide. It is important for the government to strike a balance between anonymity, privacy and cyber-security threats (i.e., crime), but that remains one of the biggest challenges.

It is evident that ICT has facilitated the rise in civic engagement and the power of people – but more research must be done to understand the distribution of this power across the spectrum of new technology platforms. While there is a groundswell in bottom-up, participatory political actions, the ever-increasing importance of the top down structures and the annual conclaves of political and economic elites and state actors remain.

Adam Segal

There are multiple types of coalitions and 'spaces' within cyberspace. These spaces are very different and various. Cyberspace has to be broken down, classified and taken apart. The work by Ethan Zuckerman and the role of "bridge bloggers" is not only bridging between cultures and languages, but between different coalitions and spaces in cyberspace. This process is not a zero sum game but one of slow accretion from the power of the state to the power of the people.

There is a growing, central tension between transparency and accountability. As different ICT technologies and platforms are subjected to variable degrees of controls. There is a need to analyse the behaviour of various actors over the Internet, the changing dynamics of actor-actor interaction in China, as the Chinese government is currently listening to debates by citizens. Contrary to the popular view, this debate is not leading to any kind of uprising among activists in China. Instead, it is a demonstration of the fact that ICT has forced the Chinese government to think about accountability and transparency concerns as a way of increasing citizen's trust in the state.

The future of the Internet is probably not American but Chinese. There are 500 million Chinese online with potential for another 700 million to go online in the years ahead. Chinese hackers are influencing international politics as non-state actors. There are new types of coalitions and themes promoted by the Chinese governments in an effort to influence, shape or set global norms in cyberspace. China is also able to influence international politics with a presence in Tunisia and Middle East/North Africa and is involved in managing the Internet with its set of norms. For example, China is currently sending ICT experts to countries with lower ICT capabilities. China is providing its surveillance technology equipment and therefore pushing its own set of competing standards in the technology domain. At a recently held conference in London (November 2011), the Chinese government tried to get its guidelines for the International Code of Conduct accepted.

Projects like Minerva underlined the value of interdisciplinary research by institution happening by way of student and researcher engagement across the discipline boundaries.

Open Discussion

Multidisciplinary Research

How do you get interdisciplinary research from universities and overcome institutional barriers?

- Multidisciplinary university research initiatives are trying to create research that is more than just the sum of its parts.
- Work in the 1970s on transnational relations and influence of sociologists and economists on work, an outstanding example is the Munk Center at the University of Toronto.

Data and politics

There is now more data on more people, i.e., in parallel to the Arab uprising, also economic protests in Tel Aviv with data available through cell phones. Can we keep up?

- It is possible to measure certain factors but the challenge is to reveal causal relations between those factors and changes in politics.
- Some literature presents founders of www as political actors and while that is true for some of its architects there were also some political radicals with a particular political agenda.
- Facebook and Google were created without deeper political aspirations but it was Twitter and its founder Dorsey which realized that it could be for political purposes.
- In the Arab uprising governments shut down profiles on social media platforms, crucial role of private companies.

Social Learning

How do actors succeed or fail to learn?

- Learning in government is splintered.
- Simulation gaming potential to get people in government to talk.
- Learning by activists, example of Syrian activists .

China brought in experts from all over the globe on particular issues to then learn lessons from these experts

- Chinese government strategy is to control social unrest, to deploy lots of police forces in key locations but potential internal challenges because the degree to which Chinese system is stove piped.
- Since 1978 onwards, Chinese government has been trying to learn, from outside models and actors, in this rapidly changing world of technology.

**Lumpy and discontinuous learning in government is often due to external events
(article in Strategic Studies on learning from nuclear domain)**

- Impact matrix can be established by developing methodologies (for example, network analysis & system dynamics modelling) to assess three aspects: what people are doing, how they are doing it and if they are acting within the boundaries of ethical behaviour.
- ICT leads to collective actions – from people to group levels.

The State

- States have the monopoly on the use of force.
- Weber stated states have monopoly on legitimate use of force.
- Weber's definition defines the problem away.
- The question of monopoly of state power will be clarified only after norms in cyberspace have become more established. Before that, we can kick the can by sticking to the conventional definition of power (as monopoly on power is upheld by the state assuming legitimate usage of power).

II. How do we listen: new ways to analyze the messages

Framing Questions

How do different parties (groups, states, etc.) listen, interpret and react to messages?

How effective are the different parties at framing, collecting, accessing, or distributing messages?

How do messages from one group (or constituency) affect the responses, activities, or messages of other parts groups (or constituencies)?

What new research provides added insights on these issues?

Panel

Moderator

Michael Siegel, *Sloan School of Management, MIT*

Presentations

Gary King, *Department of Government, Harvard University*

David Beaver, *Linguistics Department, University of Texas at Austin*

Adam Berinsky, *Political Science Department, MIT*

Presentations

Michael Siegel

In 2005, Siegel (along with Stuart Madnick, Nazli Choucri, John Mallery, Daniel Goldsmith and others) began a Defense Advanced Research Projects Agency (DARPA) contract looking at state stability and insurgency. At the time, they provided a definition for stability involving loads and capacities. Through the contract, they developed models of the relationships between dissidents, insurgents, governments, etc. Part of the result was the realization that the state did not get to the insurgents early enough - and that “teasing” them back into the population is a low-cost way of maintaining stability.

The research provided a significant improvement over the understanding of insurgencies. But states remain the dominant actors; what is new, though, is the speed of communication. This led to a focus on the role of cyber venues, either by dissidents or by states. Several cases were done that *both* supported and contradicted the hypothesis that cyber was important to this model of insurgency. This work led to integrating cyber into our insurgency model. Several of these factors were about the intensity, circulation rate, and effect of messages.

Slides at the end of Session II.

Gary King

The workshop has so far been concerned with the effect of the massive changes in technology on politics, society, and so forth. It is not clear what the effect of 'big data' will be on politics, but the real big change that can already be measured is the enormous effect the data revolution is having on social science research. It represents an historic change in the field of research if there is shift from simply studying phenomenon to actually getting to the point where the problems identified previously in the workshop can be addressed and potentially solved.

The evidentiary base of social science has rapidly expanded. In the last 50 years, there has been an explosion in surveys, aggregate government statistics, in-depth studies and other forms of datasets. In the next 50 years, we will see a similar explosion of data, in addition to innovations in academic data sharing and the data replication movement (e.g., Dataverse⁴), government e-records and sophisticated statistical methods. This continuing "march of quantification" is the official end of a quantitative-qualitative divide in the social sciences and humanities. It is a very exciting time in social science research.

Opinions of activists (which would have numbered hundreds or thousands of interviews in a field research context) now number in the millions of political opinions spread globally by ICT on a daily basis. At last count, one billion tweets are now generated every 4 days.⁵ Another example cited are surveys generated by surveying 500,000 people carrying accelerometers in cell phones to measure exercise. This approach allows an understanding of the social context by using the continuous record generated by each individual. In the area of economic development, satellite images of night-lights, roads and farms are used for research purposes.

Social scientists do not care about the needle in the haystack (individual document classification), they care about the haystack (category proportions). The individual "tweet" of the individual user is not of interest to the social scientist. For example, biological sciences are becoming social scientists with the same unit of analysis (the human being) but thousands of variables and patterns of the 2,000-3,000 similar observations.

A new research project focusing on automated text analysis is used to read billions of social media posts to understand blogosphere opinions of presidential candidates. An example of an application in politics was the reaction to a botched joke by presidential candidate John Kerry. Political strategists were able to see an obvious reaction to this event instantly in the blogosphere. Commercialized in 2008, the product that evolved from this initial research effort is now called Crimson Hexagon⁶ and continues to collect data from all social media posts.

An example is the recent development of a new method, Unbiased Category Proportions. It was then applied to Chinese blog posts (at least the posts which ones were not taken down by the government). Other types of data such as unstructured text (emails, speeches, blogs, newspapers, etc.), commercial activity (credit cards, sales data, produce RFIDs), geographic location (cell phone, GPS), health information (digital health records), biological sciences (genomics, brain images), satellite imagery (electoral activity, social media, web artifacts and multiplayer games/virtual worlds) all hold potential for quantitative research in the social sciences.

The central point is this - there are enormous, emerging social science opportunities ahead - representing an historical shift from studying to understanding & solving big societal issues and problems. If you are interested in exploring opportunities and areas of collaboration, see <http://gking.harvard.edu>.

Slides at the end of Session II.

David Beaver

A major research effort has been started by the Linguistics Department at the University of Texas at Austin and the Department of Psychology at the University of Memphis in Social Language Processing, specifically Linguistic Inquiry and Word Count (LIWC).

LIWC is the statistical analysis of texts and the use of specific word types e.g., pronouns or the use of first person pronouns. The research is using LIWC as it relates to deceptive behavior. A few examples of LIWC results include; academically successful college students used more nouns in their admissions essays than less academically successful students. Another example of a result derived from LIWC research is tracking positive and negative emotion words around the events of 9/11. The research reflects a prolonged period of positive emotion after three days of extraordinary negative emotion.

Coh-Metrix⁷ is a set of tools to analyze text coherence and the narrativity of text. The tool is able to illustrate that people get more coherent when they tell a story. For example, is there coherence to the speeches of Egyptian President Hosni Mubarak? And how do the speeches map to the events in Egypt over the last 30 years? Coh-Metrix can also be applied to the tweets of the Egyptian revolution or the Libyan revolution - revealing such characteristics

as the volume and temperature; emotion, positive, negative, anger, religiosity and violence present in the coherence and narratively of the text.

Other tools include Latent Semantic Analysis (LSA), topic models and machine classifiers (e.g., Google search or spam filters using machine learning techniques). The use of linguistic analysis does not tell you *what* is happening but it does reveal that something *is* happening - giving clues about potential escalations. Social Language Processing techniques can be used in the strategic analysis of individual speeches or large collections of social media data. Automated analysis reveals patterns mirroring independently identified historical events. Every organization or nation leaks massive amounts of text. Social Language Processing converts this information glut into psychologically, socially and politically significant data.

Slides at the end of Session II.

Adam Berinsky

What happens when people get bad, irrelevant, or unimportant messages - and what can be done about it?

Take the example of the “Birther” debate surrounding Obama’s U.S. citizenship. Google trends on this topic show two big peaks: one in 2008 around the election, one in 2011. Part of the research is to understand why, again in 2011, people became really interested in this topic.

Survey methods were used to investigate these beliefs. In July of 2010, the Polimetrix survey showed only half of those surveyed say “yes” to “Do you believe Obama was born in the U.S.?” The research also focused on rumor rejection rates.

Other examples include Kerry’s alleged lies about his Vietnam service; Rumors that the FBI and CIA steadily supply guns and drugs in the inner city; 9/11 “Truther” question; and Roswell extra-terrestrial spaceships. Significant portions of the population believe these examples. Indeed, the general result is that 75% of the population believes something crazy about something and, as a result, are susceptible to rumors. There are large differences in rejection rates of partisan rumors by partisans, but not on non-partisan rumors.

So how do we get people on the right track? How do we get them to reject these rumors? Rumors are sticky – once they are out there, it’s hard to get rid of them. There is a classic WWII study of the widespread rumor that U.S. Japanese internment camps were “pleasure jaunts.” One option as a response: direct contradiction. An example is the debunking flu vaccine myths. Direct contradiction works great in the short term, but people don’t retain that, on the basis of more familiarity with the myth than the counter-evidence.

There is an example of a potential solution taken from a study of the health care “death panels” and rumors taken from actual quotes. One control mechanism is to provide correcting evidence (this shouldn’t work). The study then corrected for the partisan aspect by providing a Republican or Democratic quote. So four conditions emerge for the examination of the belief in the rumor (or the rumor rejection rates). Following are the results:

- Control: 47%
- Rejection, rumor only: 46%
- Rejection, rumor correction: 57%,
- Republican correction: 63% (Democratic correction: 56%).

Providing a corrective from a Republican, to republicans, for this Republican-focused rumor is the most effective rumor debunking strategy. Of course, the effect decays over time – a week later, all corrections are less effective.

Slides at the end of Session II.

Open Discussion

Changes in Communication Contexts

How ephemeral are emotions expressed in tweets? Also, the deep institutions of organizations are influenced by their rumors.

- People have been communicating all the time but that notion of privacy has changed, for example, social media posts has cut into email traffic and made it public and the broadcasting capability given to users.
- The big change is not just tweets. People have always communicated. It’s just too large numbers of emails. Our conceptions of privacy have radically changed. Emails are private, but not blog posts and now blogs are greater than email. So our conversations are public. Thus, the young have a broadcasting capability, and the consequences are unknown.
- We have a basic change that we have low-cost access to information.
- There is a solid finding that even a false belief does not last very long. There is an experiment on an issue where people select their own media types. What’s going on in the information environment? There’s no difference in the way of transmission; it’s only whether or not they got correction.

Explosion of Data

There is a concern regarding explosion of data and the differentiation between fact and noise as well as the question of outcome. The real challenge is how to understand how the outcome is influenced by their causal relationship with behavior or action online.

- Finding answers in the explosion of data is difficult. But we can now measure opinions extremely accurately. We can do some of these things extremely well. We don't have measures of the outcome yet. So the problem is not that the data aren't good enough, it's that we don't have enough data. Opinions are now expressed very accurately and there are techniques to analyze the new data and measure it but no measures for the outcome.
- The commercial sector is not doing the analytics that we think they might be doing to understand what the outcome is. They collect the tweets or blog posts and show those directly; they do not do long-term correlations with sales, for example. They have access to all sorts of data, but are not using it well. It is important to analyze the data in depth and over time and not to simply face the amount of data.
- There are some cases where we do have the outcome. Hedge funds, for example, which try to mine tweets to play the market. However, it doesn't work. We want to know: can you be wrong? Compared with the truth, how often are you getting it right. It's easy to do post-hoc analysis, to look at your temperature plot and label important peaks.

Rumors

Is there evidence of governments or political organizations using rumors to further their cause? Using social media to stir things up?

- It is difficult to say if government is using it for misinformation but government is using techniques to analyze data. We don't have current data on that. But sentiment analysis is big commercially. Government is also using these analyses, just to find out if the message is getting through.
- NGOs are important too.
- Most political campaigns use rumors. The difference now is not that they're trying to manipulate opinions, they get instant feedback, they don't even have to wait overnight for a poll. They need to get better, though. Political campaigns have used rumors in the past but the difference today is that there is immediate feedback.
- How Obama has reacted to the birth certificate controversy is an example, it's not just about speed, it's about strategy. There is a team, which consults with the White House, and the thought was not to confront it but to avoid giving it legitimacy. Considerations and impact of direct engagement, and the like dominated. It is very hard to counter these rumors.

How good are you at predicting whether a rumor will catch on?

- There is lots of work on this. Level of disgust and anxiety are good predictors. More emotionally engaging rumors make people more likely to spread them. Many industrial organizations work on this.

Opinion and Social Media

When looking at how widespread an opinion is, how do we correct for intensity of belief? How are users of social media different from users of email? Are we almost measuring the same thing?

- It is an important theoretical question of whether to count everyone equally or based on various qualifiers.
- We are not measuring the same thing; we are measuring the expressed opinion. We are looking at whoever speaks, but you may not want that. One may want a truly random sample. One may want to look at intense expressions. There are many ways of approaching opinions.
- It depends on how the story is being told and what is highlighted, so there is a variety of factors that create quality of rumors e.g., emotions such as anxiety or disgust increasing the likelihood of the rumor being spread.

Probability

Can Bayesian priors be explored?

- Any predictive analysis will eventually be self-defeating because everyone will do it.
- If we would get a telescope that is 10,000 times better than any telescope we currently have, what would we know on the first day? Probably very little, because we do not know what we are seeing until we have invested time to analyze it. On the first day, we wouldn't know what we were looking at. But we would get there. We are on the first day.

Research Methods

In discussion with other scientists, some stated that what Minerva is doing is not basic research but specific research; are we too much captives of our own disciplines? But physical scientists say this is not basic research – you're studying particular countries at a particular time. Question: Are we applying the incorrect categories to this field? Should we move to less of a distinction between basic/applied?

- The big change that is happening is that a social science office today includes the PI typing away on code; in physical sciences, they have whole buildings and labs to do that for them. But there is a lack of resources to analyze the new data and therefore necessity to collaborate with others but other disciplines might not

have similar interests in topic or type of questions. Basic vs. applied may not matter very much but rather abstract models with practical applicability are more important, it won't be built in the same way as the physical sciences; it will be different. The ones that are most productive are the ones that start on the basic side and run all the way to the applied end.

Translation Issue

How important is quality?

- Different set of methods that can be applied to original language or translated language; human language is incredibly subtle no matter what algorithm you come up with, you can come up with an example, which will break it. It is often repeated. How much of a person do you need to listen to determine if they're vitriolic? We use the repetition, and try to avoid the pitfalls created by the subtlety. We have to be sensitive to the quantity we are trying to estimate.
- To what extent is noise and bias a particular method introduces? Different errors created by translation checked by native speakers as well as differences regarding size of error with regard to positive and negative sentiments. You have to measure the error. For the tweets, the positive and negative ones have different error rates.

How Do We Listen: New Ways to Analyze the Messages

Michael Siegel

Sloan School of Management, MIT

HOW DO WE LISTEN: NEW WAYS TO ANALYZE THE MESSAGES

Presentations:

Gary King

Department of Government, Harvard University

David Beaver

Linguistics Department, University of Texas at Austin

Adam Berinsky

Political Science Department, MIT

Discussant:

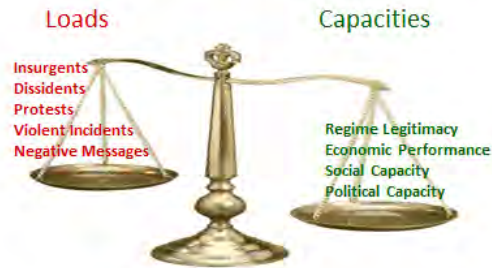
Michael Siegel

Sloan School of Management, MIT

1

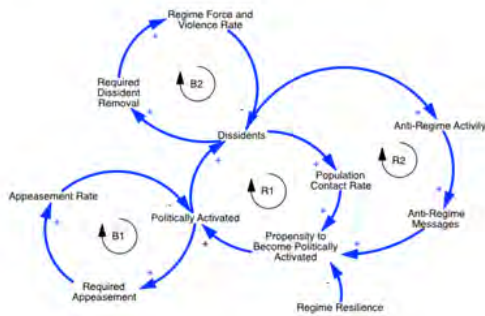
State Stability

The stability of the state is a function of the relationship between the loads (or pressures) on the system, and its capacities (or power) to manage these loads.



