The Impact of Information and Communication Technology on State Sovereignty

An Analysis of the Cyber Utopian and Cyber Skeptic Perspectives

Sara Mishra
Senior Honors Thesis
Interdisciplinary Studies
Tufts University, 2012

Contents

Extended Contents

Preface

As an Interdisciplinary Studies (IS) Major, I have been granted a certain amount of flexibility in terms of the curriculum that I pursued here at Tufts University. I have been fortunate enough to be extended formal permission to explore the intersection of government and technology through courses in numerous departments, as well as through attending several fascinating conferences and conducting interviews with a host of knowledgeable professionals. In this thesis I have attempted to fully represent the information that I have learned throughout my undergraduate academic career. It is the culmination of four years of learning about a wide variety of subjects, which all intersect in the analysis of the impact of information and communication technology networks on government in general, and for this analysis, the concept of state sovereignty in particular.

I have been interested in the topics described in this paper since before coming to Tufts University, but through the lens of the concept of "globalization." This abstract concept of how the world is becoming more interconnected appealed to me intellectually, but I found the true definition of this term to be elusive. Ultimately, it seemed clear that the widely accepted driving force for the most recent wave of "globalization" was the widespread proliferation of recent digital information and communication technologies (e.g. computers, mobile phones). I had read, "The World is Flat" by Thomas Friedman, but found that my true interest was in how these new technologies are changing the nature of government and power, rather than inspiring economic interdependence on a global scale. Consequently, when I created my IS Major, I focused on the concept of 21st Century Statecraft that is espoused by the United States State Department. However, my interests were really much broader than that, and through academic coursework I explored the role of new technologies in changing states' capabilities and how information access was redefining the traditional concept of power.

I began writing this thesis with every intent of proving how state sovereignty was being eroded by citizens who were empowered by networks of information and communications technologies. I was in a sense, the very definition of a cyber utopian, firmly convinced that it was only a matter of time before states became outdated structures of governance. As I read articles, interviewed professionals, viewed video clips, listened to podcasts, and generally absorbed more information, I realized that the most recent wave of technology might have the greatest potential to impact international politics. However, even if that were the case, it would not mean that states would cease to be the dominating power structure, nor that they would be replaced by some other structure of international governance. Instead, I became convinced that state sovereignty was largely unchallenged by these new technologies, even as states faced unprecedented challenge to their control over information access and tools of coordination.

Consequently, I decided to frame my paper in a way that would demonstrate the very debate that had been waged within my mind. I would present the evidence that showed how the use of technology was challenging and shaping state power, and how states were in turn, challenging and shaping the use of these technologies. The following analysis is an exploration of the current, shifting relationship between government and technology. It is a snapshot of the events of this moment, and therefore, may prove to be an amusing memento after these trends have more fully developed.

Acknowledgements

This thesis is the culmination of my entire undergraduate experience, and consequently I find my gratitude must be shared with all those individuals who have helped me make it to the very end. I would like to start by thanking my faculty committee: Paul Joseph, Professor of Sociology; Julie Dobrow, Director of the Communications and Media Studies Program; and Anselm Blumer, Associate Professor of Computer Science. They provided me with significant amounts of advice as I determined and then fulfilled the requirements of my major, as well as granted me their infinite (and I do mean infinite) patience throughout the thesis writing process.

I would like to thank Dean Laura Doane and Dean Karen Gould for providing me with necessary advice and support throughout my time at Tufts University. I would also like to thank Professor Greg Carleton, and the rest of the staff of the Center for Interdisciplinary Studies, for providing me with the opportunity to explore my interests no matter which discipline they happened to fall within. Also, I appreciated the advice of Assistant Direct of Peace and Justice Studies, Dale Bryan, and Dean Carmen Lowe when I was creating my IS major. Additionally, I am grateful for the instruction of Professor Jeffrey Berry, Associate Professor Jeffrey Taliaferro, Professor Paul Joseph, Lecturer Ming Chow, and ExCollege Lecturer Lauren Brodsky since the work I completed in their classes directly informed different sections of this thesis. I extend my gratitude to the many other professors who have given me help and advice throughout my undergraduate experience.

I would also like to thank all of the interviewees who shared their knowledge with me. I truly appreciate that these academics, officials, professionals, and other individuals

were willing to take the time to speak with a curious student. Specific thanks are in order for Sree Sreenivasen, the Dean of Student Affairs at the Columbia School of Journalism, and a devoted family friend who helped me get in contact with numerous informed journalists. Additionally, I extend my thanks to Joel Harding, Information Operations Holistic Advisor, a friend and mentor who also helped to put me in contact with several potential interviewees.

Lastly, I extend my gratitude to my friends and family. Specific thanks are due to Katie Meisel, for reviewing my thesis, and to Jessie Thorup, for always reminding me to keep a cool head and settle down. I would like to thank my mother, for helping to connect me with people, and for giving me her love and support. I am grateful to my father for helping me to keep perspective and for always being one to inspire levity under any circumstances. I appreciate the support of my sister and brother-in-law, and all of my other family members who bore with me through this process.

It has been a wonderful, terrifying four years. I appreciate all of the individuals who have helped make my undergraduate experience an intense academic adventure.

Introduction

“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

-Jeff Perry Barlow "A Declaration of the Independence of Cyberspace" (1996)

Problem

In the past few decades an information revolution has swept the globe, and affected the lives of billions of people. The concept of "globalization" has taken root in the minds and writings of academic scholars, government officials, industry professionals, and even average citizens. The trend of increased interaction between individuals across national borders has been enabled by a long series of developments in transportation and information communication technologies (ICT). However, in recent decades there has been an increased focus on the role of ICT networks in connecting people around the world, specifically without the assistance or interference of their respective governments. Many individuals are inspired by the potential of these new technologies to allow for an unprecedented scale of international interaction. These “cyber utopians” see these ICT networks as facilitating a fundamental shift in how people organize themselves and the very fabric of governance. However, there are also individuals who argue that these recent ICT advances are just an extension of similar technological developments in the past. These “cyber skeptics” believe that in time the impact of ICT will be subjected to the rule of governments, and even become a useful tool for state control.

At the core of the debate between these conflicting perspectives are the questions: How are ICT networks impacting the sovereignty of states? If citizens can use ICT networks to interact and coordinate with each other without relying on the government, or even in direct opposition to it, does this undermine a state's claim to authority over its territory? And, is it true that the decentralized nature of ICT networks inherently challenges the typically hierarchical structure of sovereign states? Another question that should precede those above would be: Is it even possible to suggest that networks of technology could have a significant impact on how people govern themselves, and how states are structured? These questions are important because sovereignty is a fundamental part of the state paradigm employed in international politics, and a significant paradigm shift could have an impact on the relationship between governments and citizens.

It is challenging to answer these questions in a single written analysis for several reasons. For one, they are too broad. The entire field of international relations theory is dedicated to exploring the concept of state sovereignty, and the forces that challenge it. For another, the questions lack clear definition. It is difficult to determine what characteristics a state must have to achieve "sovereignty", and there are numerous definitions for what these terms mean. For a third, it is hard to quantify the concept of "state sovereignty" as well as its contemporary opposition. Researchers who investigate this topic often quantify the amount of ICT used in a country, and the amount of coordination they inspired, but even the results of these comparisons do not fully address whether there is a reduced authority of the state structure as a whole (Meier 2011: 33).

The reality of governmental authority is highly dependent on the country being examined, and the particular conditions that surround that polity. However, the concept of "state sovereignty" is largely theoretical. If one uses a fixed definition, one can discuss the questions mentioned above from a more abstract perspective and use set criteria for examining cases where a state’s “sovereignty” may have been challenged. International

Relations (IR) Scholar Jeffrey Taliaferro describes sovereignty as “The legal principle, established through recognition by other states, that a state is the legitimate highest authority within its boundaries” (Taliaferro 2008). This analysis will employ that definition, and follow IR scholar Janice Thomson’s line of argument that: “The question is whether or not the state's ability to make authoritative political decisions has eroded; that is, whether ultimate political authority has shifted from the state to non state actors or institutions” (Thomson 1995: 216).

It is important to clarify that throughout this paper a distinction is drawn between state authority and state control. Essentially, state authority is derived from the state being recognized as the highest legitimate entity that is tasked with creating the rules that govern society, and state control is dependent on whether these rules are followed. This analysis will rely on Taliaferro’s definition of sovereignty, and Thomson’s arguments in order to establish the criteria that a shift of sovereignty from states to another form of global political organization would require the loss of states’ supreme authority (not control) within their borders. This means that the formal “state” structure would no longer be recognized, domestically and internationally, as the highest, legitimate governing body within its territory.

The discussions in this analysis will not attempt to fully answer the questions mentioned above, but will seek to explore the theories that define "state sovereignty", and the contrasting perspectives on how it is being challenged by the decentralized nature of ICT networks. This analysis will address the two main questions: What are some of the functions of ICT networks that allow citizens to challenge the authority of the state? What are some of the functions of ICT networks that allow states to reassert their authority? And it will discuss, but by no means fully answer, the third question: "What challenge does the decentralized nature of ICT networks actually present to state sovereignty?" The contrasting perspectives on the significance of ICT networks can be roughly separated into two main groups – the cyber utopians and the cyber skeptics – and this analysis will use these labels to structure its evidence and case studies. While these labels denote viewpoints that discuss the role of technology in numerous areas of life – not just as it pertains to politics – this analysis will largely focus on the arguments that relate to governance.

This analysis will take the theories and thoughts discussed by the cyber utopians and cyber skeptics and apply them to numerous case studies that illustrate the functions of ICT networks. In this way, there will be a comprehensive discussion of the challenges to and reassertions of state sovereignty. This will inform the author's own argument, that while ICT networks do not eliminate state sovereignty, they challenge states' control over actors within their borders. As a result regimes need to more actively reassert their authority in order to retain power, yet state sovereignty, as a whole still remains intact.

Significance

For the past few centuries, the state-centric system has been the dominant paradigm in the international arena. While there is significant debate over the importance of other actors, the sovereignty of states is typically accepted as a fundamental assumption, and one that is even required by international organizations such as the UN (Charter of the United Nations 1945: II). If in fact ICT networks were posing significant challenges to the sovereignty of states, this would imply that the world is currently experiencing a fundamental shift equivalent to the formation of states that was recognized in the Treaty of Westphalia in 1648. However, even if these changes are not that profound, they would still result in the restructuring of the balance of power in the international arena, and even between states and their citizens. This shift in power would mean a fundamental change in what people expect from their governments, and how people govern themselves in general.

While it is unclear whether the extreme case of a world without states will ever come into being, there are many individuals who argue that current fluctuations in international power are having an impact on citizens around the world. A predominant scholar of IR theory, Joseph Nye, argues that: "Two great power shifts are occurring in this century: a power transition among states and a power diffusion away from all states to nonstate actors" (Nye 2011: xv). He discusses how there are more and more interactions outside the control of even the most powerful states (Nye 2011: xvi), and posits that: "We have not so much a multi-polar world as a no-polar world" (Nye 2011: 113). If this is considered to be true, it will have a huge impact on how states interact with each other, and their citizens.

The United States State Department (U.S. SD) has created an entire initiative dedicated to fully leveraging the networks, technologies, and demographics that are present in a “networked world” (Ross 2011: 452), which implies that U.S officials also believe that there is a fundamental shift occurring in world politics. U.S. SD Senior Advisor for Innovation Alec Ross argues that: “Networks are a defining feature in the new global power structure. The very clear evidence of recent years demonstrates that network technologies devolve power away from the nation-state and large institutions”

(Ross 2011: 452). If citizens can use ICT networks to both consume and produce information, then they can expose corruption in China. If citizens can communicate with each other about shared frustrations, then they can coordinate protests against the government in Tunisia. If citizens can coordinate information in times of crisis, then they can provide governments and aid organizations with essential real time information in Haiti. On the other hand, if states, such as China, can subtly control citizens' access to information, then they can limit and shape their citizens' understanding of the world. If states, such as the United States, can spread their perspective to citizens domestically and abroad, then they can expand their influence on public perception. If states, such as Russia, can inspire patriotic action among their citizens, then they can launch attacks against other states without being held directly responsible.

There are functions of ICT networks that allow for citizens to challenge their government, and functions that allow states to reassert their authority. As of this moment, it is unclear whether ultimately states will once again subject these new technologies to their control, and limit their citizens' use, or if there will truly be a seismic shift in the relative power between state and non-state actors. However, the significance of this tension is undeniable. The challenge that ICT networks pose to state sovereignty inspires dreams of nothing more and nothing less than the possibility of a new world order.

Structure

The previous paragraphs outline the *problem* this analysis addresses and its larger *significance*. In the following paragraphs of this introduction, several key terms will be *defined* in order to promote consistent use throughout this paper. The next section of this analysis will explain the *methodology* used to collect research. The primary research gathered for this analysis – namely the interviews – are used to support arguments throughout this paper, and fully integrated with the literature-based arguments. Consequently, the research and results components of this analysis will be written together in one section, with the primary data (interviews) included directly in the body of the paper. This section follows the methodology section and is prior to the discussion section.

The research and results section has been broken into three main sub-sections: *background literature*, *cyber utopian evidence*, and *cyber skeptic evidence*. However, within each section there will be references to contradictory evidence or to debates between conflicting theorists. The *background literature* section will discuss network theory from a social perspective, as well as provide information about the current structure of ICT networks and what events have shaped their development. It will also outline the main arguments of the cyber utopians and the cyber skeptics, which will define the remaining structure of the paper.

The *cyber utopian evidence* section will focus on the functions of ICT networks that support the utopian perspective and discuss how citizens are challenging state authority through the use of ICT networks. Within the *cyber utopian evidence* section there are two main sub-sections: *information* and *coordination*. The *information* section will discuss how ICT networks are changing the way people create, consume, and transfer information. The *coordination* section will discuss how people are using this information to communicate and coordinate with each other through ICT networks. The *coordination* section is further broken into two more sections: the first, *activism,* will focus on how ICT networks – particularly social media sites – have been used to coordinate protests and inspire political activism, and the second, *assistance*, will focus on how ICT networks have been used to coordinate international efforts to provide aid during times of political and environmental crisis.

The *cyber skeptic evidence section* will focus on those functions that support the skeptic perspective, and discuss how states are using ICT networks to reaffirm their authority. Within the *cyber skeptic evidence* section there are two main sub-sections: *control* and *force*. The *control* section will discuss how states are finding ways to control the information made available through ICT networks, and to spread their own message in order expand their influence. The *control* section is further broken into two more sections: the first, *censorship*, will focus on how states are finding ways to censor the information available through ICT networks, and the second, *influence*, will focus on how states are using ICT networks – particularly the Internet and its social media sites – to expand their influence on their citizens as well as foreign publics. The *force* section will discuss how states are using these networks to expand their military capabilities, and even to inspire the jingoistic actions of patriotic citizens.

Within all of these sections, several case studies will be discussed in order to illustrate the various uses of ICT networks. These case studies will exemplify situations where ICT networks are challenging state authority or supporting it. At the end of each sub-section the themes and examples discussed in that portion will be connected to the overarching arguments of the skeptics and utopians.

At the end of this paper, there will be a *discussion* section that explains the writer's perspective and how it has been informed by the information gathered during the research process, specifically through the interviews of various informed professionals. The writer will *conclude* by summarizing the information discussed in the paper, by discussing what topics were not explored but perhaps should have been included, and by expressing her views on future trends.

Definitions

The very foundation of this analysis rests on establishing a definition for "state sovereignty" that will serve as the measuring-stick by which all of the evidence is examined. In addition, it is important to define the meaning of "ICT" networks and related concepts in order to maintain consistency throughout this analysis. The following definitions are by no means absolute, but they are a widely accepted or have been well thought out by scholars.

According to international relations scholar Jeffrey Taliaferro the **State** can have three meanings:

> (1) A generic term for the main units in any international system over history, regardless of those units' internal composition or territorial scope. (2) A specific form of political community that originated in Western Europe during fifteenth and sixteenth centuries, which later became the predominate form of political community throughout the globe during the late nineteenth and early twentieth centuries. In this definition, the "state" differs from other forms of political organization in that there is clear hierarchy within the political community, defined territorial borders, some extractive capacity vis-à-vis civil society, and where the government claims a monopoly on the legitimate use of force within its own territory. (3) A synonym for the government or administrative apparatus of a state, as distinguished from civil society (Taliaferro 2008).

This analysis will use all three definitions at various points. The terms state and government will often be used interchangeably, however, the discussion of "state sovereignty" will rely on the second definition.

A commonly accepted definition of **state sovereignty** is "supreme authority within a territory" (Stanford Encyclopedia of Philosophy). "Authority" in the sense that the state is recognized as a legitimate actor that has the right to command and be obeyed. “Supreme” in the sense that the state is considered superior to all authorities under its purview. “Within a territory” in the sense that the state has authority within particular borders and membership is typically defined by residence within that space (Stanford Encyclopedia of Philosophy). This definition does not ignore the fact that other entities have authority within states (i.e. religious institutions), but asserts that the state is the supreme or highest authority within that territory. Taliaferro similarly describes sovereignty as “The legal principle, established through recognition by other states, that a state is the legitimate highest authority within its boundaries” (Taliaferro 2008). This definition will be used within this paper. International relations theorist Janice E. Thomson also describes the definitions put forth by the two competing schools of IR thought: “For liberal interdependence theorists sovereignty is defined in terms of the state's ability to control actors and activities within and across its borders. For realists, the essence of sovereignty is the state's ability to make authoritative decisions in the final instance, the decision to make war” (Thomson 1995: 213). These definitions correspond with the views of the cyber utopians and cyber skeptics respectively, and will be used to explore both perspectives throughout this analysis.

Thomson argues: “sovereignty is best conceptualized in terms, not of state control, but of **state authority**. State control has waxed and waned enormously overtime, regions, and issue-areas while the state's claim to ultimate political authority has persisted for more than three centuries” (Thomson 1995: 214). She adds: “ The question is whether or not the state's ability to make authoritative political decisions has eroded; that is, whether ultimate political authority has shifted from the state to non state actors or institutions”

(Thomson 1995: 216). Based on Thomson's arguments, the author of this analysis will argue that a shift of sovereignty from states to another form of global political organization would require the loss of states' supreme authority within their borders. This means that the formal "state" structure would no longer be recognized, domestically and internationally, as the highest governing body within its territory.

According to the World Bank, **Information and Communication Technology (ICT)** consists of the hardware, software, networks, and media for the collection, storage, processing, transmission and presentation of information (voice, data, text, images), as well as related services (World Bank ICT Website). ICT is composed of **Information and Communication Infrastructure (ICI)** and **Information Technology (IT).** ICI Refers to physical telecommunications systems and networks (cellar, broadcast, cable, satellite, postal) and the services that utilize them (**Internet**, voice, mail, radio, and television) (World Bank ICT Website). IT refers to the hardware and software of information collection, storage, processing, and presentation (World Bank ICT Website). The **Internet** is not a network, but a vast collection of different networks that use common protocols and provide certain common services (i.e. E-mail, news, remote login, file transfer) (Tanenbaum 2003: 50). **Cyberspace** is a nebulous term, but is described by U.S. Deputy Defense Secretary Gordon as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Schachtman 2008). It is essentially the virtual world that is generated on top of ICT infrastructure. The terms above will be further examined in later sections, and many other key terms will be defined throughout this analysis.

It is important to note that the literature discussed in this analysis predominantly focused on the Internet or the Web applications it hosts (i.e. e-mail, forums, blogs, social media sites). The Internet is a fundamental service generated by ICT networks, and exemplifies their potential for political impact through citizen use. In certain sections the author may refer to ICT networks in general, or discuss the Internet or mobile phone networks in particular. In other words, this analysis at times narrows its focus due to the nature of the materials that were reviewed. This narrowing will be specified at necessary points.

Methodology

The methodology for this analysis involved collecting a wide variety of primary and secondary materials. These materials were collected from the websites of various institutions that focus on the role of ICT in society, such as the Harvard Berkman Center and the United States Institute of Peace. They were also found through e-lists provided by these institutions, as well as personal recommendations from family, friends, professors, and other helpful associates. Information was also taken from the blogs and websites of individuals who are following related topics, as well as from the social networking sites – specifically Facebook and Twitter – of these individuals. The topic that is explored in this paper is highly contemporary, and consequently, a large amount of the sources – articles, audio recordings, video recordings, and others – discussed the inferences and perspectives of professionals and their comments on recent, relevant events. This information is supplemented with first-hand research collected by the writer.

The writer gathered primary source material for each section of this thesis by interviewing individuals from numerous fields, each of whom were well informed about the topic of questioning. A complete list of these individuals is included in the bibliography of this paper, although, the names of several interviewees were withheld at their request. Throughout this analysis, the credentials of the interviewees are directly included in the discussion of their thoughts and attached to their quotes. The general selection criteria for these individuals was that they be affiliated to a well-established government, technology, media, or academic-related institution, and that their positions be directly related to the theme being investigated.

For the topic of crisis mapping, interviews were conducted with former or current crisis mappers who had significant understanding of mapping platforms and the organizations that utilize them in times of crisis and political conflict. For the topic of information and social media, interviews were conducted with activists, journalists, and bloggers who had covered or participated in protest movements or related events in relevant countries such as Egypt, Tunisia, and Syria. For the topic of government influence, interviews were conducted with U.S. State Department officials who had knowledge of government initiatives focused on using new technology to update diplomatic efforts. For the topic of cyber power, interviews were conducted with government officials and cyber-security professionals who had worked on policy surrounding cyber conflict. There were several other interviews conducted with individuals who knew relevant information about particular technologies or countries that are examined in this analysis. A few informal interviews were conducted with former students who are familiar with similar research topics in order to gather background information. These interviews were conducted in the early months of 2012, through several methods such as: in-person at offices in Washington DC and Medford, Massachusetts; on the phone; on the Skype video communication application; and through email exchanges. The interview transcripts are in the writer's possession, but have not been included in this paper in order to protect the privacy of the interviewees.

It is important to mention that the individuals interviewed were often selected because of accessibility. Several of these individuals were chosen because they are authors of sources that are included in this analysis. These individuals were contacted through blind emails, or through references provided by fellow students, professors, and industry professionals. After an interview, the subject would sometimes make suggestions about other people that might be a good source. Consequently, certain individuals were found through "snowball sampling." These interviewees are all authorities on the topics they spoke about, however, they are by no means the only ones. There are many other individuals who would have been able to provide valuable insight for this analysis and offer a different perspective. However, the writer has no personal connection to any of the individuals being interviewed, nor did she know what their views were in advance of asking her questions. The writer will attempt to represent the views of these individuals as directly as possible throughout this analysis.

Background Literature

Networks Background

In order to explore the dynamic relationship between hierarchical states and ICT networks, it is necessary to understand the concepts that support network theory. Network theorist Miles Kahler highlights the significance of these theories: “If the contest between markets and state hierarchies was an organizing feature of the 1980s, network has emerged as the dominant social and economic metaphor in subsequent decades" (Kahler 2009: 2). This sub-section will discuss general network theory, and how it applies to ICT networks and international politics. It will explore the concept of the “layered” nature of cyberspace (Choucri 2011: 9), and will explain the physical infrastructure of ICT networks, with a particular focus on the Internet. It will then discuss the elements of Internet architecture that can be considered hierarchical, and examine the administrative bodies that determine Internet protocols. Additionally, this analysis will investigate how the networked nature of the Internet impacts states, and will explore the concept of networked governance. The final paragraphs will connect networked political theory to the cyber utopian and cyber skeptic perspectives. The information discussed in this section will directly inform the following chapters that outline the functions of ICT networks that challenge and support state authority.

Network Theory

The fundamental definition of networks is a set of interconnections among nodes. These nodes can represent anything – humans, airports, cells – and any relationship between nodes can be treated as a link (Mueller 2010: 32). Network theorist Miles Kahler explains that: "Defined in its simplest form, as any set of interconnected nodes, networks are ubiquitous" (Kahler 2009: 3). Networks can refer to the mathematical tool for representing social relationships, or more importantly, it can be considered an organizational form (Mueller 2010: 31). Social network analysis (SNA) is a paradigm of social science and examines the world as a web of relationships among different organisms (Maoz 2011: 12). Network analysis is useful because it provides a distinct vocabulary for describing relationships, and it allows for the quantification of structural properties (Mueller 2010: 32). Networks are typically treated as varying along three dimensions: 1) The number of nodes; 2) the density of the network or the frequency of interactions between nodes; and 3) the structure of the network, defined as the pattern of connections between nodes (Lake and Wong 2009: 129). Efficiency is defined as the ability to transmit information across the network quickly, and robustness is defined as the ability of a network to function after the failure or removal of a node (Barbassi 2003 as cited in Lake and Wong 2009: 129).

Kahtryn Sikkink defines four common characteristics of networks: “(1) their voluntary nature and thus the possibility of exit; (2) the central role of information and learning; (3) their ability to build trust and confidence among network participants, and (4) their flexibility and adaptability compared to other organizational forms” (Sikkink 2009: 230). In addition, network theorists often describe two types of networks: those that result from intentional voluntary associations, and those that result from unplanned involuntary associations (Maoz 2011: 6). Miles Kahler describes two approaches to network analysis: networks-as-structures and networks-as-actors. The first emphasizes the structural characteristics of networks, while the second compares them to other structures and evaluates the networks success in achieving collective ends (Kahler 2009: 2). Networks-as-actors are structures and agents (Sikkink 2009: 228). They are consciously constructed and can be thought of as network organizations, rather than a decentered, associative cluster of actors with fluctuating patterns of interaction (Mueller 2010: 41). Another set of relevant terminology explains how there are "relational networks" or one mode networks –characterized by rules that define the relationship between any two units – and affiliational networks or two-mode networks – characterized by rules that define the affiliation of a unit with an event or group (Maoz 2011: 7).

ICT Networks

The ICT networks that compose cyberspace can be both networks-as-structures, and networks-as-agents. For example, certain parts of the Internet are determined formally determined by international governing bodies, while mobile phone networks grow haphazardly as new users join in. In the case of ICT networks, communications systems can be divided into different layers that work together to enable the transfer of information (Lessig 2001: 23). Professor Nazli Choucri describes four layers that characterize the Internet, and similar networks from the top down: the people or users of cyberspace, information that is transmitted in cyberspace, logical building blocks that support the structure of cyberspace, and the physical foundations or infrastructure of cyberspace (Choucri 2011: 9). In the following paragraphs each of these layers will be explored in relation to the Internet and related ICT, beginning with the physical infrastructure

Physical Layer

There are many different mediums that can be considered information communication technologies, and consequently, there are numerous overlapping networks enabling transfers of data. There are two principle categories for ICT: (1) information-processing technologies that store, manipulate, and display information (i.e. random-access memory (RAM), supercomputers); and (2) communications technologies that transmit and receive the information from one place to another (i.e. local area network (LAN) connections between printers and computers) (Rosenau and Johnson 2002: 59). Some other common examples of ICT include: cellular telephony, direct dial digital telephony, television, communications satellites, worldwide courier service, satellite TV broadcasting, computers, and of course, the Internet (Sadowsky, Zambrano, and Dandjinou 2004: 7). These networks rely on interconnected computing devices, and so their infrastructure is built from "PCs and servers, supercomputers and grids, sensors and transducers, and various sorts of networks and communications channels. Communications may occur over wires or fibers, via radio transmission, or by the physical transport of the computing and storage devices from place to place" (Choucri 2011: 10). These technologies are produced by private companies and purchased by individuals around the world. While private companies operate ICT networks, there are international organizations dedicated to determining the protocols and standards that these technologies and networks rely on.

Logical Layer

The logical building blocks that networks rely on differ based on the technologies involved. In the case of the Internet, the Internet Protocol (IP) addressing scheme is essential for allowing the coordinated transfer of information between computers throughout the world. On the Internet, every sub-network and device (i.e. computers, printers, smart phones) is assigned a number called an IP address, which serves as its identifier throughout the world. It is therefore important to ensure that IP addresses are properly allocated, and kept track of (MacKinnon 2012: 211). These IP addresses are used in conjunction with the transmission control protocol (TCP), to move packets of data from a source to a destination. The TCP/IP framework forms the foundation for the logical layer of the Internet from which web applications such as Facebook can be developed (Choucri 2011: 11). As Nazli Choucri describes: "The nature of cyberspace—its strengths and its limitations, derive more from the decisions made at the *logical* level than the physical level. The Internet provides a set of capabilities that are intentionally separated or divorced to a great extent from the details of the technology that underpins it" (Choucri 2011: 10). The IP addressing scheme at the logical level contains a significant amount of hierarchy, which is important to recognize as it has implications on how information flows can be controlled.

Hierarchies

Hierarchy is useful for certain ICT when it conserves valuable, scarce network resources. For example, the traditional telephone network was very hierarchical as it relied on two scarce resources transmission capacity and intelligent switching capacity (Cowhey and Mueller 2009: 178). Arguably, the Internet is not limited by these constraints due to an abundance of bandwith, and an exponential growth in processing power. However, in his research, Matthew Hindman has found that “powerful hierarchies [are] shaping a medium that continues to be celebrated for its openness. This hierarchy is structural, woven into the hyperlinks that make up the Web” (Hindman 2009: 19). Individuals that use links on the Internet are typically unaware of how their actions are defining its structure (Kahler 2009: 7). However, Hindman argues that this hyperlink determined structure is an important form of filtering, and that despite it being an unintentional product of the larger ecology of online information. “The link structure of the Web is critical in determining what content citizens see" (Hindman 2009: 14). Furthermore, Hindman explains that the structure of the Internet means that not all choices are equal, and some sites will consistently rise to the top of Yahoo!’s and Google’s search results, while others are never indexed (Hindman 2009: 15). The prioritization of certain information on the Internet highlights the fact that there is a certain amount of hierarchical processing even in ICT networks.