2

Insurgency and State Stability



3

CHANGING DYNAMICS

"States remain the dominant actors on the world stage, but they are finding the stage far more crowded and difficult to control."

What is new -- and what we see manifested in Egypt today -- is the speed of communication and the technological empowerment of a wider range of actors."

- Joseph Nye, Jr. 2011

4

ROLE OF CYBER?

Benkler argues that the Internet has created an environment where it is increasingly difficult for governments to suppress democratic aspirations of citizens (Benkler, 2006)



Authoritarian governments are effectively using the Internet to suppress free speech, hone their surveillance techniques, and disseminate cutting-edge propaganda. (Morozov, 2011)

DOES IT EVEN MATTER?

People protested and brought down governments before Facebook was invented. They did it before the Internet came along. Barely anyone in East Germany in the nineteen-eighties had a phone.... People with a grievance will always find ways to communicate with each other. How they choose to do it is less interesting, in the end, than why they were driven to do it in the first place.

For [Shirky]... to be anything close to persuasive, he has to convince readers that in the absence of social media, those uprisings would not have been possible."

— (Gladwell, 2011)

5

CYBER CASES

REGIME CHANGE

Philippines 2001 Resignation of President Joseph Estrada. The protest was arranged, in part, by forwarded text messages reading, "Go 2 edsa. Wear blk." The crowd quickly swelled, and in the next few days, over a million people arrived, choking traffic in downtown Manila.

Spain 2004 Demonstrations organized by text messaging led to the quick ouster of Spanish Prime Minister José María Aznar, who had inaccurately blamed the Madrid transit bombings on Basque separatists.

Moldova 2009 The Communist Party lost power when massive protests coordinated in part by text message, Facebook, and Twitter broke out after an obviously fraudulent election.

Source: Shirky, 2011

NO CHANGE

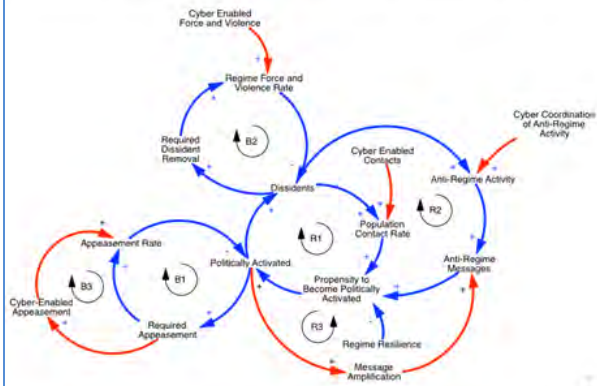
Belarus 2006 Street protests (arranged in part by e-mail) against President Aleksandr Lukashenko's alleged vote rigging swelled, then faltered, leaving Lukashenko more determined than ever to control social media.

Iran 2009 During the June 2009 uprising of the Green Movement in Iran, activists used every possible technological coordinating tool to protest the miscount of votes for Mir Hossein Mousavi but were ultimately brought to heel by a violent crackdown.

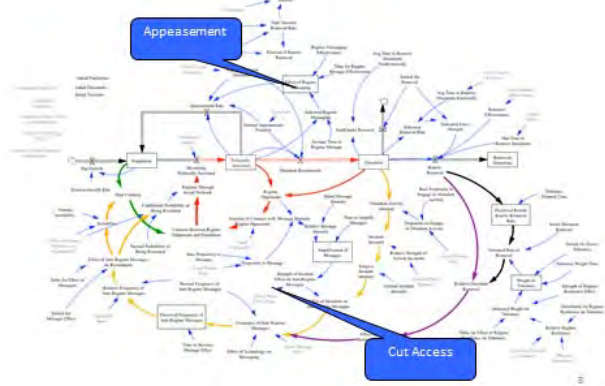
Thailand 2010 The Red Shirt uprising in Thailand in 2010 followed a similar but quicker path: protesters saw vvy with social media occupied downtown Bangkok until the Thai government dispersed the protesters, killing dozens

6

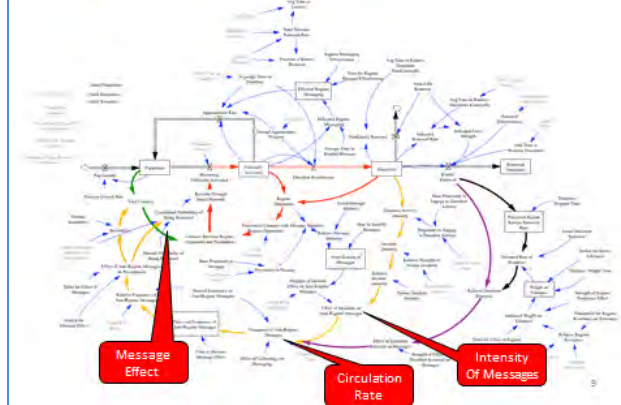
Cyber, Insurgency and State Stability



CAPACITIES – How Do We Listen?



LOADS – How Do We Listen?



The Social Science Data Revolution

Gary King

Institute of Quantitative Social Science, Harvard University

The Social Science Data Revolution

Gary King

Institute for Quantitative Social Science
Harvard University

(People, Power, & CyberPolitics Workshop, MIT, 12/8/11)

Gary King (Harvard, IQSS) The Data Revolution 1 / 12

The Changing Evidence Base of Social Science Research

The Last 50 Years:

- Survey research
- Aggregate government statistics
- In depth studies of individual places, people, or events

The Next 50 Years: Spectacular increases in new data sources, due to...

- Much more of the above
- Shrinking computers & the growing Internet: data everywhere
- The replication movement: academic data sharing (e.g., Dataverse)
- Analogue-to-digital transformation of government records
- Advances in statistical methods, informatics, & software
- *The march of quantification*: through academia, professions, government, & commerce (*SuperCrunchers*, *The Numerati*, *MoneyBall*)
- The end of the quantitative-qualitative divide

Gary King (Harvard, IQSS) The Data Revolution 2 / 12

Examples of what's now possible

- **Opinions of activists:** $\approx 1,000$ interviews \rightsquigarrow millions of political opinions in social media posts (1B every 4 days)
- **Exercise:** A survey: "How many times did you exercise last week?" \rightsquigarrow 500K people carrying cell phones with accelerometers
- **Social contacts:** A survey: "Please tell me your 5 best friends" \rightsquigarrow continuous record of phone calls, emails, text messages, bluetooth, social media connections, electronic address books
- **Economic development in developing countries:** Dubious or nonexistent governmental statistics \rightsquigarrow satellite images of human-generated light at night, or networks of roads and other infrastructure
- Many, many more...

Gary King (Harvard, IQSS) The Data Revolution 3 / 12

How to Read Billions of Social Media Posts

Daniel Hopkins and Gary King. "A Method of Automated Nonparametric Content Analysis for Social Science" *AJPS*, 54 (2010): 229-247

- 1 Downloaded & analyzed all English-language blog posts every day. (We learned: The university is not a research, not production, environment!)
- 2 Commercialized in 2008:



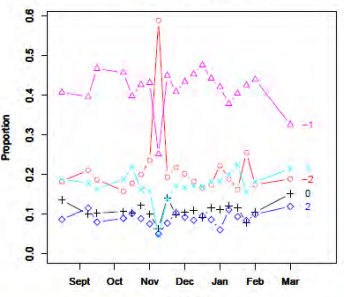
- 3 CH collects *all* social media posts, runs huge servers with our methods
- 4 **Crimson Hexagon Academic Grant Program** to be announced soon (I.e., easy to do what I'll describe today)

Gary King (Harvard, IQSS) The Data Revolution 5 / 12

Example: Reactions to John Kerry's Botched Joke

You know, education — if you make the most of it ... you can do well. If you don't, you get stuck in Iraq.

Affect Towards John Kerry



Gary King (Harvard, IQSS) The Data Revolution 6 / 12

Data and Quantities of Interest

- **Input Data:**
 - All social media posts (or other documents)
 - Categories (e.g., posts about US candidates: extremely negative, negative, neutral, positive, extremely positive, no opinion, not a blog)
 - Example documents from each category
- **Quantities of interest**
 - Computer science: **individual document classification** (spam filters, Google searches)
 - Social Science: **category proportions** (% of email which is spam; % negative comments about Obama; % of Egyptian posts supporting the regime; support for different solutions to the Euro \$ crisis)
- **Estimation**
 - Classifications add up to proportions only if accurate
 - High classification accuracy \neq unbiased category proportions
 - 70% classification accuracy is high \Rightarrow disaster for category proportions
 - New methodology \rightsquigarrow **unbiased category proportions**, (even when classification accuracy is low)

Gary King (Harvard, IQSS) The Data Revolution 7 / 12

What Else Can We do With this?

- You choose:
 - Data: country, documents, language
 - Categories: based on sentiment, topics, people, events, etc.
 - (often pre-censorship)
- You provide: example documents for each category
- Results: Highly accurate category proportions over time
- Qualifications:
 - Opinion not sampled randomly; but no pop quizzes about unknown subjects
 - Measures the ongoing conversation: the classical notion of "activated public opinion"
- Potential academic applications: very widespread

Gary King (Harvard, IQSS)

The Data Revolution

8 / 12

Some New Data Types

- 1 **Unstructured text:** emails (1 LOC every 10 minutes), speeches, government reports, blogs, social media updates, web pages, newspapers, scholarly literature
- 2 **Commercial activity:** credit cards, sales data, and real estate transactions, product RFIDs
- 3 **Geographic location:** cell phones, Fastlane or EZPass transponders, garage cameras
- 4 **Health information:** digital medical records, hospital admittances, google/MS health, and accelerometers and other devices being included in cell phones
- 5 **Biological sciences:** effectively becoming social sciences as genomics, proteomics, metabolomics, and brain imaging produce huge numbers of *person-level variables*.
- 6 **Satellite imagery:** increasing in scope, resolution, and availability.
- 7 **Electoral activity:** ballot images, precinct-level results, individual-level registration, primary participation, and campaign contributions

Gary King (Harvard, IQSS)

The Data Revolution

9 / 12

Some More New Data Examples

- 1 **Social media:** facebook, twitter, social bookmarking, blog comments, product reviews, virtual worlds, game behavior, crowd sourcing
- 2 **Web surfing artifacts:** clicks, searches, and advertising clickthroughs. (Google collects 1 petabyte/72 minutes on human behavior!)
- 3 **Multiplayer web games and virtual worlds:** Billions of highly controlled experiments on human behavior
- 4 **Government bureaucracies:** moving from paper to electronic data bases, increasing availability
- 5 **Governmental policies:** requiring more data collection, such e.g., "No Child Left Behind Act"; allowing randomized policy experiments; Obama pushing data distribution
- 6 **Scholarly data:** the replication movement in academia, led in part by political science, is massively increasing data sharing

Gary King (Harvard, IQSS)

The Data Revolution

10 / 12

Enormous Emerging Opportunities for Social Scientists

- For the first time: **technologies, policies, data, and methods** are making it feasible to attack some of the most vexing problems that afflict human society
- A massive change from **studying problems** to **understanding and solving problems**
- And then there's you & me:
 - In legislatures, courts, academic departments, . . . , change comes from replacement not conversion
 - Will we wait to be replaced? or put in the effort to convert and learn how to use the new information?

Gary King (Harvard, IQSS)

The Data Revolution

11 / 12

For more information



<http://GKing.Harvard.edu>

Gary King (Harvard, IQSS)

The Data Revolution

12 / 12

Social Language Processing: A new way to analyze a big heap of messages

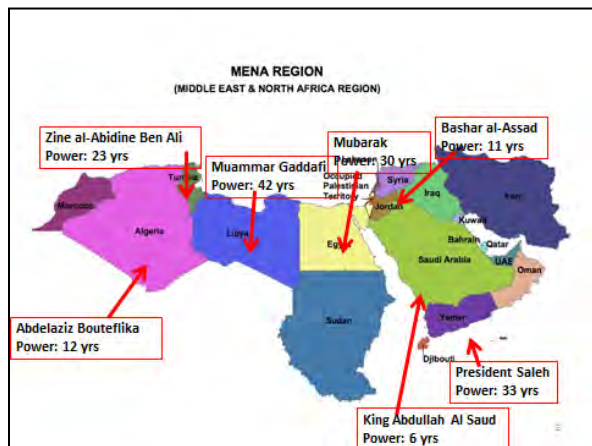
David Beaver

University of Texas, Austin, Department of Linguistics

Social Language Processing: A new way to analyze a big heap of messages

Project PIs	
David Beaver (<i>dib@mail.utexas.edu</i>)	UT Austin, Linguistics
Jeff Hancock	Cornell University, Communications
James W. Pennebaker	UT Austin, Psychology
Art Graesser	University of Memphis, Psychology
Coauthors	
Joey Frazee	UT Austin, Linguistics
Chris Brown	UT Austin, Linguistics
Xiong Liu	Intelligent Automation Inc. (I.A.I.)
Fred Hoyt	University of New England
Nia Dowell	University of Memphis, Psychology
Fazel Keshkhar	University of Memphis, I.I.S.
Cindy Chung	UT Austin, Psychology

Acknowledgments: this work was funded by a Minerva award through the National Science Foundation (NSF 0904813,0904809,0904822), "Modeling Discourse and Social Dynamics in Authoritarian Regimes", and by the ARI (W91WAW-07-C002).

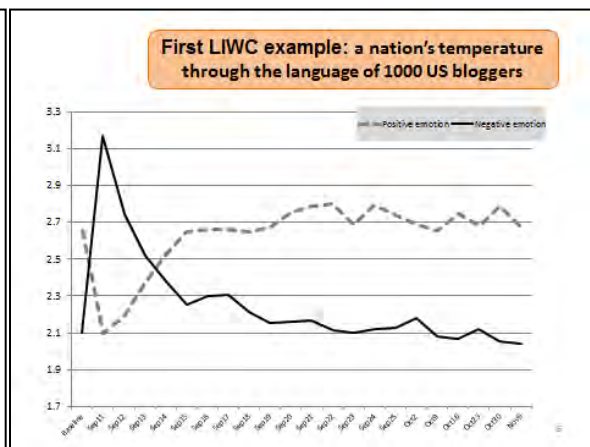


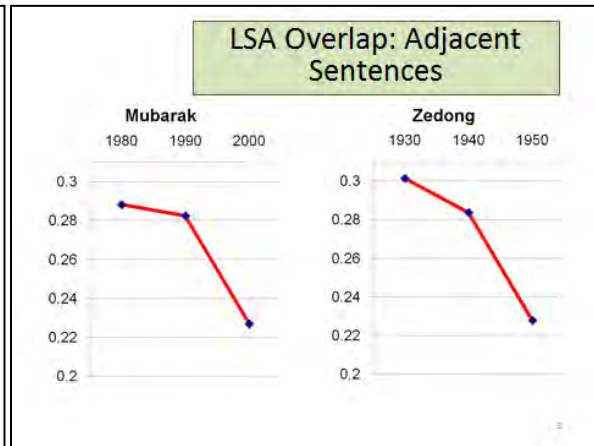
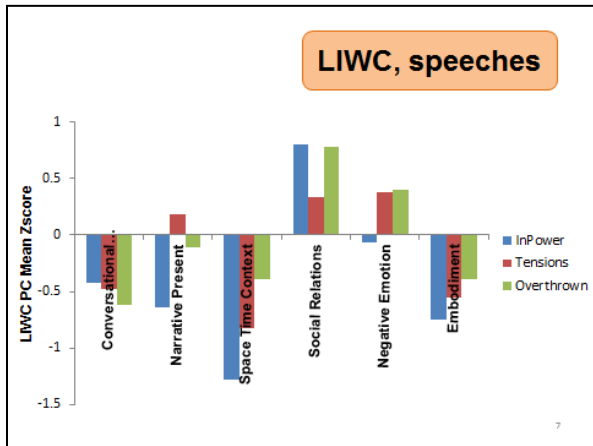
Specific tools

- **Linguistic Inquiry Word Count – LIWC**
(Pennebaker, Booth, & Francis, 2007)
- **Coh-Metrix**
(Graesser, McNamara, Louwerse, & Cai, 2004)
- **Latent semantic analysis and Topics models**
(Landauer, McNamara, Dennis, & Kintsch, 2007)
- **Machine Classifiers, e.g. Max. Ent.**
(Berger, DellaPietra, & Della Pietra, 1996)

Applying strategic language analysis

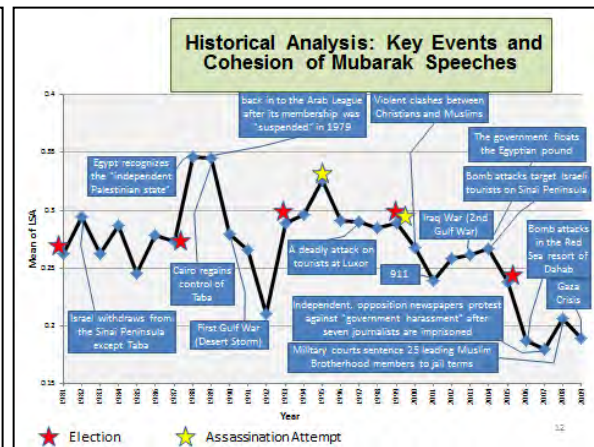
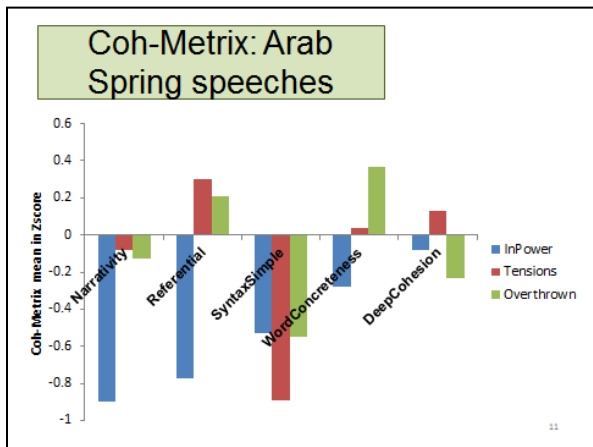
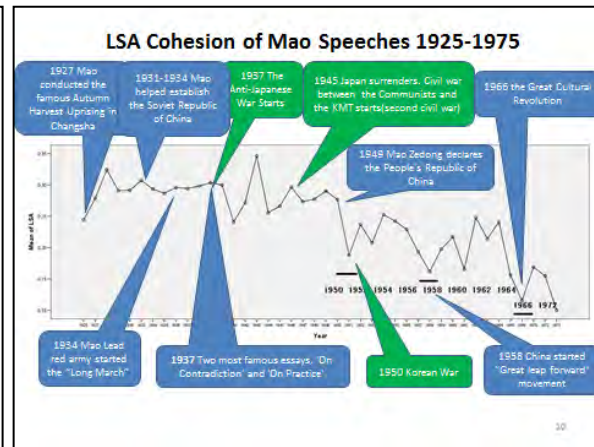
- **Method:** psychologically and linguistically motivated analysis of political speeches, military communications, and social media.
- **Research Question:** can semi-automated analyses provide information about the nature and stability of a nation?