Information Layer

While the physical and logical structure of the Internet, and other ICT networks is highly relevant, many social scientists are recognizing that it is the flows of information, or contents of the transmission between networks, that matter most (Webster 2002: 81). Nazli Choucri describes these flows as the Information layer, where the creation, capture, storage, and processing of information and “content” takes place. Information in cyberspace can take many forms including the shared music and videos, the stored records of businesses, and the pages of the World Wide Web (Choucri 2011: 11). One example of information is the content on the blogs created by average Internet users. These blogs extend the use of web pages in two significant ways: they make the web "writable" as in anyone can create content and share it, and they allow other readers or users to write on the blog (Benkler 2006: 216-217). On the Internet interacting with others is simple, as is generating and consuming content. However, the Internet was not designed as a distribution channel for media, but as a communications network, which then gradually grew capable of communicating rich media content. Its architecture was created to privilege the transmission of data, not the identification or control of what was conveyed (Karaganis 2007: 257). Users have determined what information is transmitted on ICT networks.

User Layer

The fourth layer of the Internet and ICT networks is people, because they are not just passive users, but also unintentional architects that define and shape the character of the technologies they utilize (Choucri 2011: 12). As Nazli Choucri explains: "If people contribute to Wikipedia, then Wikipedia exists. If people tweet, then Twitter exists. This is a critically important, definitional, feature of cyberspace" (Choucri 2011: 12). In addition to the users, the administrative bodies that govern the Internet determine its structure and functionality. These administrative groups make decisions about standards that shape the very nature of how the Internet is structured, and how users transfer information. These groups are charged with three main tasks: (1) develop technical standards; (2) allocate and assign resources such as IP addresses and domain names; and (3) establish the policies and procedures governing the interconnection of ISPs and their use of physical telecommunication facilities (Cowhey and Mueller 2009: 181). These decisions determine the level of decentralization or hierarchy present in the Internet, and establish which organizations have authority over which structural elements. These decisions influence how users can share information, even more so than the physical structure of the Internet.

Internet Governance

The International Corporation for Assigned Names and Numbers (ICANN) is in charge of coordinating IP addresses, and the Domain Name System (DNS) that attaches these numbers to the names users enter into their browsers (Sadowsky, Zambrano, and Dandjinou 2004: 10). For example, the IP address 74.125.224.244 is assigned to Google.com in the United States. The Internet Assigned Numbers Authority (IANA) allocates blocks of IP addresses to the regional Internet registries (RIR), and Internet service providers (ISPs) or similar organizations pay to become members of their specific RIR (MacKinnon 2012: 211). The Internet Engineering Task Force (IETF) is responsible for developing and testing the standards upon which the Internet rests (Sadowsky, Zambrano, and Dandjinou 2004: 10). All of these groups, along with numerous others, are responsible for the operation of the network, and ensure that it is interoperable, functional, stable, secure and effective over the long run. It is interesting to note that "[Internet administration] is concerned with functions that did not exist prior to the Internet, most obvious being the coordinated cooperative management of a very large, global packet switching network based upon hierarchical, open, decentralized network administration" (Sadowsky, Zambrano, and Dandjinou 2004: 9).

Network theorist Miles Kahler writes that in two cases – standards setting and resource allocation on the Internet – governments have delegated authority to nongovernmental networks (Kahler 2009: 18). As described above, there are many groups that work in conjunction to manage the Internet. Despite the fact that these groups are geographically and organizationally distributed, they work within an open, coordinated framework, and are bound by a common set of standards and modalities of actions (Granovetter 1983: 10). However, Lawrence Lessig points out an important fact: "The Internet is a network of networks… These networks connect over wires. All of these wires, and the machines linked by them, are controlled by someone" (Lessig 2011: 26).

The Tier 1 ISPs provide the Internet's backbone functions, coordinate their activities through formal groups, and have peering arrangements to provide connectivity to other ISPs (Sadowsky, Zambrano, and Dandjinou 2004: 10). These are private companies that manage the physical infrastructure of ICT networks, such as AT&T or Verizon in the United States, NTT communications in Japan, or Tata communications ("Who Are the Tier 1 ISPs?"). Internet companies such as Google and Facebook also play a role in shaping user experiences of the Internet, and in the case of Google, helping to prioritize information. Additionally, there are technology companies such as Microsoft, Apple, Intel, or Cisco that provide the hardware that form the physical infrastructure of ICT networks. All of these companies support and participate in the work of open standards organizations and coordinating bodies that maintain the global addressing and domain name system (i.e. IETF, ICANN, or RIRs) (MacKinnon 2012: 19). It is people who define the content that is transmitted on ICT networks, and who define their physical and logical structure. ICT networks are complex and rely on many different actors and groups in order to function. The development of ICT networks as a whole has signaled new capabilities in communication.

ICT Development

In the past few centuries, there have been several revolutions in communications. Cherie Steel and Arthur Stein describe three significant revolutions that have occurred in the past two centuries. The first occurred in the nineteenth century with the invention of the telegraph, because at that time this "point to point" technology allowed for information to travel faster than people or any mode of transportation (Steele and Stein 2002: 28-29). T The second revolution described the development of broadcasting technologies that allowed for private and public entities to send out information from one source to many people and places at once (Steele and Stein 2002: 28-29). The third revolution is occurring in the present day, and is characterized by the development of the Internet and networking, linking any number of distant sites in multidirectional communications (Steele and Stein 2002: 28-29). These revolutions have resulted in a slow shift in transmission and reception capabilities from "single to single" as in telephones, to "single to many" as in radios and televisions, to "many to single" as in comment forms submitted on a company website, and last, to "many to many" (Rosenau and Johnson 2002: 59-60).

The Internet allows for not only large numbers of information transmissions and receptions but also great diversity in the sources of transmission and reception (Rosenau and Johnson 2002: 59-60). However, according to political scientist Joseph Nye it is not just the increased capabilities of modern ICT networks, nor their speed that characterizes the contemporary information revolution. It is the enormous reduction in the cost of transmitting information. According to Nye, "This dramatic change in the linked technologies of computing and communications is changing the nature of government and accelerating the diffusion of power" (Nye 2011: 115).

International Networks

Until this point this analysis has focused on the concept of networks as they apply to information communication technologies, and the administrative bodies that operate them. However, network theory is not limited to any particular unit of analysis, and networks can be used in the context of international relations to describe the connections between states, and other organizations operating across borders. According to Miles Kahler, network analysis contributes to the examination of three theoretical debates in international politics: the relationship between structure and agency, competing definitions of power, and the efficacy of emerging forms of international governance" (Kahler 2009: 2). According to network theorist Zeev Maoz: "The central argument of [Networked International Politics (NIP)] is simple: international relations have evolved as a set of interrelated cooperative and conflictual networks. These networks coevolve in constant interaction with each other, and this interaction has important implications for the behavior of nations and for the structure of the international system" (Maoz 2011: 6). However, there are also scholars that argue that network theory does not directly address issues relating to politics (Lake and Wong 2009: 130). Still, Miles Kahler argues that in international relations, it is realistic to assume that there is some awareness of network structure (Kahler 2009: 8). Furthermore, he sees networks as new contributors to international governance, and as requiring careful evaluation (Kahler 2009: 20). The decentralized coordination of the various organizations that govern the Internet has been conceptualized as a kind of networked governance (Mueller 2010: 6). According to Milton Mueller, there is the possibility that this concept of networked governance could be adopted by states, and therefore bridge the gap between national institutions and global connectivity (Mueller 2010: 6).

Miles Kahler argues that within a network, positioning defines three distinct forms of power: bargaining power, social power, and the power of exit (Kahler 2009: 12). Bargaining power is particularly interesting because it implies that states that are the sole link between clusters of highly connected states and could gain influence as power brokers within the network (Kahler 2009: 12). This perspective offers new possibilities for soft power. Additionally, Kahler believes that there are parallels between social power in international networks, and soft power in international relations, implying that network position can have an impact on states' ability to influence others (Kahler 2009: 13). Similarly, Kathryn Sikkink argues that power in networks depends on structural position in a field of connections to other agents as well as actor capabilities or attributes. According to her, dyadic measures of influence seem inadequate in a world of networked states (Sikkink 2009: 245).

Joseph Nye states: "On many transnational issues, empowering others can help us to accomplish our own goals. In this world, networks and connectedness become an important source of relevant power (Nye 2011: xvii). His viewpoint can be considered cyber utopian in its emphasis on mutual empowerment. Milton Mueller also supports this positive perspective and argues that: “networks that combine state and non-state actors can overcome some of the limitations of government based on territorial sovereignty (Mueller 2010: 6). Juliann Emmons Allison argues that information technologies have empowered subnational groups demanding recognition, which has resulted in a significant challenge to the nation-state (Allison 2002: 7). Miles Kahler offers a more moderate view: "A networked perspective challenges conventional views of power in international relations. At the same time, attention to the exercise of power refreshes network analysis by questioning its overly consensual and trust-laden view of networks (Kahler 2009: 11).

Network Limitations

Cyber utopians often describe networks in opposition to hierarchies, but this distinction is difficult when defining the boundaries of networked politics (Kahler 2009: 6). Miles Kahler also notes that when a networked organization engages in competition with a hierarchical organization, as in a state, the network will become more centralized or the hierarchical constituents will become more influential (Kahler 2009: 123). Additionally, while there is the possibility that networks can allow for more interconnectedness, they are not without flaws. The consensual nature of networks makes collective decision-making slow and difficult, and because members of networks are free to enter an exit as they choose, there is a low level of commitment (Mueller 2010: 49). Network theory is being applied to international relations, but Kathryn Sikkink argues that it is important to recognize that: "Networks exist because other actors, mainly states but also international organizations, have created them and delegated authority to them"

(Sikkink 2009: 232). The legal basis for the modern system of international relations relies on the principle of sovereignty to distinguish states from other entities (Choucri 2011: 21). This hierarchical view of the international system will continue to be studied, but international relations scholars will also want to understand how political networks integrate with states (Sikkink 2009: 245).

Transition

It is important to remember that the concept of networks is a model imposed on physical and social phenomenon. They can be applied to anything, including states, but this application does not mean that the world has become more networked, nor does it herald the creation of a new kind of society (Mueller 2010: 32). However, among cyber utopians there is considerable discussion of ICT networks inspiring the creation of a more "networked world." In the next section, the cyber utopian perspective will be examined.

Cyber Utopians Background

In general, the cyber utopian perspective tends to emphasize the positive role ICT networks play in encouraging information sharing, collaboration, economic development, and democratization. In the context of this analysis cyber utopians are individuals who argue that networked technologies have the power to erode state authority. However, in reality the cyber utopian perspective is quite varied, and even individuals who endorse the power of ICT networks recognize that they also have flaws and limitations. The cyber utopian perspective has its roots in traditional international relations theory. Those who follow it often argue that technology has played a role in challenging states for decades, and provide historical examples. There are several main arguments of the cyber utopians. As discussed in the previous chapter, they often focus on how ICT networks inherently resist state control due to their decentralized nature. They also emphasize how these technologies are changing the amount of information citizens can access, and the way citizens access it. Last, they emphasize how these ICT networks facilitate communication and coordination, with a specific focus on the impact of social media sites. This section will explore the arguments commonly considered part of the cyber utopian perspective, and explain some of the views of academics and researchers who subscribe to it.

International Relations Foundation

The cyber utopian perspective seems to stem from the liberal interdependence definition of sovereignty. Many cyber utopians argue that state authority is being eroded because ICT networks make it difficult for states to control information and the online coordination of their citizens. International relations theorist Janice E. Thomson explains: “For liberal interdependence theorists sovereignty is defined in terms of the state's ability to control actors and activities within and across its borders” (Thomson 1995: 213). The cyber utopian perspective focuses on how networks are reducing the centralized points where states could exert control. Network theorist Milton Mueller explains five different ways that the Internet puts pressure on the nation-state: (1) it globalizes the scope of communication, and makes attempts at jurisdictional overlay (i.e. creating borders on the Internet) more costly; (2) it facilitates a huge increase in the scale of communication which can overwhelm the capacity of government processes to respond; (3) it distributes control as decisions about Internet protocols are not aligned with any political units; (4) it creates new non-state institutions, such as ICANN or the IETF, that have authority over the internet; (5) it changes the polity by reducing the cost of group action (Mueller 2010: 4). These different functions challenge state control over their citizens’ actions.

The former U.S. State Department Director of Policy Planning, Anne-Marie Slaughter, argues that in the twentieth-century the world fit the billiard-ball model, with self-contained states colliding with one another, but that “the emerging networked world of the twenty-first century, however, exists above the state, below the state, and through the state” (Slaughter 2009). Recently, constructivist and liberal theories of international relations – which emphasize the role of non-state actors and stress cooperation – have been challenging structural realism – which emphasizes that states seek power in an anarchic international system by leveraging their capabilities (Maoz 2011: 15). In a network system, the neorealist view of international structure as a distribution of capabilities is inverted, and power is defined by persistent relationships (Kahler 2009: 12).

Like liberal theorists many cyber utopians argue that national governments are being forced to share their power with citizen groups including the political, social, and security roles that define sovereignty (Mathews 1997). In the traditional Westphalian system of international politics, there are territorially fixed states with a single, secular authority, and no authority above them (Mathews 1997). Cyber utopians argue that this system of state power is dissolving, “states will remain the dominant actor on the world stage, but they will find the stage far more crowded and difficult to control” (Nye 2011: 113).

What distinguishes cyber utopians from liberal theorists is the emphasis on technological developments as being the key driving force in this change. Liberals believe that conflict is rooted in misperception, and consequently, increased communication has a pacifying effect because it reduces ambiguity and encourages international interdependence (Steele and Stein 2002: 26). According to political scientist Juliann Emmons Allison, there is a rich body of literature on international cooperation that suggests that ICT is likely to facilitate more pacific international relations by: “(1) increasing the amount of contact among individuals and nations; (2) improving the quality of interpersonal and diplomatic communication; (3) extending economic interdependence and (4) deepening the democratic processes that permit the pacific inclinations of individual citizens to influence their nations' strategic decisions” (Allison 2002: 6).

In the cyber utopian perspective the contemporary information revolution has resulted in increased communications across boundaries, and improved interdependence (Keohane and Nye 1998: 83). Cyber utopians emphasize that the telecommunications revolution has broken government control over information collection and management, and that this has led to an increase in the number of players who matter (Mathews 1997). Furthermore, they often focus on how information technologies encourage the reciprocal communication on which democracy thrives (Kedzie and Aragon 2002: 123). Researchers Christopher Kedzie and Janni Aragon investigated the situations in which political coordination caused states to limit access to ICT networks, and simultaneously found that: “In all cases, the results indicate that 'electronic network connectivity' is a significant predictor of 'democracy'” (Kedzie and Aragon 2002: 110). Utopians argue that democratic states must recognize that their citizens’ use of technology can promote their values – such as freedom, equality, and human rights – without their involvement (Schmidt and Cohen 2010).

Cyber utopians argue that governments must adopt new tactics in order to further their national interests, and make decisions that account for the rise in citizen power and the changing nature of the state (Schmidt and Cohen 2010). Political scientist Joseph Nye writes that "Two great power shifts are occurring in this century: a power transition among states and a power diffusion away from all states to non-state actors" (Nye 2011: xv). He argues that the information revolution reduced the costs of computing and communication, and the communication technologies that were once the purview of governments and corporations are now available to everyone (Nye 2011: xvi). His mentee, Anne-Marie Slaughter has coined the term “collaborative power” to describe the power conferred to groups of individuals who coordinate with each other in order to reach common goals (Slaughter 2011). In the cyber utopian perspective, power is no longer monopolized by states, and ICT networks have allowed for citizens to have an impact.

History

The introduction of the Internet, the mobile phone, and the current wave of information communication technologies into the realm of international relations has inspired cyber utopians to herald a transformation of world politics. This is not the first time that a new technology has invoked such a response. In America in 1910 Norman Angell argued that economic interdependence would render war irrational, and in the 1970s modernists believed that multinational corporations and international organizations were eroding the territorial state with the help of telecommunications and jet travel (Keohane and Nye 1998: 81). Throughout history utopians have pointed out the moments when technology has had a particularly clear impact, and even now the cyber utopians rely on these examples to bolster their arguments that communications technology can directly impact a state's authority.

One example often cited by cyber utopians is the Iranian revolution of 1979. Many historians believe that audiocassettes recorded by Ayatollah Ruhollah Kohmeini, the religious figure exiled by the authoritarian regime, were used to incite others to join in rebellion (Tehranian 1997). Ayatollah Khomeini was able to distribute these tapes of his speeches to more than 9,000 mosques (Schmidt and Cohen 2010). Clay Shirky, a cyber utopian writer, argues that communications during the Cold War did not cause governments to collapse, but did help citizens take power from the state when it was already weak (Shirky 2011). He says that the state's ability to use violence was weakened, and that civil society had grown stronger, resulting in a shift in the balance of power Shirky 2011). He also compares the contemporary significance for media's political impact to the historical role of the printing press, describing how it supported social change by strengthening the public sphere (Shirky 2011). Cyber utopians argue that the pursuit of science and technology compels open societies, because even more so than the fax machines that infiltrated Soviet universities, satellite footprints do not respect national borders, and telephone wires penetrate even repressive societies (Barber 1992).

The Internet required the software and protocols of the World Wide Web to become revolutionary, because they enabled general browsing and hyperlinking (Goldsmith and Wu 2006: 52). According to ICT scholar Jonathan Zittrain, "the crucial element of the PC's success is not that it has a cheap processor inside, but that it is generative: it is open to reprogramming and thus repurposing by anyone." (Zittrain 2008: 19) The cyber utopians of the 1990s argued that the freedom of the Internet was engineered into its protocols, and that technology could solve the problems of politics through consensus or freedom of association without the need for a formal authority (Mueller 2010: 2). The structure of the Internet allows individuals to have a greater voice than in the case of traditional media because there are avenues of discourse around the bottlenecks of older media, whether they are controlled by governments or media owners (Benkler 2006: 271). The reduced costs of communication allow for an effectively infinite transmission of information, and increase interdependence among societies (Keohane and Nye 1998: 83).

Basic Arguments

In the cyber utopian perspective access to the Internet is not simply a privilege, but a human right. Researcher Ethan argues "[t]he internet is the most efficient system we've ever built to allow people to seek, receive and impart information and ideas, and therefore we need to ensure everyone has unfettered internet access." (Zuckerman 2010) In his view a great deal of the work on Internet censorship is motivated by the conviction that everyone should be allowed to freely share and consume information. At the U.S. State Department, Secretary of State Hillary Rodham Clinton has fully embraced the Internet freedom cause. She sees the access to the Internet as an exercise of free speech and civil liberties in networked society (Sinnreich, Graham and Trammell 2011: 4). U.S. SD Senior Advisor for Innovation Alec Ross, argues that: "Networks are a defining feature in the new global power structure. The very clear evidence of recent years demonstrates that network technologies devolve power away from the nation-state and large institutions. Some cyber utopians argue that globalization has led to a special emphasis on networks across countries, and that it has led to a decline in the significance and sovereignty of the nation-state." (Webster 2002: 82) This emphasis on networks becoming the dominant international structure is a large component of the cyber utopian perspective.

Networks

The former U.S. State Department Director of Policy Planning, Anne-Marie Slaughter argues that we live in a "networked world," and describes the power of terrorist groups as being an example of how small, mobile networks of people can challenge even powerful militaries (Slaughter 2009). Other utopians argue that new technology is challenging traditional power structures by allowing millions of citizens to coordinate political action quickly and without conventional leadership (Apps 2011). Furthermore, because ICT networks like the Internet have no formal center, they are not as easy to control at a single-point like the mass media, and restrictive governments face higher costs if they attempt to do so (Benkler 2006: 271). Cyber utopians argue that the decentralization implied by communications means that it is more difficult for states to exercise central control and lie about their actions, and that this is resulting in the redefinition of the relationship between citizens and their rulers (Steele and Stein 2002: 35). Global communications like Direct Broadcast Satellite (DBS) ignore national borders and inherently undermine the traditional boundaries and sovereignty of nations by broadcasting foreign programming without impunity (Tehranian 1997). Some cyber utopians argue that because governments are hierarchical, with centralized leadership and decision-making, they are simply incompatible with all the possibilities that new technologies create (Mathews 1997). Others add that hierarchical systems can suffer crucial blows if the centralized authority makes mistakes or is removed from power, while networks have greater resilience and redundancy and are more difficult to shutdown or break (A. R. "Can You Social Network Your Way to Revolution?" 2010).

Contemporary cyber utopians focus on how governments have begun to adapt to the challenges posed by networks. Anne Marie Slaughter argues that, in general, governments are moving toward a more networked structure. She remarks that a report from the Center for Strategic and International Studies in 2007 called for U.S. diplomats to be decentralized, connected, and based in multiple locations, as in a network (Slaughter 2009). Additionally, network theorist Milton Mueller argues that there is evidence that challenges of Internet governance are changing nation-state politics in the domain of communication and information policy, as different governments must find ways to interact with networked organizations like the IETF and ICANN (Mueller 2010: 7). He also argues that there are four ways in which these Internet-based network organizations might lead to institutional change: (1) by formalizing and institutionalizing the network relations themselves; (2) by states' attempts to impose hierarchical regulation upon networked forms; (3) by states' utilization and adoption of networked forms; (4) by changing the polity; namely, by realigning and expanding the associative clusters around governance institutions (Mueller 2010: 46).

As these processes continue to shape how states interact with the Internet and other ICT networks, they may come to operate in a more networked fashion. As political scientist Jessica Mathews expresses it: “The question now is whether there are new geographic or functional entities that might grow up alongside the state, taking over some of its powers and emotional resonance.” (Mathews 1997) As is evident from this section, the cyber utopian perspective would argue that new organizations are in the process of using ICT networks to challenge state authority.

Information

The cyber utopians often emphasize how ICT networks are changing the ways citizens consume information, and allowing them to produce information on their own. In their view, networked relations are a new mode of peer-to-peer production, in which everyone is a producer of content as well as a consumer (Mueller 2010: 35). One argument is that the Internet functions as a digital printing press, allowing any motivated citizen to express his views to a potential audience of millions, and thereby broadening the public sphere (Hindman 2008: 268). A writer for the *Economist* explains: “On social networks, anyone and everyone becomes a producer of content, and this function is taken away from central actors susceptible to control by the powerful. Where social networks penetrate, governments cannot control the story” (A. R. "Can You Social Network Your Way to Revolution?" 2010). He even goes as far as to argue that in a world in which information cannot be controlled, government abuses of power may become more costly, and therefore only occur on rare occasions. The view that social networking sites could eventually make protests unnecessary falls to an extreme end of the cyber utopian spectrum (A. R. "Can You Social Network Your Way to Revolution?" 2010).

In the cyber utopian perspective the government is losing its control over the information its citizens can access, and this empowers citizens to coordinate with each other outside of the view of their government. In democratic societies the media allows for many voices of society to be heard, and these voices constitute public opinion and are integrated into the government’s operations (Tehranian 1997). However, in their research of the American mass media Elihu Katz and Paul Lazarsfeld found that there is a two-step process where information is transmitted by the media, and is then echoed by friends, family members. This theory is still valid in contemporary society as politically active individuals can spread their viewpoint to apolitical associates through social media. For many individuals who are not interested in politics, it is through the second social step that their political opinions are formed, and this is where the Internet and social media can have an impact as friends and associates can debate their views online, publicly and privately (Slaughter 2009).

In a *Forbes* article, Erik Kain describes his belief that social media such as Twitter help to create “mutual knowledge” where isolated individual knowledge can be shared, and grassroots activists can redistribute the control of information and level the informational playing field (Kain 2011). Similarly, Internet researcher Zeynep Tufecki argues that during times of strong upheaval, the ability to know that others know what one knows can create a cycle of further dissent and upheaval. She explains that governments try to control information in order to prevent the majority of ordinary people from facing cognitive dissonance between their compliance with the regime, and having issues (Tufecki 2011). In these cases citizen journalism is powerful, because people with cell phone cameras can increase shared knowledge, and inspire others to decry the regime (Tufecki 2011).

Cyber utopians often herald the rise of citizen journalism as facilitating the exchange of information in opposition to repressive governments. They stress how more than 50 percent of the world's population has access to either cell phones (five billion users) or the Internet (2 billion), or both, and that citizens can use these technologies to form virtual communities, empower themselves, and challenge government authority (Schmidt and Cohen 2010). In the utopian perspective, the media will become a collaborative enterprise between traditional news organizations and citizen journalists (Schmidt and Cohen 2010). Journalist Erik Kain argues that outside intervention is not possible in every case of authoritarian brutality, and that citizens must do it themselves. In his view technology is partly responsible for the revolutions in Libya, Yemen, and Bahrain, and for the fragility that followed (Kain 2011). Furthermore, he points out that the fact that foreigners have access to reports from Yemen and Libya on Twitter is astounding, and that this sudden, widespread profusion of information challenges governments' control over regime secrets (Kain 2011). However, Anne-Marie Slaughter emphasizes that it is not just the increased access to public information that is valuable, but the increased ability for citizens to communicate privately among themselves. She highlights how the focus of information access, particularly by users in the West, underestimates the value of how tools like cell phones enable local coordination (Slaughter 2009).

Coordination

Cyber utopians argue that increased communication facilitates coordination because people are able to learn if other people share the same concerns as them, and are willing to act. Communication shapes political and social behavior because it alleviates the uncertainty that often surrounds decision making (Kedzie and Aragon 2002: 107). If people can use ICT to contact each other and learn of their shared thoughts and motivations, they might choose to collaborate in order to bring about mutual goals. The infrastructure of the Internet and other ICT can also change patterns of participation. For example, email appeals, text messages, or comments on Facebook could each appeal to a different set of citizens (Hindman 2009: 16). While some cyber skeptics have decried Facebook or other social networks being used as a tool for political coordination, they have the possibility of reaching citizens that might not otherwise be informed. Furthermore, while social networks often rely on weak ties, these ties can be incredibly important in merging densely connected social circles, and integrating separate groups in society (Granovetter 1983: 220). Cyber utopians argue that social networks, social media, and the Internet in general, can form a new public sphere, or counter-public, that is difficult for the state to control (Tufecki 2011).

Cyber utopians often emphasize how ICT has empowered citizens and encouraged greater collaboration among non-state actors. They discuss how non-governmental organizations (NGOs) can use these technologies – such as PCs, faxes, and the Internet – in order to share information across national boundaries and form a global civil society (Kahler 2000: 156). Citizens can create petitions through Internet applications such as Facebook, and this can help build movements just as in the real world (Hilder 2011). The site Avaaz.org is an example of this type of web-based movement. Since its launch in 2007, it has grown to over 7 million members world wide, who are dedicated to issues such as building democratic movements and civilian reconstruction (Hilder 2011). The Ushahidi crisis mapping platform is another networked organization that works across borders in order to provide information during times of crisis. However, there is a wide variety of transnational groups and a significant portion of them are dedicated to economic rather than humanitarian pursuits. Transnational corporations (TNCs) use ICT networks to coordinate channels of production and distribution, as well as the activities of their employees. Individuals who support economic globalization argue that government power has been undermined by economic actors that can threaten to take their profits elsewhere. The power of firms to exit a domestic economic network poses a challenge to state hierarchical control (Kahler 2000: 158). The cyber utopians argue that a new global civil society has emerged in the form of NGOs, TNCs, transnational media corporations, and intergovernmental organizations (IGOs), and other groups that exist side-by-side with traditional states (Tehranian 1997).

Cyber utopians tend to focus on the role that ICT networks play in challenging government authority. The next section will focus on the cyber skeptic perspective.

Cyber Skeptics Background

In general, the cyber skeptic perspective tends to emphasize the negative role ICT networks play in facilitating censorship, surveillance, propaganda distribution, and attacks on other states. Additionally, cyber skeptics are generally dedicated to disproving the arguments of cyber utopians, which they regard as idealistic or historically ignorant. In the context of this analysis cyber skeptics are individuals who argue that networked technologies do not have the power to erode state sovereignty, and often they even allow for states to reassert their authority. However, in reality the cyber skeptic perspective is quite varied, and even individuals who believe that ICT networks just are another tool for state control recognize that they can be used by citizens for political purposes. The cyber skeptic perspective has its roots in traditional international relations theory. Those who follow it often argue that throughout history there have been many cases of idealists heralding a new world order as a result of a recent technological development. There are several main arguments of the cyber skeptics. They focus on how ICT networks are still bound by international boundaries and the laws of the governments they operate within. They also emphasize how these networks can be controlled and censored by governments, or even used to spread government propaganda. Furthermore, they refute cyber utopian claims that ICT networks can be used to coordinate successful citizen movements. Last, they emphasize how states can even organize attacks on other states by encouraging patriotic citizens to launch cyber attacks on ICT networks. This section will explore the arguments commonly considered part of the cyber skeptic perspective, and explain some of the views of academics and researchers who subscribe to it. It will also refute cyber utopian arguments as this composes a significant part of the cyber skeptic perspective.

International Relations Foundation

The cyber skeptic position seems to stem from the realist definition of sovereignty. Many cyber skeptics argue that state sovereignty remains uncontested because ICT networks do not prevent states from censoring information or using force to prevent the assembly of their citizens. International relations theorist Janice E. Thomson explains: For realists, the essence of sovereignty is the state's ability to make authoritative decisions – in the final instance, the decision to make war (Thomson 1995: 213). Realists stress that although individual states have often faced challenges to their control over their citizens, the state paradigm itself has remained constant. They argue that institutions of communication and information are not having an effect on state dominance, and minimize the influence of non-state actors (Mueller 2010: 3). Furthermore, they believe that the Internet should be bordered, and that territorial governments are required to provide the public goods the Internet relies on (Mueller 2010: 3). Political scientist Joseph Nye remarks that while some information protocols of the Internet can be considered public goods, the infrastructure of the Internet is a scarce proprietary resource located within the boundaries of sovereign states (Nye 2011: 143). Cyber skeptics generally believe that the dominant role of states is guaranteed, but there are also some who question whether this will change going forward (Schmidt and Cohen 2010).

Cyber skeptics take issue with the cyber utopian arguments against their viewpoint. Evgeny Morozov is a renowned cyber skeptic (or self-described cyber realist) who often counters utopian claims about the Internet and other ICT with examples where technology has been used to bolster governments' authority and even harmed unknowing citizens seeking the freedom of cyberspace. Morozov argues that because cyber utopians cannot bury cyber realism, they have reduced its validity by equating it with the view that the Internet does not matter (Morozov 2011). On the contrary many cyber skeptics believe that the Internet and other ICT have had a significant impact, but one that is not purely beneficial to citizens or those who strive for the freedom of information and communication. The technologies that facilitate communication can be used to help rulers keep tabs on their citizens and build support by controlling what version of events citizens see (Steele and Stein 2002: 26). Some cyber utopians even argue that this improved control is beneficial because it improves stability and decreases the possibility of conflict spilling over to other states (Steele and Stein 2002: 26). With regard to the principle of ICT access as a human right and a freedom of speech issue, cyber skeptics argue that these first amendment type arguments do not reflect universal values, and they are not written into the Internet's architecture (Goldsmith and Wu 157). Cyber skeptics argue that cyber utopianism fails to recognize that the Internet penetrates all of political life, and not just the areas that are conducive to democratization (MacKinnon 2012: 191).

Network theorist Miles Kahler argues that "One does not need to predict an inevitable backlash against globalization or international openness to suggest that those who are threatened by contemporary economic and political trends may use the same technological tools to achieve different goals" (Kahler 2000: 162). Essentially, cyber skeptics are not arguing that ICT networks are irrelevant, and many even accept that in certain cases they are outside of state control. However, they argue that new technologies can be used for multiple political programs, and that they can be as effective a tool for states as they are for citizens. Kahler highlights how in any wave of technological innovation initial predictions adopt the metaphor of a tidal wave, but that in reality traditional institutions tend to adapt to these shifts rather than be swept away by them (Kahler 2000: 161). Some institutions will adapt quickly, while others may adapt over time, but they will not be washed away. The moderate cyber skeptic perspective tends to follow Kahler's argument that "Governments have not been rendered ineffectual or obsolete by economic integration and technological innovation, but their practices will change, and the relative importance of their functions will also shift" (Kahler 2000: 161).

History

Cyber skeptics often focus on how previous technological revolutions were met with the same idealistic zeal that characterizes the contemporary cyber utopian perspective. Evgeny Morozov writes that historians must have been very amused in 1996 when an article in *Wired* magazine described the Internet as replacing the public square and allowing average citizens to have the ability to participate in national discourse. He explains that from the railways, to the telegraph, to the television, and then to modern ICT, there has hardly appeared a technology that was not praised for its ability to raise the level of public debate, introduce more transparency, reduce nationalism, and create the mythic global village. Time and again, the same arguments have been made concerning technology's potentially revolutionary impact on government. However, in each case these technologies were subjugated by traditional forces (Morozov 2011: 275).

Cyber utopians often describe the introduction of ICT networks as being akin to the Gutenberg printing press in its potentially revolutionary impact. While the printing press was revolutionary, it was also an incredibly centralized medium. Repressive governments had the ability to use the printing press as a tool for control – through the distribution of propaganda – and oppression – through outlawing the publishing of dissident views (Schmidt and Cohen 2010). In its early days, the telegraph was considered by some to be a cord that would bind together all the nations of the earth, and serve as an instrument of exchange throughout the world (Morozov 2011: 276). Similarly, radio technology can allows users to both broadcast and receive content, but the majority of individuals only received the information broadcasted from a central point of production (Press and Williams 2010: 34) . Furthermore, Morozov argues that while many of the late 20th century revolutions in Europe were considered "telerevolutions," the television aspect seems to be a minor point (Morozov 2011). He notes that while communications play a role in uprisings, the individuals involved may not have the clearest view on their significance (Morozov 2011). New technologies may have the potential to affect social relations in one way or another, but cyber skeptics argue that the nature of the potential that is fully realized depends on the specific political and economic systems in which they are employed (Press and Williams 2010: 34).

Technology that is expected to have one particular impact can also gain significance in ways that their proponents did not anticipate. Morozov argues that: "Technologies that were supposed to empower the individual strengthened the dominance of giant corporations, while technologies that were supposed to boost democratic participation produced a population of couch potatoes" (Morozov 2011: 275). However, Morozov also recognizes that it is dangerous to assume that there are no technologies that will have a political outcome in particular social environments. The idea that "technology is neutral" is misleading, because it depends on how it is used (Morozov 2011: 295). In the twentieth century there are numerous instances of states successfully utilizing radio or television to create and distribute propaganda (Schmidt and Cohen 2010). In the Rwandan genocide, broadcast media like the radio are thought to have inspired listeners to commit violent actions (Steeves and Kellow 1998: 126). Consequently, when the founders of Twitter declare their site to be a "triumph of humanity," it might be advisable that they first assess the possibility of the Web application being used to incite violence in some future conflict (Morozov 2011: 279). While certain types of Internet and certain applications that run on it do pose political challenges to repressive governments, others reinforce their authority, and some states are even seeking to develop an Internet that serves-state defined interests rather than challenging them (Kalathil and Boas 2003: 3). Cyber skeptics stress that ICT are not inherently a force for good, nor do they automatically challenge state control. ICT are tools and their impact depends on how they are used.

Basic Arguments

Cyber skeptics argue that the international imperative to declare ICT access a human right is misplaced. In a *New York Times* article, Vinton Cerf argues that technology is an enabler of rights, not a right itself. (Cerf 2012). The Internet is often characterized as being political by its very nature, but it is only a set of connections or protocols between computers and other devices, and it can have no impact apart from its use by human beings (Kalathil and Boas 2003: 1). Cyber skeptics argue the focus must be placed on the uses of these technologies, rather than on the technologies themselves. After all, the value of technology changes over time. At one point if you did not own a horse you were at an economic disadvantage, but now it is a luxury good that is far from necessary (Cerf 2012).

Cyber skeptics also question the concept of “Internet freedom” as a policy goal, and ask about how policies should be coordinated around such a generic doctrine (Morozov 2010). At the heart of every debate about the Internet is a debate about free communication, or essentially the freedom of speech, and whether its regulation should be global or local (Goldsmith and Wu 2006: 150). Cyber utopians prefer that information be unfiltered on a global level, and argue that this would have an inherent positive, democratizing effect on the world (Kalathil 2003). However, cyber skeptics highlight that information is not free and never has been, in the sense that the labeling, organizing, and filtering of information is important so that it can be readily consumed (Goldsmith and Wu 2006: 51). On the Internet, information filtering is especially important because the ease with which people can publish content results in an overwhelming amount of information (Goldsmith and Wu 2006: 52). Cyber skeptics argue that the freedom of speech is not bound to any particular technology, and that a certain amount of filtering and organization is necessary for a successful information medium. They see the Internet is valuable as a means to an end, but not as an end itself (Cerf 2012).

Cyber skeptics emphasize that the role of the Internet and other ICT is often not as powerful as cyber utopians argue. The flaw with cyber utopian arguments is that they obscure the ways in which technology might produce a political outcome, and do not specify the mechanisms by which the downfall of a regime may occur (Kalathil and Boas 2003). Furthermore, they rely heavily on anecdotal evidence, and do not provide the full context. Cyber skeptics point out that cyber utopians assume that the Internet is static, and that its control-frustrating characteristics – namely its networked structure – are maintained as it is adopted in different countries (Kalathil and Boas 2003: 2).

In the cyber skeptic perspective, it is important to recognize the revolutionary potential of the social relations fostered by Internet and digital media, but at the same time be realistic about the forces that shape and constrain the impact of these technologies (Mueller 2010: 5). Cyber skeptics tend to point out statistics that demonstrate the limited usage of the Internet in an effort to provide a more realistic assessment of the proliferation of these technologies. Internet, mobile, and general ICT penetration is rapidly increasing, but the majority of individuals use these technologies for private, apolitical functions. Furthermore, access is still far from universal. The world has 7 billion people, and an estimated third are using the Internet. Still, in 2006 developing countries composed 44% of the world's total number of Internet users, and in 2011 that number had increased to 62% (Kokolis 2012). Cyber skeptics focus on finding realistic estimates of ICT use, and examining the impact of these technologies in an appropriate context.

Hierarchy

Cyber skeptics refute utopian claims that the Internet and other ICT lack hierarchy, and that the networked organizations that govern them are an inherent challenge to states through their very structure. Network theorist Miles Kahler highlights the revolutionary rhetoric that has surrounded the Internet or other innovations in ICT, and explains that these arguments describe a new world in which traditional forms of organization based on hierarchy and boundaries will be transformed (Kahler 2000: 161). He notes that the cyber utopians assume normative affinity or that the social and political consequences of a technology will represent the nature of that technology. This belief implies that technologies that are decentralized and horizontal in their application and easily extend beyond borders will favor organizations of a similar character (Kahler 2000: 150). Based on this argument, because the state is hierarchical and territorially delimited, innovations are believed to undermine the authority of the state, and to be difficult for the state to utilize for their own purposes (Kahler 2000: 150).

However, cyber skeptics assert that hierarchy is not absent from ICT networks, and are not as egalitarian as the utopians imply. The technical and regulatory foundations of the Internet are hierarchical, as they are controlled by centralized organizations like ICANN and oligopolistic owners of network access such as companies like AT&T (Sinnreich, Graham and Trammell 2011: 2). Additionally, Kahler argues that resources and technologies flow from the industrialized countries to the developing countries, and that "with that asymmetry comes agenda control, the ability to frame or edit information that enters the network, and the selection of acceptable interlocuters in the developing world (Kahler 2000: 159). Furthermore, political scientist Joseph Nye remarks that while some aspects of the Information Revolution help the small; some help the already large and powerful (Nye 2011: 117). The information revolution is leading to a diffusion of power, but larger states still have larger resources (Nye 2011: 118). Cyber skeptics argue that networked technologies are still contained within states, and that hierarchical organizations can use these technologies as well as those that are networked.

Cyber skeptics emphasize that borders are still relevant in shaping the Internet and other ICT networks. They argue that cyber utopians overlook how much cyberspace overlaps and rests on the traditional world in which power is still determined by geographically based institutions (Keohane and Nye 1998: 82). While cyber utopians see the Internet as a borderless medium that does not rely on geography, cyber skeptics recognize that national borders reflect real and important differences among peoples in different places, and this is translated into cyberspace (Goldsmith and Wu 2006: 49). Certain Internet services rely on geographical distinctions between users. For instance, a local flower delivery service may have a website that can take orders, but they are still bound to the area in which they operate (Goldsmith and Wu 2006: 59). Furthermore, the efficacy of Internet communications depends on the physical location of the underlying hardware through which data travels, such as routers, exchange points, fiber-optic cables, phone lines, cable lines, satellites, and microwave transmitters (Goldsmith and Wu 2006: 54). This infrastructure is built through the efforts of private companies responding to consumer demand, and so often it is concentrated in dense wealthy population centers, and this reinforces connections between centers of power and influence (Goldsmith and Wu 2006: 56). Cyber skeptics argue that if economic and political power are concentrated in certain geographical regions, this will be reflected in ICT networks.

Cyber skeptics state that governments have strengthened borders on the Internet by employing powerful ‘top-down’ techniques to control the Internet (Goldsmith and Wu 2006: 49). The Internet links national networks, but there are still distinctions based on language, politically motivated technological barriers (i.e. firewalls), and the legal systems that shape regional Internet content (Goldsmith and Wu 2006: 149). Legal scholar Lawrence Lessig argues that governments can regulate the Internet by controlling its underlying code, and shaping the legal environment in which it operates (Kalathil and

Boas 2003: 3). There are those who argue that while borders may result from the conflict in laws, a bordered Internet is valuable because it allows different value systems to coexist on the same planet (Goldsmith and Wu 2006: 152).

Control

Cyber skeptics argue that states can use ICT networks to limit the information their citizens can access and even use them to influence their own citizens as well as foreign publics. In the cyber utopian perspective, states will need to refrain from exerting too much control over information if they want to benefit from the positive socioeconomic developments these technologies generate. However, cyber skeptics argue that states can effectively filter information on the Internet and other ICT networks while still reaping the rewards of technological innovation. At the heart of this debate is a concept known as the "dictator's dilemma." In 1985, Former U.S. Secretary of State George Shultz wrote that:

> "Totalitarian societies face a dilemma: either they try to stifle these [information and communication] technologies and thereby fall further behind in the new industrial revolution, or else they permit these technologies and see their totalitarian control inevitably eroded. In fact, they do not have a choice, because they will never be able entirely to block the tide of technological advance" (Kedzie and Aragon 2002: 105).

Poltical scientist Christopher Kedzie expands that this dilemma has raised the opportunity costs of censorship, "forcing despots to revisit their structure of preferences, make new choices, and expose themselves to the unintended consequences" (Kedzie and Aragon 2002: 106). In essence, if dictators allow ICT to spread within the country it poses a threat to the regime, but if they do not, they are cut off from the rest of the world (Tufecki 2011).

The dictator's dilemma is not limited only to governments, however. Clay Shirky argues that the phrase “the conservative dilemma,” coined by media theorist Briggs, is more appropriate because it applies to leaders of democratic governments as well as leaders in business and religion (Shirky 2011). In his view the dilemma is created by new media that increase public access to speech or assembly and force states to account for differences between their view of events and the public’s (Shirky 2011). States that are bent on maintaining their monopoly on information use many tactics to interfere with ICT networks such as: online, shutting down political websites or portals; offline, by arresting journalists, bloggers, activists, and citizens; by proxy, through controlling Internet service providers, forcing companies to shut down specific websites or denying access to disagreeable content; and, in the most extreme cases, shutting down access to entire online and mobile networks (Howard, Agarwal, and Hussain 2011). While both democracies and authoritarian regimes participate in network interventions and control information, authoritarian regimes conduct shutdowns with greater frequency (Howard, Agarwal, and Hussain 2011).

Cyber utopians argue that because of the conservative’s dilemma states will refrain from shutting down ICT networks in order to avoid the negative economic and social consequences. Additionally, if a government were to shutdown Internet access or ban cell phones, it would risk radicalizing otherwise pro-regime citizens (Shirky 2011). However, the cyber utopians argue that governments are willing to bear the consequences of an Internet shutdown if it is politically necessary, which is supported by the Egyptian Internet shutdown enforced by the Hosni Mubarak regime during the protests in 2011 (Shirky 2011). Still, the Egyptian protests continued despite the shutdown and this provides an interesting case study that will be examined in a later section.

Cyber skeptics argue that states have other effective means of controlling information on ICT networks. Clay Shirky describes how two responses to the conservative dilemma are censorship and propaganda. Additionally, he argues that the more effective source of control is enforcing the silence of citizens, through physical or psychological coercion (Shirky 2011). Shirky cites Ethan Zuckerman's "cute cat theory of digital activism" which emphasizes how governments will avoid shutting down tools such as social networking sites that appeal to a large apolitical population seeking innocent content (e.g. cat photographs) even as they target those specifically designed to defeat state censorship (e.g. proxy servers) (Shirky 2011).

Cyber utopians stress that governments do not set up or operate international ICT networks, and that they have limited influence over those groups that do. However, cyber skeptics emphasize that while private companies provide the infrastructure of ICT networks, control access to that infrastructure, and operate the applications run on those networks, governments can exert their authority by influencing these intermediaries (Sinnreich, Graham and Trammell 2011: 5). When capital and information is consolidated within a set of centralized corporate severs, this moves control away from local computers and disempowers users (Sinnreich, Graham and Trammell 2011: 7). Governments can then control local Internet intermediaries in order to prevent offshore Internet harms (Goldsmith and Wu 2006: 156). Additionally, ICT providers and Internet-based companies are profit-driven corporations and at times their economic interests outweigh the supposed moral imperative to resist state control.

The social networking site Facebook has been praised by cyber utopians for providing a platform for political mobilization in Tunisia and Egypt. However, Journalist

Jillian York describes how Facebook is often under scrutiny for its privacy and free expression policies, and unlike Google and Twitter, it avoids being considered a political tool (York 2011). While users may treat Facebook as a public space it is a private enterprise that mines data on its users and prioritizes profit (York 2011). Even companies like Google that do embrace their political nature find themselves forced to choose between becoming a tool of repressive states in the pursuit of profit, or forgoing an entire market to avoid compromising their neutrality. Internet service providers have even used their control over networks to block communication for ideological reasons, such as when AT&T censored speech critical of President George Bush during a live webcast (Marra 2007 as cited in Sinnreich, Graham and Trammell 2011: 6). Cyber skeptics argue that it is important to more critically examine the role of companies like Facebook and Twitter in promoting freedom movements, and also to confront how companies were encouraged by Western governments to create the tools of censorship used around the world (Morozov 2011).

Cyber skeptics argue that technology can be used to censor and control information just as it can be used to distribute it. They stress how repressive regimes have purchased information filtration technologies that were created by private firms for Western corporations, law enforcement officials, and intelligence agencies (Morozov 2011). Many cyber utopians tend to overlook the complicity of western firms. The U.S. State Department places a heavy emphasis on Internet freedom, and yet they granted Cisco, a company that provides parts for China's Great Firewall, an award in recognition of its "good corporate citizenship" (Morozov 2011). Since Western governments make use of these monitoring technologies, they will keep being produced and then sold overseas to repressive governments. (Morozov 2011)

In the cyber utopian perspective the conservative's dilemma makes it difficult for states to develop precise censorship mechanisms that could block political activity and permit economic activity. Additionally, while the corporate intermediaries that provide access to the Internet or software applications can block information at a state's request, this power is diminishing as because not even governments can stop, control, or spy on all sources of information all the time (Schmidt and Cohen 2010). However, cyber skeptics argue that this has been proven false as governments such as China have mastered the art of keyword based filtering allowing them to censor sites based on URLs and even text within pages (Morozov 2011: 96). The censorship of information can be carried out by technological components (i.e. routers) of networks as data is being transported. As journalist Benjamin Barber writes: These technologies lend themselves "to surveillance as well as liberty, to new forms of manipulation and covert control as well as new kinds of participation, to skewed, unjust market outcomes as well as greater productivity" (Barber 1992).

Influence

Cyber skeptics emphasize that states can use ICT networks to directly distribute or encourage the spread of information that favors their perspective. Some skeptics may concede that the Internet and similar technologies can empower dissidents and pro-democracy activists, but they argue that this is balanced or even outweighed by the ability for states to use these technologies to control their populations (Morozov 2011). Evgeny Morozov remarks that China's censorship system is commonly called a "Great Firewall" but highlights the fact that “All walls, being the creation of engineers, can be breached with the right tools. But modern authoritarian governments control the web in ways more sophisticated than guard towers” (Morozov 2011). Some repressive governments have begun to actively deploy regime friendly bloggers to spread talking points on the Internet (Morozov 2011). They also use data on social networking sites in order to accurately target which individuals should have limited access, and which should be allowed to browse freely (Morozov 2011). In this way, repressive regimes like China can minimize censorship and reap the economic benefits of ICT networks.

Cyber utopians note how states can also use social networking sites, social media sites, and the Internet generally to engage in diplomacy with foreign publics. Global communication seems to have generated three new types of diplomacy: public, citizen, and virtual diplomacy. Public diplomacy is when governments appeal directly to the citizens of other countries, while citizen diplomacy is when ordinary citizens represent their country in their interactions abroad. Virtual diplomacy describes fully leveraging technology in these various diplomatic efforts such as using video conferencing (Tehranian 1997). The U.S. State Department has launched a 21st Century Statecraft initiative dedicated to fully employing new technologies in their interactions with foreign publics. While cyber utopians might view this in a positive light due to the emphasis on Internet freedom, cyber skeptics focus on how it is still a clear example of a state using ICT networks to bolster its self-representation capabilities.

Force

Cyber skeptics stress that new information and communication technologies have been used to expand states' military capabilities. While the cyber utopians stress the use of ICT networks by citizens in opposition to states, governments are capable of using them against their citizens, and against other states. ICT scholars Cherie Steele and Arthur Stein remark on how throughout time communications have been double-edged: they have been used for war and have generated conflict even as they have increased international communications and understanding (Steele and Stein 2002: 31). New technologies have often increased the scale and scope of political and military control, and as states have embarked on imperial conquests they often relied on improved communications technologies, and created the required infrastructure in the lands they conquered (Steele and Stein 2002: 31).

Communications changed the battlefield by increasing the importance of swift, accurate information, and allowed for centralized command because generals could gather information in one place and then give orders to soldiers from afar (Steele and Stein 2002: 31). Network theorist Miles Kahler writes that the current revolution in military affairs (RMA) caused by ICT networks could have deep consequences because they allow for enhanced real-time intelligence capabilities; the addition of information processing to older conceptions of command, control and communications; and advances in the use of force with greater speed and precision, as witnessed in the Gulf War and later military strikes against Iraq (Nye and Owens 1996 as cited in Kahler 2000: 150). The importance of communication to national security has meant that each new communication technology is an arena of rivalry for the world's great powers (Steele and Stein 2002: 31).

Cyber skeptics largely accept that ICT networks have altered states' military capabilities and have impacted international power dynamics, but they do not presume that this will impact the sovereignty of states. Kahler argues that ICT networks challenge state boundaries, and that the traditional hierarchy of force between great powers has been undermined by the spread of these technologies (Kahler 2000: 151). He describes how some people view the low cost of the new technologies as a sign that the international military hierarchy could be revised as weak states gain more power (Kahler 2000: 151). He also emphasizes that information technologies could produce new forms of warfare that will not be waged solely by states, because the deeper integration of ICT networks could result in new vulnerabilities that can be targeted by individuals and groups as well as other states (Kahler 2000: 151). ICT networks are also enabling the networked coordination of violent non-state actors. Al-Qaeda, Mexican drug cartels, the Mafia, and the Taliban are all using technology to recruit individuals, terrify local populations, and threaten democratic institutions (Schmidt and Cohen 2010). Furthermore, there are growing concerns that non-state actors will be able to utilize ICT networks in order to conduct acts of "cyber terrorism" or create havoc through their actions in the digital realm. Cyber utopians tend to focus on the positive coordination that results from ICT networks, but cyber skeptics highlight the negative consequences as both states and non-state actors can use these networks to instigate violence.

Cyber skeptics tend to focus on the role that ICT networks play in sustaining government authority. The next section will discuss how the changing nature of information production and consumption impacts state authority.

Cyber Utopian Evidence

Information

ICT networks have changed the manner in which information is produced, distributed, and consumed. In particular, the Internet has been referred to as an ocean of information, and this seems an apt description given its scale and depth. In the past media outlets served as gatekeepers that helped the public to determine what information was important or newsworthy. These were hierarchical institutions that had set methods for assessing accuracy, and determining which sources could be relied on and which could not. Social media provides users with the ability to access instantaneous, raw accounts of events as they happen, which has changed the way people think about the news. Any individual with a cellphone can take video footage and become an amateur journalist, simply by posting the videos to sites like YouTube. This allows citizens to instantly spread information about government corruption, or the atrocities committed by repressive regimes. Even in democracies, organizations such as WikiLeaks can serve as whistleblowers about government practices. The cyber utopians would argue that now that people have direct access to the information, they do not need intermediaries to choose which voices matter. However, the cyber skeptics assert that there are new gatekeepers that determine which information is relevant: the search engines that allow users to sift through huge amounts of information. The ability for anyone to produce information on the Internet has led to a huge increase that has changed the manner in which people consume information. States often seek to control information flows in order to influence their citizens, and ICT networks challenge this control.

Access

Information proliferation has resulted as part of the ICT networks and now people all over the world can access vast quantities of information. In the past few decades world ICT use has greatly increased. In 2006 the number of Internet users was estimated at 1.151 billion people, and in 2011 that number had increased to 2.421 billion ("Key Global Telecom Indicators for the World Telecommunication Service Sector"). In the case of mobile phones, there has been an increase from 2.747 billion subscriptions in 2006 to 5.981 billion subscriptions in 2011 ("Key Global Telecom Indicators for the World Telecommunication Service Sector"). These shifts have been magnified in developing countries, which increased their share of the world's total number of Internet users from 44% in 2006 to 62% in 2011 (Kokolis 2012). These numbers are even more impressive when one considers that in 1997 "only" 70 million people were connected to the Internet, and only 200 million people owned mobile phones (Zuckerman 2008: 2). The Director of Corporate and Policy Communications at Google, Bob Boorstin, stresses that the growth of mobile phones is perhaps more important because they are cheaper, their capacity to handle data is improving, and according to the World Bank, more than two-thirds of the world's population lives within the range of a mobile phone network (Boorstin 2008).

The Internet and mobile phones are different from broadcast media – like radio and television – or print media like newspapers and magazines – in that they are less expensive to produce, and in that they are inherently participatory (Zuckerman 2008: 2). Users can create content as well as consume it, and as these tools have spread, the pool of people sharing information has expanded both locally and internationally (Zuckerman

2008: 2). Bob Boorstin playfully argues that it is intimidating how people are uploading ten hours of video to YouTube every minute (as of 2008), and questions if this is best human kind has to offer (Boorstin 2008). However, this huge amount of information can lead ICT users to feel “information overload” in which news seekers are overwhelmed in their search for trustworthy news (Nordenson 2008). While journalists used to determine what information was considered relevant, for better and for worse they are not as influential on ICT networks.

Gatekeepers

The flow of information is bound by the infrastructure of recent ICT networks, but it is not bound by gatekeepers in the same way that traditional media has been. In the past there were editors who determined which content should be considered important, or which content users should access. Political scientist Matthew Hindman explains that for many observers, the most important political impact of the Internet is that it removes traditional media gatekeepers (Hindman 2009: 12). The theory of gatekeeping, credited to sociologist Kurt Lewin (1947), argues that social channels often had points at which gatekeepers filtered some items, while others were allowed to pass (Hindman 2009: 12). David White (1950) applied the framework to the media in his study of the criteria by which newspaper editors determine wire stories worthy (Hindman 2009: 12). Traditional journalism has operated on the gatekeeping principle. Journalists served as an intermediary because people could not spend the time to go out and collect information, and then synthesize and integrate it into a clear picture (Hindman 2009: 12).

In the contemporary context, Bruce Williams and Michael Delli Carpini (2000) have argued that new media do not have “gates,” and therefore does not have gatekeepers (Hindman 2009: 12). Now, the Internet and social media sites such as twitter provide information, and the traditional media do not have as much influence. However, Hindman argues that in the modern day, gatekeepers remain an important part of the information landscape of the Internet. He explains that traditional news organizations and broadcast companies still have prominence on the web, but more notably: "Search engines and portal Web sites are an important force, yet a key part of their role is to aggregate thousands of individual gatekeeping decisions made by others" (Hindman 2009: 12). Search engines like Google prioritize information that many people have linked to and accessed. Although they are just expressing the preferences of Internet users, these search engines become gatekeepers because they assist users in navigating the Internet, but are not purely equal in how information is represented. Similarly, social media sites such as Facebook and Twitter have also become gatekeepers. The Internet has changed the identity of gatekeepers and their role, as well as the gatekeeping process itself (Barzilai-Nahon 2005)

Standards

At this time it would appear that broadcast and print journalism is still the major source of news for most of the worlds’ inhabitants. In the United States 41% of individuals say they get most of their news form the Internet, while 66% say they get it from television ("Internet Gains on Television as Public's Main News Source”). However, this is rapidly changing, and in the United States the percentage of people saying that the Internet is their main source of news has risen 17% from 2007. In institutions of traditional journalism, information is gathered, refined, edited, and then presented to the public. The Internet does not have a universal editor, and consequently Internet consumers must learn to be wary and find sources that they can trust (Gillmor 2008: 4). If citizens observe information on the Internet with a critical eye, then they can discern what information to believe, or discredit, but there is the danger of users becoming misinformed from false information found online (Gillmor 2008: 4). However, there are some standards relied on by formal information sources on the Internet, namely Wikipedia. This site is known as the "free encyclopedia" that "anyone can edit" and its platform allows users to easily edit information on the webpage without special software or technical knowledge (Reagle 2010: 162). While the content can be edited by anyone, the organization requires formal citations and footnotes for its entries and submits each article for revision (Cohen 2011). On Wikipedia there is still fact checking and the synthesis of information from formal sources. The site is not completely accurate, but it does have methods in place to assess veracity, and it serves as a model for how standards can be established online. However, many people consume raw information from social media sites such as Twitter, YouTube, or Facebook, on which there is no process of assessing the accuracy of the contributed content.

Social Media

The Internet has enabled billions of citizens to "publish, share, mix, comment and upload media to a more dynamic online environment (Howard 2011). Journalist Alex Howard writes: "That two way communication, enabled by new, highly accessible and scalable Web technologies, is generally called "social media" (Howard 2011). Media

Researchers Andreas Kaplan and Michael Haenlein argue that the era of social media probably started around 20 years ago when Bruce and Susan Abelson founded ‘Open Diary,’ a social networking site that created a community for online diary writers, but this claim has been disputed. A year later, the term ‘weblog’ was first used, and truncated as ‘blog’ when one blogger jokingly transformed the noun ‘weblog’ into the sentence ‘we blog’ (Kaplan and Haenlein 2010: 60). As the availability of high-speed Internet access continued to increase, social networking sites such as MySpace (2003), Facebook (2004), and Twitter (2006) have been created. These social sharing sites have resulted in the coining of the term ‘‘Social Media,’ and contributed to the term’s contemporary prominence (Kaplan and Haenlein 2009: 60). Social media is a new tool through which people can communicate and publish information. In a political context, its use can change patterns of participation. For example, email appeals, text messages, or comments on Facebook could each appeal to a different set of citizens (Hindman 2009: 16). There is much debate between cyber skeptics and cyber utopians about the relevance of these sites in inspiring activism, but their value as a tool for general information sharing and collaboration is widely accepted.

Instantaneous Reporting

On social media sites, information is posted directly by those who are experiencing an event, and others can instantaneously access this content. Everyone can contribute information, just as they can consume it, and everyone has a voice. The President of Arab Alliance of Freedom and Democracy, Wael Nawara, believes that this instantaneous reporting is very powerful: “If an individual thinks of idea, and posts it on

Twitter, it can be instantly seen by thousands of people. If it is good, it can be re-circulated until it reaches many more"(Nawara 24 March 2011). Additionally, social media can help set the agenda for traditional news media because it can gather ideas from many people at once and represent trends, while it would take energy and expense for reporters to physically seek out these people (Miel and Faris 2008: 30).

Instantaneous reporting largely provides shallow information without significant context, and this can impact how users understand the unfolding of events. Journalists are often responsible for fully investigating a subject, processing the information, and representing it accurately. Still, technological advances have also made it such that they must be able to report as quickly as possible. In television, the networks apply pressure on their correspondents to file reports as soon as they arrive at a location. As a result reporters do not have time to express the context and meaning of events, and their reports may be incomplete distorted or even misleading, which could impact government policies if leaders are using these media as a principal source of information (Gilboa 2002: 734). If users with political influence do not critically examine the information that they absorb, the rapid, raw representation of information on social media sites could have a negative social impact.