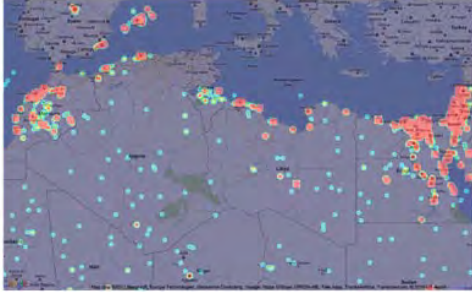


Chinese Cohesion

在中国人民面前摆着两条路。
光明的路和黑暗的路。
有两种中国之命运。
光明的中国之命运和黑暗的中国之命运。
现在日本帝国主义还没有被打败。
即使把日本帝国主义打败了。
也还是有这样两个前途。
或者是一个独立、自由、民主、统一、富强的中国。
就是说，光明的中国。
中国人民得到解放的新中国。
或者是另一个中国。
半殖民地半封建的、分裂的、贫弱的中国。
就是说，一个老中国。
一个新中国还是一个老中国。
两个前途。
仍然存在中国人民的面前...

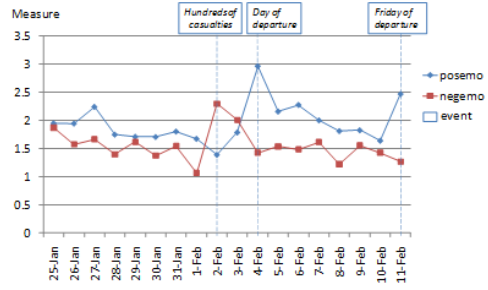


Tweets in the Arab Spring



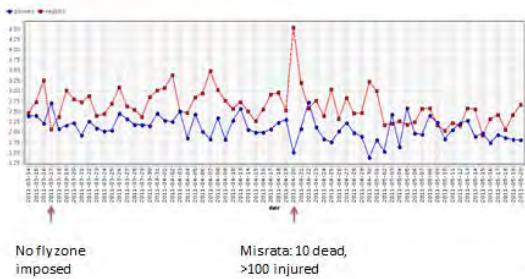
13

Emotion in Egypt revolution tweets



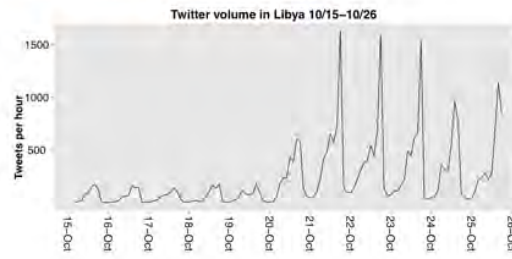
14

Emotion in Libya tweets (pt. 1)



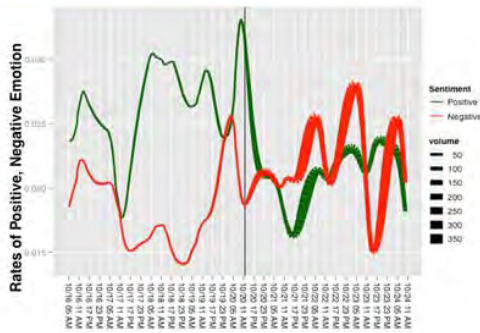
15

When Libyans tweeted 10/16-10/24



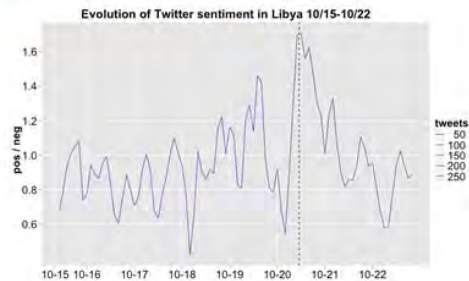
16

Emotion in Libya 10/16-10/24



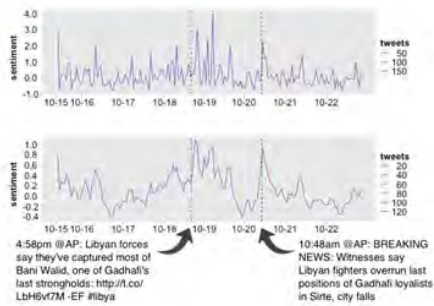
17

Libyan emotion ratio 10/16-10/24



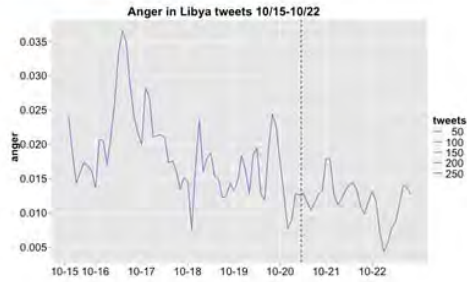
18

Smoothed Libyan emotion ratio 10/16-10/24



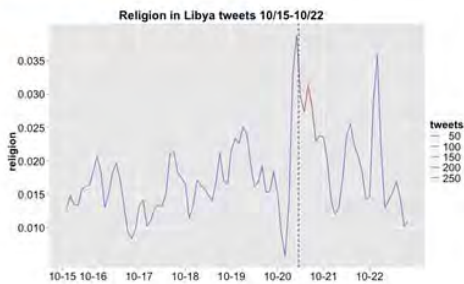
15

Anger in Libya tweets



20

Religion in Libya tweets



21

Death in Libya tweets



22

Conclusions

- *Social Language Processing* techniques can be used in strategic analysis of:
 - individual speeches
 - large collections of social media data
- Automated analysis reveals patterns mirroring independently identified historical events
- Every organization or nation leaks massive amounts of text: *Social Language Processing* converts this information glut into psychologically, socially, and politically significant data.
- Your mission, should you choose to accept it...
Interpret that data!

23



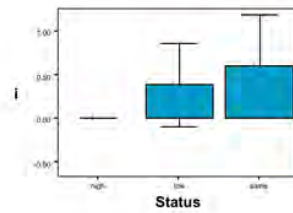
24

**A final Example of SLP in action:
Status in Iraqi military communications**

- Sample of 60 letters drawn from the Iraqi Perspectives Project (IPP; Woods et al, 2006).
- Twenty letters were selected from the IPP database for each of three conditions:
 1. high status -> low status
 2. low status -> high status
 3. equal status

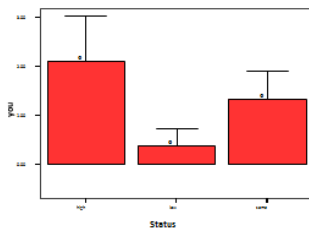
25

1st Person pronouns in Iraqi military transmissions



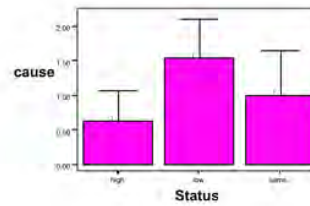
26

2nd Person pronouns in Iraqi military transmissions



27

Causal words in Iraqi military transmissions



28

Interpreting the word count data

- Clearly low-level word frequency varies with status.
- But what does it mean?
- And can we do anything useful with it?

29

Using Machine Classifiers to build a predictive model of status

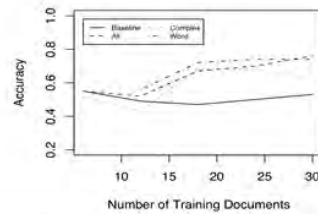


Figure 1 Performance of Binary Maximum Entropy Classifiers for Hi/Low vs Lo/Hi Status for Military Transmissions in the IPP Database

30

Sample mistranslations

- **Timestamp:** 2011-10-20T14:12:54
- **Original:** اللهم أكبر الله أكبر الله أكبر لا إله إلا الله والله أكبر والله الحمد الحرية للشعب الليبي الحرة والمرة لليبي عاشت ليبيا حرة
- **Machine translation:** *God is great, God is greater for the largest agency Elaallah and God is great and thank God for the freedom of free people of Libya and Libya's pride lived Libya is free*
- **Liwc pos/neg:** 10
- **Human translation:** *God is Great! God is Great! God is Great! There is no god but God and God is Great and God is the Praised! Freedom for the free Libyan people and glory to Libya, free Libya lives!*
- **Note:** *la ilaha 'ila Allah لا إله إلا الله* "[there is] no god but [the] God" is translated as "for the largest agency"

31

- **Timestamp:** 2011-10-20T14:1:2
- **Original:** شكر المهدى زيو شكر محمد نوس شكر علي جابر شكر الحلبوس شكر بنغازي شكر مصراته شكر الجبل العزبي شكر الزنتان شكر الزاوية شكر ليبيا
- **Machine translation:** *Thank you, thank you Mohammed Mahdi ZEW Nbus Thanks Ali Jaber Lhalboss Thank you Thank you Thank Benghazi Misurata Thank western mountain Alzentan Thank you Thank you Thank you to Libby corner*
- **liwc pos/neg:** 10
- **Note:** *liybya* gets translated as "Libby corner."

32

- **Timestamp:** 2011-10-20T17:16:36
- **Original:** ليبيا حرة معص مات انا ليبي حر واقتخر ليبيا حرة
- **Machine translation:** *Libya's Muammar free I'm Matt Libby a free and proud Libby is free*
- **liwc pos/neg:** 7
- **Human translation:** *Libya is free! Mu'ammr has died! I am a free Libyan and I take pride in free Libya!*

33

- **Timestamp:** 2011-10-20T17:14:32
- **Original:** ومن كان يحب الله!! من كان يحب معمر فأن معمر قد مات... الله أكبر والله الحمد وعاشت ليبيا حرة... فأن الله حي لا يموت
- **Machine translation:** *The likes of Muammar al-Muammar, the dead!! It was like God, God is alive to senior underwriter God is great and thankfully lived Libby is free...*
- **liwc pos/neg:** 6
- **Human translation:** *Whoever used to love Mu'ammr, verily Mu'ammr has died! And whoever used to love God, verily God lives and does not die! God is Great and God is Praised and free Libby lives!*

34

Selected References

- J. Hancock, D. Beaver, C. Chung, J. Frazee, J. Pennebaker, Z. Cai, & A. Graesser, Social Language Processing: A Framework for Analyzing the Communication of Terrorists and Authoritarian Regimes (2010), Behavioral Sciences of Terrorism and Political Aggression 2:2 (pp. 108-132).
- Fara, N., Challita, E., Assi, R. A. & Hajj, H. (2010). 'Sentence-level and document-level sentiment mining for Arabic texts', Data Mining Workshops, International Conference on O, 1114-1119.
- Hayeri, N., Chung, C., Booth, R. J. & Pennebaker, J. W. (2010). LIWC for Arabic texts. Austin TX: www.LIWC.net.
- O'Connor, B., Balasubramanyan, R., Routledge, B. R. & Smith, N. A. (2010). From tweets to polls: Linking text sentiment to public opinion time series, in 'Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media'.
- Pennebaker, J. W., Booth, R. J. & Francis, M. E. (n.d.), Linguistic Inquiry and Word Count (LIWC2007): A text analysis program.
- Pennebaker, J. W., Chung, C. K., Ireland, M., Gonzales, A. & Booth, R. (n.d.), The development and psychometric properties of LIWC2007.
- Brown, C., J. Frazee & D. Beaver (2011) Evolution of Sentiment in the Libyan Revolution, Working Paper for the NSF Minerva Project: Modeling Discourse and Social Dynamics in Authoritarian Regimes, NSF 0904913 at the University of Texas at Austin, <https://webspace.utexas.edu/dlb97/libya-report-10-30-11.pdf>

35

Rumors, Truths, and Reality: A Study of Political Misinformation

Adam Berinsky

Department of Political Science, MIT

Barack Obama citizenship conspiracy theories

From Wikipedia: In the scriptural.

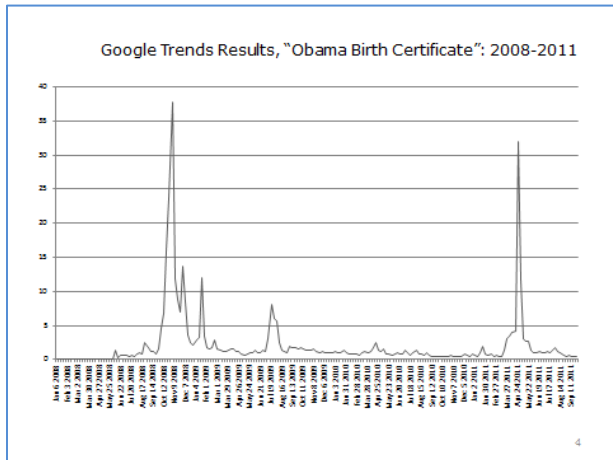
Conspiracy theories about the citizenship of Barack Obama are those that reject the legitimacy of the United States citizenship of President Barack Obama and are typically in the President of the United States. Some of these conspiracy theories allege that Obama was born in Kenya and Hawaii, and that his birth certificate is a forgery. Other allege that Obama is a citizen of Indonesia, or that someone he had contact with in high school had fabricated for a year a journal entry titled the United States, which is a requirement to be President of the United States under Article Two of the United States Constitution. These conspiracy theories are most prominent as well following Obama's victory in the Democratic primary in June 2008 and 2009 and support of the President Obama and anti-Obama conspirators, and often in such 2008 following a breach by anti-sectarian Justice Court.

These claims are presented by a number of fringe activists and political commentators who claim to have the right to disregard Obama's birth, leading to being confirmed as President, or to a false additional proof that he is qualified. These men that will not be named to the Supreme Court of the United States.^[1] Some of these men were provided to have been.^[2] Although Obama was confirmed as president last by Congress on January 20, 2009,^[3] such cases as in President or "Obama" is "Obama" (although not that his position). These conspiracy theories are frequently called "Obama" or "Obama" to describe their particular false claims. "Obama" is often used as a "Obama" conspiracy theory.^[4]

The Obama conspiracy theories are a 2007 website copy of his birth certificate for his services related to a "Certificate of Birth" for Barack Obama was born in Honolulu, Hawaii, on August 1, 1961. Frequent repetition of these conspiracy theories is significant in that it has been related to a conspiracy of "Obama" birth certificate, and that the act of the "Obama" certificate of his birth, as the document is not required to read "Obama" certificate. These conspirators have a long history of conspiracy to make arrangements or other political forces that has influenced the nation and therefore government officials, a conspiracy of false news mentioned that the certificate released by the Obama conspiracy to submit the official birth certificate.^[5] Some claim the Phoenix Department of Health spokeswoman, Inara Shika (now the Obama) "She has been a quiet force in helping Obama certify."^[6] However, the Director of the Department has confirmed that the year "for the Obama" signed birth certificate as record is consistent with true policies and practices.^[7]

This document, under appropriate official, were prepared and signed by Obama's conspiracy to have the right of a link of Wikipedia to acknowledge a "Obama" certificate, members of the U.S. Congress and some executive have approved and used the legislation to require guidelines, conditions or provide documentation of their qualifications or the particular website mentioned, following.

2



July 2010 Polimetrix Survey

- Do you think that Senator John Kerry lied about his actions during the Vietnam war in order to receive medals from the U.S. Army?
 - Yes: 35%
 - No: 34%
 - Not Sure: 31%

6

July 2010 Polimetrix Survey

- Do You Believe that Barack Obama was Born in the United States of America?
 - Yes: 55%
 - No: 27%
 - Not Sure: 19%

5

July 2010 Polimetrix Survey

- Do you think the FBI and the CIA make sure that there is a steady supply of guns and drugs in the inner city?
 - Yes: 15%
 - No: 63%
 - Not Sure: 22%

7

July 2010 Polimetrix Survey

- Do you think that people in the federal government either assisted in the 9/11 attacks or took no action to stop the attacks because they wanted the United States to go to war in the Middle East?
 - Yes: 18%
 - No: 64%
 - Not Sure: 18%

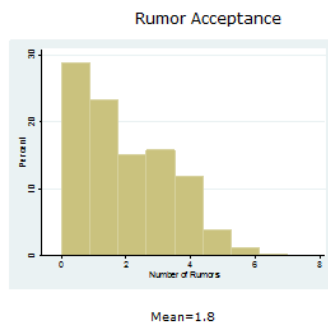
8

July 2010 Polimetrix Survey

- Do you believe that a spacecraft from another planet crashed in Roswell, New Mexico in 1947?
 - Yes: 22%
 - No: 45%
 - Not Sure: 33%

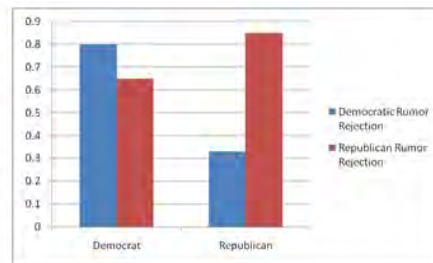
9

Distribution of Beliefs



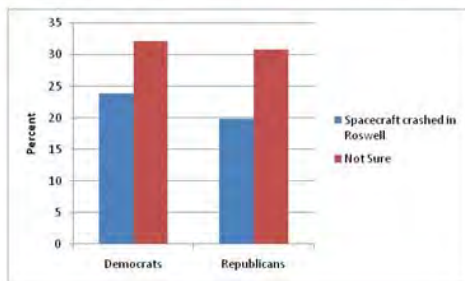
10

Partisan Divisions...



11

...But Only on Partisan Questions



12

How Can We Correct Rumors?

- Rumors are sticky
- Direct contradiction?
 - Intuitive: Fiction vs. fact
 - Reinforcing rumors: correction backfire
 - Schwarz's theory of fluency
 - Counter-arguing?
- Source credibility
 - Motivated reasoning
 - Not all arguments are equally effective
 - The role of partisanship

13

"People can die from the flu." TRUE
Influenza (flu) is a highly infectious disease of the lungs, and it can lead to pneumonia. Each year about 1.15 billion people in the U.S. are hospitalized and about 36,000 people die because of the flu. Most who die are 65 years and older. But most children less than 2 years old are as busy as those over 65 to have to go to the hospital because of the flu.

"Even if I get the vaccine, I can still get a mild case of the flu." TRUE
The vaccine usually protects most people from the flu. Sometimes a person who receives flu vaccine can get the flu, but will feel less sick than without the vaccine. Flu vaccine will not protect you from other viruses that sometimes feel like the flu.

"The side effects are worse than the flu." FALSE
The worst side effect you're likely to get with injectable vaccine is a sore arm. The most used flu vaccine might cause nasal congestion, runny nose, sore throat and cough. The risk of a rare allergic reaction is far less than the risk of severe complications from influenza.

"Not everyone can take flu vaccine." TRUE
You might be able to get the protection if you are allergic to eggs used in making the vaccine, are sick with a high fever, or have had a severe reaction to the flu vaccine in the past.

"Only older people need flu vaccine." FALSE
Adults and children with conditions like asthma, diabetes, heart disease, and kidney disease need to get flu vaccine. People who are active and healthy can benefit from the protection the flu vaccine offers.

"You must get a flu vaccine before December." FALSE
Flu vaccine can be given before or during the flu season. While the best time to get flu vaccine is October or November, getting immunized in December or later can still protect you against the flu.

For more information on immunization questions call the toll-free number: 800-232-2522 Visit: www.cdc.gov/flu

May 2010 Internet Panel

- 1608 interviews
- Subject: Death panels/health care reform

Rumor Only

Health Care Reform: Will There Be Death Panels?

By JONATHAN G. PRATT
Published: November 15, 2009

WASHINGTON, DC – With health care reform in full swing, politicians and citizen groups are taking a close look at the provisions in the Affordable Health Care for America Act (H.R. 3962) and the accompanying Medicare Physician Payment Reform Act (H.R. 3961).

Discussion has focused on whether Congress intends to establish "death panels" to determine whether or not seniors can get access to end-of-life medical care. Some have speculated that these panels will force the elderly and ailing into accepting minimal end-of-life care to reduce health care costs. Concerns have been raised that hospitals will be forced to withhold treatments simply because they are costly, even if they extend the life of the patient. Now talking heads and politicians are getting into the act.

Betsy McCaughey, the former Lieutenant Governor of New York State has warned that the bills contain provisions that would make it mandatory that "people in Medicare have a required counseling session that will tell them how to end their life sooner."

Iowa Senator Chuck Grassley, the ranking Republican member of the Senate Finance Committee, chimed into the debate as well at town-hall meetings, telling a questioner, "You have every right to fear... [You] should not have a government-run plan to decide when to pull the plug on Grandma."

Rumor + Correction

Health Care Reform and Death Panels: Setting the Record Straight

By JONATHAN G. PRATT
Published: November 15, 2009

WASHINGTON, DC – With health care reform in full swing, politicians and citizen groups are taking a close look at the provisions in the Affordable Health Care for America Act (H.R. 3962) and the accompanying Medicare Physician Payment Reform Act (H.R. 3961).

However, a close examination of the bill by non-partisan organizations reveals that the controversial proposals are not death panels at all. They are nothing more than a provision that allows Medicare to pay for voluntary counseling.

The American Medical Association and the National Hospice and Palliative Care Organization support the provision. For years, federal laws and policies have encouraged Americans to think ahead about end-of-life decisions.

The bills allow Medicare to pay doctors to provide information about living wills, pain medication, and hospice care. John Rother, executive vice president of AARP, the seniors' lobby, repeatedly has declared the "death panel" rumors false.

Rumor + Republican Correction

Health Care Reform and Death Panels: Setting the Record Straight

By JONATHAN G. PRATT
Published: November 15, 2009

WASHINGTON, DC – With health care reform in full swing, politicians and citizen groups are taking a close look at the provisions in the Affordable Health Care for America Act (H.R. 3962) and the accompanying Medicare Physician Payment Reform Act (H.R. 3961).

However, a close examination of the bill by non-partisan organizations reveals that the controversial proposals are not death panels at all. They are nothing more than a provision that allows Medicare to pay for voluntary counseling.

The new provision is similar to a proposal in the last Congress to cover an end-of-life planning consultation. That bill was co-sponsored by three Republicans, including John Isakson, a Republican Senator from Georgia.

Speaking about the end of life provisions, Senator Isakson has said, "It's voluntary. Every state in America has an end of life directive or durable power of attorney provision... someone said Sarah Palin's web site had talked about the House bill having death panels on it where people would be euthanized. How someone could take an end of life directive or a living will as that is nuts."

Rumor + Democratic Correction

Health Care Reform and Death Panels: Setting the Record Straight

By JONATHAN G. PRATT
Published: November 15, 2009

WASHINGTON, DC – With health care reform in full swing, politicians and citizen groups are taking a close look at the provisions in the Affordable Health Care for America Act (H.R. 3962) and the accompanying Medicare Physician Payment Reform Act (H.R. 3961).

However, a close examination of the bill by non-partisan organizations reveals that the controversial proposals are not death panels at all. They are nothing more than a provision that allows Medicare to pay for voluntary counseling.

The Democratic Congressman who wrote the now-famous provision in the House health care bill has responded as well.

Speaking about the end of life provisions, Democrat Earl Blumenauer of Oregon has said the measure "would merely allow Medicare to pay doctors for voluntary counseling sessions that address end-of-life issues... [the existence of death panels is] a blatant lie, and everybody who has checked it agrees."

May 2010 Death Panel Results (Attentive Sample)

	Control	Rumor Only	Rumor+ Correction	Rumor+ Republican Correction	Rumor+ Democratic Correction
Yes	21	21	16	14	18
No	47	46	57	63	56
Not Sure	33	34	28	22	26

N=874; $\chi^2(8)=15.54$ Pr=0.05

20

May 2010 Euthanasia Results (Attentive Sample)

	Control	Rumor Only	Rumor+ Correction	Rumor+ Republican Correction	Rumor+ Democratic Correction
Yes	12	17	14	15	17
No	57	46	60	69	60
Not Sure	31	36	26	16	24

N=876; $\chi^2(8)=23.95$ Pr=0.002

21

Euthanasia Results by PID (Attentive Sample)

Democrats

	Control	Rumor Only	Rumor+ Correction	Rumor+ Republican Correction	Rumor+ Democratic Correction
Yes	5	5	7	3	10
No	68	67	68	85	78
Not Sure	28	28	25	13	12

N=367; $\chi^2(8)=14.42$ Pr=0.071

Republicans

	Control	Rumor Only	Rumor+ Correction	Rumor+ Republican Correction	Rumor+ Democratic Correction
Yes	22	33	28	27	19
No	50	25	39	61	49
Not Sure	28	42	33	12	32

N=334; $\chi^2(8)=24.32$ Pr=0.002

22

May 2010 Support for Health Care Reform (Attentive Sample)

	Control	Rumor Only	Rumor+ Correction	Rumor+ Republican Correction	Rumor+ Democratic Correction
Support	51	42	46	48	37
Oppose	49	58	54	52	63

N=876; $\chi^2(4)=9.00$ Pr=0.06

23

Euthanasia Panel Data

Wave 1

	Control	Rumor Only	Rumor+ Correction	Rumor+ Republican Correction	Rumor+ Democratic Correction
Yes	13	18	13	15	18
No	58	43	58	68	61
Not Sure	59	38	29	18	21

N=696; $\chi^2(8)=23.2$ Pr=0.03

Wave 2

	Control	Rumor Only	Rumor+ Correction	Rumor+ Republican Correction	Rumor+ Democratic Correction
Yes	12	18	15	16	21
No	57	43	51	58	53
Not Sure	31	38	34	26	25

N=696; $\chi^2(8)=12.2$ Pr=0.14

24

III. People, Power & Pressures on Governance: Threats & Opportunities

Framing Questions

What evidence do we have that cyberspace enables people to put pressure on governments?

Does the cyber participation of people influence the distribution of power in international relations?

How have governments responded, if at all, to any cyber-enabled power of people?

Can we identify new opportunities or modes of behavior for people, the state and the international community?

What will be the effect on international relations now and in the future?

Panel

Moderator

Melissa Hathaway, *Harvard Kennedy School*

Panelists

Chappell Lawson, *Political Science Department, MIT*

Joel Brenner, *Cooley LLP*

Roger Hurwitz, *Computer Science and Artificial Intelligence Laboratory, MIT*

Presentations

Melissa Hathaway

Three main themes are central to the discussion of people, power, and pressures on governance: These are (a) people and governments, (b) privacy, and (c) government control over the Internet.

Even Machiavelli talked the about political implication of technologies. Politics sometimes supports technologies and sometimes discriminates against it. There are citizen services,

voting on the Internet, democratic decision making, and we have to balance surveillance, privacy, and anonymity. Conversations always come down to the theme of regime stability – and the choice of shutting down versus listening to the nature of the informant.

What is the evidence that cyberspace is able to put pressures on governance?

Joel Brenner

(Author of the recently released “*America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*”)

There is an increasing transparency in our lives, both positive and negative. Transparency is *the overarching* trend in this panel discussion.

The relationship between privacy and transparency is similar to what Shakespeare said about drink and lechery:

“It provokes the desire but it takes away the performance. Therefore much drink may be said to be an equivocator with lechery: it makes him and it mars him; it sets him on and it takes him off.”

There are remarkable examples in the last few years about how this effects governments. Government is all at once a dis-intermediary and the government is an intermediary. For example, CIA rendition flights were exposed by hobbyist plane spotters who made notes in paper and pencil of the tail numbers of aircraft coming and going from large city and small regional airports. This analog, individual tracking information was then correlated with other plane spotters around the world. Instantly, people could see whether a plane that was at Andrews Air Force Base and Guantanamo went to Poland, Romania, Egypt, etc.

The tail number of planes has always been available to the general public. Now, individuals are able to find all this information with just a laptop – along with the registrant of the aircraft and if the tail number marking has changed with the lifetime of the aircraft. You cannot change the tail number and get with it anymore. In the struggle in Iran or the Wikileaks controversy, transparency is the core matter in all cases.

Roger Hurwitz

With new vulnerabilities, how will the government protect us? How can various stakeholders work together (the government and/or utilities) for the protection of the individual? Is there a deficit of democracy? Is democracy exacerbated or ameliorated by the Internet?

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 necessarily anxious to make public. This inadvertence should be considered besides just the idea of transparency (voluntary or involuntary).

For example, Hungary, for the first time ever, published the budget of their country, which was a big change. People can see things like murders of citizens of Iran on their sidewalk, which has an effect on the Iranian regimes standing around the world. The difference between transparency and publicity is not just that we know that it happens, but that we care enough to say something about it that might affect our relationship to the government. No government can hide what it does to its citizens – whether it is a journalist through video, but publicity leads to a spirit of caring at the global level.

In the U.S., there is a tendency to see all good things coming together in the final stages. We assume that society as a whole is changing with the assumption that because we're demonstrating through an Internet demonstration, that there exists a secular liberal society that was the source of that demonstration. In short, we need to recalibrate our assumptions.

Chappell Lawson

When it comes to the political implications of new digital technologies on large-scale events like regime change, etc. – there is an enormously rich potential for research and there are also significant theoretical gaps (i.e., what should we expect to happen as a result of diffusion of new media technologies?). 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 latter concept is much less well researched. There is no evidence that communication transmitted through new technology is more persuasive (or has a higher level of efficacy) than traditional technology. However, the propensity to act on one's attitude can be influenced by the low barriers to entry and access of the technology in becoming an active citizen. There are the added issues, however, of the source credibility of the information and the fact that the sheer amount of information and images can sometimes quickly contradict one another - impeding action.

So what is the fundamental difference of the Internet from other communications mediums in *changing attitudes* and *getting people to act*? Where do we expect to see this fundamental impact in the medium? Political scientists expect the impact of the Internet to apply equally, but this only happens in certain places where:

1. People have access to these new media technologies;
2. Where states were sufficiently weak and structured and cannot control the Internet;

3. Where state actors are resented by citizens; and
4. Where there are few civic organizations with capacity to mobilize citizens.

Thomas Paine's *Common Sense* is an example – there was an attitude-changing element of this book by the author (i.e., why monarchical rule is terrible – all aimed at changing American attitudes towards the mother country). Paine also talks about how we can attack British naval power. This portion of the book is not quoted as often - but this goes to this notion of the propensity to act on your attitudes (i.e., how it was possible to actually defeat the British).

But what of the format of the message? If one receives a piece of information by e-mail there is no reason that this format should be more persuasive than if the message was received via television. Particularly salient, the Internet is influential in affecting the propensity of people to act during a coup or conflict.

For example, people could see the Soviet coup in 1992 or Romanian revolution or hear Gorbachev's articulation of doctrine. By the very viral nature of the Internet, you do not have to wait for the television station to broadcast it. If regime change is about the willingness of security forces to attack demonstrators – then the question is how many people can gather in one place at one time, which is potentially where the Internet fundamentally excels (i.e., mobilization).

Open Discussion

Government

At this time, regime change in the United States, is the regime that is under threat, or the “establishment” – media narrative was 100% on establishment of deficit, after Occupy Wall Street, that narrative was totally gone and has been replaced with narrative about 99% and 1% – the establishment collapsed and no one noticed it? What is under attack? Regime or establishment? The Occupy movement triggered the collapse of establishment by changing narrative to 99% and 1%.

- The U.S. is not under threat but the administration is. The difference between the UK and the U.S. government – the government is not under any danger in the United States, what is under attack is both the government in the UK sense (administration) and the elites in the government – overstated the fact that cliques have collapsed – little early.
- The principle of consent of the governed and how it relates to the Internet. “Consent of the governed” – one of the things that the social networks do, does this degree of zero friction tend to increase or tend to decrease the new consent of the governed?
- There has been a gradual increase in constant plebiscites by creating feedback loops

that did not exist and by accelerating these feedback loops.

- We must consider the crucial role of atomized citizens and their behavior in the aggregate.

Data Matters

There are ambiguities on the relationship between data and prediction. To ask if social science is more like economics, begs the question why did economists not predict the economic crisis

- Depends on how we measure things – what we might see is constant use of plebiscite – the notion we have created feedback loops where none existed and accelerated the ones that do exist, this makes governing quite different as a practical matter.
- Constant plebiscite is in the making. This is the issue raised earlier. The level of tweets on a budget proposal, payroll tax cut extension, becomes taken into account, this is indeed a concerning thing about the consent – there are going to be swings “issue by issue” – as a result of providing social services, and that unions and political parties have done, thinks that there is a lot of “noise” – problem in politics is enabled by the new wave of communication technologies – long term political organizations.

Expectation of assumptions – because you are able to gather all this data, you can predict the future – we understand these equations and understand exactly what is going to happen – if economists are so smart, why aren't they rich and why didn't they stop this crisis? Why didn't we understand the details underlying assumptions?

- We're not doing our job when it comes to cyberpolitics, as we haven't articulated clear arguments that we can directly verify
- But we recognize that the social sciences are making quite extraordinary progress towards predictive analysis. (Note the issue in *Foreign Affairs* on regime change, etc.)

Privacy

Discussions with students seem to indicate students do not care about privacy except for if it threatens their job even though it might constitute a long-term threat to freedom in America. What do people perceive with respect to that? Is that a problem?

- What is privacy? What type of information do we want others to know and who? Also, there is less embarrassment over the revelation of certain issues. It is not threatening but shows a change in the notion of privacy and is comparable to village

life but lacks constraints on village behavior. It is an issue of trust and behavioral constraint.

- It is not off base at all, that's an important phenomenon – issue of definition, personal secrecy, what do we not want others to know because that would give them something that they could know, how they could shame us?

There may also be dimensions or features to the privacy issue:

- People are less shamed than they used to be. There is now mass advertising relating to sexual dysfunction, or adult diapers – that people a generation ago wouldn't talk to their own doctor about.
- Let's not leave McLuhan out of this – he was a prophet – discussing aspects of village life – what we don't have are village constraints on behavior – people in DC or Boston drive differently than small towns – when you drive badly, or are rude or shout at people, you won't see that person again. In a small town, you'll see them before the day is out again. Those are constraints – we have certain aspects of village life and not others – trust and behavioral constraints

And there are generational issues:

- The same holds for in the MIT village. Separate question as to whether it's a village – MIT – if I'm wearing a bathing suit, but if everyone else is also, it's not a problem. It is only a problem if everyone else is wearing a suit, if pictures of that is distributed widely would be embarrassing – MIT students think everyone is wearing a bathing suit and older generations thinks everyone is in a suit.
- We don't fear the police for expressing ourselves politically.

IV. CyberPolitics and democracies: Where are we headed?

Framing Questions

What evidence is there that cyberpolitics is influencing traditional political behavior?

How are different governments reacting to increased cyber access by various constituencies?

What new or notable simulation or other tools have been developed to help us understand political participation in democratic societies?

Panel

Moderator

James Dougherty, *Council on Foreign Relations*

Panelists

Archon Fung, *Harvard Kennedy School*

Peter Brecke, *Political Science Department, Georgia Institute of Technology*

Ethan Zuckerman, *Media Laboratory, MIT*

Presentations

Archon Fung

Participatory democracy and technology calls for new hypotheses. The analogical thinking hypothesis is incorrect: some of the thinking in the field of politics and technologies tries to draw the analogy between the experience of technology & the technological domain. Since technology transformed other domains (music, film, e-commerce, the book, streaming video) the conclusion is that technology will also lead to similar changes in politics.

There is a plausible reason why this hypothesis is wrong: a fundamental difference in demand. The rise of killer technologies (e.g., Blockbuster and Netflix in the media domain) is not available in the political domain because it is characterized by collective action.

There are four hypotheses to this discussion:

(1) *Disintermediation Hypothesis*: The primary effect on politics of ICT is that it makes large organizations less relevant because it reduces the organizational friction and coordination costs. ICT is also limited because there are still a number of collective action problems.

- (2) *Public Sphere Hypothesis*: ICT allows more people to communicate and get ideas out, reducing the domination of the public sphere by capital and capital equipment. ICT allows for more voices to be heard, but it's inconclusive whether ICT hurts or helps democracy overall. This enables people to cluster into affinity groups, and improves function all around. An important caveat is this: ICT opens up public spheres that are controlled by authoritarian regimes. ICT improves the quality of democracy in places where governments are controlling.
- (3) *Transparency Hypothesis*: What ICT fundamentally does is make information more available and more credible and legitimate. The transparent Kenyan budget-tracking tool is an example of fiscal transparency by the state.
- (4) *Organizational Amplification Hypothesis*: What ICT does is amplify the functions of existing organizations gradually? This hypothesis is less radical than hypothesis (1) and (2) but more incremental. The hypothesis is based on the notion that people will buy technology to advance their platform and to communicate or propagate their message. There is great potential for growth in the field of political science to enable organizations to utilize ICT to achieve their goals.

Finally, there is the ever-present issue of information becoming knowledge and wisdom. Two individuals may both hate the current regime, but are unaware of each other's similar position. 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*.