A computer science professor at Boston Univeristy, Azer Bestavros, argues that social media changes the feedback mechanism of media, or the interaction between society and news sources. He points out that when people post real-time information: "there is something fundamentally different between feeling like someone can respond in minutes versus nothing will happen for several days, weeks, or even months" (Bestavros 19 March 2012). Instead of submitting an op-ed to a newspaper and then waiting, people can write on their own blogs and receive instant feedback. Every citizen can become a source of information, or essentially, a journalist.

Citizen Journalism

Individuals become citizen journalists when they take out a mobile phone and tweet posts or record events as they happen. When this information is posted online, everyone can view the content and form conclusions about what it means. Jan Schaffer has said that: “The use of cell phones for gathering and disseminating news is part of a larger shift worldwide toward citizen media, which gives ordinary citizens the ability to spread and receive information as never before” (Schaffer 2008). These posts and videos can also be found and retransmitted by traditional journalists on radio, television, or other mediums, and then reach millions of additional individuals. Some news organizations have even folded social media into their potential network of information such as CNN’s iReport.com or Al Jazeera English’s the stream (Schaffer 2008). This citizen generated information can be used to create a counter narrative to governments’ official representation of events. This has proven especially powerful when videos depicting government brutality are posted on YouTube and re-circulated through traditional media outlets. This was certainly the case in Egypt during the protests that occurred in January of 2011.

Counter Narratives (Egypt)

During the Egyptian protests of January 2011, satellite networks such as Al Jazeera would obtain videos gathered by citizen journalists and display them on television. The Egyptian state television channels supported President Hosni Mubarak, and even went as far as to play old video of an empty Tahrir Square instead of broadcasting the images of people protesting (Walker and Orttung 2011). The videos taken by citizen journalists countered official narratives, and allowed viewers, both domestically and abroad, to see for themselves what was actually happening and how the government was treating its citizens. Television is still the predominant form of media in Egypt, and there is over 50% penetration ("Egypt Passes 50% Penetration Mark"), which means that the broadcasts of videos collected by citizen journalist can reach a significant portion of the country that do not utilize social media. NPR Social Media Production Assistant Ahmed Al Omran covered the protests, and explains that that: "There is a feedback loop as social media provides raw information for broadcasters who then create the context that defines the narrative of the revolution" (Al Omran 15 March 2012). Additionally, if regional television stations show videos of protests in one country, those images can impact citizens in other countries as well. Prior to the January 2011 protests, Egyptians were able to view videos of the successful revolution in Tunisia. The President of Arab Alliance of Freedom and Democracy, Wael Nawara, believes that there was a sense among Egyptians that "If the Tunisians could do it, we can too," and this was part of the inspiration for the January round of protests (Nawara 24 March 2012). This fear of citizens being inspired by the revolutions in other countries is likely what motivated China to censor information about the Egyptian revolutions (Rauhala 2011). The rise of citizen journalism has changed what information viewers have access to, and how they contextualize images of conflict.

Accountability (China)

The direct reporting of information on the Internet and social media can also help highlight cases of corruption or incompetence that governments might otherwise cover up or ignore. In the context of development, technology is being used to improve how critical information and services can reach beneficiaries (i.e. of humanitarian aid), and when a transfer is not completed, technology can be used to find the responsible party (Antsey and McCarthy 2011). Essentially, social media can be used to improve transparency and government accountability. A recent case in China highlights this function. In the aftermath of a train crash in the Zhejiang Province in China, government officials attempted to attribute the incident to weather or technical reasons, but bloggers' expressed skepticism and outrage on the Chinese microblog Sina Weibo (Wines and LaFreniere 2011). Leaked propaganda directives showed that reporters were directed not to run investigative reports or commentary, or to link the incident to the country's rail development program (Murphy 2011). The government attempted to avoid discussing the crash and the complete lack of coverage by state media caused many concerned citizens to believe that the government was covering up vital information (Murphy 2011). The government attempted to censor the online conversation about these protests, but that only sparked further outrage. Ultimately, a state official apologized for the crashes. In this case social media was an effective tool for encouraging the government to come forward. There are other examples of social media being used to fight corruption in countries such as Slovakia, Georgia, Moldova, Kyrgyzstan, Kenya, India, and many others ("New Study on the Use of Social Media in Fighting Corruption").

Transparency (United States)

The ability for social media to be used to reveal government secrets is not limited to repressive regimes. In the United States there is the controversial case of the leak of State Department cables on the WikiLeaks website, a self-described media organization. In February of 2010, Private First Class Bradley Manning took the secret information off of the computers at the State Department, and gave them to WikiLeaks which posts information that counters the official narratives espoused by those in power (Fenster 2011: 10).

This event is similar to the leak of the Pentagon Papers by Daniel Ellsberg during the Vietnam War (Fenster 2011: 13). However, unlike Ellsberg who had to take pains to photocopy the documents, and get them to the right sources, with WikiLeaks, contributors can upload information from any location and it is instantly distributed throughout the Internet (Mulrine 2011). Furthermore, the site can be hosted on different servers around the world, and this redundancy makes the site resilient or difficult to shut down by any particular government. Also unlike the Ellsberg case, WikiLeaks is not a traditional newspaper or broadcast media provider and consequently, it is still unclear what protections they have under the law of numerous countries. In this case the website has taken on the whistleblowing function of traditional news organizations, but there is still significant debate in the U.S. over whether this constitutes as a journalistic enterprise, and whether WikiLeaks' actions are defended as freedom of speech (Gjelten 2010).

In a letter to WikiLeaks the U.S. State Department argued that the organizations' actions were illegal. As a result of this the online payment company PayPal blocked the account through which WikiLeaks has been receiving donations. The PayPal Vice

President of Platform, Mobile, and New Ventures specifically cited the State Department's declaration that the site was illegal as the reason why it suspended service, and noted: "We [...] comply with regulations around the world, making sure that we protect our brand" (Bosker 2010). In addition, while the site had been able to route their traffic through Sweden, it was later determined that Swedish protection did not extend to WikiLeaks because the organization did not have a publication license, and that sources are not protected in all cases (Jonasson 2010). The Swedish protection of sources is one of the strongest in the world, but a server placed in Sweden is not protected by these laws (Jonasson 2010). In June of 2010, Icelandic members of parliament enacted laws that include protection for whistle blowing sites such as WikiLeaks, and make the country a safe haven for journalists (Mackey 2010). The WikiLeaks model of decentralized, digital distribution of illegally obtained classified documents resists state attempts at information control and containment (Fenster 2011: 13), but states are able to influence intermediaries and impact sites like WikiLeaks indirectly.

Cyber Utopian Perspective

The cyber utopian perspective focuses on how there has been an increase in networked as opposed to hierarchical information flows, and that this makes it more difficult for governments to repress information at whim. In the past news bureaus would gather, filter, edit, and then distribute information, but now people everywhere are instantly producing and consuming information through ICT networks. On the Internet there are many centers of information and states cannot control any particular institution in the same way as broadcast or print media. Additionally, because there are no universal editors on the Internet, every voice can be expressed, and it is not the purview of news organizations to determine what information is valuable. In this way, the gatekeeper function of the traditional media has been challenged if not eliminated. While search engines have become a new type of gatekeeper, they determine information priority based on data gathered from Internet users, and essentially reflect patterns of existing preferences rather than imposing their own. Anyone can produce content on the Internet, which is different from constrained production of broadcast media.

Citizen journalists can report on events in real-time, and even capture video that is then utilized by traditional outlets. Social media have become tools for citizens to express information critical of their government, and in Egypt, China and the United States, they have encouraged greater transparency and accountability. Renowned cyber utopian scholar Clay Shirky writes that: "As the communications landscape gets denser, more complex, and more participatory, the networked population is gaining greater access to information, more opportunities to engage in public speech, and an enhanced ability to undertake collective action… these increased freedoms can help loosely coordinated publics demand change" (Shirky 2011). He adds that the use of social media tools (i.e. text messaging, e-mail, photo sharing, social networking sites) does not guarantee any particular outcome, and that conversations about their effects on political action often revolve around dueling anecdotes. However, he feels that it is fair to argue: "these tools probably do not hurt in the short run and might help in the long run -- and that they have the most dramatic effects in states where a public sphere already constrains the actions of the government (Shirky 2011). This will be further explored in the next section, which focuses on political activism.

Cyber Skeptic Perspective

The cyber skeptic perspective focuses on how networked information does not imply that everyone's voice is heard equally, nor does it prevent governments from controlling information through means other than pressuring news organizations. Although Internet access has been increasing dramatically, it is still far from being universal. On the Internet everyone may be able to produce content, but there is such an overabundance of information that not everyone's content will be noticed. The increased access to information does not necessarily mean that people are more informed, and without gatekeepers individuals must use their own preferences as a guide, which can result in nichification. In order to navigate the Internet, users may still rely on trusted institutions in which case there are still gatekeepers. Search engines are essential to filtering the Internet, but they do monetize the prioritization of information by having "sponsored links" from paid clients. Furthermore, while search engines reflect patterns of use, this means that sites that receive greater traffic will be emphasized and sites that do not will remain in anonymity.

The absence of standards for most information on the Internet means that there is no guarantee of its accuracy, and yet there is the possibility that people may believe what they find. Social media is a useful tool for providing shallow real-time information, but at this point it still has limited penetration and it relies on other traditional media in order to reach those who do not go online. Additionally, while social media sites provide real-time reporting, they do not provide context, and they can cause people to form distorted views of what is occurring. While citizen journalists can report on regime atrocities, they are vulnerable to retaliation in which case they have no institutional backing to rely on. Citizen journalists also are not bound by the standards of any particular journalism institution and consequently there is no guarantee of the accuracy of their reports. Furthermore, while sites such as WikiLeaks may claim to be a part of the free press, governments can argue that they do not deserve the same protections as legitimate news organizations. The U.S. State Department was able to influence the private intermediaries that provided the financial infrastructure for the website, even if they could not shut the site down in total. Even Sweden did not offer protection to the site because it did not have a publication license. The Internet and other ICT may change the way people produce and consume information, but it is not without government interference. Last, access to information does not inherently imply that people will coordinate with each other. This will be further explored in the next section, which focuses on political activism.

Integrated Perspective

ICT networks support the Internet that many users obtain information from. Social media sites on the Internet allow citizens to access and share information across borders in real-time, without the government or traditional media organizations serving as an intermediary. If one employs the liberal definition of sovereignty – that sovereignty is defined by the states' ability to control actors and activities within and across its borders (Thomson 1995: 213) – then ICT networks are in fact challenging state sovereignty by dispersing the "gates" where governments can exert control over information. Traditional media have centers of production where information is refined and then distributed to the general public. The government can exert its influence at this central point and define the information that the public can access. However, networks have many central points, which makes it more challenging for the state to control information. Information control is important to states because if they can limit awareness of their flaws, they can better manage dissent. Internet researcher Zeynep Tufecki posits that governments try to control information in order to prevent the majority of ordinary people from facing cognitive dissonance between their compliance with the regime, and their criticisms of the regime (Tufecki 2011). She adds that citizen journalism is powerful, because people with cell phone cameras can increase shared knowledge, and inspire others to decry the regime.

Still, the diffusion of information production has not resulted in a challenge to the supremacy of a state's authority within its borders. Specific regimes may find that their self-representation has been compromised by the revelation of secret information (U.S.), that they can not prevent awareness of dissenters (Egypt), or that they can not cover up incidents of corruption or negligence (China). Yet this does not mean that the state ceases to be considered the supreme governing structure within its territorial boundaries. The American, Chinese, and Egyptian governments do not disappear if particular regimes are challenged or ousted from power. The loss of control over information represents a challenge to states' control, but by no means eliminates its authority completely. State sovereignty remains intact in the face of the diffused information proliferation facilitated by ICT networks.

Transition

User access to ICT networks such as the Internet and mobile phone service is increasing at a rapid rate and will only continue to grow. Search engines have become a new type of gatekeeper, as the influence of traditional media institutions is challenged by additional sources of information, such as social media. These new information sources provide access to instantaneous information, and allow users to be producers as well as consumers. Citizen journalists can have an effect on their government by distributing information that would otherwise be ignored by state controlled media institutions. Democracies and repressive regimes are finding that they face new challenges from these information networks. While cyber utopians assert that these changes will result in a more sophisticated information environment, cyber skeptics emphasize that the additional complexity may be challenging for users rather than beneficial. These shifts have an effect on how citizens view the world, and how they interact with the authorities that seek to control them. As citizens are better able to share their concerns and criticisms of their government, they may become inspired to take action and seek reform. The next section will explore the role of ICT networks in facilitating collective action, and its subsequent effect on state sovereignty.

Coordination

Activism

Communication is essentially the sharing of information. The widespread diffusion of ICT has allowed for information exchanges on an unprecedented scale. The Internet, and social media sites in particular, create a new public sphere where political discourse can occur. The communication in this space can facilitate coordination for political purposes, and the ability for citizens to communicate can empower them to take collective action and advocate for government reform. There is a debate over whether these media can truly inspire protest given that they are thought to rely on "weak ties." However, in Tunisia young activists relied on these social media tools to protest the government and ultimately, they successfully instigated a regime change. In Egypt, citizens learned about the events in Tunisia through ICT, and they too used social media as a tool for expressing dissent and coordinating protests. Even in the United States, the Occupy Movement relied on social media to communicate among its members and coordinate the activities of their Occupy camps as well as their protests of societal injustices. Cyber utopians stress that as long as states allow for any virtual congregation on the Internet, it will be possible for citizens to coordinate actions in the real world. However, cyber skeptics focus on the fact that ICT are not responsible for political action. It is people who coordinate these events and who attend them, and social media is no different from any other communication tool. ICT networks are undoubtedly used to coordinate action, but their necessity is still a topic of debate. The use of ICT networks to coordinate protests, movements, uprisings, revolutions, and other collective action challenges states' control of their citizens.

Public Sphere

The use of ICT networks has allowed for a more decentralized structure of information sharing. On the Internet an individual can post information that is then accessible by billions around the world. The networked nature of the Internet is not inherently political, but it can facilitate citizens' access to political information. Furthermore, it can provide a domain where people can exchange ideas and communicate with each other. The concept of the "public sphere" relates increased information and communication transmission to political discussion and coordination. Sociologist Jürgen Habermas defines the "public sphere" as being a domain of our social life in which a public opinion can be formed, a portion of which is even constituted through private conversations (Habermas 1989: 398). Habermas states: "Citizens act as a public when they deal with matters of general interest without being subject to coercion; this with the guarantee that they may assemble and unite freely, and express and publicize their opinions freely" (Habermas 1989: 398).

Communication can occur through print and broadcast media, and they too are a part of the public sphere. When the public discussions concern issues related to the practice of the state, that is a political public sphere. Network theorist Yochai Benkler argues that the networked information economy has reduced the cost of becoming a speaker, and the cost of speaking across societal boundaries (Benkler 2006: 12). In his view there has been a shift from a hub-and-spoke architecture with unidirectional links, as in mass media, to a distributed architecture with multidirectional connections among all nodes, as in social media (Benkler 2006: 12). He argues that this networked public sphere will allow for any point of view to be expressed, and if it is interesting to others, it will be elevated through collective filtration (Kelly 2008: 14). In other words, in the modern era the public sphere also exists through social media and it provides a space for people to discuss political issues.

In repressive regimes, this new public sphere can be particularly potent because it is a place where dissent can be voiced, as opposed to through state controlled media. Communication is valuable in and of itself, but this new public sphere can also facilitate coordination as citizens share information about the intent to take action or events that are being executed. Communications researcher Christopher Kedzie argues that: "Communication is the most important force for organizing political and social behavior. This observation inheres from the uncertainty and lack of information that contextualize decision making" (Kedzie 2002: 107). As people learn that others share their same concerns, they become more assured in their view. As people communicate with each other about their shared frustrations, they may choose to take action knowing that there are others willing to act with them. Furthermore, as network theorist Milton Mueller notes: “By converging different media forms and facilitating fully interactive communication, the Internet dramatically alters the cost and capabilities of group action. As a result, radically new forms of collaboration, discourse, and organization are emerging” (Mueller 2010: 4). Social media sites facilitate coordination for birthday parties or class reunions, and similarly they can be used to plan political meetings and protests, or encourage other forms of action such as petitions and fundraising.

Strong and Weak Ties

Cyber utopians argue that social media facilitate the coordination of collective action. They argue that social networks map ties in the real world into a virtual space, and even enable users to connect with people they may not have a relationship with in real life. However, cyber skeptics counter that these sites rely on weak ties that do not have the strength to result in political action. Network theorist Miles Kahler argues that:

> “Strong ties among network members may produce cliques, nodes that display dense links to each other, but few, if any, ties to those outside the clique. This pattern of network formation may appear among groups with ‘strong ideological and/or cultural affinities’ coupled with emotional resonance. Clique formation may promote effective collective action by the clique, but it poses barriers to the widening of action. Nodes with weak ties outside the clique networks may play a critical role in extending cooperation and collective action; those with weak ties may play a disproportionately influential role within the wider network as a result" (Kahler 2009: 111).

Essentially, strong ties bind groups closer together and create dense clusters of association, but weak ties connect these clusters and facilitate cooperation between clusters. Sociologist Mark Granovetter argues that each person has their own dense social grouping, as well as loose acquaintances. It is these acquaintances that serve as a bridge between social groups, and these groups would not be connected at all if it were not for the existence of weak ties (Granovetter 1983: 202).

Through these ties, strong and weak, people can become aware of information they had not previously noticed, and can be notified of events that others in their social circle are attending. Social media can serve as a tool for political coordination, if users choose to participate in events and demonstrations as a result of learning about them online, or from other individuals who learned of them online. On social media sites it is easy for event coordinators to reach out to possible participants through rapid information sharing, and in the case of social networking sites like Facebook, through personal connections. Social media tools allow for clear communication to a large number of individuals in a short amount of time. The utility of social media becomes apparent when examining their role in recent political movements, such as the protests in Tunisia in winter of 2010, the protests in Egypt in early 2011, and the Occupy Movement in the fall of 2011.

Political Protest (Tunisia)

In Tunisia, social media was used to spread information about political causes and coordinate protests in early 2011. The start of that round of protests is considered to be December 17th, 2010 when an unemployed Tunisian man, Mohamed Bouazizi set himself on fire to protest against joblessness (*Global Voices Tunisia Revolution*). Other suicides followed, and these inspired protests throughout the country with demands for improved economic opportunities and the reform of the government of President Zine El Abidine Ben Ali (*Global Voices Tunisia Revolution*). The protestors and security forces faced off for about a month resulting in several fatalities, and on January 13th President Ben Ali gave a speech in which he promised to step down in 2014. Shortly after this, the country's Internet censors were turned off. Within a day President Ben Ali had fled the country, and two days later on January 15th parliament speaker Fouad Mebazaa became interim president.

Throughout the Tunisian Revolution activists used social media sites such as Twitter, Facebook, and YouTube as well as forums and personal blogs in order to post information and media content about the protests as they occurred (Olivarez-Giles 2011). Activists would post information online about a political person who had been killed or assaulted by the regime and use it as a rallying point for protests. A member of the Tunisian Youth Patriots, activist Montassar Anas Jemmali, says that at first he used

Facebook for connecting with friends or watching videos, but after the 13th of January it was how he learned about the reality of events in the country: “It was about how [we] could react, organize more events, call people to protest, spread videos, and communicate with foreign TV channels like France 24 and Al Jazeera” (Jemmali 23 February 2012). Activists would rely on social media for information about current events because they distrusted the local traditional media, which was considered to be a mouthpiece for the regime (Jemmali 23 February 2012). However, activists did try to encourage reporting on Tunisian events by foreign press with the hope that if outsiders saw the abuses of the current regime they would withdraw their support, and take a neutral stance (Jemmali 23 February 2012). Jemmali believes that: “[Social media] had a big impact on Tunisian youth. The protests were a result of their strong intervention with Facebook and Twitter, because they see everything and are very sad about what is happening to their country (Jemmali 23 February 2012).

Protestors would take video recordings with their mobile devices and then upload them to the Internet to show how the regime was mistreating its citizens. Marc Lynch suggests that: “analysts not think about the effects of the new media as an either/or proposition (‘Twitter vs. Al Jazeera’), but instead think about new media (Twitter, Facebook, YouTube, SMS, etc) and satellite television as collectively transforming a complex and potent evolving media space” (Lynch 2011). He argues that without social media, the images of Tunisian protestors might never have escaped the repression of the Ben Ali regimes, and that the broadcast of these videos on Al Jazeera brought those images to the Arab public and even to many Tunisians who were not aware of what was happening in their country” (Lynch 2011). This highlights the role of traditional broadcast media as serving as a loudspeaker for the information posted on social media. This amplifying effect was particularly relevant when the Ben Ali regime was toppled, and videos showing the protestor's success were shown throughout the Middle East, and the world.

Jemmali explains that: “Tunisia is a reference. The revolution in Tunisia has had an impact in Nigeria, Morocco, Egypt, Bahrain, Saudi Arabia, Kuwait, France, New York, and Spain. Tunisia gave the example that we are able to change our destiny. There is no person in the world that can’t believe Tunisia, about the region. Some are surprised, some people think that it couldn’t happen, but it did” (Jemmali 23 February 2012). People in other countries saw that the Tunisian government, an authoritarian regime, could be toppled, and so they asked: why not us? The success of the protests in Tunisia became an inspiration for other protests in the region, including those in Egypt.

Political Protest (Egypt)

In Egypt social media users were able to watch events unfold in Tunisia by following relevant hash tags on twitter. They saw the events unfold in real time, even as the Ben Ali regime was ousted from power. This built a revolutionary mood in Egypt, in which protests had been going on since 2005 (Nawara 24 March 2012). In January of 2011, Egyptians rose up in protest of the regime of President Hosni Mubarak. The protests touched off on January 25th 2011, which was a holiday honoring the police. Crowds filled Tahrir Square, and although the protests began peacefully, security personnel began to beat protestors and used water cannons. This was subsequently called the “Day of Rage” (Michael 2011). On January 27th, the government shut down communications, and on January 28th Mubarak announced that the government would step down (Kanalley 2011). On February 1st, Mubarak announced that he would not run for re-election, and on February 2nd, communications services were reinstated in Egypt (~Fayed 2011). On February 11th, President Hosni Mubarak resigned and left Cairo (Imam 2011).

Unlike in Tunisia where there were few reporters on the ground, in Egypt the mainstream media, local and international, played an important role in providing the information that fueled the protests (York 21 March 2011). However, the story of Khaled Said, a young activist who was brutally tortured to death in 2010, was largely propagated on Facebook. He was a young professional who resembled so many of Egyptian's politically active youth, and he became a symbol for all of the suffering endured at the hands of the police, and the corrupt regime that supported them. He was a rallying point for Egyptian youth, but there were many underlying issues that inspired protestors to demand government reform. The President of Arab Alliance of Freedom and Democracy, Wael Nawara, believes that the protests resulted from a combination of factors:

> "Protests had been going on since 2005. The only difference was the rising level of activism, and the diminishing political space for discourse. In the November 2010 elections the ruling power had a low approval rating, and their re-election was a kind of final spark, which led to the January 25th demonstrations. There was a sense among Egyptians that 'If the Tunisians could do it, we can too.' So it was combination of things: anger at Mubarak, at the ruling party, at attempts to re-instate the Mubarak regime, at the rigging of elections, and at corruption charges that were taking place and leaked in newspapers" (Nawara 24 March 2012).

President Mubarak had been in power for several decades and many people saw him as an obstacle to government reform and progress.

The protests built naturally over time, and as tension grew, social media represented this dissatisfaction. When people commented on the protests and discussed their political viewpoints on social media, all of their associates could see what they said, and a political climate was created. In this way people who may not have previously had much interest in politics can end up learning more through exposure to information from their associates. There is a viral element as information spreads throughout the network, and people share it and react to it (Nassar 18 November 2010). Additionally, it can be argued that social networks inspire people to attend protests because they publicize an individual's intent to do so. Political scientist Susanne Lohman has altered threshold models of collective action to incorporate a signaling approach in which the revelation of private information may initiate an information cascade and thereby promote collective action (Lohman 1994 as cited in Kahler 2009: 111). Network theorist Miles Kahler argues that the concept of an information cascade can be applied to incorporate networks, because “network links could facilitate information diffusion and cascades more rapidly than the broadcast model of information incorporated in Lohmann's model" (Kahler 2009: 111). This concept would apply to social media networks as well. If many people say they are going to an event on Facebook, then others may think "This may be worth me going to that event," which increases attendance and fuels greater participation (Bestavros 19 March 2012). In this case, even the illusion of widespread involvement can be relevant to inspiring collective action. Sites like Facebook even show who is confirmed for an event in real time, which is a much clearer indicator than protest coordinators could hope to obtain through non-technological means. Whether or not those individuals attend, social media sites can still provide coordinators with information about what level of awareness or activity their campaign has inspired.

The use of social media in protests also inspires involvement because parties outside of the protests can feel involved. Everyone in the world could understand the events in Egypt as they happened by following social media. Not only the Egyptian diaspora, but citizens of any country could follow the protests in real time, and this helps generate international interest. Many journalists relied on Twitter to stay informed and get up to the second coverage of events, and even used them as an informal reporting tool. Rawya Rageh, an Al Jazeera English reporter, says that she uses Twitter: “primarily in a professional capacity. I tweeted heavily during the first days of the revolution before communications were cut by the Mubarak regime late Jan 27.” (Rageh 18 March 2012). Since one goal of the dissidents is to highlight the regime's brutality, it is valuable to gain an international following. When foreign governments are supporting the authoritarian regime facing dissent, protestors can focus their efforts on highlighting how citizens are being abused (Jemmali 23 February 2012).

Additionally, in the United States the traditional media often framed stories of the Egyptian protests through narratives that focused on the role of Facebook or Twitter, companies that U.S. citizens recognize and can identify with. There was also a significant coverage of Wael Ghonim, the Google employee who was detained by the Egyptian police. In the U.S. this emphasis on social media has likely fueled unrealistic claims about its importance, and presented a utopian view of the protests, with technology serving as a savior for the oppressed people of Egypt. However, as Rageh points out: “People make revolutions, not technology” (Rageh 18 March 2012).

Still, the government clearly recognized the threat posed by coordination in this online public sphere. On January 28th, 2011, the Mubarak regime imposed restrictions on ISPs effectively shutting down the Internet and mobile phone networks. The exact nature of this shutdown will be discussed in the section focused on government control of ICT networks. In the context of social media, this development demonstrates that the Egyptian regime clearly saw the coordinating power of social media and mobile communications as a threat worth mitigating. However, this shut down also highlights how protestors may have used social media as a tool for coordination, but they were not dependent on it. Journalist Ashraf Khalil notes that: "[Social media] was crucial up to a certain point, but once the popular anger had successfully shifted to the streets, it became less necessary. The government shutdown of the Internet completely failed to blunt the momentum of the protests—so it obviously wasn't necessary by then" (Khalil 27 March 2012). The success of the revolution came after the Internet had been shut off, implying that it is not necessary for the protests to occur, though it is a useful tool. Additionally, there are people who argue that the lack of Internet access during that period of time resulted in people having more free time and that they needed to take to the streets in order to learn what was happening after communications were disrupted (Howard, Aggarwal, Hussein 2011: 3). Regardless, the shutdown of ICT networks demonstrates that the government saw it as a threat and a tool that supported the ongoing protests of the regime.

It is possible to overestimate the impact of social media, especially if those describing its value are users. This is because social media can essentially form its own bubble, where people who are surrounded by the information these sources provide, think it is important to non-users who are not aware of it. An Arabic and Comparative Literature Professor at Boston University, Margaret Litvin, notes that:

> "When you are in [a Twitter bubble] they seem like the only reality, but when you step outside them you see what they really are. It doesn't apply to the country as a whole. Social media is its own world, and for people who inhabit it, it is terribly important... At the most crucial moment last January and February people kept going even when the Internet was down. That being said, without groups like 'We are All Khalid Said' and the Internet in general, people at American University [in Egypt] may never have heard of the protests" (Litvin 12 March 2012).

Rawya Rageh adds that: "In the end, you also need to bear in mind the level of poverty in

Egypt and that Internet penetration, which is arguably not that low, still isn't big enough to launch a revolution without real street cred" (Rageh 18 March 2012). Users can come to believe that the populations that are active on these sites represent all of society, when in fact they are often an elite minority. In Egypt Facebook penetration is relatively high for the region, but even then it is estimated at being around 13% of the population, although the majority of Egyptians who use the Internet, use Facebook ("Egypt Facebook Statistics"). When citizens were asked what was their primary source of news during the revolution, only 6% listed Facebook (IRI Egypt Index). The majority of people, 84% relied on television as their primary source of news. People outside of Egypt can come to have inaccurate views of social media proliferation, since the sites are public and can be viewed by interested individuals all around the globe (Bestavros 19 March 2012). This results in an inaccurate representation of Egyptian social media users, and Egyptian society as a whole.

Still, social media clearly creates a space for political dialogue among those who do make use of it. Georgetown Adjunct Professor of Media and Communications Adel Iskandar notes that: " a collective consciousness is developing in these social media that allow people to know they are not alone, not a voice in the wilderness. There was a community that developed, solidarity helped catapult many oppositional movements, and challenged the institutions' monopoly on what is right and what is wrong in knowledge creation" (Iskandar 19 March 2012). He points out that the traditional media portrayed Khalid Said as a drug addict, and that the forensic medical report did not report on the beating he had received from police forces. He argues that had social media not existed, there would have been only one narrative, and that social media can challenge this monopoly on information, and bring people together (Iskandar 19 March 2012). Since the government and traditional media have failed to create public discourse, and in fact actively seek to repress it, the new commons of the Internet has a significant place in society.

Wael Nawara described social media in Egypt as creating a public space that runs parallel to reality, and allows for greater freedom of discourse:

> "The regime was cracking down on political space, media space, the opposition, and monopolizing all the formal space. So people have to find a parallel space. That is a characteristic of parallel state; whenever a formal state or subsystem fails, another subsystem emerges through self-organization. Media and political space have failed to provide people with room to express themselves, and to exercise their political rights. So the blogs, Facebook, Twitter, and the rest of social media start to provide that kind of alternative space" (Nawara 24 March 2012).