Peter Brecke

The basic idea of Isaac Asimov's *Foundation Series* was to simulate the future. Another formative book: *Psychohistorical Crisis* by Donald Kingsbury was inspirational. Turning Asimov on its head - to figure out where we want to go through the conscious design of a society led to 'Democracy 2.0'. Democracy 1.0 is what we currently live in now in 21st century. Democracy 2.0 is fundamentally about empowerment and participation.

The first step has been to identify the core elements of democratic governance (the current set of institutions and rules). The next goal is to determine a metric for how well we are governed.

The Human Well Being (HWB) index is a framework that was formulated to be a measure of social well-being, security, freedom, prosperity, social mobility, civic participation, and good governance.

A methodology being developed for individuals to voice their dreams and articulate their ideas about how society should operate is a place to make a contribution to the preferred societal design. The ideas can be specific or general. It is a venue in which good,

generalizable ideas can ‘rise up’ and be exposed to larger audiences. This methodology is called the *Preference Determination Process (PDP)*. It is a platform to discuss and debate alternative societal designs and the resources and activities needed to reach them. Ideally, this model builds upon existing participatory processes such as Locally-Managed Marine Areas in Fiji or Jirga in Afghanistan.

The PDP can be deployed at different technological levels: both face-to-face meetings such as design charrettes done by urban planners and computer-based venues for interaction (such as Facebook and Second Life) should be used to maximize participation. PDP should be voluntary and inclusive in terms of who can participate. Another important design element is the ability for people to choose whether they want to focus on local or global issues.

The Alternative Testing Model (ATM) is a tool to help those participating in the PDP to discern, to the best of our knowledge, the likely consequences of different choices regarding:

- Governance structures
- Rules for institutional behavior
- Policies to deal with different issues

Through formative thinking on the functionality of the ATM, people should be able to query the ATM (i.e., a computer simulation program) in order to model the likely consequences (to the best of our knowledge) of making a particular choice. Users must be able to query the ATM to any level of detail (theory, data, etc.) in order to better understand how it arrived at the conclusions. Users must also be able to try out their own alternatives (which others can challenge).

Some early, fundamental problems need to be overcome to make an ATM:

- Designing components of the ATM – *The Integration of Social Processes*
- Establishing a basis for accepting ATM results – *Theory and Evidence*
- Transforming theories into computable code of the ATM – *The Representation of Theories*
- Modeling the spread of ideas in a population – *The Spread of Ideas*
- Process for assembling the ATM – *A Pathway to the ATM*

They are all currently under construction.

Slides at the end of Session IV.

Ethan Zuckerman

There are activist populations that used digital media in 2011: the Arab Spring, the Occupy movement and Russia (which were literally playing out while the ECIR Workshop convened). The three reasons why digital media are important to activism:

(1) *Social Media Mobilization Thesis* (Clay Shirky): The basic premise is that it just takes a click of a mouse to mobilize people. This theory is false because it works independent of the advent of the mobile phone. People can get mobilized based on plain old telephone service (POTS), talking with people at church, etc. There is not necessarily a quantum shift from the Internet. However, the ability of a government to shut down a system in the moment of political turmoil (The Egyptian disruption of Internet service for example) is unprecedented. What is the cost of this? To conclude, thesis 1 is an important thesis, but not revolutionary.

(2) *Attention Thesis* (The Tunisia Model): For this thesis, there are parameters based on the way the events in Tunisia played out. To start, the Tunisian village was cut off from rest of the world Facebook heavily monitored by Tunisian government countrywide. However, information on Facebook was picked up by the Tunisian diaspora, aggregated by these “bridge bloggers”, then attracted interest from mainstream media broadcast outlet Al-Jazeera. Broadcasting of the information by Al-Jazeera did not trigger Tunisian government concern because Al-Jazeera was not present on the ground⁸. In summary, the parameters of the Tunisia model are:

- Facebook is thoroughly monitored by state actors.
- Media gets posted, gets translated and made available to media organizations by “bridge bloggers” (usually members of a diaspora community) – who then broadcast it (Twitter, Facebook, YouTube, etc.).
- Al-Jazeera then agrees to broadcast it.

Today, because of the Tunisian uprising, there are more efforts to control the Internet more robustly by other state actors. How is the digital realm changing government? For the activist community, censorship is the sincerest form of flattery. This behavior is a very interesting, revolutionary development. Social media therefore is a way of influencing current social practices. The growing challenge is circumventing censorship. The role of social media and its use by activists in relation to government control is illustrative. Activists in Egypt are aware that the government is monitoring the social media sites, so social media is not necessarily used for political discussion. Instead, it is used as one of the tools in political activity or used with the knowledge it is being monitored and therefore, the communications are adaptive.

It is interesting that Iran did not shut down the Internet during the Green Revolution (even though much more centralized than in Egypt). Instead, Iranian government slowed Internet access down significantly – but kept email communication active to continue its use for commercial activity.

(3) *Need of New Media Thesis*: In Russia there is a desperate attempt to create new type of media because traditional media is heavily controlled by the government. A nationalist and a democratic fringe is heavily involved in this attempt to create a new type of media. At the

same time, two significant Distributed Denial of Service (DDoS) attacks by two criminal botnets shut down state-controlled media websites. These botnets were used to take down media groups that were trying to pull data on election violations. To be clear: criminal botnets have been used to shut down coordination and aggregation of information on the problems with the election. This suggests that these models are not purely effective for the activists (as tool usage is omnidirectional by all types of state and non-state actors). But, with this jamming of media sites, we can see what mechanisms are important for enabling dissidents to voice their political message online.

In some final observations (which are a part of the upcoming book *Access Contested*):

- Russia has not yet bothered to filter the Internet but instead makes it difficult to speak. As a result, they shut down certain people's services and/or websites. There is a display of control aspects being employed during the recent December 2011 contested election. It will be interesting to see how this develops.
- Tunisia: The government is blocking Google sites, YouTube, Twitter, Facebook, etc. Facebook was considered a great rallying point, so blockage of service by the state actors was a huge loss. The activist's solution was e-mailing people and encouraging them to use a joint Facebook proxy site. The number of people on Facebook had seemingly declined because the people were using this secret backdoor access point.
- It is difficult to determine what a dictatorial government intercepts from the individual when people log into Facebook. Many different encryption tools being used by the administration to pocket people's password.

Open Discussion

Filtering

What is the ultimate effect on the legitimacy of the regime? Compare the effectiveness of the multi-layers of Russia, Iran, and China? Which is most/least effective?

- Iran is effective in filtering the Internet: There is a fairly robust blogging community. China knows it can't fight social media so what it does instead and Chinese social media created instead. China may be the most effective. In Russia, however, there is a legitimate nationalist group and a liberal group. Russian drum protest to fight election results. Impressive technical skills of oppression demonstrated in Russian.
- Distributed Denial of Service (DDoS)-There are two ways to proceed:

1. Hire outside criminal group like a botnet and batter a site down.
 2. Mobilize a movement to launch this attack. A suggestion “hide behind big rocks” like Amazon.
- New hybrid strategies are developing: The media and Internet and how they are linked together. You determine truth by its acceptance in the market place of ideas.
 - The ultimate effect on the legitimacy of the regime. Early reports from Russia suggest they have paid a high price in legitimacy. Compare effectiveness of Iran, China, and Russia. China has a multi-level scheme.

In terms of longer-term legitimacy, which of these models is likely to be most/least effective? What is the effect on legitimacy of regime, for example, Russia paying a high price in terms of legitimacy for the devices used; China on the other hand has a multilayered scheme controlling for example ISPs but also local level down to the community level; Which model is likely to be most/least effective? Iranian, Russian, China?

- In these models, the first was about Iran, the second China, and the third Russia. Iran has been effective. China had the incredible innovation because China knows it cannot control social media so instead Chinese government built Chinese social media, which is surprisingly active and open and includes political activity. An enormous amount of imagery comes across, and a lot of it is about politically sensitive topics (e.g., censorship). Putin is going to suffer some real harm, not just from the extent which he will be forced to mobilize, but also from the steps he’s already taken. Increasingly from the Nationalist side of Russia we are seeing desperate techniques – DDoS, or Twitter bots, when they can’t get real people. In the long run, the technical skills of Russian oppression are impressive. They have raised the game. China will win in the end.

Distributed Denial of Service Attacks (DDoS)

What are some details on reports regarding Russian DDoS attacks in comparison to the 2007 DDoS attacks in Estonia? When there is a DDoS attack, what needs to be done to repair it or get back to normal? What about botnets? Were these unrelated to the DDoS?

- In 2007, Russian nationalist launching DDoS attacks whereas in 2011, DDoS attacks carried out by two criminal botnets, which have taken down some real heavy weights. What was interesting about Russia vs. Estonia is that it was a voluntary botnet. Arbor networks spend a lot of time tracking these botnets, their Command and Control structure, and where they’re coming together for an attack. What do we do about it? Surprisingly hard. The short answer is that it is hard for most small organizations to survive a good DDoS.

DDoS attacks have become a national security threat and it is mostly funded by credit card fraud, and if the U.S. would just get its act together and implement good credit card security. But there are measures that could have already been taken a long time ago.

- Netherlands model is another option where ISPs are very aggressively shutting down infected computers and putting them into walled gardens informing users that their computer has been compromised and needs to get fixed because ISPs have come together.
- There is still a lack of understanding of linkages between various types of media.

Movement of Information

Thinking of the total ecosystem, there is research that shows that information moves back and forth from Facebook to TV or back. How do they multiply each other?

- This is a place where we are hoping to get a lot of help from the Political Science community. Right now there are neat papers on how Twitter works. We do that because we can get good data. But if the real stuff happens at the interface between Twitter, newspapers, blogs, and radio shows, that's hard. We realized analyzing political blogs that we needed transcripts every time Rush Limbaugh goes on the air.
- It is really important. Almost all the examples you can think of are hybrids. WikiLeaks for example. We need a lot of work to understand it. That's one dimension. A second dimension is what exactly the content is. Oliver Wendell Holmes quote, idea of the truth getting accepted in the marketplace of ideas, whereas now people are arguing for "let the best meme win", a much different idea.

Democracy 2.0: An Example of a CyberPolitical Governance Form

Peter Brecke

Sam Nunn School of International Affairs, Georgia Institute of Technology

Background and Motivation

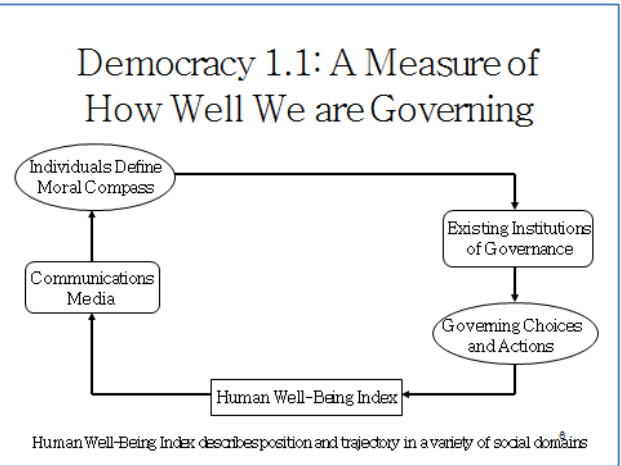
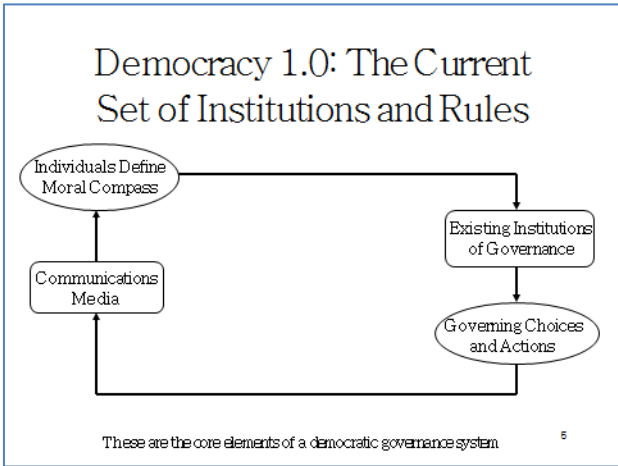
- Asimov's *Foundation* series
 - Hari Seldon, Prime Radiant, Seldon Plan
 - The Second Foundation used the computational model to lead to a better society
- My work since then has been to give us this type of capability
- Flip Asimov's vision on its head
 - Kingsbury's *Psychohistorical Crisis*
- We should through a democratic process design and implement the societies we would like to live in

3

Goal of Society Design Process

- To come up with desired societal designs
- Societal designs are descriptions of societies in terms of what we think are the important characteristics of societies
 - Part of that description is how well-off the population is with respect to fundamental aspects of the human condition: security, freedom, prosperity, social mobility
 - Another part pertains to the structure and operations of the mechanisms of governance
- Democracy 2.0 is a societal design that possesses a built-in society design process

4

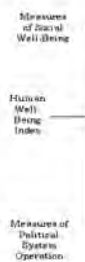


Human Well-Being Index

- A measure of six important dimensions of life in a society germane to governance
 - 4 dimensions pertaining to the circumstances of the members of a society, social well-being
 - 2 dimensions pertaining to the governance system's ability to achieve or maintain desired values of social well-being
- The measure includes distributional considerations
- There is an expanding empirical measure

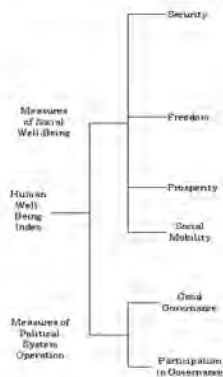
7

Figure 1
First Level of the Human Well-Being Index



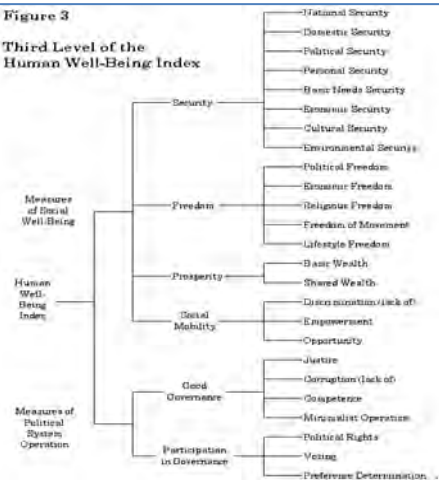
8

Figure 2
Second Level of the Human Well-Being Index

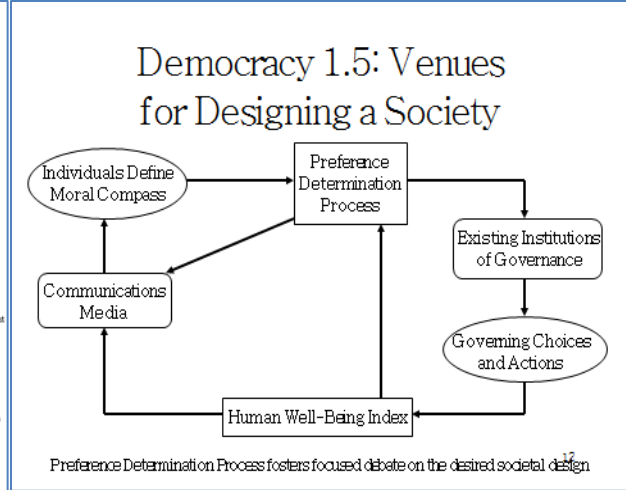
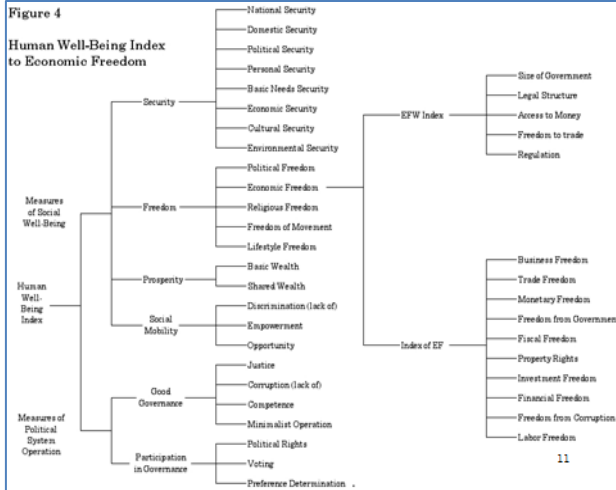


9

Figure 3
Third Level of the Human Well-Being Index



10



Preference Determination Process (PDP)

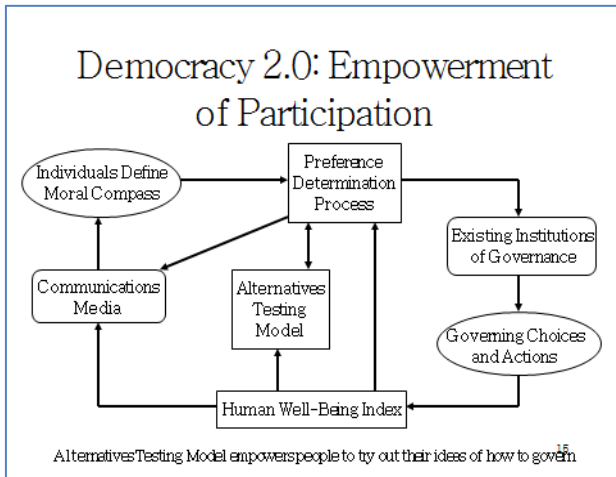
- A vehicle for individuals and groups to voice their dreams and articulate their ideas about how society should operate
 - A place to make a contribution to the preferred societal design
 - Ideas can be specific or general
- A venue in which good, generalizable ideas can "rise up" and be exposed to larger audiences
- A place to discuss and debate alternative societal designs and activities needed to reach them
- Ideally builds upon existing participatory processes such as Locally-Managed Marine Areas in Fiji or Jirgas in Afghanistan

18

Different Technological Levels for the PDP

- Both face-to-face meetings such as Charrettes done by urban planners and computer-based venues for interaction such as Facebook and Second Life should be used to maximize participation
 - Voluntary and inclusive in terms of who can participate
- People should be able to choose whether they want to focus on local or global issues

19



Alternatives Testing Model (ATM)

- A tool to help those participating in the Preference Determination Process
- A tool to help people discern, to the best of our knowledge, the likely consequences of different choices regarding
 - Governance structures
 - Rules for institutional behavior
 - Policies to deal with different issues

16

Use of the ATM

- People should be able to query the ATM, a computer simulation program, what are the likely consequences (to the best of our knowledge) of making a particular choice
- Users must be able to query the ATM to any level of detail (theory, data, etc.) how it arrived at the conclusions it did
- Users must be able to try out their own alternatives (that others can challenge)

17

Elements of Creating an ATM

- Below are fundamental problems that need to be overcome to make an ATM
 - Design and components of the ATM
 - *"Integration of Social Processes"*
 - Establishing a basis for accepting ATM results
 - *"Theory and Evidence"*
 - Transforming theories into computable code of the ATM
 - *"The Representation of Theories"*
 - Modeling the spread of ideas in a population
 - *"The Spread of Ideas"*
 - Process for assembling the ATM
 - *"Pathway to the ATM"*

18

V. Social Media & Social Action Learning from Experience

Framing Questions

What do we know about the types of social media shaping political protest in different contexts or countries?