At a time when the Egyptian government had placed significant restrictions on communication and coordination in all other forums, the Internet and social networks were largely unfiltered (El Ghobashy 22 March 2012). In Egypt, social media created a public sphere that encouraged discourse that was otherwise repressed in the physical world.

Political Protest (United States)

The use of social networks in Egypt inspired individuals who were involved in the Occupy Movement that began several months later in the United States (Ackerman 2011). The Occupy Movement began in New York in September of 2011 with the group "Occupy Wall Street." Occupy protestors took over physical public space in numerous cities and towns in order to start a conversation about numerous injustices, but primarily the growing income inequality in the United States. The author of this paper interviewed several members of the Occupy Boston movement during its encampment period in the fall of 2011. This section includes her understanding of the movement's media strategy as informed by these interviews. The Occupy Movement's media strategy was focused on creating an alternative narrative to the one that was being portrayed by government officials, and even traditional news outlets. Protestors found that their message was not being accurately expressed, and sought to control their own public representation through the use of social media.

Every member of the Occupy Movement was allowed to represent the Occupy protests to the media, and there was no specific public representative. The Occupiers noted that broadcast and print media did not represent the complexity of the movement, and that journalists continuously said the movement has "no message," rather than embracing the multitude of unique messages provided by protestors. The protestors resisted creating one platform, or having one list of goals, because they believed that it would make it easier for officials to dismiss them. An Occupy Boston member, Kate Perino, argued that attempting to use media as a broadcast mechanism for the movement's ideals was counter productive: "If we make an imaginary list of media demands, that makes it easier to for them to reject, dismiss, and ridicule us. We would be happy if the media were saying okay people, we need discourse… The U.S. could use a place for pretty heavy conversations" (Perino 6 November 2011). Instead, Occupy members video-recorded many of their General Assemblies and protests in order to establish their own media coverage of events. These videos were used to spread information within the movement, rather than appeal to mainstream media channels.

In reference to the Occupy Movement, Network theorist Yochai Benkler believes that: "I think the online component was critical — the ability to stream video, to capture the images and create records and narratives of sacrifice and resistance" (Preston 2011).

Occupy citizen journalists also posted videos online that depicted the forceful tactics of the NYPD, in order to demonstrate how the government was treating peaceful protestors. An Occupy Boston member, Aliza Howitt explained that: “The famous quote by Ghandi, ‘first they ignore you, then they laugh at you, then they fight you, then you win’ very faithfully reflects how the media has treated the movement. But we have viral videos on YouTube of police brutality. Now they are making fun of us, and the police are fighting us, but we still have yet to win. We kind of won, because everyone is focusing on economic issues. This is the result of the protests” (Howitt 6 November 11).

Protestors used social media in order to facilitate communication among members and spread information about the movement. The movement had a clear goal of operating without establishing a formal hierarchy. Protestors made use of social networks to help coordinate protests, marches, and other events, as well as to organize day-to-day operations in each of the locations. Occupy composed of a series of interconnected networked organizations, and they relied on social media to coordinate their various working groups. Through the use of social media, protestors were largely successful at creating a functioning organization without formal leadership. Occupy did not accidentally become a movement with a decentralized, networked leadership and involvement, but rather intentionally avoided hierarchal structures as it developed.

Cyber Skeptic Perspective

The cyber skeptics argue that social media does not cause revolutions and in fact, it can even hinder collective action if people equate activism online to activism in the physical world. In the article “Small Change,” renowned cyber skeptic Malcom Gladwell touched off a firestorm of debate between cyber skeptics and cyber utopians. His provocative thesis was that in modern times “we seem to have forgotten what activism is” (Gladwell 2010: 43). His argument focused on the sit-ins during the Civil Rights Movement of the 1960s, and he largely relies on sociologist Doug McAdam’s analysis of high risk and low risk activism. He cites how McAdams found that it was not ideological fervor that determined which participants stayed involved in the movement, but rather the important factor was having strong ties with other activists. McAdams concluded that high-risk activism is a “strong tie phenomenon (Gladwell 2010: 43). Gladwell expands that social media is built around weak ties, which are not associated with dedicated activism. He argues that Facebook is a tool for managing acquaintances, which is a source of new ideas and information, but does not inspire high-risk activism (Gladwell 2010: 45). He cites how Facebook groups dedicated to social causes gain a great deal of support because they do not ask for very much from their members, and there is no personal risk.

The phenomenon of social media users only participating in online political campaigns is commonly referred to as “slacktivism” (Shirky 2011). In Gladwell’s view, social networks increase participation, but not activism. Renowned cyber skeptic Evgeny Morozov argues that it is reasonable to assume that online campaigning can cannibalize its offline brethren. He adds that if psychologists are correct and the motivation for people to support political causes is to become happy, then Facebook groups might make them just as happy as writing letters to their elected representatives or organizing rallies, despite the fact that online activities will have less impact on society (Morozov 2011: 190). Morozov argues that in authoritarian states “slacktivist” behaviors may give young people the wrong impression that political protest can be pinned on virtual campaigns, online petitions, or angry tweets, and that they will prefer this to the to the ineffective, boring, risky, and, in most cases, outdated kind of politics practiced by the conventional oppositional movements (Morozov 2011: 201). Cyber skeptics emphasize that social media can hinder collective action.

Gladwell specifically mentions social media as being a networked technology, but argues that true activism relies on hierarchical organizations. He argues that the network structure is resilient and adaptable in low-risk situations, but that the consensus decision-making process and loose ties are not compatible with high-risk activism (Gladwell 2010: 47). He closes his argument by criticizing Clay Shirky's emphasis on social media as a platform for activism:

> "It is simply a form of organizing which favors the weak-tie connections that give us access to information over the strong-tie connections that help us persevere in the face of danger. It shifts our energies from organizations that promote strategic and disciplined activity and toward those which promote resilience and adaptability. It makes it easier for activists to express themselves, and harder for that expression to have any impact" (Gladwell 2010: 47).

Gladwell's article inspired a significant amount of criticism from members of the cyber utopian perspective, as well as moderates, and many other writers set out to prove him wrong.

Cyber Utopian Perspective

About a year after Gladwell's article, he and Clay Shirky co-authored an article expressing their differing perspectives on the revolutions in Tunisia and Egypt. Gladwell argued that "just because innovations in communications technology happen does not mean that they matter" and asked: "What evidence is there that social revolutions in the pre-Internet era suffered from a lack of cutting-edge communications and organizational tools? In other words, did social media solve a problem that actually needed solving?" (Gladwell and Shirky 2011). Shirky responded by arguing that the "competitive landscape gets altered because the Internet allows insurgents to play by different rules than incumbents," and he breaks Gladwell's question into two parts: "Do social media allow insurgents to adopt new strategies? And have those strategies ever been crucial?" He answers: "Here, the historical record of the last decade is unambiguous: yes, and yes" (Gladwell and Shirky 2011). Shirky argues that digital networks have greatly decreased the cost of and increased the spread of information, and improved the speed and scale of group coordination. He agrees with Gladwell that these tools do not allow uncommitted groups to be more effective, but argues that they do allow committed groups to play by new rules. As he expressed in an earlier article: "The fact that barely committed actors cannot click their way to a better world does not mean that committed actors cannot use social media effectively (Shirky 2011). He closes by emphasizing that even as state reactions increase in sophistication and force, social media alters the dynamics of the public sphere, and the state is always forced to counter a more empowered public (Gladwell and Shirky 2011).

Other writers also took issue with Gladwell's argument. In a blog post, social media researcher David Weinberger concedes that Gladwell is right to debunk the belief that the Internet would sweep away all institutions, and replace traditional forms of governance, but notes: "At this point, however, those are strawpeople. Find me someone who believes that these days" (Weinberger 2010). He argues that the Internet has had an impact on traditional institutions by changing the ecology around them. As an example he notes that citizen journalism has not eliminated traditional journalism, but instead a new media environment has emerged (Weinberger 2010). The events in Egypt exemplify this shift, where social media can provide raw data to a core online population, and broadcast media can provide context and vastly expand the viewing audience. During the Egyptian protests, images of police brutality were captured by citizen journalists, and these videos were aired on satellite television stations such as Al Jazeera English. As a result, many more individuals were able to view these amateur videos, because traditional media institutions chose to spread this raw footage. Weinberger takes issue with Gladwell's comments on networks, arguing that hierarchies and networks are not exclusive: "networks can be powerful tools for hierarchies. Likewise, networks are never entirely flat. They can have a local center that makes decisions and organizes actions" (Weinberger 2010). He adds that networks have their own methods for creating a strategy, as in a member puts an idea forward, and either it catches on through networks and weak ties, or it does not. Other writers question Gladwell's point that hierarchies are "prone to conflict and error," by questioning: "Hierarchies are not "prone to conflict and error?" (Brecher and Smith 2010).

Weinberger also argues that strong ties evolve from weaker ones, and that casual interactions can strengthen these ties. This statement is supported by the research of Doug McAdams, the same author Gladwell relied on to bolster his arguments. McAdams argues that research on identity transformation suggest that playing at being an "activist" is a prerequisite to becoming one. A recruit may leave a rally better integrated into a movement, and more likely to participate in other low-risk activities. McAdams argues that: "each succeeding foray into safe forms of activism increases the recruit's network integration, ideological affinity with the movement, and commitment to an activist identity, as well as his receptivity to more costly forms of participation. It is this type of gradual recruitment process that is likely to foster high-risk/cost activism" (McAdams 1986: 69). When this theory is applied to social media, it implies that people that play at being an activist online can slowly become more involved in a movement through low risk activities like joining a political Facebook groups or follow political twitter feeds. This can in time lead to greater identification with the movement and a commitment to high-risk activism. A writer for the *Economist* supports this view, and argues that Twitter and Facebook reduce the cost of minor interactions, which can lead to more minor interactions, which can also help in the maintenance of strong relationships (A. R. "Can You Social Network Your Way to Revolution?" 2010). The writer emphasizes that: "These platforms make it easier to maintain friendships through trying times and circumstances" (A. R. "Can You Social Network Your Way to Revolution?" 2010).

Writer Mary Joyce points out that McAdams emphasized that it is how "embedded" individuals are in a community that determines whether their ties are strong or weak, and that this quality of 'embededness' relies on inter-personal relationships. She argues it is possible for people to form strong ties on the Internet, and points out that the hackers that belong to the infamous Anonymous group – who mostly do not know each other offline or know each other's real names – have formed relationships with each other, and are willing to engage in coordinated risky behavior (Joyce 2011). Jeremy Brecher and Brendan Smith highlight how the Internet can also encourage strong ties by connecting people, and offer computer-initiated dating as a prime example. They argue that social networking sites are valuable in that they play an important role in finding and connecting people who are beginning to think and feel similar things: "They can help participants deepen their understanding and form common perspectives. They can help inform those who use them of possible courses of action" (Brecher and Smith 2010).

Brecher and Smith also refute Gladwell's arguments about the Civil Rights Movement, pointing out that the sit-ins at Greensboro, N.C. in 1960 better represent the image of the dense social networks of a community engaged in a powerful struggle. Strong ties may contribute to the emergence of deep commitment to a cause, but that does not rely on hierarchies. Brecher and Smith make a particularly strong point: "Social networking websites are not a form of organization at all; they are a means of communication. Comparing Twitter to the NAACP is like comparing a telephone to a PTA. They are not the same thing, they don't perform the same kind of functions and therefore their effectiveness or lack thereof simply can't be compared" (Brecher and Smith 2010). They concede that Gladwell is right in arguing that social media "are not a natural enemy of the status quo," but add that the important question is whether social media can contribute to effective social action, not whether social media can substitute for that process. Their argument is that: "A telephone system is not a PTA, but it can sure as heck be useful for getting a few hundred people out to confront the school board or vote in the school board election" (Brecher and Smith 2010).

Cyber Skeptics Rebuttal

Cyber skeptics have also generated responses to the cyber utopians' criticisms of Gladwell's argument. Writer Bill Wasik questions: "If the medium for those communications shifts from word of mouth, to printed flier, to telephone, then to texts and Twitter, what does it really matter? Technology becomes an important part of the story only if it’s changing the nature of the events — and the nature of the social groups that are carrying them out” (Wasik 2011). Cyber skeptic Evgeny Morozov argues that cyber utopians have tried to bury cyber realism by designing their own straw-man interpretation of the realist perspective, equating it with the view that the Internet does not matter (Morozov 2011). He argues that Gladwell’s critics ignore that Gladwell accepts that the Internet can be an effective tool for political change when used by grassroots organizations and has written as such. Morozov argues that showing the Internet was used to organize protests in the Middle East does not counter Gladwell’s argument, instead, cyber utopians would need to establish “that there was no coordination of these protests by networks of grassroots activists – with leaders and hierarchies – who have forged strong ties (online or offline or both) prior to the protests” (Morozov 2011).

Morozov notes that Tunsian and Egyptian cyber-activists did not only collaborate online, but also offline at workshops that he had attended in Cairo in May 2009. Morozov argues that the reason cyber utopians became angry is that while crowds were still occupying Tahrir Square, Gladwell suggested that the protestors’ grievances deserve more attention than the tools the used to organize (Morozov 2011). Morozov agrees with Gladwell, and argues that just as discussing the role of the telegraph in the 1917 Bolsehvik revolution is now the purview of a handful of academics, the examination of the role of social media in political protests will become similarly outdated: The fetishism of technology is at its strongest immediately after a revolution but tends to subside shortly afterward ”(Morozov 2011).

Integrated Perspective

ICT networks support the Internet and other technologies that many users rely on to communicate. Social media sites on the Internet allow citizens to collaborate and coordinate, without the government or traditional media organizations serving as an intermediary. If one employs the liberal definition of sovereignty – that sovereignty is defined by the states' ability to control actors and activities within and across its borders (Thomson 1995: 213) – then ICT networks are in fact challenging state sovereignty by facilitating communication and coordination outside of states' control and even in opposition to them. Social media create a new public sphere where people can discuss their shared concerns. This communication shapes political and social behavior because it alleviates the uncertainty that often surrounds decision-making (Kedzie and Aragon 2002: 107). These spaces allow for the expression of dissent, and when users realize that others are willing to act, they can coordinate collective action in the real world. Citizens rely on these tools to organize movements that advocate for governmental reform. These tools can assist in planning and executing events and actions in opposition to the state. Controlling collective action is important to states because if they do not, there is the possibility that dissatisfied citizens will dismantle them.

Still, the ability for citizens to coordinate collective action through ICT networks has not resulted in a challenge to the supremacy of a state's authority within its borders. Specific regimes may find that their citizens are able to organize decentralized protest movements without central leadership (U.S.), while other regimes may find that their citizens have become too powerful to repress and are consequently ousted from power (Tunisia and Egypt). Yet this does not mean that the state ceases to be considered the supreme governing structure within its territorial boundaries. The Tunisian, Egyptian, and

American states do not disappear if particular regimes are challenged or ousted from power. The decreased control over citizens' coordination of collective action represents a challenge to states' authority, but by no means eliminates it completely. State sovereignty remains intact in the face of the coordinated collective action of citizens that is facilitated by ICT networks.

Transition

On the topic of the role of social media in inspiring or coordinating political action, the debate between cyber skeptics and cyber utopians is particularly fierce. Cyber skeptics emphasize that these technologies are just tools, and new technologies are no different from the ones that preceded them. Cyber utopians stress that recent ICT developments have the potential for greater political impact than those in the past, and that social media facilitates coordination at an unprecedented level. The examples of Egypt, Tunisia, and the Occupy movement support the idea that social media can play a significant role in the coordination of contemporary protest movements in that it facilitates the creation of a new public sphere, and provides an additional medium through which people can become aware of political debate, and share their concerns with others. While social media may rely on weak ties, those ties can serve as bridges between groups of people who might otherwise remain in their own dense clusters of relationships. While it is not clear the extent to which ICT networks are facilitating political protest, they clearly serve as a medium for people to communicate and coordinate with each other. Civil society organizations can use ICT networks to coordinate their efforts. As citizens are better able to coordinate with each other, they can form organizations that do not rely on central hierarchical leadership to function, and operate across boundaries. The next section will explore the role of ICT networks in crisis mapping organizations, and how they relate to state sovereignty.

Assistance

Citizens can use ICT networks to coordinate actions against the government, but they can also use them to coordinate with the government yet still operate outside of its control. There are groups of citizens who are taking advantage of ICT networks in order to better allocate resources in times of crisis. During chaotic moments, such as environmental disasters and political upheavals, crisis mapping groups gather real time data through the use of ICT networks, and represent it geographically in order to help assist people in distress. They are volunteer-based and provide information to state or non-state actors in order to coordinate help to those in need. However, these groups do encounter different challenges when operating in political conflicts as opposed to environmental disasters, and this changes how they report information. These groups highlight the cyber utopian ideal of individuals collaborating without the need for hierarchical leadership. They interact with governments, but are not subordinate to them, and their networked nature allows them to be flexible during times of crisis. The use of ICT networks by civil society organizations, like crisis mappers, exemplifies how networked organizations can take on functions traditionally considered to be the purview of states. This does not challenge state control directly, but does present a possible alternative for future governance.

Networked Organizations

Civil society advocacy groups are often looked to as examples of networked organizations, meaning they do not rely on a formal hierarchical structure for decision-making or coordination purposes (Mueller 2010: 6). International relations scholar Joseph

Nye argues that while earlier transnational flows were heavily controlled by formally organized structures such as multinational corporations or the Catholic Church, the lower costs of communication in the Internet era have opened the field to loosely structured network organizations and even to individuals (Nye 2011: 120). Additionally, networks are suited to situations that require rapid and reliable information, and consequently, they can provide the information and transparency that are necessary preconditions for government accountability. This means that, in theory, human rights advocacy networks can use their distribution capabilities to provide detailed information about human rights violations or other secret information, which can then be used by other governments or international organizations to hold the violator accountable (Sikkink 2009: 233). Furthermore, network theorist Milton Mueller argues that networks that combine state and non-state actors can overcome some of the limitations of government based on territorial sovereignty (Mueller 2010: 6).

Crisis mapping groups are networked civil society groups that can work with states or other organizations to provide effective assistance during times of chaos. Crisis mapping relies on three components: crisis map sourcing, or the methodology by which information is collected; crisis map visualization, or the way in which the information is rendered on a dynamic, interactive map; and crisis map analysis, or the application of statistical techniques to spatial data for pattern detection (Meier 2011). There are numerous groups dedicated to crisis mapping. This analysis will mainly examine the Ushahidi platform, which has been used in 132 countries around the world (Vaisman 2011).

Ushahidi Platform Background

The word *Ushahidi*, which is Swahili for witness, refers to both a platform for information mapping and an organization that actually coordinates crisis maps. The platform by itself can be used to map anything from potholes that need to be fixed, to local traffic patterns (Perino 7 March 2012). If a map is crowdsourced it means that a mass of people are relied on to input information, often through mobile messaging, rather than a select team. The platform was created for events in Kenya in 2008 during the violence that occurred following the elections (“Ushahidi"). One of the founders was tracking data that documented human rights abuses, and found that she could not keep up with all of the information she received. She wrote a blog post asking why there could not be a Google map that expressed all of this information. Another blogger saw it and realized that there absolutely could, and so they created Ushahidi (Meier 19 March 2012). The Ushahidi team geographically mapped the information and included pictures and stories (Perino 7 March 2012). A former Ushahidi member, Kate Perino, also works in another mapping group known as the Standby Task Force (SBTF), which uses the Ushahidi mapping platform. The SBTF group focuses specifically on crisis mapping in political situations, and often coordinates with humanitarian groups in order to provide assistance during times of crisis.

Environmental Crises (Haiti)

These crisis mapping groups collect data from various different sources and represent it on a map that can be referred to by governments, non-governmental organizations (NGOs), and concerned individuals. They have been used all over the world in many different scenarios. The aftermath of the 2010 earthquake in Haiti is a particularly strong example of the coordination capabilities of crisis mapping. In that earthquake, more than 230,000 people died, and there was significant destruction in some of Haiti's most populous areas (Heinzelman and Waters2011: 1). The international community responded immediately, but the traditional disaster-response system of relief actors concentrated on information sharing among teams from within these international organizations (Heinzelman and Waters2011: 1).

The students at the Fletcher School of Law and Diplomacy began collating information they found on the Internet and Twitter about Haitians who were seeking help (Perino 7 March 2012). Humanitarian organizations were not as adept at dealing with this data, and providing aid was made even more challenging since the geography of Haiti was physically changed by the earthquake (Perino 7 March 2012). Individual communications from Haitians were lost in the system, as the United Nations and relief organizations largely relied on collecting intelligence through internal channels. Their system lacked the ability to aggregate and prioritize outside data, which made it difficult to include local intelligence (Heinzelman and Waters2011: 3).

The Ushahidi platform was set up at Fletcher, but the coordinators were not prepared for the volume of reports they received. Student volunteers were trained to do different tasks, such as translate the received messages, or locate the address or city block that the message came from (Perino 7 March 2012). The Ushahidi team received reports about trapped persons and medical emergencies, as well as requests for food, water, and shelter. These were plotted on maps and were updated in real time (Heinzelman and Waters2011: 1). As the map evolved to become more accurate, it developed into an important tool and was used by official groups such as the Red Cross, USAID, and even government forces on the ground in Haiti. Responders on the ground could access Ushahidi and use the data to determine how, when, and where to direct resources (Heinzelman and Waters2011: 1). Mobile phone penetration is incredibly high and Haitians could SMS Ushahidi through a shortcode, which allowed citizens to send messages describing their location, and situation (Perino 7 March 2012). In Haiti, Ushahidi was a valuable tool for coordinating information that traditional humanitarian organizations could not process. It is an example of how networked information gathering can be a challenge for hierarchical institutions used to relying on internal channels. The Ushahidi platform has been used in numerous other crises such as in the aftermath of the Pakistani flood in 2010, or in the ongoing unrest in Libya and Syria.

Political Crises (Libya)

Ushahidi is a valuable platform in times of crises, but there is the possibility that the public sharing of information can be harmful as well as helpful, especially when it is used in political situations rather than environmental crises. One of the founders of Ushahidi, Patrick Meier, remarked that he would try to dissuade mappers from using the platform in certain highly hostile environments. He explained that when populations are reporting on attacks by a government or other militaristic forces, there is the possibility that the platform could be hacked and the identities that reported the information could be revealed (Meier 19 March 2012). This would mean that people using the platform could be put in more danger because of the information they provide. Security experts can reduce vulnerabilities in these mapping platforms, but the possibility of exploitation cannot be fully eliminated and users must be educated about the risks. The possibility of authoritarian regimes using these tools to track down dissident citizens is a clear example of why it is important to focus on the realities of how ICT networks are being used.

If a crisis mapping platform is reporting on a conflict that has two sides, it does not want to favor one or the other, or provide information that could further the conflict. A former Standby Task Force volunteer, Kate Perino, described how in the case of Libya, crisis mappers decided to put a 48 hour delay on the public map in order to prevent the data from being used by one side or another to continue the violence (Perino 7 March 2012). Reputable organizations could still see the real-time data by establishing contact with the mappers, and so its humanitarian purpose was preserved (Perino 7 March 2012). In political crises, there are also additional challenges with verifying the data that is reported, because one side might try to use the platform to manipulate information about the activities of their adversary, and fabricate stories about them. This is mediated if mappers receive multiple distinct reports of the same incident, but there is always the possibility of regimes using the platform to spread misinformation (Perino 7 March 2012).

Ushahidi Platform Challenges

Verification issues also arise in environmental crises. After the Chilean earthquake in 2010 the Ushahidi Chile team received a report that said: "Please send help, i am buried under rubble in my home at Lautaro 1712 Estación Central, Santiago, Chile. My phone doesnt work" (Ford 2011). A similar message was submitted through twitter shortly after, but when the police investigated two days later the reports were proven false. Ushahidi is constantly working to improve its verification process, and create a system that can, among other abilities, address whether information is correct, and if it is incorrect, determine whether it was a deliberate act of misinformation or merely incomplete (Ford 2011). There are additional dangers from crisis mapping in environmental disasters that are unrelated to verification. In the aftermath of the Haiti earthquake, human traffickers were trying to locate children by using posts on the map. The volunteers had to swiftly take down all of that information. Crisis mappers must constantly balance providing accurate information, and avoiding the revelation of information to exploitative parties.

There is also an additional challenge for crisis mappers, which lies in the nature of the mission of humanitarian organizations. Kate Perino describes that groups that operate in conflict zones must maintain neutrality in order to avoid becoming politicized, and considered part of the conflict (Perino 7 March 2012). However, at times it is not clear whether crisis mappers are taking a political stance simply by sharing information. If videos of a regime's atrocities are posted, as they have been in the case of Syria, that inherently implies that the organization sharing the information is against the government. Kate Perino remarks that: "when you share information that a powerful government does not want you to have, that is in itself revolutionary" (Perino 7 March 2012). Standby Task Force Coordinator Anahi Ayala Iacucci puts it best:

> “Open data is not and cannot be neutral, unless you decide to open only certain data and not others, in which case it is not really open data. Information is and will always be power, and I think that the events in Egypt and Tunisia showed this very clearly. If you are sharing data you are sharing power and as such you are compromising the establishment that hide himself behind that power. Freedom of information comes from this, and it is considered one of the pillars of democracy. So, if you are releasing open data in a restricted environment, or under a repressive regime, you are not being neutral, you actively acting against that regime” (Iacucci 2011).

Consequently, crisis maps that track the human rights violations of a regime are fundamentally not neutral by definition.

Decentralized Structure

These crisis mapping groups are often operated solely on a volunteer basis, and individuals often complete various tasks within the organization. The Standby Task Force (SBTF) is organized in a horizontal fashion, which means that as opposed to there being a chain of command, there are those who are recognized as being more experienced, and they coordinate the group's actions (Perino 7 March 2012). Furthermore, if an individual wants to take on more of a leadership role, they too can become a coordinator by learning from those who have a more complete understanding. Coordinators cannot remove people from the group; a communal decision must be reached (Perino 7 March 2012). Kate Perino, an SBTF volunteer, finds that sometimes organizations working with the crisis mappers will not understand the networked nature of crisis mapping because they are used to getting information from their own people, or official sources (Perino 7 March 2012). These traditional organizations are structured hierarchically and expect that there will be particular individuals whose job is to collect information, as opposed to coordinators that complete various different tasks in order to represent information gathered from many sources (Perino 7 March 2012).

Cyber Utopian Perspective

These decentralized information-gathering networks and their teams of volunteer operators are a perfect example of the networked organization lauded by cyber utopians. Crisis mappers are able to organize vast amounts of information and coordinate with multiple other actors in order to provide humanitarian assistance. The platform can assist state actors as well as non-state actors and individuals. Even when states do make use of the information these volunteers gather, they do not control the crisis mapping process itself. These civil society networks are not challenging state authority directly, but they do provide information that allows people to be more aware of a government's actions. Additionally, U.S. SD Senior Advisor for Innovation Alec Ross argues that: "There is a shifting view of political power from hierarchies, including governments, to networks and citizens. This is made possible by communication technologies… the hyper-connectivity of citizens leads to the empowerment of citizens at the expense of state" (Ross 5 April 2012).

The crisis mapping platform is an example of how ICT networks have enabled services that can coordinate action between states, NGOs, and civilians in a positive way that benefits society. Their relevance to this analysis is largely in that the present a possible alternative medium for resource allocation outside of government control. While these maps are often used by states and state agencies, there are also cases where they are used solely by civilian groups. These sites have the potential to allow citizens to coordinate responses in a decentralized manner without any need for state mediation. If there were to be an alternative to the hierarchical structure of states, it would likely require tools such as crisis mapping platforms, which allow for the decentralized gathering, synthesis, and representation of information.

Cyber Skeptic Perspective

Cyber skeptics emphasize the flaws with crisis mapping platforms, as well as diminish their overall significance. Evgeny Morozov writes:

> "The reason why many projects that rely on crowdsourcing produce trustworthy data in natural disasters is because those are usually apolitical events. There are no warring sides, and those who report data do not have any incentives to manipulate it. The problem with using such crowdsourced tools for other purposes—for example, documenting human rights abuses or monitoring elections, some of the other uses to which Ushahidi has been put—is that the accuracy of such reports is impossible to verify and easy to manipulate" (Morozov 2011: 271).

The decision of the Standby Task Force to add a 48-hour delay on Libya is meant to remedy the possibility of the information being used for negative purposes, but the challenge of verifying crowdsourced information is present in every scenario. Even in the aftermath of the earthquake in Chile there was misinformation on the Ushahidi platform, which wasted the effort of the police who went to investigate. In political conflicts Morozov argues there is always the possibility that one group will create erroneous reports in order to accuse their opponents of wrong doing (Morozov 2011: 271). Furthermore, he argues that these maps can give a general idea of the scale and nature of abuses, but they are not helpful in the overall context of reporting human rights violations, where even small inaccuracies can invalidate the reports from an NGO (Morozov 2011: 271). A Co-founder of Ushahidi, Patrick Meier, himself admits that these platforms should not necessarily be used in hostile situations where parties have reasons to manipulate the data, and more importantly, states might be able to determine the identities of the individuals who submitted reports. If these platforms are not properly secured, they could hurt the very people they were intended to assist.

Integrated Perspective

ICT networks support advanced data-gathering techniques, such as crowdsourcing, and facilitate real time information analysis and distribution. Crisis mapping groups are networked organizations that can adapt to different situations in order to gather large quantities of data and represent them on geographical maps. If one employs the liberal definition of sovereignty – that sovereignty is defined by the states' ability to control actors and activities within and across its borders (Thomson 1995: 213) – then ICT networks are in a sense challenging state sovereignty by enabling civil society groups to facilitate resource allocation outside of their control. However, crisis mapping sites provide information to state and non-state actors alike, in order to facilitate assistance efforts in times of crisis. While these groups may seek to avoid assisting violent parties during times of political crisis, they do not inherently operate in opposition to states. U.S. SD official Alec Ross argues that the empowerment of citizens is at the expense of the state, but arguably, crisis mapping shows how ICT networks can facilitate collaboration between states and citizens. Crisis mapping represents the possibility for powerful new networked organizations. Rather than there being a hierarchical chain of command, decisions are made by consensus, and members are not limited by geographic location.

Crisis mappers operate outside of state control, but not necessarily in opposition to it. The ability to synthesize data and represent it in a way that assists in resource allocation has not resulted in a challenge to the supremacy of a state's authority within its borders. Instead ICT networks can provide information that supports government efforts during environmental crisis (Haiti and Chile), in addition to reporting on acts of violence between parties locked in political conflict (Libya). Still crisis mapping represents the possibility for a new type of organization that can coordinate civilians to share resources without necessarily relying on states. It does not require hierarchical leadership, and it represents what a possible alterative to state control might be. With tools like crisis mapping, NGOs could be empowered to provide assistance without state intervention, and in time this could empower citizens to fulfill functions of the state, such as resource allocation, all on their own.

However, at this time the state clearly does not cease to be considered the supreme governing structure within its territorial boundaries, even if citizens are empowered to assist each other outside of its control. The Haitian, Chilean, and Libyan governments do not disappear if non-state actors coordinate aid efforts during times of crisis. The empowerment of citizen networks can represent a challenge to states' authority, but it can also function in conjunction with the state. Furthermore, it by no means eliminates the state completely. State sovereignty remains intact in the face of the sophisticated information gathering, analysis, representation techniques of networked organizations.

Transition

Crisis mapping groups exemplify the cyber utopian ideal: a networked organization utilizing ICT networks in a way that clearly benefits society. However, cyber skeptics make valid points about the possible cases of misinformation and exploitation that could result from states or militant groups accessing the data. In cases of environmental and political crises, there are various challenges to utilizing the Ushahidi platform in a way that provides valuable information without compromising the safety of the reporters. Still, citizens can use these tools during times of crisis and the data can provide humanitarian organizations with the details required to assist in relief efforts. These crisis mapping organizations represent the flexibility that networked organizations possess, and how they can at times provide certain services better than traditional hierarchical aid organizations. They can coordinate with state actors in order to provide relief, but at times they also operate in opposition to a state by the very nature of reporting on corruption or acts of brutality. They do not challenge governments directly but they provide information that is outside of state control. While citizens can use ICT networks to coordinate protests or relief efforts, states are becoming more adept at using these tools to control the information their citizens' can access. The next section will explore the role of ICT networks in facilitating censorship, and how this reinforces state authority.

Cyber Skeptic Evidence

Control

Censorship

States are continuingly becoming more aware of the ways in which ICT networks facilitate the sharing of information and collective action. Repressive regimes struggle to censor the politically inflammatory information that citizens can access through these technologies, particularly the Internet, and to discourage the use of these tools for coordinating activism. However, when states limit the proliferation of free information, they risk reducing the social and economic benefits of ICT development. This “Dictator’s Dilemma” is exemplified by the Egyptian government's decision to shut down the Internet, which hurt the country economically and did not stop the protestors. Instead of taking drastic measures to limit physical access to the Internet, states must find ways to control the information that these media carry. The Chinese government excels at controlling information, and has developed methods of using technology to censor topics they have determined as being a threat to their authority. China also influences the private companies that serve as intermediaries for ICT networks, and forces them to engage in censorship if they want to profit from Chinese economic markets. Additionally, China encourages self-censorship on the Internet in the same way that they do in the press. When all else fails, China will locate those spreading harmful information and punish them in order to stop them from voicing their dissent and to discourage others from doing so as well. Even the democratic governments of United Kingdom and the United States have sought to limit the use of ICT in order to prevent political unrest. Around the world governments are finding ways to limit information that inspires dissent. Still, even as the government manages to control information, dissidents find new technologies to resist them. States often seek to control information flows in order to influence their citizens and in certain cases, prevent political coordination. ICT networks challenge this control.

Dictator's Dilemma (Egypt)

Authoritarian regimes that seek to censor politically inflammatory information must always balance these attempts with their desire to retain the economic and social benefits of these technologies. This is referred to as the "Dictator's Dilemma" and it is often defined as: if dictators allow ICT networks to spread within their countries, it poses a threat to their respective regimes, but if they do not, their countries are socially and economically cut off from the world (Tufecki 2011). Clay Shirky argues that the phrase "the conservative dilemma," coined by media theorist Briggs, is more appropriate because it applies to leaders of democratic governments as well as leaders in business and religion (Shirky 2011). This analysis will refer to both terms.

The ICT network shutdown during the Egyptian protests of 2011 is a perfect example of this dilemma. On the morning of January 28th, desiring to prevent the further coordination of protests, the Egyptian government cut off all communication in the country (Ghonim 2012: 212). It shut down all three cellular operators, Internet services, and short messaging services (SMS) (Ghonim 2012: 212). The Egyptian government was able to shut down the Internet relatively easily because it controls the limited number of fiber-optic links to networks outside of the country, and the licensing agreements of all Internet service providers (e.g. Vodafone) precluded them from challenging a shutdown order (MacKinnon 2012: 51). However, it is argued that this had the opposite effect of what the government had intended, as more people took to the streets, some in order to just to find out what was happening (Howard, Aggarwal, Hussein 2011: 3). This shutdown implied that the government saw these ICT networks as a valuable tool for the opposition.

Clearly, it was worth any costs to stop the use of these networks, because the shut down had a significant economic impact. The Organization for Economic Co-operation and Development (OECD) reports that the shut down of Internet and mobile services resulted in direct costs of minimum 90 million USD. This amount refers to lost revenues due to blocked telecommunications and Internet services, which account for around 3-4% of Egypt's yearly GDP (""The Economic Impact of Shutting down Internet and Mobile Phone Services in Egypt"). However, this amount does not include the secondary impacts, which resulted from a loss of business in other sectors such as e-commerce, tourism, and call centers. The IT services and outsourcing sector in Egypt brought in around 1 billion USD in 2010, and it relies heavily on these networks ("The Economic Impact of Shutting down Internet and Mobile Phone Services in Egypt"). Ultimately, the protests were not deterred by the absence of the Internet. Individuals who became frustrated by the regime's tactics may have even begun to support the protestors'. The Mubarak regime did not benefit from shutting down the Internet, and instead the entire country suffered significant economic losses.

The Egyptian case is a particularly strong example of the results of the dictator's dilemma, but generally regimes do not resort to such dire measures in order to control information flows and online coordination. Egypt is a country that has had a history of more lenient censorship practices. As of 2003 the government had not taken concrete steps to control the content available on the Internet, even though it did so with other media (Kalathil and Boas 2003: 123). In fact the government's tactics were considered unusual within the region because of the enthusiasm with which it extended Internet connectivity without overt efforts at Internet censorship (Kalathil and Boas 2003: 122). Consequently, it follows that it was not prepared to control the politically inflammatory information that was being circulated online. Social media researcher Alexandra Dunn notes that: "Egypt has traditionally limited its involvement to monitoring the communications of actors, and not controlling the topography and content available in online spaces" (Dunn 2011: 16). Other countries have focused on censoring the content available on ICT networks as opposed to bluntly shutting off access. These governments have had more success in limiting the information that their citizens have access to. China is a particularly good example of a country whose government uses many tactics in order to censor dissent online, and prevent coordination.

Censorship Technology (China)

China is renowned for its "Great Firewall" which uses technology to scan data for information it wants to censor. The Chinese firewall is known to employ a Cisco "Secure Intrusion Detection System (IDS)" which means that routers examine the content of data packets to see if they match China's filtering rules. Chinese network providers do not provide the details of their firewall, but researchers at the University of Cambridge have developed a model based on their observations. The firewall operates through several steps: (1) a data packet arrives at the router and is placed into a queue; (2) the packet is passed to an IDS and the content is inspected; (3) if the packet's content is found to have one of the keywords the government has censored then the connection is reset and the packet does not arrive at its intended destination (Clayton, Murdoch and Watson 2006). Essentially, if a router finds that it is transmitting content that contains inappropriate keywords then it does not transmit that data. Because the packets containing the requested information are not successfully routed to their final destination, users cannot access the pages that rely on these connections. The Chinese system is particularly well thought out because it does not tell individuals that they are intentionally being blocked from certain information (MacKinnon 2012: 35). There is no screen that says "Blocked by the Chinese State," but rather users will encounter a "site not found" page, a network time out screen, or a page describing an HTTP error code, such as 404 which signifies page is missing (Goldsmith and Wu 206: 94). This makes it challenging for users and researchers to determine whether the page is unreachable because of censors, or just technical difficulties. Citizens are not sure if the government prevented them from accessing a site, or if it truly was the wrong link to a page.

China is able to control the information its citizens' access by inserting censorship technologies into the network, and so the country smoothly navigates the dictator's dilemma. People can still access the Internet and so the social and economic benefits are preserved, and yet the government is able to prevent inflammatory content from encouraging dissent. These technologies are actually created by western firms, such as Cisco, which has inspired controversy in their corporate home countries as well as human rights groups around the world (MacKinnon 2012: 169). These technologies were created in the early 1990s and were originally meant for American corporations that wanted to filter employee access to the Internet. The original purpose of these filtering technologies was to allow employees to use the Internet for work, but prevent them from accessing leisure sites like ESPN (Goldsmith and Wu 2006: 94). However, the company successfully marketed its technologies to the Chinese as a tool for censorship. This is only one case of a private company choosing profits over a democratic political agenda, but there are many others that have surfaced as well.

Intermediary Control (China)

The physical routers, servers, and fiber optic cables that carry the Internet have geographical locations within government jurisdictions, and the companies that run them are subject to the governments' laws (Nye 2011: 128). Similarly, the companies that provide Internet services are still subject to the laws of the territory within which they operate, even if they are based in a different country. The Chinese government excels at encouraging these intermediaries to censor information. Private companies are allowed to operate in China as long as they submit to the regime's demands. The government pressures companies that provide Internet services, such as Google, and this determines how these intermediaries interact with providers or consumers of information content (Goldsmith and Wu 2006: 85).

In 2010 the company Google decided to stop its local operations in China after the leadership felt they could no longer offer their services without becoming a tool of the repressive regime. Google claimed that the Chinese government was hacking into its servers in order to access the accounts of political dissidents (BBC News 2011). The company had agreed to censor its results, despite its motto of "don't be evil," because the provision of some search engine services was thought to be better for civil liberties than a complete withdrawal from the country (BBC News 2011). The company did withdraw as a result of the intrusions on the Gmail accounts of human rights activists (Gaudin 2010). However, commentators have noted that this may have been in the company's self interest since it was second in the market to the native Chinese search engine Baidu (MacKinnon 2012: 177). Still, political scientist Rebecca MacKinnon argues that the decision "was also a statement about Google's relationships with governments and citizens worldwide, and about the entire Internet's future. Google made a decision that was both good for Internet freedom and in its long-term self-interest" (MacKinnon 2012: 177). In the past, a similar controversy arose when the Chinese government convinced Yahoo to hand over information about dissidents who were using the site (MacKinnon 2012: 133). Both search engines had at one point cooperated with the Chinese government to filter search results in accordance with the country's laws.

In this way, influencing intermediaries is another way in which China exerts control over the information that its citizens have access to. Rather than denying these companies the right to operate in China, the government forces them to cooperate with its regime of censorship. While the companies have the option of pulling out entirely, the allure of China's huge markets is difficult to resist, and companies often end up cooperating with the government. However, Google did decide to leave the country, and sacrifice the profits it would have gained from this market. Still, Rebecca MacKinnon argues that Western companies and financiers have helped to legitimize a political innovation that she calls "networked authoritarianism" in which corporate networks are turned into an extension of government power (MacKinnon 2012: xxii).

Self-Censorship (China)

The Chinese government excels at inspiring companies to engage in self-censorship, and it uses this tactic on media outlets, and the public at large. They promote this self-censorship through regulation, policing and punitive action (Kalathil and Boas 2003: 26). Chinese officials will make it very clear what topics they do not want the media to discuss, and then punish those who do not listen by denying them access to information, or pursuing the reporters in the courts and imprisoning them (Kalathil and Boas 2003: 141). The public punishment of dissidents is an authoritarian tactic to discourage others from expressing views critical of the government. However, authorities can reach a tacit understanding with private companies about what behavior is and is not acceptable (Kalathil and Boas 2003: 147). Even citizens understand the boundaries of acceptable Internet use, and officials can exploit this to create an environment where comprehensive censorship is not necessary (Kalathil and Boas 2003: 141). China excels at the use of these "soft" control methods, and focuses on controlling the information on ICT networks as opposed to limiting access.

Liberal Regime Censorship (United States)

The decision of whether or not to censor or shutdown ICT networks is not limited to authoritarian regimes. Many liberal democracies choose to censor different types of content, for instance, on the Internet, the United States government polices pornography that includes children and imposes harsh penalties on individuals who view or transmit it. Additionally, in the United States there has been at least one case where government officials decided to limit communications with the intent of dissuading the coordination of protests. On July 3rd, 2011 a homeless man in California was killed by Bay Area Rapid Transit (BART) officers, inciting protests by local community members (Silverman 2011). These protests were often located at train stations, and BART officials reported that when protesters gathered at the Civic Center Station in San Francisco on July 11th they blocked train doorways and held train doors open which made it necessary for other stations to be shut down (Silverman 2011).

As a result, when BART officials heard that another set of protests were being coordinated through the use of mobile devices for August 11th, they made the decision to shut down power to cellular towers stretching from downtown to the San Francisco (Collins 2011). This action was meant to prevent potential protestors from using social media to help others avoid police while demonstrating (Silverman 2011). The Deputy Police Chief Benson Fairow stated that: "It all boils down to the safety of the public…It wasn't a decision made lightly. This wasn't about free speech. It was about safety" (Collins 2011). However, some civil society organizations, such as the Electronic Frontier Foundation, compared the shutdown to the actions of the Mubarak Regime in Egypt during the protests of January 2011. A staff attorney at the Northern Californian American Civil Liberties Union wrote that: "The government shouldn't be in the business of cutting off the free flow of information. Shutting down access to mobile phones is the wrong response to political protests, whether it's halfway around the world or right here in San Francisco" (Collins 2011).

When BART officials released a statement on August 20th, they implied that they were allowed to employ prior restraint in order to prevent conduct that could be harmful to commuters. However, the communication between protestors was not itself responsible for generating a threat, and critics argue that the limiting of communication for the sake of preventing protests is akin to a violation of free speech (Silverman 2011). First Amendment Center Director Gene Policinski argues that while there is no constitutional right to use a cell phone, and while restricting them does not inherently challenge free speech, it would not be appropriate if the government were to seize printing presses in order to prevent editorials that incited violence, nor is it appropriate in the case of these new technologies (Silverman 2011). The United States is still establishing its own laws on when the government can lawfully limit ICT networks.

Liberal Regime Censorship (United Kingdom)

In the United Kingdom government officials have also questioned whether it is acceptable to limit the use of ICT networks during times of political instability. During the riots in early August of 2011, mobile phones, social media sites, and other new technologies were used as tools to assist in the coordination of the riots. British Police say small groups of youths used text messages, instant messaging on their phones, and social media platforms such as Twitter to coordinate their attacks and stay ahead of authorities (Yelaja 2011). A government panel interviewed thousands of people affected by the riots and concluded that: "From the evidence around the August riots and from what people have subsequently told us, it seems clear to us that the spread of rioting was made worse both by televised images of police apparently watching people cause damage and loot at will, and by the ability of social media to bring together people determined to act collectively" (Halliday 2011). In the aftermath of the riots, Prime Minister David

Cameron went as far as to question whether it would be acceptable for the government to ban people from using Twitter, Facebook, or their BlackBerrys when they know that they are planning to commit acts of violence, disorder, or criminality (Sabbagh 2011).

The security firm Unisys surveyed 973 adults, and found that 70 percent of all respondents said they "completely agree" or "somewhat agree" that during outbreaks of civil unrest, social media sites and Blackberry services should be temporarily shutdown to prevent coordinated criminal activity (Whittaker 2011). However, among 18 to 24-year-olds there was greater resistance to online measures. Ultimately, the U.K. Home Secretary Teresa May met with several Internet companies, and announced afterward that the government has "no intention of restricting Internet services" but would instead focus on how social media could be used constructively during times of crisis (~McMillan 2011). In advance of this meeting, Facebook and Twitter had made it clear that they "strongly warn the government against introducing emergency measures that could usher in a new form of online censorship" (Halliday 2011).

In the United Kingdom a group of citizens have also used social media to identify those who participated in the riots after the fact. A Google Group called "London Riots Facial Recognition" uses facial recognition technologies to identify looters who appear in online photos (Perez 2011). They post pictures on a website where other people can look at them, and write the name of the individual. If enough people identify the photo as a particular person, the police will be notified. In the aftermath of the riots, social media was also used to coordinate clean up efforts (Yelaja 2011). Still, the question of whether or not it is acceptable to limit communication and public coordination for the sake of convenience is one that relates to authoritarian and democratic regimes alike.

Circumvention Tools

Even as governments are able to gain greater control over the Internet, citizens find new means of evading censorship. In the aftermath of the Tsunami in Japan, Clever Industries, LLC provided an emergency communication app that allowed communications to occur despite the fact that communication towers were blown away (Redmond 2 March 2012). This technology creates peer-to-peer mesh networks instantly, and enables users to evade government censorship. Another technology for censorship circumvention called Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet ("Tor: Overview"). It allows users to prevent users from tracking them or to connect to sites or messaging services that are blocked by local ISPs ("Tor: Overview"). It does this by connecting a user to several intermediate "proxy" nodes in a network, in order to hide the origin of a request for data (Morozov 2011: 169). Cyber utopians stress that state censors can be overcome through the development of better circumvention techniques.

These circumvention technologies must be fully vetted before individuals rely on them. The software Haystack was widely celebrated by the media and even the U.S. State Department as being a valuable tool for censorship circumvention (Kang 2010). However, it was ultimately revealed that the program had serious flaws that could result in users being identified by the authoritarian regimes they were attempting to evade (Kang 2010). As people find ways to connect their technologies to each other as opposed to private intermediaries that can be influenced by the government, there will be a greater possibility for networked communication that resists government control. However, cyber skeptics argue that these technologies of resistance can have negative consequences if they are hacked and manipulated by state authorities. Security is incredibly important for circumvention tools, and if they are not safe, then users can be putting themselves in danger despite their going out of their way to avoid it.

Cyber Utopian Perspective

Cyber utopians point out that the government cannot be everywhere at once, and that the amount of content on the Internet is in itself a defense against absolute censorship. The Egyptian government's shut down of the Internet was not successful, and it caused significant economic damage proving that the "dictator's dilemma" is relatively accurate. States may choose to limit ICT networks and work with private intermediaries to exert their control, but that will not prevent new applications and programs from being created. Social media researcher Alexandra Dunn notes that:

> "Barring a major trend reversal, the technological know-how of activists—in the tactical use of circumvention and anonymity technology—will outpace that of the government. This cat-and-mouse game will require governments wishing to quarantine political communication to scale up the direct force of media interference from precise filtration and monitoring of content to full quarantine and shutdown of media infrastructures" (Dunn 2011: 16).

Cyber utopians are betting that ICT network users will continue to find new techniques of resisting state control faster than the state can find ways to impose it.

Cyber Skeptic Perspective

Cyber skeptics highlight that while the dictator's dilemma dissuades governments from limiting Internet access, it does not prevent them from doing so. Evgeny Morozov notes that a crucial assumption behind the dictator's dilemma is that it would be impossible to design precise censorship mechanisms that could block openly political

Internet activity but allow Internet activity that facilitates economic growth (Morozov 2011: 169). He argues that this assumption has been proven false, as governments are able to filter content based on keywords and block access to websites based on the URLs and even the text of their pages (Morozov 2011: 169). The firewall in China illustrates how the government can prevent users from accessing politically inflammatory content, and yet have no impact on the rest of their Internet experience.

Cyber skeptics also stress how democratic governments that insist on Internet Freedom are still determining whether there are cases in which they too would limit ICT access. In the United States and the United Kingdom the government has considered the possibility of limiting ICT networks during times of upheaval. California BART platform officials actually chose to do so. Furthermore, while there are technologies aimed at preventing users' privacy on the Internet, people often believe that they are more secure than they truly are. For instance, the program Tor guarantees the anonymity of those that use its proxy network. However, if the data transferred is unencrypted, it is possible to view the content being transferred and infer who the sender is. Morozov notes that Swedish researcher Dan Egerstad was able to read government documents, diplomatic cables, and intelligence estimates that were transferred through Tor because they were not encrypted, and then determine exactly who sent them (Morozov 2011: 170). In the case of the Haystack software, citizens were nearly put at risk because of the over zealous support of a product that had not been fully vetted. Cyber skeptics note that the very same circumvention tools that can help citizens, can also pose a threat to them if they are not used properly.

Integrated Perspective

ICT networks support the Internet that many users obtain information from. Social media sites on the Internet allow citizens to access and share information across borders in real-time, without the government or traditional media organizations serving as an intermediary. If one employs the liberal definition of sovereignty – that sovereignty is defined by the states' ability to control actors and activities within and across its borders (Thomson 1995: 213) – then ICT networks are in fact challenging state sovereignty by dispersing the "gates" where governments can exert control over information, and establishing a public sphere that facilitates the expression of dissent and collective action. However, states are developing methods to censor information at various points within the network. There are specific technologies that can prevent the transmission of politically inflammatory content. While traditional media institutions do not determine what information is produced and distributed en masse on the Internet, governments can now influence the private companies that serve as intermediaries between citizens and Internet services.

Ultimately, states are increasing their ability to limit information, and thereby inhibit its potential political impact. The diffusion of information production has not resulted in a challenge to the supremacy of a state's authority within its borders. While the dictator or conservative's dilemma is alive and well, different regimes manage these challenges to control through a variety of tactics. Those governments that choose to shut down ICT networks completely do seem to face economic costs (Egypt), and in liberal democracies, face social costs (United States and United Kingdom). However, other regimes are able to encourage ICT use for economic and apolitical social purposes while discouraging dissent (China). In these cases, the state clearly does not cease to be considered the supreme governing structure within its territorial boundaries. Certain regimes may be ousted from power (Egypt), but none of the governments disappear. States are reestablishing their control over information, and reasserting their authority State sovereignty remains intact in the face of the diffused information proliferation facilitated by ICT networks.

Transition

Internet circumvention technologies pose a challenge to state censorship tactics, but there are still flaws with the various tools being used. China has proven to be able to implement a firewall that limits the majority of its citizens' access to politically inflammatory material. The government also uses soft control by implicitly threatening private companies that do not go along with their demands. Furthermore, officials encourage self-censorship by releasing regulations that make it clear what topics citizens are expected to avoid and the punishment that will occur if they do not. China is an example of a country that is successfully navigating the "dictator's dilemma," and has avoided the need for national-scale shutdowns of its ICT networks. Egypt, however, has a history of limiting ICT users as opposed to the information that is transmitted on networks. This likely played a role in the governments' need to shut down all communications in order to limit citizens' access to politically inflammatory information during the protests of January 2011. Even democratic regimes, such as the United Kingdom and the United states, need to determine if there are situations in which they are willing to limit ICT networks. Some governments are successfully subjugating ICT networks to their control while others are still struggling to find methods that balance their reliance on these new technologies with maintaining authority within their borders. States are able to use ICT networks to produce information that represents their perspective just as they are able to censor it. The next section will explore the role of ICT networks in increasing states' influence domestically and abroad.

Influence

Governments can use social media in order to express their viewpoints, and to influence both their own citizens and those abroad. The government in Bahrain used social media to inspire citizens to identify protestors and to target these protestors for humiliation. In China, the government not only expresses itself through official pages dedicated to spreading information about the regime, it also reportedly hires citizens to blog about positive aspects of the government. The United States has launched an extensive campaign to use social media to expand its influence abroad. The 21st Century Statecraft initiative launched by the United States focuses on using tools such as Twitter and Facebook to engage with foreign publics in a new form of diplomacy. In general, there is a shift in how diplomacy is being conducted as foreign populations can interact directly on the Internet without their government's involvement. The concept of citizen diplomacy, or individuals representing their country through their actions abroad, has been accepted by the U.S. State Department. Cyber utopians see this increased communication between citizens and governments as a positive encouragement of civic discourse. However, cyber skeptics emphasize that these techniques allow states to enhance their influence through the use of ICT networks, strengthening their influence as opposed to diminishing it. The Internet and social networking sites tie people together across boundaries. However, people are still tied closer together within their countries than to people outside, and governments can still shape how people interact within their borders. States are able to use ICT networks to expand their influence at home and abroad.

Propaganda (Bahrain)

In February of 2011, a series of prodemocracy demonstrations took place in Bahrain inspired by the revolutions in Tunisia and Egypt (MacKinnon 2012: 62). The Shi'ite majority that composes about 70% of Bahrain's population demanded more equality and representation in government from the Sunni minority that controls most of the government (Wellman 2011). A month later the Sunni regime organized a bloody crack down on the protestors. The government detained approximately 600 individuals, and it is estimated that security forces killed around 30 protestors (MacKinnon 2012: 62). ICT networks, specifically the Internet and mobile phones, were used to coordinate protests. The social networking site, Facebook, was also used as a tool for coordination, and videos taken of these protests, such as those at the Pearl Roundabout traffic circle in Manama, the capital of Bahrain, were posted on sites like YouTube (Wellman 2011). However, the Bahraini government also found uses for these social media tools, and used shared photos, videos, and posts on these Web sites to identify protestors and retaliate against them.

An Al Jazeera English featured documentary on the Bahraini protests describes how the government launched Facebook campaigns to encourage ordinary citizens to post the name and workplace of people who had participated in protests, and were therefore "traitors" (*Shouting in the Dark* 2011). These lists of names were then tracked down, and when the government arrested someone, it was reported on Facebook. It is said that the trend of using evidence gathered from social media began on the state television where the media criticized football players who had participated in protests (*Shouting in the Dark* 2011). Ultimately many sports professionals were detained for their pro-democratic actions. One Bahraini describes further negative consequences of social media use: "I’m working with students who got expelled - over 100 in different institutes, who were all expelled and had their scholarships pulled for Facebook updates and Blackberry [smartphone] messages. Most of these Facebook statuses were screenshots taken from their friends and handed in to the investigative committees” (Wellman 2011).

Government supporters would even create pages dedicated to the defamation of particular protestors and many citizens did choose to lend their voices to insulting or demeaning these "traitors" (MacKinnon 2012: 63). One particular Facebook campaign focused on a girl whose reading of a dissident poem had been captured on video and posted online. On a Facebook page the government encouraged people to demand that she be arrested and tortured, and eventually she was in fact detained (*Shouting in the Dark* 2011). In this way, governments can also use the coordinating power of the Internet against individuals and targets that they choose. This is a clear example of how states can use social media to expand their influence. While the Internet can be a tool for dissent and activism, it can just as easily be a tool for state propaganda, just like television, radio, or other media.

Public Representation (China)

In China, the government makes active use of social media as a tool for spreading official messages. The government not only censors content on blogs or Internet forums, it actually creates content. In China, bloggers are hired to post favorable comments about the regime and its actions. The “50-cent” party is a group of online commentators dedicated to improving Chinese public relations through social media sites (Bristow

2008). Its name stems from the fact that commentators are reportedly paid 50 cents per positive post (Bristow 2008). In one case a bureau commentator noticed a disgruntled citizen's post about the police, and coordinated counter-messages by 120 government supporters. There are reports that the Chinese government is setting up special centers dedicated to training commentators in these kind of spin doctor tactics (Bristow 2008).

Cyber skeptic Evgeny Morozov discusses how the Chinese government countered online criticism that followed the death of a prisoner (Morozov 2011: 118). In 2009, Li Qiaoming, a twenty-four-year old peasant living near Yuxi City was arrested for illegal logging. He was reportedly killed by fellow inmates, but over 70,000 commentators wrote about the event on the site QQ.com and many accused the Chinese police of a cover up (Morozov 2011: 118). The government responded by reaching out to Chinese Internet users and asking them to become "Netizen investigators," and out of the thousands that applied, 15 individuals were selected. This commission was not allowed to view any evidence, and could not create a conclusive report, and as a public relations tactic police released a formal statement apologizing to the victim's parents for allowing their son to be beaten to death by inmates (Morozov 2011: 118). It was later discovered that these investigators were all employees of state owned media, but it was still a clever tactic to alleviate tensions online. A senior official with Yunnan's propaganda department stated that: "A matter of Internet public opinion must be solved by Internet methods" (Morozov 2011: 119). The Chinese government is skilled at using social media to influence its citizens. While governments may use the Internet to address the concerns of their citizens, they may simultaneously encourage the widespread acceptance of their perspective.

Online Presence

Other governments are using the Internet and social media to create an online presence as well. In Egypt many state institutions have Facebook pages that present information about the government, and provide a place for updates or direct messages to the public. For example, even the Supreme Council of the Armed Forces of Egypt has a presence on Facebook (Irizarry-Gerould 29 February 2012). Certain official institutions in Tunisia also use social media (Jemmali 29 February 2012). The United States has made sure that its embassies have Facebook pages, and has used tools such as YouTube to coordinate conferences that encourage conversation between young tech-savvy media users from several different countries (Carlson 16 March 2012). It is not the only country that has recognized the importance of representing official institutions on Facebook. However, in the following paragraphs it will be made apparent the United States is notable in its attempt to influence both domestic and foreign populations through social media.

Public Diplomacy (United States)

In recent years, the State Department (SD) of the United States has decided to integrate social media into its tools for engaging the publics of foreign nations. The State Department calls this "21st Century Statecraft" and defines it as "The complementing of traditional foreign policy tools with newly innovated and adapted instruments of statecraft that fully leverage the networks, technologies, and demographics of our interconnected world" (U.S. SD Website). The State Department believes that the three fundamental networks of international relations – trade, communications, and mass media – all operate through the Internet, resulting in a "triple paradigm shift converging on a common infrastructure " (U.S. SD Website). The State Department's initiative focuses on encouraging Internet freedom, a vibrant civil society, and innovation within government institutions. Officials recognize that diplomacy is no longer conducted through government to government channels, but also through government to people channels – as in public diplomacy – and people to people channels – as in citizen diplomacy (Ross and Posner 2010).