- Does the use of social media shape new ideas or transmit prevailing ones?
- What functions do uses of social media provide? For example, create new constituencies? Aggregate potential ones? Shape multiplier effects? Other?

What about the behavior impacts of social media uses by governments, civil, society, other?

Is there any of escalating vs. de-escalating effects of social media on social behavior in conflict situations?

Is there a convergence or divergence worldwide in learning from experience?

Panel

Moderator

Venkatesh "Venky" Narayanamurti, *Harvard Kennedy School*

Presentations

Fergus Hanson, *Lowy Institute, Sydney, Australia*

Evann Smith, *Department of Government, Harvard University*

Robert Laubacher, *Sloan School of Management, MIT*

Introduction

Venkatesh "Venky" Narayanamurti

Due to the interaction between technology and the social context of their implementation, innovations often are hybrids and do not manifest themselves at extreme ends. The future is not just about technology - but socio-technology.

Presentations

Fergus Hanson

A video clip from a recent meeting of the Council on Foreign Relations was shown, where ex-Google CEO Eric Schmidt shared that he is:

“Extraordinarily excited about the scale of the mobile revolution” and his thoughts on the potential of the opportunity which lies ahead – which lies primarily in the developing world (1 billion global citizens going online via mobile devices which are as powerful as supercomputers were a few years ago) with a cost reduction which will make it all possible. People will not only be able to talk to each other, but “they can develop apps, organize in new and innovative ways and change the world.”⁹

Someone in Eric Schmidt’s position may be excited about the potential market that lies ahead. As William Hague stated: “achieving agreement about the future of cyberspace will take time. But this is one of the great challenges of our time and we need to pursue it with the same intensity as efforts to eradicate global poverty or tackle climate change.”

Authoritarian regimes have realized the power and danger of social media. As a result, censorship is being stepped up. In the face of “Internet Freedom” agenda (as laid out by the State Department under Secretary Clinton), a commitment has also been made to a more subversive diplomacy – using web tools to undermine governments and international organizations. Cases of eDiplomacy illustrate this new trend.

Subversive technologies initially focused on China but broadened as result of the Arab Spring. An example is an “Internet in a Box” or “Media in a Suitcase” developed by the New America Foundation. The device allows for the development of what is the equivalent of a panic button for activists – allows activists to communicate even when governments shut down the Internet, send out messages to their contacts when they have been arrested or to delete all contacts immediately in case of arrest.

InterNews is another case study. InterNews gives activists tools to circumvent government control and conceal identity when visiting certain popular sites on the Internet. Advertised in 12 countries (Bahrain, Burma, China, Egypt, Iran, Ethiopia, Syria, Tunisia, Vietnam, Yemen, Turkmenistan, Uzbekistan) InterNews was downloaded half a million times.

NERD (Near-Eastern Regional Democracy) is another suite of tools, consisting of 3 programs: tool development, secure communications, and digital safety training for analysts. It is difficult to measure how effective this tool is. These tools are used by activists to mount protests for both laudable and questionable means.

The U.S. government has a set of websites in foreign languages presenting U.S. foreign policy to audiences abroad in an effort to counter extremism. The Digital Outreach Team Unit, set up in 2006, espouses positive images of U.S. and combats extremism in three different languages to challenge counter-conspiracy theories with facts. The success of the program caused Al-Qaeda to mount their own digital outreach team to counter U.S. State Department efforts in this counter-information effort. Overall, these sites have not all produced positive outcomes. Digital outreach of this nature sometimes provides soft messages about the U.S. The USAID funded Internet Freedom Campaign – providing technical assistance and developing a network of technical experts in the security domain to assist activists in the field.

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 do not agree with what they do?

Hanson's presentation is available upon request.

Evann Smith

The determining role of social media must be challenged. In 2004-2005, youth activists emerged and moved outside the constituted spaces of unified structure. The issues of risk (i.e., personal risk), relationships and the role of the Internet became salient.

High-risk mobilization requires strong ties and demands trust. The Internet builds weak ties and transmits homogeneous information. The Internet lowers the cost of communication, the ability to penetrate networks and increases the number of weak ties available to activists. In this context, social media accelerates the spread of information and its penetration of strong tie networks.

The relationship between social media and the mainstream media played an important role. Starting in 2005, social media expanded the reach of a limited social media network. The mainstream media enhances the credibility of social media content. Activists called upon Al-Jazeera for help broadcasting the message to promote protesting efforts to the world. This example is a clear case of how a mainstream media outlet amplified and expanded the reach of a cyber-network. *Mainstream media enhanced the credibility of social media content because television broadcast acted as quality control.* Al-Jazeera enhanced the credibility of these messages by broadcasting them to a larger, perhaps even global audience.

While not a mainstream media outlet, in an interesting twist, iPhones were just banned in Syria. There is also a large Islamist presence online. Social media did not cause the Egyptian uprising, but it did impact the complex networks through which it occurred. Uprisings are a self-organizing system.

Future research is needed on the sequence of events. The Arab experience is often viewed as a “Twitter/Facebook” revolution, but this view is fundamentally wrong because,

1. The revolution has not officially occurred yet; and
2. It denies the roots, the processes, and the history that brought people to the point of political action prior to the advent of social media tools.

To Egyptians on the ground, the revolt was the beginning. In 2005, it began to shift, with activists moving outside the institutionalized norms for communication. Before 2005, there were only 30 blogs. Blogs then experienced exponential growth - *but this growth did not necessarily translate into action*. A factory strike case that was organized via Facebook, failed.

From May 4, 2008 through July 23, 2009, political action in the Arab world was organized via social media but failed - and the pattern of failure repeated. What happened? Social media indirectly impacted this failure by reinforcing the network structure. It was not until 2010 that individual action took place.

Slides at the end of Session V.

Robert Laubacher

The Climate CoLab is a research project at the MIT Center for Collective Intelligence.¹⁰ Collective Intelligence leverages the wisdom of the crowds. Over the past decade or so, a new approach has emerged to tackle large, complex problems. Examples include Linux, Wikipedia, and Google. When one conceives of Google as a whole – including the millions who create links on the World Wide Web, the Google company crawlers that collect information about those links on an ongoing basis, and its clever algorithms that parse all this data and serve up bits of it to users when they type a search query – the entire system is a remarkable example of collective intelligence.

Global climate change is a problem of daunting scope and complexity. The Climate CoLab seeks to harness the collective intelligence of large numbers of people to address climate change and promote sustainable development. The Climate CoLab does this by:

- Breaking down the large overall problem into parts.
- Structuring crowd activity with contests (similar to other scientific and innovation contests i.e., the *X Prize*). Invite broad community to submit proposals. Expert review and community voting enable the wisdom of the crowd to judge the highest quality material. The top rated proposals are then presented to the UN and Congress.
- Using simulation models to discipline the entire process.

CoLab community growth to date includes:

- More than 35,000 unique visitors from 160+ countries.
- 40 countries with 100+ visits including U.S., Canada, EU members, Australia, New Zealand, and Japan plus Argentina, Bolivia, Brazil, China, Columbia, Hong Kong, India, Indonesia, Mexico, Philippines, Russia, Singapore, S. Korea, Thailand, Ukraine.
- More than 3600 registered members (10+ percent of visitors become members).

CoLab work to date includes:

- 2009-2010
 - Software development and community recruitment.
 - Proof of concept contests.
- 2011
 - Contest on green economy, one of two major themes at the UN's 2012 Rio+20 conference.
 - Continued community development, with particular emphasis on social media.
 - Building stronger linkages to policy makers and NGOs.

2012 Plans for the CoLab include applying hyper-specialization by breaking down macro problems into groups of key issues (e.g., reduce emissions through industrial reuse of materials, adaptation for agriculture, etc.). The community will then propose potential actions in each domain. Finally, the community will develop comprehensive proposals by selecting one option from each domain and noting the interdependencies between domains.

The overall goal is to connect with the world of policymakers. So far, there has been a dual response: some policymakers are enthusiastic about the prospect of the wider participation the CoLab can facilitate, while others express skepticism about the involvement of non-expert, unaccredited participants.

Slides at the end of Session V.

Open Discussion

Theoretical Implications

Evann Smith's research on Egypt includes important theoretical implications showing that events such as the Arab Spring do not occur out of thin air

- Research based on theory of complex systems and adaptive systems grounded in analysis of empirical data.

Weak and Strong Links Between People

- The Facebook announcement of "I'm going to the protest" was not enough to push people to go out and risk personal safety. The political context is still being shaped.

How true is the claim that the Internet creates only weak links? So, what is the empirical grounding for assuming weak links? Could it be small groups of strong-tied groups? There is evidence otherwise: what is the empirical basis for the weak tie finding?

- Finding indicates that it is more likely that an activist will show up with his/her brother rather than someone he is friends with on Facebook.

State Advocacy vs. Political Subversion

At what level does state advocacy of human rights rise to the level of political subversion of another state?

- The answer depends on who you speak with and is different for different countries. After WikiLeaks, we had to calibrate Hillary Clinton's "Internet Freedom" vision.

Social Media and the Egyptian Uprising

Evann Smith

Harvard University

A Twitter Revolution?
The Role of Social Media
Conclusion

Social Media and the Egyptian Uprising

Evann Smith
Harvard University
December 8, 2011

Evann Smith Social Media and the Egyptian Uprising

A Twitter Revolution?
The Role of Social Media
Conclusion

A Twitter Revolution?



Evann Smith Social Media and the Egyptian Uprising

A Twitter Revolution?
The Role of Social Media
Conclusion

Domestic Mobilization
International Impact

Risk, Relationships, and the Internet

High risk mobilization

- requires strong ties

The Internet

- builds weak ties
- which transmit information

Social media accelerates the spread of information and its penetration of strong tie networks.

Evann Smith Social Media and the Egyptian Uprising

A Twitter Revolution?
The Role of Social Media
Conclusion

Domestic Mobilization
International Impact

Tweeting Outward

- **ishta_dreams** @3arabawy first video up, <http://www.youtube.com/watch?v=U3IEhQMPyWE> Crowds avoiding oncoming tear gas and police in Tahrir #jan25 #egypt
- **AthiGeleba** BREAKING: @Twitter is blocked in Egypt as protests ensue. Ustream has a live feed of the streets in Cairo. <http://bit.ly/hUxKvt> #Egypt
- **bleekerK** RT @weddady: URGENT: REQUEST to ALL EUROPE & US tweeps on #Jan25 PLEASE ASK YOUR MEDIA TO COVER #EGYPT NOW
- **FourYawkeyWay** #Jan25 Friend near Tahrir Square says there are 35,000 people there. #Egypt #sidibouzid

Social media helped increase the domestic audience costs of public action for the U.S. administration.

Evann Smith Social Media and the Egyptian Uprising

A Twitter Revolution?
The Role of Social Media
Conclusion

Conclusion

Social media did not *cause* the Egyptian uprising.

But it did impact the complex networks through which it occurred.

Evann Smith Social Media and the Egyptian Uprising

Harnessing Collective Intelligence to Address Climate Change

Robert Laubacher

Research collaborators: Thomas W. Malone, Joshua Introne, John Sterman, Hal Abelson, and Gary Olson

Vision

- Global climate change is a problem of daunting scope and complexity
- Over the past decade or so, a new approach has emerged to tackle large, complex problems
- The Climate CoLab seeks to apply this approach by harnessing the collective intelligence of large numbers of people to address climate change



2



How the Climate CoLab works

- Break down problem into parts
- Structure crowd activity with contests
 - Invite community to submit proposals
 - Discipline process using models
 - Selection of best proposals by
 - Experts
 - Community voting

3



Breaking down the problem



4



Structuring activity with contests



- All users work individually or in teams to produce proposals
- Experts select finalists based on feasibility and uniqueness
- Users work to improve proposals based on expert feedback
- All users & experts vote to select winners

5



Inviting crowd to submit proposals

Coordinate

6



Expert vetting of proposals

Climate CoLab Expert Council

- | | | |
|---------------------|-----------------|------------------|
| Markus Amann | Michael Prather | Robert Watson |
| Shoibal Chakravarty | Richard Richels | Mort Webster |
| John Christy | Jayant Sathaye | John Weyant |
| Martin Heimann | Gavin Schmidt | Tom Wigley |
| Henry Jacoby | Robert Socolow | Gary Yohe |
| Stephen Kosslyn | Susan Solomon | Charles Zender |
| James McCarthy | Massimo Tavoni | Kirsten Zickfeld |
| William Moomaw | | |

*Contest judges

7

Selection of top contributions

2010 contest results

- 1 category (global)
- 29 proposals total
- 3 honorable mention
- 4 finalists
- 403 votes
- 3 winners
- UN-Congress briefings

2011 contest results

- 2 categories (global and national)
- 64 proposals total
- 12 semi-finalists
- 8 finalists
- 1750+ votes
- 5 Winners
- UN-Congress briefings

8



Work to date

- 2009-2010
 - Software development and community recruitment
 - Proof of concept contests
- 2011
 - Contest on green economy, one of two major themes at UN's 2012 Rio+20 conference
 - Community development with social media
 - Twitter remarkably effective for spreading the word
 - Linkages to policy makers and NGOs

9



Community growth to date

- More than 35,000 unique visitors from 160+ countries
 - 40 countries with 100+ visits including U.S., Canada, EU members, Australia, NZ, and Japan plus Argentina, Bolivia, Brazil, China, Columbia, Hong Kong, India, Indonesia, Mexico, Philippines, Russia, Singapore, S. Korea, Thailand, Ukraine
- More than 3600 registered members (10+ percent of visitors become members)

10




2012 plans

- Applying hyperspecialization to the CoLab
 - Break macro problem into group of key issues (e.g. reduce emissions through industrial reuse of materials, adaptation for agriculture)
 - Community proposes potential actions in each domain
 - Community develops comprehensive proposals by selecting one option from each domain
- Experts vet resulting comprehensive proposals and community/experts select best ones

11



References

-  Climate CoLab <http://climatecolab.org>
- Climate CoLab video <http://techtv/videos/4171-the-climate-collaboratorium>
- Collective Brainpower, *MIT Spectrum*, Summer 2010, <http://spectrum.mit.edu/articles/normal/collective-brainpower/>
- MIT Center for Collective Intelligence <http://cci.mit.edu/>

12



VI. Three Visions: Highlighting the “Next Generation” of Challenges for People, Power, and CyberPolitics

Framing Questions

What is the vision for the future of the Internet - or alternative futures thereof?

- How “fixed” are the features of the present Internet?
- How do Internet architectures influence cyberpolitics in international relations?

What are possible developments in “people power” given the growth of social media?

- Do recent “revolutions” and “protests” in various parts of the world reflect unexpected idiosyncrasy or systemic trends?
- How do we expect governments to react? Do we anticipate any movement toward “Global People Power”?

What are the research priorities relevant to “people, power, and cyberpolitics”?

- Are there particular “unknowns” that require more immediate attention than others?
- What is a “positive future?”

Panel

Moderator

Stuart Madnick, *Sloan School of Management, MIT*

Presentations

Herb Lin, *U.S. National Research Council of the National Academies*

David Clark, *Computer Science and Artificial Intelligence Laboratory, MIT*

Jonathan Zittrain, *Harvard Law School*

Presentations

Herb Lin

Views expressed are those of Herb Lin, and no one else.

There are a couple of fallacies in the study of cyberspace – namely, that, in principle, a bordered Internet is impossible and that the environment is not reactive. There is no reason “cyber borders” cannot exist – and we hear increasing calls for tailoring the Internet to serve various segments of society, i.e., – copyright/entertainment industry, critical infrastructure, etc. The dominance of ‘offensive postures’ in cyberspace is largely true. According to computer science, good defense is impossible—that is, offense always beats defense—and so deterrence needs to happen. Then the political scientists and the policy people say that deterrence is impossible without good attribution—so we need to rely on better defense. And if you find this circular state of affairs intellectually unsatisfying, you’re not alone.

Then some analysts say that offensive operations are needed to eliminate cyber threats, so we acquire offensive capabilities in cyberspace. But any adversary would simply compromise a third party’s computers to launch an attack against us, or hold some of his own computers in reserve in an unattackable location. So why should we believe that our offensive cyber capabilities can eliminate cyberthreats against us?

As for the nonreactivity of the cyber environment, it is true that in the past, governments have been asleep at the switch and have been largely unaware of the power of the Internet. But recent events suggest that governments are no longer asleep, and they are at least aware of the Internet’s power, even if they may not know how to handle it yet. Moreover, despite the systemic difference between autocratic and democratic governments, both types of government have shown signs of moving in the direction of being more suppressive. Nation-states are reasserting themselves. There is concern with the use of social networks to control people and the monitoring of chats, Facebook and Twitter by government agencies, and many governments are moving to assert more and more control over various parts of cyberspace.

Regarding the rise of “people-power,” yes, we are seeing it happen. However, governments have many tools to intervene and use social media tools. It is not clear where the balance of power falls. Perhaps people will have transient advantages—but governments will eventually catch up and take action.

David Clark

The discussion is not one of the future of the Internet, but possible future(s) of the Internet(s). The more important question: *who* is driving the future of the Internet? This question is something you may not think about if your prerogative is profit or power and

control. Is there a 3rd way out? In a National Defense University publication chapter of “*CyberPower and National Security*”¹¹ – the core argument is that technologists do not necessarily determine the future of the Internet.

Social scientists ask questions that are not driven by performance but questions of power and control. Engineers are not trained to think about such things. Social scientists, however, can sometimes be wrong because they do not understand the Internet. You do want to evaluate futures in terms of controls and powers. The question then becomes how best to compare these possible futures.

Living at the packet layer, it is astonishing what is happening at the information level and the difference between the rates of change at the application level compared to the protocol level (for example – the switch to Internet Protocol Version 6 [IPV6]). The packet layer is not interesting anymore. While the application and information layers are far more interesting.

The domain name system (DNS) is going to be a contentious area regarding control because of the ability to control the user’s experience. You do not need to use a DNS – you can just type the internet protocol address. When DNS was designed, during that design process we thought about resilience, not in terms of whether or not it could be controlled. Piracy is another area of interest. The United States removes a lot of content from the Internet with regard to content piracy.