The State Department has organized certain programs such as international technology delegations, Haiti relief coordination, mobile banking, an Apps for Africa competition, and many others (U.S. SD Website). In addition to hosting information on Twitter and Facebook, the State Department has even coordinated real-time conversations between Secretary of State Hillary Clinton and activists in other regions of the world, such as the Middle East (Carlson 16 March 2012). These technologies allow the State Department to receive feedback from other parts of the world, and get an idea of what people think about the United States. However, a senior State Department official cautions that while social media is a valuable tool: "It is important to not forget the one on one element, or the last three feet. Diplomacy is meant to bridge the last three feet between a person facing a person, and digital technology is one way to bridge that distance, but every interaction matters" (U.S. State Department Official 28 March 2012).

Social media allows for the rapid exchange of ideas between the US and foreign publics, but it does not replace actual person-to-person contact, just facilitates it. That being said, this form of technology-leveraged diplomacy allows states to have a direct influence on the hearts and minds of foreign publics. U.S. SD Senior Advisor for Innovation Alec Ross states that: “If you think about the traditional way in which communications used to take place – government to government, pinstripe suit diplomat to pinstripe suit diplomat – social media has completely disrupted that and done so for the better. Look at the State Department: there are several hundred social media accounts, that publish on a dozen different platforms” (Ross 5 April 2012). He adds that as a diplomat, this has given him the ability to communicate in real time, largely un-intermediated. Indeed the concept of public diplomacy as a whole demonstrates how states now have the ability to interact directly with foreign publics without their government’s involvement.

Citizen Diplomacy (United States)

On the Internet, citizens can also interact directly with each other without going through government channels. The reputation of a country and its culture will be defined abroad by these interactions, and consequently the government has an investment in making sure citizens represent them in a positive light. Communications scholar Majid Tehranian notes that people or citizen diplomacy is a bottom-up process, in which ordinary people can represent their country and have an impact on political relationships (Tehranian 1997). He argues that improving global transportation and communication have made it possible for citizens to engage in the diplomatic “game” that was historically reserved for foreign policy experts (Tehranian 1997). Former Ambassador and State Department Official Brian Carlson explains that the term citizen diplomacy has been around for about 25 years (Carlson 16 March 2012). There is an Office of Citizen

Exchanges that is dedicated to encouraging Americans to go abroad and interact with citizens of other countries. They facilitate American speakers appearing in events at foreign conferences, and establish relationships between American and foreign universities (Carlson 16 March 2012).

In November of 2010, The U.S. State Department Office of Public Diplomacy & Public Affairs partnered with the U.S. Center for Citizen Diplomacy in order to host the U.S. Summit & Initiative for Global Citizen Diplomacy in Washington DC. The author of this paper attended this conference and this paragraph includes her views informed by that experience. The topics of discussion ranged from how to best encourage youth service to the role of citizen diplomats in improving global health. In the "Policy Recommendations to Facilitate the Use of New Media in Citizen Diplomacy" panel, the discussion centered around how involved governments should be in encouraging or limiting new media as a tool of citizen diplomacy. The consensus appeared to be that governments should not repress the use of these technologies, and they can even encourage them to a mild extent, but, mainly, the citizens must determine how these technologies should be used. Another panel, "Recommended Tools for Facilitating the Use of New Media in Citizen Diplomacy" focused more narrowly on specific technology based services, and provided compelling examples of how these new services could be used to increase interconnectivity (e.g. youth video exchanges, online translation services, mobile phone chat-rooms). This conference demonstrates the U.S. State Department's dedication to facilitating citizen diplomacy. In this way, the U.S. government can expand its influence by creating frameworks for interaction that present Americans in a positive light.

Cyber Skeptic Perspective

Cyber utopians often that argue that the Internet will provide a space for communication that will challenge state authority, but they often do not account for how the regimes will use this same space. There is a false assumption that states cannot manipulate information online, but propaganda can be spread through social media and websites just as it can be spread through television, radio, and other mediums. The situation in Bahrain demonstrates that states can actually expand their influence online, and encourage coordination that supports their goals. The 50-cent party in China demonstrates how states can find innovative tactics for alleviating pressures caused by online dissent. This example contrasts with the one mentioned in the information section of this paper, where a Chinese government officially apologized in order to quell citizens' anger over the mishandling of information about a train crash.

While public and citizen diplomacy enable greater cross-border communication, these efforts are still coordinated by state actors with a vested interest in the outcome. The United States may encourage peaceful interactions between citizens throughout the world, but it has a specific agenda in doing so, and seeks to represent itself in a positive light. Furthermore, the political scientist Rebecca MacKinnon points out that the U.S. State Department cannot escape from the contradictions between its Internet freedom policies and their pursuit of national security, counterterrorism, trade, and copyright interests (MacKinnon 2012: 195). The U.S. government may emphasize democracy and human rights, but ultimately, they too are seeking to create borders on ICT networks. Cyber skeptics argue that the Internet and social media can be used for propaganda purposes and that they support a state's authority and ability to control information.

Cyber Utopian Perspective

The cyber utopians focus on how the information on ICT networks can be used to challenge regimes, and often overlook how they can expand states' use of those same technologies. Still, the concepts of public diplomacy and citizen diplomacy do challenge the typical hierarchy of states that used to rely solely on formal diplomatic communications. While diplomacy used to be the realm of diplomats and ambassadors, the proliferation of ICT has resulted in the state having an increased ability to communicate directly with the populations of different countries. International relations scholar Joseph Nye argues that: "For States to succeed in the networked world of the new public diplomacy, they are going to have to learn to relinquish a good deal of their control, and this runs the risk that nongovernmental civil society actors are not aligned in their goals with government policies or even objectives" (Nye 2011: 108). Essentially, while entities such as the U.S. State Department may create initiatives, host events, or sponsor like-minded organizations, public diplomacy and citizen diplomacy still occur with less government intermediation and control.

Nye argues that public diplomacy can encourage the expression of dissent from abroad which rather than detracting from a regime, can increase the credibility of its message. A society that can tolerate dissent may seem more attractive, and this image can benefit a state (Nye 2011: 108). ICT networks can be used to challenge the authority of particular regimes, and external sources of information can undercut a regime (Steele and Stein 2002: 36). The U.S. SD's use of social media to communicate with foreign publics without government intervention could pose a challenge to authoritarian regimes. In the last century broadcasting technologies were used for this same purpose (Steele and Stein 2002: 36).

Integrated Perspective

ICT networks support the Internet that many users obtain information from. Social media sites on the Internet allow citizens to access and share information across borders in real-time, without the government or traditional media organizations serving as an intermediary. If one employs the liberal definition of sovereignty – that sovereignty is defined by the states' ability to control actors and activities within and across its borders (Thomson 1995: 213) – then ICT networks are in fact challenging state sovereignty by dispersing the "gates" where governments can exert control over information, and establishing a public sphere that facilitates the expression of dissent and collective action. However, states are also capable of using these tools to spread their own perspective and expand their influence. States can use social media to create a presence online, and to interact with citizens in a new way. States can use ICT networks to better interact with foreign publics without their governments serving as an intermediary.

Ultimately, states are increasing their ability to spread their own perspective, and thereby influence their citizens and those in other countries. The diffusion of information production has not resulted in a challenge to the supremacy of a state's authority within its borders. States can even increase their authority by encouraging citizens to believe what their government tells them, and to act in ways that their government condones. States can encourage citizens to report on each other through ICT networks, and therefore utilize their citizens as a tool for implementing national rules. Some governments use ICT networks to convince citizens to report on and demean dissidents (Bahrain), while others focus on diffusing dissent (China) or explaining their viewpoint to foreign publics (U.S.). In these cases, the state clearly does not cease to be considered the supreme governing structure within its territorial boundaries. Certain regimes may face challenges to their accounts of events, but these can be addressed or dismissed, and states can counter with new tactics for manipulating public perception (China). States are using ICT networks to expand their influence domestically or abroad, and reasserting their authority. State sovereignty remains intact in the face of the diffused information proliferation facilitated by ICT networks.

Transition

The Internet and social networking sites allow people to communicate across national boundaries. Citizens can interact with each other without their governments' involvement or even their awareness, and establish relationships independent of their nationality. Consequently, states seeking to expand their influence can do so by creating environments that facilitate positive relationships, which will then reflect favorably upon the government. Governments can influence how their citizens interact by creating official channels, even if they cannot constantly monitor all of their exchanges. Additionally, states can directly influence their citizens' behavior and expand their influence by using the Internet as a tool for disseminating their own perspective. In Bahrain the government used social media to convince its citizens to report on dissidents, and also targeted them with humiliating smear campaigns. In China, the government engages in advanced public relations manipulation and actually hires online commentators to better represent its perspective on the Internet.

Consequently, it is clear that information on ICT networks does not inherently challenge state authority, because the same tools that can be used against the state can be used to spread the state's message. States can use the Internet and social media to expand their influence domestically and abroad. The next section will explore the role of ICT networks in increasing states' military and coordination capabilities.

Force

As states are increasing their reliance on ICT, and integrating them into their economic and social infrastructure, vulnerabilities in digital networks can become an excellent target for attacks by adversary states. The Internet was not created with security in mind, because the individuals who defined its use saw it as a depoliticized zone where the free flow of information would enable greater sharing and learning around the world. However, this lack of security has resulted in states being able to use ICT networks as a means for attack. The Stuxnet worm in Iran exemplifies how ICT networks can serve as a medium for the transmission of coded “cyber attacks”, and demonstrates that these attacks can have physical consequences that may even threaten states' other military capabilities. Furthermore, states can use the coordinating power of the Internet to their benefit if they can incite citizens to commit nationalistic acts of aggression. In the case of the Estonian Cyber riots of 2007, the Russian government was suspected of assisting its citizens in the coordination of attacks against Estonian networks as a sign of political protest. Furthermore, in 2008, Russian citizens used cyber attacks to support the nations’ physical military campaign against Georgia. Conflict waged through ICT networks contradicts the ideals held by cyber utopians, although citizens do coordinate with each other to launch patriotic cyber attacks. Cyber skeptics note that as states seek to defend themselves against attacks in cyberspace, they subjugate the Internet to their territorial sovereignty and limit the free flow of information. In their view, cyberspace is entering a Westphalian Age, where states boundaries and domains of control are as clearly defined as they are in real life. States can use ICT networks to increase their military capabilities, and inspire citizens to act in a way that supports their interests.

Internet Security

The Internet was not created to be a secure network, but instead a platform that facilitated the sharing of information (Nye 2010: 5). Consequently, private and public enterprises that have sought to use the Internet to expand their operations found that they must innovate new security measures. The Internet suffers from glaring security problems that can result in vulnerabilities for sites that are not properly secured. There are three main challenges to Internet security: base security of Unix system, local network security and security of Internet connections ("Internet Security"). The Unix operating system was designed by programmers for use by other programmers, and host security relies on proper system configuration by the administrator. If the accounts on the system are compromised, or if hosts that connect to the system are compromised, this can affect the security of the entire network ("Internet Security"). However, there are technologies dedicated to alleviating these security concerns, such as firewalls.

Firewalls can determine what actions will be permitted or restricted on a network, and provide more advanced authentication techniques. Firewalls can also filter packets that pass through a router based on information like source or destination IP address. Last, firewalls can filter connections through software applications in order to support remote connection services such as TELNET, or file transfer services such as FTP ("Internet Security"). These technologies can address security vulnerabilities in the Internet, but they can also be used by states to filter information on the Internet. IP addresses can be traced to their source in order to find hackers or cyber criminals, but they can also be used to find dissidents. Using techniques such as deep packet inspection

(DPI) can be helpful for ISPs interested in preventing the spread of viruses or the transfer of illegal material, but it also means that these companies have access to the information that is transferred through their networks, infringing on users privacy (Wawro 2012). This technique is used in China to censor information on sites like YouTube (Wawro 2012). The previous paragraphs only begin to discuss the complexities of Internet security, but the main takeaway is that the same tools that can be used to increase Internet security can be used for censorship and repression.

Key Terms

In recent years, states have found they are vulnerable to attack through ICT networks. States face threats that are common to all ICT users, but they also are the targets of sophisticated programs that can be designed to harm one specific country. In order to discuss case studies of cyber attacks it is useful to establish certain definitions. A Hacker is an individual with knowledge of computer security that tends to specialize in either exploiting vulnerabilities, or finding ways to prevent them, depending on whether they are motivated by self-interest. Arguably, the term cracker better describes hackers that are dedicated to exploiting vulnerabilities, since the term hacker has now come to mean any dedicated programmer. Often, the term hacker refers to malicious actors ("Internet & Cyber Crime Terms and Definitions"). Software that runs automated tasks over the Internet is referred to as an Internet bot, and malware is software that is designed to infiltrate or damage a computer system without the owner's knowledge ("Internet & Cyber Crime Terms and Definitions"). A zombie computer is a computer attached to the Internet that has been compromised by a hacker, computer virus, or Trojan horse, and a botnet is a large collection Internet bots that run on these zombie computers ("Internet & Cyber Crime Terms and Definitions").

These botnets can be used to perform malicious tasks under remote direction, such as launch distributed denial-of-service (DDoS) attacks which overload routers with requests for information causing them to crash or making it impossible for valid requests to be answered in a timely manner (Mueller 2010: 23). A computer virus is a program that can copy itself and infect a computer without the permission or knowledge of the user, while a computer worm is different in that it does not need attach itself to an existing program, and instead uses networks to send copies of itself to other computers often causing damage in the process ("Internet & Cyber Crime Terms and Definitions"). States and individuals can purchase botnets on the Internet and access them remotely as a source of computing power (Dam, Lin, and Owens 2009: 222). States can rely on multiple tactics when seeking to use the Internet as a weapon.

Stuxnet Worm

In June of 2010 American cyber security experts discovered a computer worm named "Stuxnet" ("The Meaning of Stuxnet" 2010). It is the first malware known to target and infiltrate industrial supervisory control and data acquisition (SCADA) software that is used to run chemical plants, factories electric power plants, and transmission systems worldwide (Clayton 2010). This malware was found to have infiltrated an Iranian nuclear facility at Natanz, but it also infected 60,000 computers total including those in India, Indonesia, China, Azerbaijan, the United Kingdom, and the United States among others (Farwell and Rohozinski 2011: 23). It caused the motors for the nuclear centrifuges to switch between high and low speed intervals which damaged the machines, and even tampered with the system reporting mechanisms in order to conceal that any change had taken place (Farwell and Rohozinski 2011: 24). This meant that although the centrifuges were being forced to malfunction, the computers that monitored these machines reported that they were operating perfectly, and it took visual reports for the malfunctioning centrifuges to be discovered.

Stuxnet is a sophisticated program that is designed to penetrate and exert control over remote systems autonomously (Farwell and Rohozinski 2011: 23). Iran's nuclear facility was "air gapped," or not connected to the public Internet, and so the worm was introduced by unsuspecting employees using infected USB drives (Farwell and Rohozinski 2011: 23). The Stuxnet worm had the ability to "fingerprint" the computer system it infiltrates, meaning that it is meant for one particular system, in this case the Iranian plant (Clayton 2010). The perpetrator is assumed to be a state because of the level of complexity required to investigate and fully understand the specific SCADA infrastructure being used in Iran (Clayton 2010). However, at this point it is not clear which state actually conducted the attack, although Israel is considered the unofficial culprit (Zetter 2011). The Stuxnet attack exemplifies how states are using the Internet to expand their military capabilities, and use the medium for attacks. These actions directly conflict with the intent of the founders of the Internet, and provide support for a cyber skeptic view of the proliferation of ICT networks.

Cyber Riots (Estonia)

In 2007, the Estonian government wanted to relocate a Soviet era statue depicting an unknown soldier of the Great Patriotic War, despite the protests of the country's ethnic Russian population (Bronk 2008: 132). Public interest in the story grew, and it became a rallying point for the citizens of Russia as well as the Estonian Russians. The Russian government propagated anti-Estonia messages on the state-controlled media in order to incite further agitation among its citizens (Mueller 2010: 23). After the statue was moved Russian-language Internet forums and blogs lit up with angry discussions, some of which outlined potential Estonian Internet targets and provided instructions on how attack them (Mueller 2010: 23). Russian citizens then launched a cyber attack on Estonian banks, media outlets, and other services providers (Swaine 2008).

The Russians used botnets coordinated through the black market, and orchestrated a series of DDoS attacks that crippled the Estonian cyber infrastructure for 3 weeks (Swaine 2008). What was remarkable about these attacks is that they were later found to have been orchestrated by Russian citizens who were interested in punishing the Estonian government for nationalist reasons, rather than the Russian government directly (Schmitt 2010: 151). The IP addresses of several attacks were traced to Russian government institutions, and it is believed that officials played a role in encouraging the attacks, but there is no evidence that the government formally coordinated citizens' actions (Schmitt 2010: 151). This is an example of how a government could exert its power by inspiring citizens to take autonomous patriotic actions, rather than directly orchestrating an attack (Nye 2011: 127). This example of citizens using ICT networks to expand state influence for military purposes demonstrates how they can become a tool for nationalism, rather than just in opposition to governments.

Cyber and Kinetic Conflict (Georgia)

The cyber war against Georgia in 2008 is another example where the Russian government is suspected of having been involved in the coordination of civilian cyber attacks (Russian Invasion of Georgia 2008). On the 7th of August a large number of Georgian Internet servers were seized and placed under remote control, and on the 8th of August, Russia commenced its invasion of Georgia (Russian Invasion of Georgia 2008). Various analysts have tied the attacks to the Russian Business Network (RBN), a network of criminal hackers with close links to the Russian mafia and government (Dam, Lin, Owens 2009: 174). A researcher who tracks the activity of the RBN, Jart Armin, released data that claims to demonstrate that the servers responsible for rerouting visits to Georgian sites were under the control of RBN and influenced by the Russian government (Russian Invasion of Georgia 2008). Websites such as "stopgeorgia.ru" provided information about potential Internet targets and the tools necessary to orchestrate an attack. The registration information of this website was shown to reveal a connection to the RBN.

Armin argues that the RBN is tied directly to the Russian government, which seems circumstantially supported by the attacks being perfectly timed to execute in conjunction with the physical invasion of Georgia. On the 27th of August, there was a large DDoS attack aimed at Georgian websites, and mainly the Georgian Ministry of Foreign Affairs, though the attacks died down after many had been successfully blocked (Russian Invasion of Georgia 2008). These attacks were not the work of "hacktivists" just interested in the laughs, but incredibly well planned and tightly coordinated (Russian

Invasion of Georgia 2008). Similar to the Estonian cyber riots, this case exemplifies how states can benefit from the Internet and expand their capabilities militarily as well as diplomatically. Governments are not only finding ways to maintain their authority on the Internet, they are able to expand their power.

Cyber Espionage (China)

In addition to physical attacks, governments can use the Internet as a way to collect information about other countries, as well as their own citizens. Cyber espionage describes how states are using the vulnerabilities in networks to steal data from each other, as well as private enterprises. This has been described as a new type of economic warfare, and is changing the way that states observe attacks on their sovereignty (NBC News 2011). If a country can access the information guarded by their adversaries, specifically with regard to military technology, then they can develop and enhance their capabilities without having to invest in the research.

The ongoing conflict over intellectual property laws between the United States and China has taken on a new dimension as Chinese hackers exploit network vulnerabilities in order to steal American research (Maginnis 2011). The United States sees Chinese cyber espionage as a danger to national security. The Pentagon’s 2011 report on the Chinese military claims that the government conducts cyber intrusions in order to extract information from defense websites, and argues that whatever the government cannot buy, they steal (Maginnis 2011). Apparently, Chinese espionage has resulted in the Americans losing their encryption, cruise missile, and stealth technologies to China (Maginnis 2011).

Economic espionage can even be offensive as well as theft oriented. The Pentagon report states that China plans to use cyber attacks to "constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities" (Maginnis 2011). However, to a certain extent it is expected that all governments will use various tactics to spy on the actions of their rivals, and consequently, the United States is likely culpable as well. Still, the use of the Internet as a means for states to exploit each other's vulnerabilities is not in line with the cyber utopian perspective. Cyber espionage exemplifies how the loss of control over information can actually affect a state's military capabilities. The monopolization over sophisticated weaponry can provide states with additional power, and this is eroded when other states are able to steal information about weapons systems and then build comparable ones of their own. The impact of information theft on military capabilities exemplifies how ICT networks can be used to increase states' military strength, and improve their means to exert control over their territory.

Cyber Skeptic Perspective

From the cyber skeptic perspective the above cases all illustrate how ICT networks can expand a state's capabilities in terms of military force and economic influence. In the case of Estonia and Georgia, the Russian government's involvement in coordinating the cyber attacks seems limited and unclear, but they benefitted from the patriotic actions of their citizens. If nationalism can motivate non-state actors to take action on behalf of the state, this enhances the state's authority as opposed to detracting from it. In the case of Stuxnet, the Internet became a tool for a sophisticated attack on an

Iranian nuclear facility. While it is not definitive that this was a government-sponsored action, experts believe that the level of sophistication implies a state actor is responsible. There are clearly states that benefit from this outcome, such as Israel and the United States.

The increased possibility of ICT networks being used as a medium for attack means that governments can make the case for exercising greater control. In the name of protecting citizens, they can argue for increased use of filtration techniques such as deep packet inspection of the information on ICT networks. International relations scholar Joseph Nye emphasizes that: "Providing security is a classic function of government, and some observers believe that increasing insecurity will lead to an increased role for governments in cyberspace. Many states desire to extend their authority in cyberspace and seek technological means to do so" (Nye 2011: 144). Political scientists Chris Demchak and Peter Dombrowski argue that cyberspace is about to enter its own Westphalian Age: "From the Chinese intent to create their own controlled internal Internet, to increasingly controlled access to the Internet in less-democratic states, to the rise of Internet filters and rules in Western democracies, states are establishing the bounds of their sovereign control in the virtual world in the name of security and economic sustainability" (Dombrowski and Demchak 2011: 32). They argue that Stuxnet marks a new chapter in Internet governance, because it signifies that ICT-leveraged attacks can pose a significant threat. In their view: "All states, in one way or another, will reach out to control what they fear from the Internet—the lack of sovereign control over what comes through their borders. Thus the transformation from frontier to regulated substrate across cyberspace has begun" (Dombrowski and Demchak 2011: 35).

Cyber Utopian Perspective

Cyber utopians tend to overlook the militaristic possibilities of ICT networks, however, in doing so they ignore proof of how citizen coordinated cyber attacks challenge state authority. Nye points out that the attacks in Estonia were “the product of large-scale, transnational, spontaneously organized collective action. It was made possible by the Internet and its capacity for quickly sharing information and software tools and for mobilizing like-minded but dispersed and mostly anonymous groups of people” (Nye 2011: 24). From this perspective, the attacks in Estonia were an example of coordinated citizen activism being leveraged in opposition to a formal state, just not their own. The cyber riots in Estonia still demonstrate the power of networked individuals resisting a state’s hierarchical decision making, but in this case a foreign government was targeted.

The Georgian case illustrates that citizen efforts can bolster Russian capabilities, but it also demonstrates how citizens can successfully attack another country and disrupt their information infrastructure. It makes one wonder what these citizens would be capable of if they did choose to turn against their own government. While every country that uses ICT networks faces the threat from domestic hackers, there has yet to be a coordinated attack by citizens against their own government, that matches the scale of the Estonian or Georgian cases. Nye points out that the Estonian case underscores the absence of a clean division between state and non-state actors in a networked environment (Nye 2011: 26). While cyber utopians may prefer to avoid thinking of militant political activism as an example of the strength of networks, these cases illustrate that citizen cyber power is a force in its own right.

Integrated Perspective

ICT networks support the Internet that many users obtain information from. Social media sites on the Internet allow citizens to access and share information across borders in real-time, without the government or traditional media organizations serving as an intermediary. In certain cases these ICT networks can facilitate coordinated citizen action. As states increase their reliance on ICT networks, they develop new vulnerabilities in their information and even physical infrastructure that can be exploited by state and non-state actors. If one employs the liberal definition of sovereignty – that sovereignty is defined by the states' ability to control actors and activities within and across its borders (Thomson 1995: 213) – then ICT networks are in fact challenging state sovereignty by allowing citizens to coordinate cyber attacks outside of state control that can even cause physical destruction. If one employs the realist definition of sovereignty – that sovereignty is defined by the states' ability to make authoritative decisions, namely the decision to make war (Thomson 1995: 213) – then ICT networks complicate the very nature of sovereignty by allowing citizens to instigate semi-autonomous attacks that can either imitate war, or support actual kinetic warfare (Georgia). However, states are also capable of using these tools to launch cyber attacks and increase their own military capabilities. States can inspire citizens to attack particular adversaries without being held officially responsible.

Ultimately, states are increasing their military capabilities through the use of ICT networks. The ability for citizens to coordinate cyber attacks has not resulted in a challenge to the supremacy of a state's authority within its borders. States can even increase their authority by increasing their military capabilities (Stuxnet), and inspiring patriotic hackers to target adversary states (Estonia), or to bolster the effectiveness of physical military campaigns (Georgia). In these cases, the state clearly does not cease to be considered the supreme governing structure within its territorial boundaries. However, more so than any of the other functions of ICT networks that are discussed in this paper, the ability for citizens to coordinate cyber attacks has the greatest potential to challenge state authority. If one examines the liberal and realist definitions of sovereignty, citizen cyber attacks pose a challenge to government's authority, because they offer the potential for legitimate force that is outside of state control. Still, this analysis has taken a very distinct view of sovereignty that implies that it is only challenged when the state ceases to be the supreme authority within its territorial boundaries. State sovereignty remains intact in the face of citizen coordinated cyber attacks through ICT networks.

Transition

Cyber utopians and cyber skeptics can both find evidence for their arguments in examining case studies of cyber attacks and cyber espionage. The Internet was not designed to be a secure medium, but rather one that facilitated the sharing of information The Estonian cyber riots of 2007 and the Georgian cyber attacks of 2008 are two examples of citizen networks coordinating patriotic action on behalf of the state. The Stuxnet virus that targeted Iran in 2010 is another example of how ICT networks are being used to expand states' military capabilities. Attacks can also take the form of economic sabotage and espionage, and the United States is struggling to find new methods of protecting its data against Chinese intrusions. While citizens are challenging state control over information, coordination, and even the legitimate use of force, the sovereignty of states appears to remain intact. The fabric of cyberspace is still in flux, and it will remain to be seen whether states can fully subject ICT networks to their authority and created borders in cyberspace, or must adapt to this new borderless domain.

Discussion

This section will synthesize all of the evidence presented in previous sections in order to support the author's argument that while ICT networks do not eliminate state sovereignty, they challenge states' control over actors within their borders. As a result regimes need to more actively reassert their authority in order to retain power, yet state sovereignty as a whole still remains intact. This section will also include some of the ideas that the author developed in the process of writing this paper.

Synthesize Evidence

Networks are a set of interconnections among nodes. That is the fundamental concept. Networks are simply a term to describe relationships, and they can be applied to people, cells, countries, ideas, or really anything at all. So when individuals argue that the world is becoming more networked, what does this actually mean? Clearly they are not referring to the earth as part of a network of planets. The term "networked world" is describing networks of human interaction. The argument is that as people are better able to communicate through the use of technology, new connections will be formed and the network of human relationships will grow larger and even more complex. In the cyber utopian perspective, this argument implies that societal structure across borders is fundamentally shifting away from hierarchical organizations, such as states, towards decentralized networks of individuals, for example crisis mapping groups. In the cyber skeptic perspective, hierarchal organizations are not fundamentally challenged by networks, and often subjugate them to their control, or force them to take on more hierarchical qualities.

In international relations, this debate is encapsulated in the general conflict between the realist view that states are the primary unit of analysis, and the liberal view that connections between non-state actors can also impact the international system. In general, state sovereignty is defined as supreme authority within defined territorial boundaries. However, liberal interdependence theorists argue that sovereignty is defined by states' ability to control actors within and across borders, and realist theorists argue that it is the states ability to make authoritative decisions, in particular the decision to make war (Thomson 1995: 213). The liberal interdependence definition connects directly to the cyber utopian perspective. Cyber utopians often cite examples where states have lost control over their citizens' ability to exchange information or coordinate collective action. The realist definition and the general definition directly connect to the cyber realist or skeptic perspective. Cyber skeptics often stress that states are still the recognized structure of governance, and still have the ability to use force domestically and abroad. This analysis has similarly argued that states still retain authority within their borders, despite challenges to control.

The cyber utopians of the 1990s argued that the absolutes of the Westphalian system were dissolving, and that the computer and telecommunications revolution were leading to the decline of states and the rise of non-state actors (Mathews 1997). Even in current times the cyber utopian perspective is defined by individuals who argue that the use of ICT or the services they generate can pose a significant challenge to state authority. However, in reality the networked nature of ICT do not challenge state authority, but rather the ability of particular regimes to exert control over actors and activities within their borders. Cyber utopians are addressing the liberal interdependence definition of sovereignty, but this is only one definition, and it is one that has a particular flaw.

International relations theorist Janice E. Thomson argues: “State control has waxed and waned enormously over time, regions, and issue-areas while the state's claim to ultimate political authority has persisted for more than three centuries” (Thomson1995: 214). A state does not lose its sovereignty when it loses control of economic policy, trans-border flows, or even the actions of its citizens, because there was never a time when states control over anything was assured or secure (Thomson 1995: 214). Cyber utopians are not wrong that states’ control has been challenged by the various functions of ICT, but they are wrong in asserting this significantly undermines states’ authority. A state still has authority even if international networked organizations operate across their borders or even if a particular regime is removed from power. In these cases supreme political authority has not shifted from state to non-state actors or other institutions. The formal “state” structure is still recognized, domestically and internationally, as the highest governing body within its territory.

This is not to say that the cyber skeptics are completely correct in dismissing the impact of ICT on state control. These new technologies do empower citizens to exchange information and to coordinate with each other new ways. The Internet may have gatekeepers in the form of search engines, but it is still different from when publishers and media organizations determined what content was worthy of production and distribution. Everyone can share information in real time, and the sheer volume of content makes it difficult for states to limit communications. States can rely on censorship technologies to filter the content their citizens can access, but this requires a greater investment than when they could simply control information at hierarchical centers of production. However, while states may find it harder to control information flow across their borders, this does not undermine their authority.