The role of money is important in the development of information infrastructure. The best way to predict the future of the Internet is to invest in it. *Who paid for what we currently have?* The original Internet was created by researchers who were paid by the government with the outcome of an open platform. Today, companies such as Facebook and Google drive the shape of the Internet. In short, *buy the future you want.*

Another important trend is the increase in personalization and creation of massive data. For example, there is the question of attribution on a platform like Google+. Is it possible to create profiles with fake names for activists who would like to conceal their identities?

As a society, we should be asking: who should be driving the future of the Internet? In the U.S., it is currently the private players. In response to a question regarding if there will be more activity by private actors in the area of lobbying future telecommunications and Internet policy, the private sector moves faster than the government – but the government has various ways to affect how private actors spend their money, e.g., at the lower level of the Internet such as Comcast. The likely future is one we will not like very much.

Those who are funding the future are also heavily involved in the design process. As a result, we should be asking, “who should be shaping future Internet design?” A future Internet design concept of note is Information-Centric Networking (ICN). Why not connect

people to information (as compared to a node). There are a lot of interesting ICN proposals technically – but do not think about who they just empowered, in this case router operators, or the role of money. Architectures can be designed which unleash more independence, but no money can (or should?) be made from these architectures.

Jonathan Zittrain

The baseline design of the Internet was one of decentralization both from a technical point of view and from a political point of view (e.g., - not directly linking IP addresses to national jurisdictions, an idea that has been floated with regard to IPv6).

That baseline is rapidly changing, with the rise of centralized applications such as Twitter for particular distinct services or Amazon offering website hosting services. Start-ups are more inclined to host their service at Amazon (a company with the strength to protect them). Threats like DDoS require a move to centralization through the use of Amazon cloud servers for survivability. There is the possibility of a return to three major networks (or three major providers).

This change has implications for power. DDoS, offensive state actions and sophisticated hacks are on the rise. IP layer filtering and application level filtering are also on the rise. The solution is a counterintuitive one, in that rather than pushing for engineers to accept importance of economics and the role of power, we should take a politically charged matter *and make it an engineering matter (or technical problem)*.

For example:

Public safety: A technology like mesh networking can be a lifesaver in a situation where the Internet is shut down because of a natural disaster or kill switch. Mesh networking allows everyone to use his or her portable devices regardless of a physical layer shutdown. If a company like Facebook adopts a standard mesh networking service for disaster prevention reasons, it would change the balance of power between them and governments who might want to implement a kill switch.

Mutual Aid Model: Mutual aid at the level of the individual or a company can be driven by altruistic motives or self-interest. We can harness the interests of users and companies to create interdependent webs that increase the reliability of networks. However, even this raises questions: would such a model draw in people that have the bandwidth, the processing cycles, and human power to keep the Internet decentralized? What would small business mutual aid architecture look like? How can the unit of virtual aid be applied to act as an incentive for individuals or organizations to contribute to a mutual aid effort?

These are not insoluble problems, but they have important human rights and public safety implications. Individuals and organizations who need to protect themselves and to avoid

state control mechanisms can use mesh networks, which may be initially developed as technical solutions. This approach requires the conversion of an engineering problem into an ethical argument.

Ethical tensions like these date back to the debate surrounding free software and open source software. The open source movement converted ethical arguments into practical arguments, claiming that open source software had practical advantages. Advocates, like Richard Stallman from the free software movement, are more couched in ethical and human rights arguments.

Open Discussion

Government and Social Media

Can government use social media to control people better?

- It is a worry. An oppressive government can do bad things easily. The possibility of provocateurs on the Internet to cause uprising, use to gather data on activists and map their networks.

Private Sector

What is the private sector's role in politics? Will control over technology in the private sector's hands lead to more influence in the future similar to lobbying now?

- It is a cat/mouse, move/countermove; governments are quite capable of finding tools to shape how companies spend money. For example, lower level facilities owners, governments tell them what to do/ hands-off on info layer due to the 1st Amendment until WikiLeaks happens.
- China has no hesitation messing with info layer. This is why you see different Internet in different countries. Consider lobbying; is that not money?
- We live in a period of great excitement, where industry moves faster than government. The government is quite capable of finding tools to shape their investment. This is happening at the physical layer in the U.S., but China has no hesitation to play at the Application layer.

Mutual Aid

How does mutual aid play out with following the money?

- How much aggregating many of real tiny things can make a difference at the aggregate level? So, in a mutual aid framework, it is a question of what granularity, how big the group of companies willing to play and pay.
- People (at end nodes) have too much computing power – this is basically people power. How much can people be enticed to cooperate? What will draw in people?

How many people do you need to make an impact at the aggregate levels?

- Commercial example of mutual aid is Content Delivery Networks (CDNs). How much do you need? How can we nucleate and coordinate this type of large-scale activity without a central entity? Can authority be decentralized?
- How would the mutual aid architecture get coordinated, if this has to be decentralized?

Jurisdiction

In a world without borders, can you choose which jurisdiction you want to be in?

- It's like in SnowCrash – pick your own. But if it's a major decision, big bundle, large switching costs, but then platforms present ongoing investment.
- Some people choose to use alternative courts – private using public law but faster, etc. – dispute resolution.

By picking Amazon, you are picking private law.

- If there is much bundled and there is a great switching cost, the benefits are lost.

3D Printers

The Internet is not only about dissemination of information if we think of 3D printers moving not only information, but atoms.

- It is an ethical/ jurisprudential question – can we even think about trying to regulate that? Does going physical change your mind?
- It's not guns you should be scared of. It is iGEM¹² (International Genetically Engineered Machine – a synthetic biology competition for undergraduate students). Genetic code on the Internet, build your own.

With 3D printers, the CNCs we are talking about moving not just bits, but also moving items. How does this tie into this notion of power?

- There is an ethical question. Would it be ok to regulate such a thing?
- Bits can hurt.
- It will get down to traceability of material.
- We are teaching college kids how to sequence genes.

The Future of the Internet

There is a lot of attack talk

- The Internet itself is warm and fuzzy and it is rather astonishing that it took so long for viruses to develop after the Internet existed for years vulnerable to attacks.
- There is something very powerful about the Internet. Even though mainstream experience is trivial.
- While there is the dark picture there are also signs of hope such as the tools to circumvent government control.

Positive Thoughts about the Future

- There is something very powerful here. Serious contentions arise, but that is not the mainstream experience.
- The good future is the future of future makers. They must teach not to just learn stuff, but have them write questions so others get answers. And when someone makes bad stuff, stop them.
- It will be a future of makers and the ability to make things including civil and civic defense. It is not just learning but creating new stuff – write new questions to try to answer – at every layer. We do not have to rely on others to protect us.

VII. Concluding Comments

End Note

Nazli Choucri

Political Science Department, MIT

This Workshop represents the general “state of the art” as seen by the panelists, discussants, the direct participants, and other attendees. A major “thank you” to everyone for comments and contributions and, above all, for all making this event so interesting.

We can also consider the Workshop as something of a baseline against which to signal missing pieces, track future developments, and explore contingencies and possibilities. The discussion points to the new relevance of people in international relations, the apparent changes in power distributions, and the emergent complexities for cyberpolitics – at all levels and in all contexts.

As we move forward, we must address the following questions head on: 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. Our plan is to address these in a follow-up workshop – taking into account matters of theory, methods, evidence and policy.

VIII. Poster Session: Contents

Accountability at the Application Layer

Wolff, Josephine, SM Candidate, Technology & Policy Program, MIT

Comparative Analysis of Cybersecurity Metrics to Develop New Hypotheses

Fisher, Dara, SM Candidate, ESD, MIT

Control through the Layers in the Chinese Internet

Hung, Shirley, Postdoctoral Associate, MIT

Coordinates of Cyber International Relations

Vaishnav, Chintan, Postdoctoral Associate, MIT

Cost-benefit Analysis of CERT's International Cooperation Activities Focusing on Korean Case

Cho, Yiseul, SM Candidate, Technology & Policy Program, MIT

Cyber-enabled Loads & Capacities Methods

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

Cyber International Relations Theory: Assessing the State of Art

Reardon, Robert, Postdoctoral Associate, MIT

Cyberspace as Ungoverned Space Methods

Hoisington, Matthew, LLM Candidate, The Fletcher School of Law and Diplomacy

The Dynamics of Managing Undersea Cables Methods

Sechrist, Michael P., Project Manager, Harvard Kennedy School
Vaishnav, Chintan, Postdoctoral Associate, MIT

Escalation Management in Cyber Conflict: A Research Proposal

Reardon, Robert, Postdoctoral Associate, MIT

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, 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

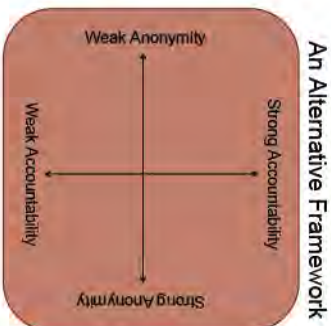
- What are the implications of implementing accountability mechanisms at the application layer of the Internet, rather than the network layer?
- Are accountability and anonymity a zero-sum game for online identities, that is, must every effort to increase accountability necessarily decrease anonymity?
- 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



Traditional Framing



An Alternative Framework

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

Malicious actors who are identified may still be difficult to hold accountable if they are located outside jurisdictional boundaries.

Populating the Quadrants



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.

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

Five national security organizations provide comparative metrics, statistical, and relational information to the public. Organizations ask why they should spend visible time and resources on this question. By demonstrating the value that event threat analysis provides in a comparative perspective. We present some insights generated through the use of the Explorations in Cyber International Relations (ICIR) Data Dashboard. In research, the dashboard consists of a simple querying and analysis tool, coupled with a database consisting of data from diverse state-level cyber data sources provided by governments, Corporate Strategy Response Teams (CSRTs), and international organizations. Users of this dashboard can select relevant security metrics and compare them to other data sources. In addition to the data, the dashboard provides an interface for data visualization (designed to support the research objectives), along with several hypothesis-generation prompts. We believe that using preliminary results suggest visible ways in which such data could be used and we hope this research will help provide the incentives for organizations to increase the quality and quantity of standardized qualitative data available.

The Data Dashboard

The Data Dashboard consists of a simple querying and analysis tool, coupled with a database consisting of data from diverse state-level cyber data sources. The dashboard was developed in partnership with the Center for International Cyber Operations (CICO) and the Center for Cyber Operations (CCO). The dashboard was developed to provide a simple querying and analysis tool, coupled with a database consisting of data from diverse state-level cyber data sources provided by governments, Corporate Strategy Response Teams (CSRTs), and international organizations. Users of this dashboard can select relevant security metrics and compare them to other data sources. In addition to the data, the dashboard provides an interface for data visualization (designed to support the research objectives), along with several hypothesis-generation prompts. We believe that using preliminary results suggest visible ways in which such data could be used and we hope this research will help provide the incentives for organizations to increase the quality and quantity of standardized qualitative data available.

Explorations in Cyber International Relations
Minerva Project at MIT & Harvard

Case Study: Software Piracy Losses

The data available through the Data Dashboard enables an interesting study in cross-country market comparisons. In Figure 1 below, the software piracy losses of seven countries are compared. At the right, it appears that China and the United States have the highest piracy rates.



Figure 1: Software piracy losses of seven countries from 2002 to 2008. The Data Dashboard also allows users to add additional data by different metrics such as market penetration, number of users, number of accounts, or other relevant data. In the case of software piracy, a new relevant data set may include 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, 2002 to 2008.

We might expect that different nations would have different levels of software piracy. One variable metric to measure the variable is the rate of internet usage. Figure 3 below uses the Data Dashboard by adding three different types of international software piracy losses, numbers of internet users, and data of law. Nations with higher rates of law enforcement display lower rates of open source versus countries with less developed legal systems.



Figure 3: Software piracy losses adjusted for Rate of Law per Internet User. This graph suggests that the absolute volume of software piracy has risen over the past decade, with the bulk of that rise in the emerging economies of China, India, and Brazil. Despite the country's rate of piracy does not seem to be correlated with whether it is a developed or less developed country. In almost all of the metrics examined, law, users and losses have increased, while the United States and Germany have exhibited the greatest increase. The graph suggests that nations with higher rates of law enforcement display lower rates of open source versus countries with less developed legal systems.

Next Steps

This workshop has sought to accomplish two related tasks. First, although limited sample data is used and sampled across the internet, we were fortunate to obtain data in broadly accessible format (including trends from existing data that did not exist on any other platform) and organizations are looking up the globe for cyber crime, financial, and other data. The data is being used to generate hypotheses and to generate hypotheses about the impact of different computer metrics could have in formulating policy conclusions. Although the international data to generate hypotheses and get against systems, our research suggests that the data could be used to generate hypotheses about the impact of different computer metrics could have in formulating policy conclusions. Although the international data to generate hypotheses and get against systems, our research suggests that the data could be used to generate hypotheses about the impact of different computer metrics could have in formulating policy conclusions.

This work is funded by the Office of Naval Research under award number N000140910557. 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.



Explorations in Cyber International Relations

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

Workshop on People, Power, and CyberPolitics

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

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.

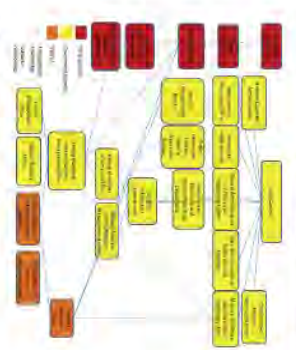
Sources include Chinese government reports and statements, Chinese and Western media, NGOs, etc. Future research should include interviews with policymakers and those involved in implementation.

Preliminary Findings

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

Users	<ul style="list-style-type: none">• Arrests and disappearances of bloggers and dissidents• Attacks on journalists and dissident email accounts• Online surveillance: "Big Mamas", 110 Cyber police, 50-year gangs
Information	<ul style="list-style-type: none">• List of "Approved Media News Sources"• Only state-owned outlets can post Internet video• Internal third-party monitoring
Applications	<ul style="list-style-type: none">• 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: Baidu, Aliyun, QQ, Baidu, Weibo, Renren
Legal	<ul style="list-style-type: none">• 8 ISPs with connections to foreign Internet backbone, most state-owned, e.g., China Telecom, China Unicom
Physical	<ul style="list-style-type: none">• Access providers• State-owned infrastructure: 8.3M km of fiber• 88303 servers from 1997-2008 on internal infrastructure• Relationships with equipment providers: Huawei, Cisco, CD135 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. Neel Choucri, Dr. David Clark



Explorations in Cyber
 International Relations
 MIT, December 7 and 8, 2011

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

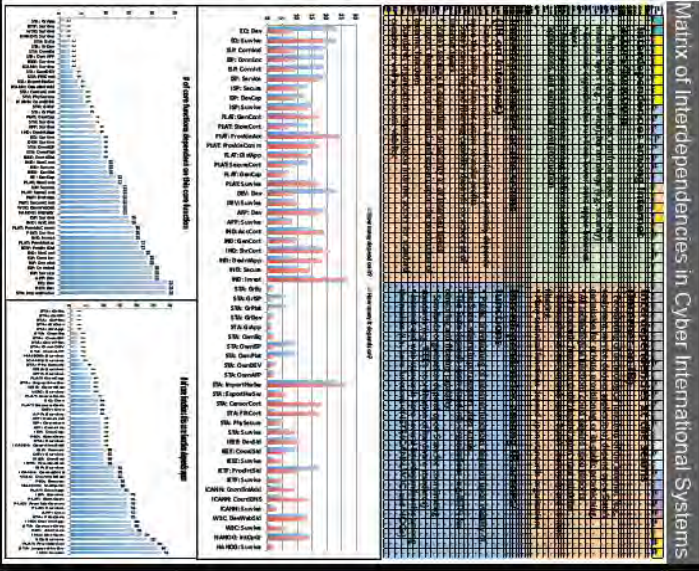
Problem

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.

The Research

Internet Actor	Abbreviation	Core Function
Equipment Providers	EQ: Devr	Design and Develop Network Equipment
ISPs	ISP: Survive ISP: Control ISP: Connect ISP: Content ISP: Service ISP: Secure ISP: DevCap ISP: Survive	Generate funds to survive Connected with domestic ISPs Connected with the international backbone ISPs Provide Internet services Secure links and servers Develop capacity to meet demand Generate funds to survive
Information/Communications Applications Platforms	PLAT: GenCont PLAT: StoreCont PLAT: ProvideComm PLAT: DisApp PLAT: SecureCont PLAT: GenApp DEV: Devr	Provide access to content Provide communications platform Develop applications Secure Content Develop capacity to meet demand Generate funds to survive
Device Makers	DEV: Survive APP: Survive	Design and develop soft devices for communications Generate funds to survive
Application Providers	IND: Survive IND: AccessCont IND: GenCont IND: StoreCont IND: DevrApp IND: Secure	Design and develop Internet Applications Secure Links/Content Invest in Internet Technologies
Individuals	IND: Invest	Invest in Internet Technologies
International Relations Actor	Abbreviation	Core Functions
State	STA: GReq STA: GISP STA: GPhal STA: GDev STA: GApp STA: OwmEq STA: OwmISP STA: OwmDev STA: OwmApp STA: ImportHwSw STA: ExportHwSw STA: GenCont	Grant private equipment providers Grant grant International/Communications Applications Platform Grant private device makers Grant private application providers Own and operate network equipment manufacturing Own and operate ISP functions Own and operate Information/Communications/Applications Platforms Own and operate device manufacturing and maintenance Import hardware/software products Export hardware/software products Generate Content
IEEE	IEEE: Survive IEEE: Control IEEE: Standard	Develop Hardware Standards Coordinate Hardware Standards Generate funds to survive
ETF	ETF: ProtinStd ETF: Survive	Produce Internet Standards Generate funds to survive
ICANN	ICANN: CoordInAd ICANN: Survive	Coordinate Internet Addresses Generate funds to survive
W3C	W3C: DevWebStd W3C: Survive	Develop Web Standards Generate funds to survive
NAVOG	NAVOG: InComp	Identify and Solve Problems of Internet Operations and Growth

Preliminary Results



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


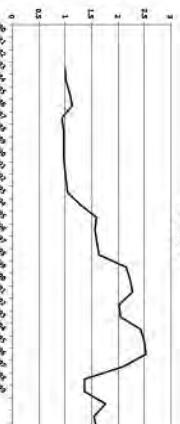
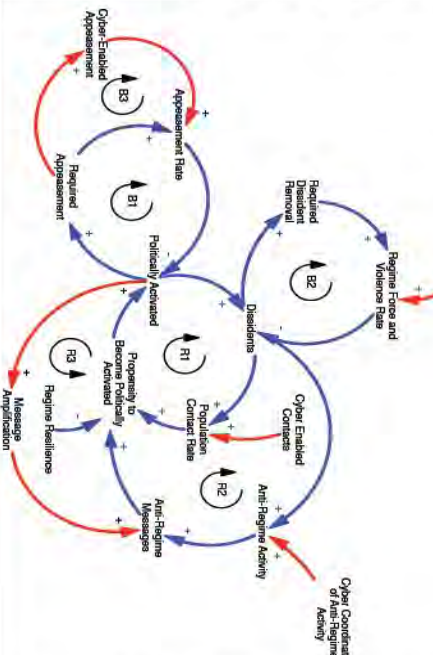
William E. Young, Jr (LtCol, USAF), PhD Student

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



<p>Problem</p> <p><i>Understanding Cyber Loads on State Resilience</i></p> <p>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.</p>	<p>The Research</p> <p>Loads versus Capacities</p> 	<p>Preliminary Results</p> <p>Resiliency Index EGYPT</p>  <p>Methodology: Choucri et al, 2006</p>
<p>Methods</p> <p><i>Qualitative & Quantitative System Dynamics Modeling</i></p> <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> ▪ message amplification ▪ appeasement ▪ coordination of anti-regime activity ▪ cyber enabled force & violence 	<p>High-Level Causal Loop Diagram</p> 	<p>Remaining Research</p> <ul style="list-style-type: none"> - 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
<p>Thank You!</p> <p>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.</p> <p>This research builds on the outstanding model and research from: Nazi Choucri, Christi Eleadis, Daniel Goldsmith, Dinitha Mistrée, Stuart E. Madnick, J. Bradley Morrison, Michael D. Siegel and Margaret Sweitzer-Hamilton.</p>		



Explorations in Cyber
International Relations
A Workshop in the World
Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Cyber International Relations Theory: Assessing the State of the Art

Robert Reardon and Nazli Choucri, Political Science, MIT

Objectives

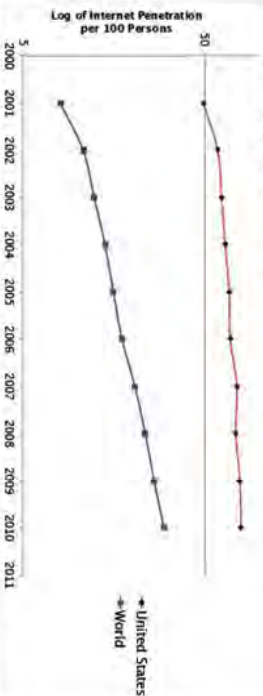
- Outline the scope of the International Relations literature on cyber-related issues with relevance to IR theory
- Frame this literature in terms of its contribution to theory building, theory testing, and issue area
- Assess the strengths and weaknesses of the literature
- Identify gaps and possible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

• 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 creating 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 cumulativeness 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 ECRJ 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 ECRJ.

This work is funded by the Office of Naval Research under award number N00019-09-1-0597. 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 Series: International Cyber Operations - The Global Dimension

Workshop on

People, Power, and CyberPolitics

MIT, December 7 and 8, 2011

<p>Problem</p> <p>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.</p>	<p>The Research</p> <p>Governance of Cyberspace: Cybersecurity</p> <p>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?</p>	<p>Preliminary Results/Results</p> <p>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.</p>
<p>Methods</p> <p>Split the issue up into two sub-issues: governance of cyberspace; and governance through cyberspace.</p>	<p>Governance through Cyberspace: Surveillance and Monitoring</p> <p>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?</p>	<p>Remaining Research/Follow-up</p> <p>What governance gaps remain? Will we see increased government control of cyberspace in the future? How will illicit groups evolve in cyberspace?</p>
<p>Thank You</p> <p><small>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.</small></p>		

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. Neel Choucri



Explorations in Cyber International Relations
 Workshop on People, Power, and CyberPolitics
 MIT, December 7 and 8, 2011

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.

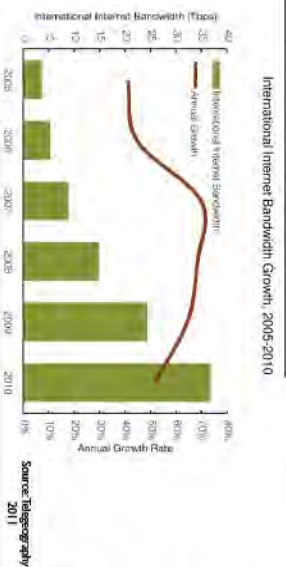
Methods

Qualitative & Quantitative System Dynamics Modeling

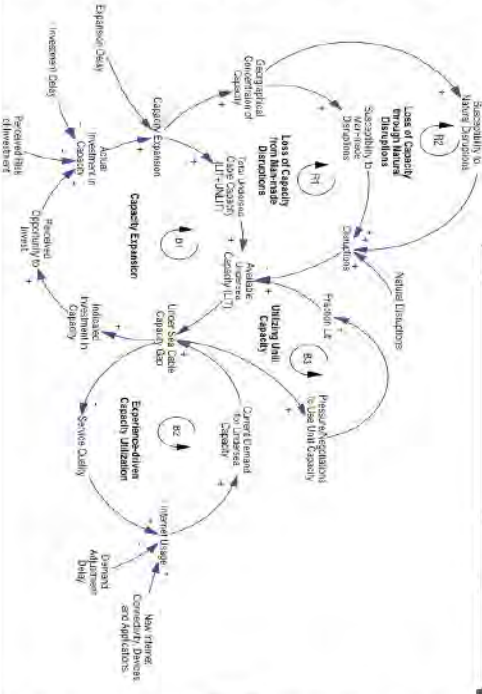
- Use a system dynamics model to identify and analyze the causal structures responsible for the above problem.
- Use emerging literature to refine the feedback structure in both dissident and state high-level cyber activity (message amplification, appeasement, coordination of anti-regime activity, force & 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.



Explorations in Cyber International Relations
 MIT, December 7 and 8, 2011

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

Escalation Management in Cyber Conflict: A Research Proposal

Robert Reardon, ECIR Postdoctoral Associate, Political Science, MIT

Research Questions	Relevant Attributes of Cyber	Implications																														
<ul style="list-style-type: none"> 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? 	<ul style="list-style-type: none"> 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. <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p style="text-align: center; margin: 0;">ATTACKERS</p> <ul style="list-style-type: none"> - State - Non-State Proxy - Autonomous Non-State Actor - Domestic </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p style="text-align: center; margin: 0;">ROLE OF STATE</p> <ul style="list-style-type: none"> - Attack Conducted by State - State Directs/Inspires/Authorizes - State Encourages Private Attacker - State Proxy Attacks Without Private Attacker - Private Attacker Not Directed by State </div> <div style="border: 1px solid black; padding: 5px; width: 30%;"> <p style="text-align: center; margin: 0;">MOTIVES</p> <ul style="list-style-type: none"> - Preparation for Kinetic Attack - Hacktivism - Terrorism - Cybercrime - Espionage </div> </div>	<ul style="list-style-type: none"> 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	Escalation Management in Different Forms of Conflict																															
<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. 	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%;">Nuclear (Cold War)</th> <th style="width: 25%;">Irregular Warfare</th> <th style="width: 25%;">Cyber</th> </tr> </thead> <tbody> <tr> <td>Paths to Escalation</td> <td>Few</td> <td>Many, Diverse, Multiple Conflicts Exist Simultaneously</td> </tr> <tr> <td>Relevant Actors</td> <td>Small Number of States, Global Interests</td> <td>Many, Diverse, Often with Regional or Local Interests</td> </tr> <tr> <td>Knowledge of Other Actors' Intentions and Capabilities</td> <td>High, Signals Relatively Easy to Send, Receive, and Interpret</td> <td>Low, Signal-to-Noise Problem</td> </tr> <tr> <td>Ability to Accurately Attribute Attacks</td> <td>High</td> <td>Low</td> </tr> <tr> <td>Risk of Deterrence Escalation</td> <td>Low</td> <td>High</td> </tr> <tr> <td>Risk of Proxy Attacks</td> <td>Low</td> <td>High</td> </tr> <tr> <td>Frequency of Attacks</td> <td>None</td> <td>High</td> </tr> <tr> <td>Damage from Attack</td> <td>Extremely High, Symmetric Vulnerability</td> <td>Variable Asymmetric Vulnerability</td> </tr> <tr> <td></td> <td></td> <td>Extremely Variable, Typically Low, Asymmetric Vulnerability</td> </tr> </tbody> </table>		Nuclear (Cold War)	Irregular Warfare	Cyber	Paths to Escalation	Few	Many, Diverse, Multiple Conflicts Exist Simultaneously	Relevant Actors	Small Number of States, Global 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	Ability to Accurately Attribute Attacks	High	Low	Risk of Deterrence Escalation	Low	High	Risk of Proxy Attacks	Low	High	Frequency of Attacks	None	High	Damage from Attack	Extremely High, Symmetric Vulnerability	Variable Asymmetric Vulnerability			Extremely Variable, Typically Low, Asymmetric Vulnerability
Nuclear (Cold War)	Irregular Warfare	Cyber																														
Paths to Escalation	Few	Many, Diverse, Multiple Conflicts Exist Simultaneously																														
Relevant Actors	Small Number of States, Global 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																														
Ability to Accurately Attribute Attacks	High	Low																														
Risk of Deterrence Escalation	Low	High																														
Risk of Proxy Attacks	Low	High																														
Frequency of Attacks	None	High																														
Damage from Attack	Extremely High, Symmetric Vulnerability	Variable Asymmetric Vulnerability																														
		Extremely Variable, Typically Low, Asymmetric Vulnerability																														
Research Plan	<ul style="list-style-type: none"> 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	<p>Author and Affiliation</p> <p>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.</p> <p>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.</p>																															

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 (2008 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?

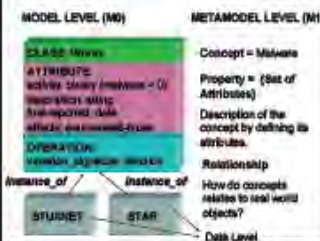
3. APPROACH

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 metamodeling 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. Narayamurti & 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 N00014081050. 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.

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. Christou; Dr. F. Field

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. Spammers disseminate 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?

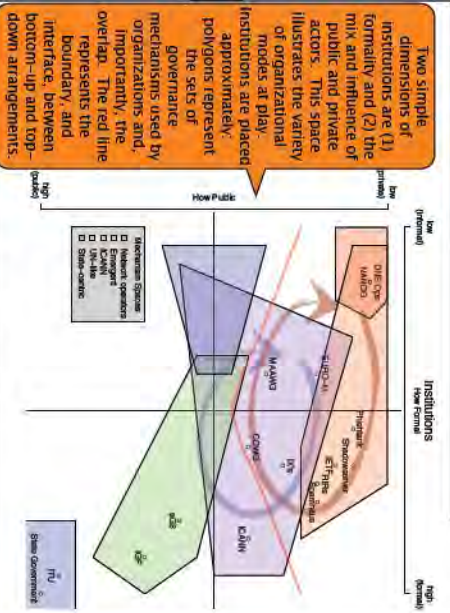
Methodology

- 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*)
- Identity policy and issue communities
- Observation of the community
- Surface causal mechanisms

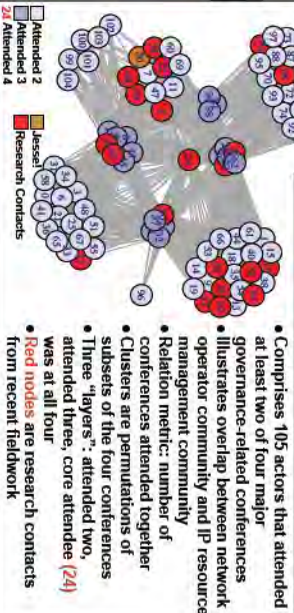


The Research

Institution Landscape and Boundaries



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

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.

Thank You!

This work is funded by the Office of Naval Research under award number N00014-09-1-0697. 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 who have contributed to this research. This work would not be possible without their help and support.



Explorations in Cyber International Relations
Workshop on People, Power, and CyberPolitics
MIT, December 7 and 8, 2011



Explorations in Cyber International Relations
 Workshop on People, Power, and CyberPolitics
 MIT, December 7 and 8, 2011

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

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

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.



Test Domain: Probable Cause

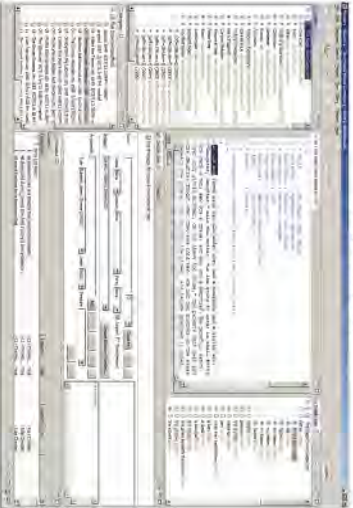
Example Case: US v Mays 466 F.3d 335 (2006)
 Police officers conducted two controlled purchases of "crack" cocaine from an address in Stoughton, Massachusetts. For the first purchase, the defendant informant allegedly purchased 0.3 grams of "crack" cocaine for \$20 from a black male named "Melvin." For the second transaction, the same informant purchased 0.3 grams of "crack" cocaine for \$20 from a black female within the informant identified as "Melvin's mother." Officer Do Lummas of the Stoughton 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 172 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, arguing that the search warrant was not supported by probable cause. He also filed an affidavit in support of his motion. The magistrate judge denied the motion. Mays further filed a motion to sever the felon-in-possession charges from the remaining charges and post-conviction motions for a new trial and judgment of acquittal. Finally, Mays objected to an enhancement in his presentence report based on a narcotics conviction he received when he was 17 years old but pled 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.

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.

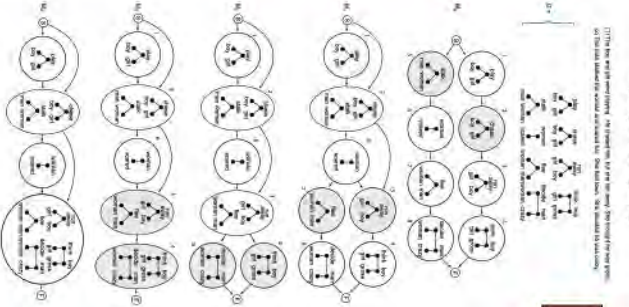
Step 1: Assemble Corpus of Appellate Cases



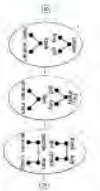
Step 2: Semantic Annotation
 (Finlayson 2008, 2011)



Step 3: Run Analogical Story Merging (ASM)
 (Finlayson 2009, 2011)



Result: Extracted Legal Principles



Evaluators 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 N00014-05-1-0537. 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.



Explorations in Cyber International Relations
 Sponsored by the Department of International Relations
 People, Power, and CyberPolitics
 MIT, December 7 and 8, 2011
 Workshop on

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

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

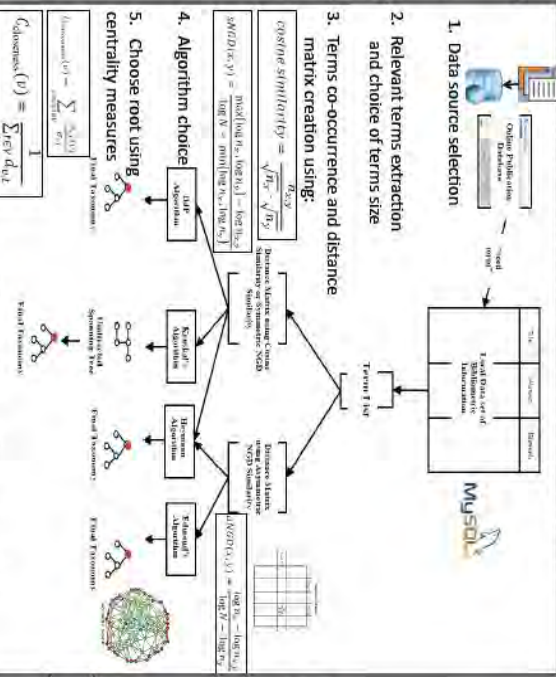
- To develop automated, publication database-independent methods for generating taxonomies.
- Advancing the algorithms in the sub-field of bibliometrics
- Applying these tools in support of the Explorations in Cyber International Relations (ECIR) research effort.
- Integration of databases of technology 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:



Meta data analysis:

social science databases	cyberspace	cyber security	social media
Behavioral Science	2773	259	459
Management Academic	906	24	30
Research Base	1912	143	26
DTIC	693	16	32
SSRN	100	1	0
Engineering Databases	1	1	0
Engineering Index	4838	305	1105
Engineering Village	4920	2501	2336
ResearchGate	2227	49	170

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 suggest 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



Cyberspace taxonomy generated from the engineering village database

Summary

- Taxonomies for scientific research bodies facilitate the organization of knowledge.
- Size of cyber related publications in social science is lagging behind those from engineering/computer sciences and they contain different terminology (see Results section).
- 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.
- 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

Doctoral 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, Basic Research in the Office of
Assistant Secretary of Defense for
Research and Engineering
U.S. Department of Defense

Jessica Stern

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

Tyson Storch

Business Development Manager
Microsoft

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

¹ Ethan Zuckerman is also an ECIR Session XX Panelist. See the session summary for his remarks.

² <http://www.ethanzuckerman.com/blog/2011/01/12/what-if-tunisia-had-a-revolution-but-nobody-watched/>

³ Lynch, Marc. (2011). The Big Think Behind the Arab Spring. *Foreign Policy*, December (190), pp. 46-47. http://www.foreignpolicy.com/articles/2011/11/28/the_big_think

⁴ <http://thedata.org/>

⁵ <http://techcrunch.com/2011/10/17/twitter-is-at-250-million-tweets-per-day/>

⁶ <http://www.crimsonhexagon.com/>

⁷ <http://cohmetrix.memphis.edu/cohmetrixpr/index.html>

⁸ Evann Smith framed this theory in a very similar fashion in ECIR Workshop Session 5. See Session Summary.

⁹ “The Digital Disruption” Eric Schmidt and Jared Cohen at the Council on Foreign Relations, November 3, 2010.

¹⁰ Climate CoLab: <http://climatecolab.org>; MIT Center for Collective Intelligence: <http://cci.mit.edu/>

¹¹ Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and national security*. Washington, D.C.: Center for Technology and National Security Policy

¹² See http://igem.org/Main_Page for more information on iGEM.