ICT facilitate communication and the Internet creates a new public sphere where people can express dissent and share mutual concerns. Social media sites could be encouraging "slacktivism," but they are serving as yet another tool that facilitates coordination. Furthermore, they could encourage political involvement from individuals who would otherwise remain uninvolved altogether. Weak ties may not inspire high risk activism, but over time they can become stronger as citizens engage in more low risk activist opportunities. Furthermore, they can tie together groups of individuals who might otherwise remain unconnected. Crisis mapping groups represent networked organizations and they can operate with state and non-state actors to assist in resource allocation during times of crisis. However, they operate outside state control, and can become politicized by posting information about government corruption or attacks on citizens. The dictator or conservative's dilemma makes censorship or ICT shutdowns a more costly decision and it forces states to evaluate their priorities. Still, this does not stop states from seeking to limit ICT to prevent citizens' expression of dissent and collective action. While states may find it harder to control their citizens' actions, this does not undermine their authority.

States can use ICT to spread their perspective and influence their citizens. The Internet and social media sites provide yet another platform for propaganda. ICT also facilitate coordination that serves to support state control as opposed to challenging it. ICT networks are also another piece of infrastructure that can be targeted during conflicts, so states that can launch cyber attacks to exploit their opponents' vulnerabilities are able to bolster their military capabilities. States can encourage citizens to take action against dissidents, or even against other adversarial states. Patriotic hackers may conduct attacks on states behalf, but other hackers challenge state control by targeting their own government. Depending on the accepted definition of sovereignty, hackers could pose a challenge to state authority because they can launch attacks that might be considered akin to warfare. Realists define sovereignty as the ability for states to make authoritative decisions, in particular the decision to make war, and in this view patriotic hackers' use of ICT challenges sovereignty. In the event that patriotic hackers declare war on behalf of their government, but without its official sanction, they would be undermining the state's authority. However, this would not mean that these non-state actors are then looked to as the overarching political authority within that territory, and therefore, the state's sovereignty would remain intact. Arguably, for the non-state actors to truly become a competing authority within that territory, they would have to become the rule making body within that region, and achieve recognition domestically and internationally.

Throughout this paper there has not been a single example of where ICT have facilitated a shift in political authority from the state to non-state actors or institutions. While the bodies that control the Internet exemplify networked governance (i.e. ICANN, IETF), as do certain international organizations such as the Ushahidi or Standby Task Force crisis mappers, states are still recognized as the formal governing structure in territories all over the world. Regimes maybe ousted, and different administrations may go in and out of power, but the state structure itself remains constant. In each case throughout this paper, and in many others analyzed by the cyber utopians and cyber skeptics, the state has remained the supreme authority within its territorial boundaries, and therefore its sovereignty remains intact.

Additional Thoughts

A Standby Task Force (SBTF) Member, Kate Perino, explained that when the SBTF was working with human rights organizations they often had to catch up "ordinary people" who think "I can use Facebook to get help" as opposed to understanding how crisis mapping truly works (Perino 7 March 2012). As she describes it, these aid organizations are organized in a hierarchical manner, and gather their information from official internal sources, so they are not used to the horizontal methodology used by crisis mappers. In networked organizations people are often assigned several different tasks, decisions are made through consensus, and the organization is flexible and adapts to include new functions. To individuals that are used to working in a hierarchy, these organizations may appear to be chaotic, and without any formal mechanism of coordination. There is no central leadership, and no assigned roles, so an outsider might assume there is no methods of group governance.

In fact, this is likely what occurred in the traditional media's representation of the Occupy Movement. In that movement, there was no formal leadership and no clear platform, which caused many journalists to describe protestors as having no demands. This lack of hierarchy made Occupy an object of criticism and scorn, as though a central leadership is a basic requirement of any movement. However, this movement was successful at coordinating encampments in several cities as well as protests and other events, all without central leadership. The movement may not have directly resulted in significant reform, but it did bring awareness to the growing income gap and financial inequality in the United States. Networked movements like Occupy, and networked organizations like SBTF show how it is possible to coordinate action without hierarchies. In these groups, it is not that members have no roles and no responsibilities, but rather that they have several shifting roles, and share responsibilities.

Another interesting thought is how the public sphere facilitated by ICT networks, specifically on the Internet, can embolden people who might not otherwise have contributed in a public sphere through personal interactions, or traditional media. For many individuals, the anonymity of online interaction allows them to speak more freely, for better and for worse. Individuals who may not feel comfortable voicing their political thoughts publicly could find that an online forum or a blog is a space where they can express themselves without impacting their reputation in real life. In repressive regimes, anonymity can also make people feel more emboldened to voice criticisms of authorities.

While authoritarian governments are developing more advanced techniques for tracking dissidents online, there is still a difference between the risk of expressing dissent online –where you might be identified and punished – and the risk of expressing dissent in the physical world – where authorities could inflict instant punishment upon finding an individual who is criticizing the regime. With online assembly there is a degree of separation between action and punishment that does not exist in the real world. If people are communicating in a chat room, the government has to identify those involved, and then target each of them separately. If people are meeting in a local café, authorities can capture everyone at once and physically deter future dissent. Because deniability is greater online, there is the possibility that people will be willing to share criticisms of the government, even if there is the same threat of punishment. This buffer between communication and retaliation may alter the decision calculus of dissenters, and make them more likely to take risks. This would mean that the government will have to employ even greater force to deter citizens from expressing dissent, which could alienate third party citizens. It would be difficult to measure this trend if it did exist, but it is an interesting thought that is perhaps worth future examination.

Another interesting thought is how social media facilitates instant, publicly available information on involvement in political groups. On sites like Facebook and Twitter, one does not need to estimate group membership or keep formal counts, this data is readily available and dynamically updated. These numbers can be very impressive, and provide quantifiable representations of levels of activism, even if their translation into physical action is limited. While the numbers on social media sites do not represent physical involvement, they represent a new type of involvement that should be seen as valuable in its own right. The emphasis on the connection between activism online and in real life can at times overlook the value of purely digital political action. Cyber skeptic Evgeny Morozov argues that if people feel satisfied by engaging in Facebook groups then they might choose to do that at the expense of writing letters to their elected representatives or organizing rallies, despite the fact that online activities will have less impact on society (Morozov 2011: 190). This is a rather short sighted view of the power of online representation on the Internet. If public officials or government administrations have Facebook pages, then citizens do not need to write them a letter, they can write comments directly on the official’s wall. Social media can facilitate a new type of direct interaction with government officials that would be equivalent to if not replace letter writing.

As for organizing rallies, arguably if it is easier to coordinate events and advertise them, this will assist collective action rather than hinder it. In the past rallies had to use single-to-single (i.e. phone calls) or single-to-many communications (i.e. radio announcements) to contact potential participants. With the Internet and social media sites, people can communicate with many individuals at once, and receive information from many individuals at once. Sharing information about a planned rally is easy because rather than making a hundred phone calls, an individual can post information on Facebook and their entire social circle will learn of it instantly. Social media sites allow everyone to observe quantifiable estimates of political activism that is not necessarily physical, but a valid form of political action nonetheless.

Conclusion

Summary

State sovereignty is typically defined as supreme authority within a territory. The liberal interdependence theorists define it as control over actors and activities within states borders, while the realist theorists generally focus on the ability to make authoritative decisions, namely the decision to make war (Thomson 1995: 213). This analysis set out to argue that state sovereignty remains intact despite challenges from ICT use because political authority has not been transferred from the state to a non-state entity.

The increased proliferation of ICT has resulted in a greater awareness of network theory among scholars, officials, and professionals. Because of the diffuse and decentralized nature of the interactions between computers, mobile phones, and other ICT, there is significant discussion on whether the introduction of these technologies has challenged state authority and led to a fundamentally "more networked" world.

The decentralized structure of ICT inspires cyber utopians to describe these networks as having political power as a result of its very physical manifestation. They argue that the decentralized nature of ICT networks will inherently challenge the hierarchical structure of states. These arguments resemble many that have occurred in the past since throughout time there have always been individuals who herald new advances in technology as being truly revolutionary. The cyber utopians argue that technology is leading to a more connected world and challenging the authority of states.

In contrast, the cyber skeptics argue that states still exert control over the infrastructure of the ICT networks. They argue that ICT networks do not inherently challenge states and that they can be used as a tool for repression and injustice.

Repressive governments can control information on ICT networks by utilizing censorship technologies. Cyber skeptics argue that the illusion of anonymity on the ICT networks can be dangerous if citizens in authoritarian regimes do not realize that they can be tracked and punished by their governments. The "cyber skeptics" argue that states retain their authority, and are expanding their control over ICT networks.

The flow of information is bound by the infrastructure of ICT networks, but it is not bound by gatekeepers in the same way that traditional media has been. Whereas previously media institutions would determine what content was considered newsworthy, and then broadcast that information to the people, the Internet allows citizens to determine for themselves what is valuable. Citizens can produce real time information as well as consume it, and they can become informal journalists. Citizens can report on their governments' actions and spread information about corruption or acts of violence.

The forums, e-lists, social media sites, short messaging services (SMS) and similar applications enabled by ICT allow individuals to correspond with others around the world. Social media sites facilitate communication between people with common interests, and when online conversations become politicized they can potentially lead to action in the real world. The Internet and social media sites compose a new public sphere where people can express dissent and discuss mutual concerns. Activists can use these tools to coordinate political action, resist government control, and advocate for reform.

The coordination of information on ICT networks can inspire the coordination of people and the allocation of resources in real life. Crisis mapping is a new platform for collecting real time information during crises and representing it on a map to assist governments and aid organizations in their relief efforts. These maps at times rely on crowdsourcing, where many people provide information through mobile phones or other devices, which mappers then analyze and relate. Crisis mapping groups interact with state and non-state actors in order to coordinate aid, and they represent an example of a networked organization.

In order to prevent coordination and collective action, authoritarian governments have found ways to limit information on ICT networks. When states are challenged by their citizens' ability to coordinate using these technologies, they can choose to shut them down, although there may be social or economic repercussions. The dictator's dilemma describes the trade off between economic development and ICT penetration and how it forces repressive regimes to constantly re-evaluate their priorities. However, states can generally avoid this decision by using sophisticated censorship tactics, and manipulating the private companies that provide and operate ICT infrastructure.

States can even use ICT networks to advance their own agendas. For instance, some countries such as China use the Internet to not only censor domestic content, but to post content in favor of the government's actions. Additionally, other countries such as the United States use social media and the Internet to spread favorable messages internationally in an attempt to influence foreign publics directly. The US State Department has an entire "21st Century Statecraft" initiative dedicated to reaching out to foreign publics through the use of social media.

States can even go as far as to use ICT networks as a means to inspire actions that are in its favor. In certain cases the government can help convince citizens to target another state and yet avoid official involvement, such as in the Estonian cyber riots of 2007. States can inspire these patriotic hackers to take action, and avoid being held responsible for any involvement. Furthermore, states can use ICT networks to expand their military capabilities and use them as a medium for targeting the vulnerabilities of their rivals.

ICT and the services that they support are essential tools that are changing the way states interact with their citizens. However, states still retain supreme political authority within their borders, and have not faced significant challenges from any non-state entities. State sovereignty remains intact despite citizens' increased use of ICT networks.

Neglected Topics

We are in the midst of significant shifts in ICT use, and consequently all around the world there are fascinating case studies as states adapt to the new information and communication environment. This analysis could have readily examined the role of Twitter in the Iranian protests of 2009, the role of mobile phones and real time television broadcasts in the Mumbai terrorist attacks of 2008, the various state targets of the hacker group Anonymous, and many other interesting examples that would fall within the categories of ICT functions: information, coordination, control, and force.

In the information section it would have been helpful to delve more into the world of blogging and forums in the examination of social media tools. In coordination it would have been interesting to explore how other international civil society organizations are using ICT. The role of ICT in encouraging development is frequent topic of discussion. It would also be worthwhile to contrast the benefits these technologies provide in some developing countries with the costs they impose on the environment and laborers in others parts of the world. In general the topic of the impact of ICT on the environment is one that should be looked at more closely. Cyber utopians who stress how technology can change the world for the better tend to overlook the environmental costs.

A huge topic that is missing from coordination, or perhaps force, is the role of ICT in criminal and terrorist networks, specifically Al Qaeda. Contemporary terrorist networks rely heavily on new technology to recruit individuals and coordinate attacks. This is also overlooked by cyber utopians who tend to emphasize the role of these technologies in resisting authoritarian regimes through relatively peaceful tactics. The growing problem of cyber crime, exemplifies the downsides to anonymity and having permeable borders on ICT networks. Additionally, it would be valuable to examine how hacking communities are targeting states and whether this is having an actual impact on their authority.

Another relevant pursuit would be to explore the concepts of Internet freedom in more depth, and then contrast that rhetoric with the creation of laws to protect intellectual property. Liberal governments at times contradict themselves as they seek to protect legal ownership online while at the same time promoting freedom of speech. It would be interesting to explore intellectual property law in general, and how peer-to-peer networks can be used for both innocent and dangerous purposes. The related topic of open access and shared information ownership would also be worth exploration.

ICT are often said to have increased economic interdependence, and it would be interesting to explore E-commerce and its effects on state authority. It would also be interesting to explore how states are using ICT to provide useful services to their citizens, or the topic of E-government. The concept of globalization refers to economic interconnectivity as well as societal, and it would be fascinating to explore this topic in greater depth. The topic of globalization is originally what inspired the author's interest in the impact of ICT on political actors.

Future

At this point state sovereignty remains intact and the international system is still dominated by states competing for power. However, ICT facilitate decentralized networked organizations that have the ability to function across borders and impact citizens around the world. At this point, networked organizations cannot provide all of the functions of a hierarchical state government. Still, they represent how flexibility and adaptability are important characteristics in the information age, as the pace of technological development is so fast and frenetic. States seek to improve their security in cyberspace, and reassert control over information and communication networks. However, in recent years the rate of innovation is so fast that states have to adapt quickly in order to keep up with their citizens' use of ICT. Governments tend to take time to adjust to technological developments, while citizens and civil society organizations can adapt quickly. Consequently, the real question is not whether states can subjugate the most recent wave of ICT, but whether they can control the next wave. Even if states can censor the Internet, will they be able to censor the next Internet? As long as the pace of technological advance does not plateau states will always be one step behind their citizens. While states retain their sovereignty in the present day, the next wave of technology may facilitate the creation of different structures that people can use to govern their lives. States remain the fundamental governing structure of today, but there is the potential for a different international system to emerge in the coming century.

Bibliography

"100 ICT Concepts." *Information and Communication Technologies*. <http://worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:21035032~menuPK:2888320~pagePK:210058~piPK:210062~theSitePK:282823,00.html>.

A, R. "Can You Social Network Your Way to Revolution?" *The Economist*. 27 Sept. 2010. <http://www.economist.com/comment/675073#comment-675073>.

Abdulla, Rasha A. "The Revolution Will Be Tweeted: The Story of Digital Activism in Egypt." *Cairo Review* 3 (2011).

Ackerman, Spencer, and Noah Shachtman. "Stealth Tech, Facebook Revolutions, Shadow Wars: The Most Dangerous Year Ever." *Wired.com*. Conde Nast Digital, 28 Dec. 2011. <http://www.wired.com/dangerroom/2011/12/most-dangerous-year/?intcid=story_ribbon>.

Ackerman, Spencer. "Egypt's Top 'Facebook Revolutionary' Now Advising Occupy Wall Street." *Wired.com*. Conde Nast Digital, 18 Oct. 2011. <http://www.wired.com/dangerroom/2011/10/egypt-occupy-wall-street/>.

Allison, Juliann Emmons. "Information and International Politics." Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age. Ed. Juliann Emmons Allison. Albany: State University of New York, 2002.

Allnut, Luke. "Facebook To Launch Global Policy Offensive (And How It Might Start Looking Like McDonald's)." *RadioFreeEurope/RadioLiberty*. 24 May 2011. <http://www.rferl.org/content/facebook_to_launch_global_policy_offensive_how_it_might_start_looking_like_mcdonalds/24184656.html>.

Anderson, Nate, and Ars Technica. "Tweeting Tyrants Out of Tunisia: Global Internet at Its Best." *Wired*. 14 Jan. 2011.

Anstey, Caroline, and Leonard McCarthy. "Technology Is Helping the Fight Against Corruption." *The Huffington Post*. TheHuffingtonPost.com, 09 Dec. 2011. Web. <http://www.huffingtonpost.com/caroline-anstey/technology-anti-corruption_b_1139022.html>.

Apps, Peter. "Insight: Social Media - a Political Tool for Good or Evil?" Reuters, 29 Sept. 2011. <http://www.reuters.com/article/2011/09/29/us-technology-risk-idUSTRE78R3CM20110929>.

Arthur, Charles. "WikiLeaks: Internet Backlash Follows US Pressure against Whistleblowing Site." *The Guardian*. Guardian News and Media, 05 Dec. 2010. <http://www.guardian.co.uk/media/2010/dec/05/wikileaks-internet-backlash-us-pressure>.

Aucoin, Don. "For Young Activists, Video Is Their Voice." *Boston.com*. The Boston Globe, 5 Mar. 2010. <http://www.boston.com/lifestyle/articles/2010/03/05/for_activists_in_the_youtube_generation_video_is_the_way_to_be_heard/?page=2>.

"Bahrain News & The Protests." *Bahrain Protest News*. 23 Apr. 2012. <http://topics.nytimes.com/top/news/international/countriesandterritories/bahrain/index.html>.

Bahrain: Shouting in the Dark. Dir. May Y. Welsh. Prod. Tuki Laumea and John Blair. Al Jazeera English, 2011. Television. *Bahrain: Shouting in the Dark*. Al Jazeera English, 4 Aug. 2011. <http://www.youtube.com/watch?v=xaTKDMYOBOU>.

Barber, Benjamin. "Jihad Vs. McWorld." *The Atlantic*. Mar. 1992. <http://www.theatlantic.com/magazine/archive/1992/03/jihad-vs-mcworld/3882/>.

Barrett, Raymond. "How a Broken Social Contract Sparked Bahrain Protests."*Csmonitor.com*. 21 Feb. 2011. <http://www.csmonitor.com/World/Middle-East/2011/0221/How-a-broken-social-contract-sparked-Bahrain-protests>.

Barzilai-Nahon, Karine. *Network Gatekeeping Theory*. Working paper. Theories of Information Behavior: A Researcher's Guide, 2005.

BBC News "Google 'may Pull out of China after Gmail Cyber Attack'" 13 Jan. 2010. <http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/business/8455712.stm?ad=1>.

Beaudry, Pierre. "The Treaty of Westphalia." *The Schiller Institute*. May 2003. <http://www.schillerinstitute.org/strategic/treaty_of_westphalia.html>.

Benkler, Yochai. The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven [Conn.: Yale UP, 2006.

Bennett, Brian. "Where Even Cellphones Aren't Safe." *Los Angeles Times*. Los Angeles Times, 09 Apr. 2011. <http://articles.latimes.com/2011/apr/09/world/la-fg-mideast-internet-20110409>.

Boorstin, Bob. "Bob Boorstin, Director, Corporate and Policy Communications at Google Talks in Venice, Italy." *CSIS | Center for Strategic & International Studies*. 2008. <http://csis.org/blog/bob-boorstin-director-corporate-and-policy-communications-google-talks-venice- italy>.

Bosker, Bianca. "PayPal Admits State Department Pressure Caused It To Block WikiLeaks." *The Huffington Post*. TheHuffingtonPost.com, 08 Dec. 2010.

<http://www.huffingtonpost.com/2010/12/08/paypal-admits-us-state-de_n_793708.html>.

Bott, Maja, Bjorn-Soren Gigler, and Gregor Young. "The Role of Crowdsourcing for Better Governance in Fragile State Contexts." *Scribd*. <http://www.scribd.com/WorldBankPublications/d/75642401-The-Role-of-Crowdsourcing-for-Better-Governance-in-Fragile-State-Contexts>.

Brecher, Jeremy, and Brendan Smith. "Is Social Networking Useless for Social Change? | Common Dreams." Common Dreams. 8 Oct. 2010. <http://www.commondreams.org/view/2010/10/08-3>.

Bristow, Michael. "China's Internet 'spin Doctors'" *BBC News*. BBC, 16 Dec. 2008. <http://news.bbc.co.uk/2/hi/7783640.stm>.

Bronk, Chris. "Hacking the Nation-State: Security, Information Technology and Policies of Assurance." *Information Security Journal: A Global Perspective*17.3 (2008): 132-42.

Buchs, M. "Examining the Interaction between Vertical and Horizontal Dimensions of State Transformation." *Cambridge Journal of Regions, Economy and Society* 2.1 (2009): 35-49.

"By Mirror.co.uk Comments 25 Aug 2011 15:11 London Riots: More than 2,000 People Arrested over Disorder." *The Mirror*. 25 Aug. 2011.

Carlstrom, Gregg. "Bahrain Youth March on State TV - Middle East - Al Jazeera English." *Al Jazeera English*. 4 Mar. 2011. <http://www.aljazeera.com/news/middleeast/2011/03/201134183528970309.html>.

Cassidy, William P. "Gatekeeping Similar For Online, Print Journalists." *Newspaper Research Journal* 27.2 (2006): 6-23. <http://jclass.umd.edu/classes/jour698m/cassidy.pdf>.

Cerf, Vinton G. "Internet Access Is Not a Human Right." New York Times 4 Jan. 2012.

Cha, Ariana E., and Ellen Nakashima. "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say." *Washington Post*. The Washington Post, 14 Jan. 2010. <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html>.

Choucri, Nazli. Cyberspace and International Relations Toward an Integrated System. Working paper. 2011.

Clark, Wesley K., and Peter L. Levin. "Securing the Information Highway."*Foreign Affairs* 88.6 (2009).

Clayton, Mark. "Stuxnet Malware Is 'weapon' out to Destroy ... Iran's Bushehr Nuclear Plant?" *The Christian Science Monitor*. The Christian Science Monitor, 21 Sept. 2010. <http://www.csmonitor.com/layout/set/print/content/view/print/327178>.

Clayton, Richard, Steven J. Murdoch, and Robert N. Watson. "Ignoring the Great Firewall of China." (2006). <http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf>.

Cohen, Noam. "When Knowledge Isn't Written, Does It Still Count?" *The New York Times*. The New York Times, 08 Aug. 2011. <http://www.nytimes.com/2011/08/08/business/media/a-push-to-redefine-knowledge-at-wikipedia.html>.

"Cold War Redux Warning over Cyberspy Threat." *CBS News Tech*. 3 Nov. 2011.

Collins, Terry. "San Francisco Transit Blocks Cellphones To Hinder Protest." *The Huffington Post*. TheHuffingtonPost.com, 13 Aug. 2011. <http://www.huffingtonpost.com/2011/08/13/san-francisco-transit-cellphone-protest_n_926135.html>.

Considine, Austin. "For Activists, Tips on Safe Use Of Social Media." *The New York Times*. The New York Times, 03 Apr. 2011. <http://www.nytimes.com/2011/04/03/fashion/03noticed.html?_r=2>.

Cowhey, Peter, and Milton Mueller. "Delegation, Networks, and Internet Governance." Networked Politics: Agency, Power, and Governance. Ithaca: Cornell UP, 2009.

Coyle, Diane, and Patrick Meier. "New Technologies in Emergencies and Conflicts." *United Nations Foundation*. <http://www.globalproblems-globalsolutions-files.org/pdf/UNF_tech/emergency_tech_report2009/Tech_EmergencyTechReport_full.pdf>.

Cull, Nicholas J. "WikiLeaks, Public Diplomacy 2.0 and the State of Digital Public Diplomacy." *Place Branding and Public Diplomacy* 7 (2011): 1-8.

Dam, Kenneth W., and Herbert S. Lin. "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities." *The National Academies Press*. Ed. William A. Owens. National Research Council, 2009.

Dombrowski, Peter, and Chris C. Demchak. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* (2011): 32-61

Dunn, Alexandra. "Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising." *The Fletcher Forum of World Affairs* 35.2 (2011): 15-24.

Dwyer, Devin, and Jim Sciutto. "Wikileaks: Stop Us? You'll Have to Shut Down the " *ABC News*. ABC News Network, 08 Dec. 2010.

<http://abcnews.go.com/International/julian-assange-wikileaks-faces-onslaught-charges-attacks-politically/story?id=12333753>.

"Egypt Facebook Statistics." *Socialbakers.com*. <http://www.socialbakers.com/facebook-statistics/egypt>.

"Egypt Passes 50% Penetration Mark." *Cellular-news*. 28 July 2009. <http://www.cellular-news.com/story/38818.php>.

"Egypt Revolution 2011 English The World Is Talking, Are You Listening?" *Global Voices*. 29 Apr. 2012. <http://globalvoicesonline.org/specialcoverage/2011-special-coverage/egypt-protests-2011/>.

"Empowering Citizens to Fight Corruption." *New Tactics*. 9 June 2010. June 2010. <http://www.newtactics.org/yi/blog/new-tactics/empowering-citizens-fight-corruption>.

Erdbrink, Thomas. "In Iran, ‘couch Rebels’ Prefer Facebook." *Washington Post*. The Washington Post, 13 June 2011. <http://www.washingtonpost.com/world/middle-east/in-iran-couch-rebels-prefer-facebook/2011/06/10/AGB9FpTH_story.html?wpisrc=nl_tech>.

Faris, David. *REVOLUTIONS WITHOUT REVOLUTIONARIES? SOCIAL MEDIA NETWORKS AND REGIME RESPONSE IN EGYPT*. Diss. University of Pennsylvania, 2010.

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* 53.1 (2011): 23-40.

Fayed, Shaimaa. "Egypt Internet Returns." *The Huffington Post*. TheHuffingtonPost.com, 02 Feb. 2011. <http://www.huffingtonpost.com/2011/02/02/egypt-internet-returns_n_817319.html>.

Fenster, Mark. "Disclosure's Effects: Wikileaks and Transparency." *Social Science Research Network*. 2012. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1797945>.

"For Activists, Facebook Is A Reluctant Platform." *RadioFreeEurope RadioLiberty*. 10 Oct. 2011. <www.rferl.org/articleprintview/2296767.html>.

Ford, Heather. "Can Ushahidi Rely on Crowdsourced Verifications?" *Idea Lab*. PBS, 28 Nov. 2011. Web. <http://www.pbs.org/idealab/2011/11/can-ushahidi-rely-on-crowdsourced-verifications325.html>.

Fuchs, Christian. "Social Media and the UK Riots: “Twitter Mobs”, “Facebook Mobs”, “Blackberry Mobs” and the Structural Violence of Neoliberalism."*Information – Society – Technology & Media*. 10 Aug. 2011.

Gaudin, Sharon. "Google Eyes Departure from China on April 10, Report Says." *Computer World*. 19 Mar. 2010. <http://www.computerworld.com/s/article/print/9173418/Google_eyes_departure_from_China_on_April_10_report_says>.

Ghonim, Wael. *Revolution 2.0*. London: Fourth Estate, 2012.

Gilboa, Eytan. "Global Communication and Foreign Policy." *Journal of Communication* 52.4 (2002): 731-48.

Gillmor, Dan. "Principles for a New Media Literacy." *Berkman Center for Internet and Society at Harvard University*. 2008. <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Principles%20for%20a%20New%20Media%20Literacy_MR.pdf>.

Gjelten, Tom. "Silencing WikiLeaks A Free Speech Challenge For U.S." *NPR*. NPR, 09 Dec. 2010. <http://www.npr.org/2010/12/09/131940669/Battle-Over-WikiLeaks-Hits-Turning-Point>.

Gladwell, Malcolm, and Clay Shirky. "From Innovation to Revolution." Foreign Affairs. Mar. 2011. <http://www.foreignaffairs.com/articles/67325/malcolm-gladwell-and-clay-shirky/from-innovation-to-revolution>.

Gladwell, Malcom. "Small Change." The New Yorker. 4 Oct. 2010. <http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell>.

Global Voices Tunisia Revolution 2011. 30 Apr. 2011. <http://globalvoicesonline.org/specialcoverage/2011-special-coverage/tunisia-uprising-201011/>.

Goldsmith, Jack L., and Tim Wu. Who Controls the Internet?: Illusions of a Borderless World. New York: Oxford UP, 2006.

Goldstein, Josh, and Juliana Rotich. "Berkman Center for Internet & Society." *Digitally Networked Technology in Kenya's 2007-2008 Post-Election Crisis*. 29 Sept. 2008. <http://cyber.law.harvard.edu/publications/2008/Digitally_Networked_Technology_Kenyas_Post-Election_Crisis>.

Granovetter, Mark. "The Strength of Weak Ties: A Network Theory Revisited." Sociological Theory 1 (1983): 201-03.

Grant, Drew. "NYPD and the City's Reaction to Occupy Wall Street." *The New York Observer*. 30 Sept. 2011. <http://www.observer.com/2011/09/the-nypd-influence/>.

Grobler, Fienie. "CNN: Social Media Is No Substitute for Journalism." *The Media Online*. 11 Jan. 2012. <http://themediaonline.co.za/2012/01/cnn-social-media-is-no-substitute-for-journalism/>.

Habermas, Jürgen. "The Public Sphere." *Jüurgen Habermas on Society and Politics: A Reader*. Boston: Beacon, 1989. 398-404.

Halliday, Josh. "Facebook and Twitter to Oppose Calls for Social Media Blocks during Riots." *The Guardian*. 24 Aug. 2011.

Halliday, Josh. "UK Riots 'made Worse' by Rolling News, BBM, Twitter and Facebook." *The Guardian*. 28 Mar. 2012.

Hanley, Charles J. "In a Wired World, the Crises Come Instantly." The Times and Democrat. 10 Sept. 2010. <http://thetandd.com/lifestyles/faith-and-values/article_75a97ebe-bc7e-11df-ac69-001cc4c002e0.html>.

Helft, Miguel. "Facebook Wrestles With Free Speech and Civility." *The New York Times*. The New York Times, 12 Dec. 2010. <http://www.nytimes.com/2010/12/13/technology/13facebook.html?emc=eta1>.

Heinzelman, Jessica, and Carol Waters. "Crowdsourcing Crisis Information in Disaster-Affected Haiti." *United States Institute of Peace*. Oct. 2010. Web. <http://www.usip.org/publications/crowdsourcing-crisis-information-in-disaster-affected-haiti>.

Hilder, Paul. "Today's Networked Activists Can Achieve Real Change." Web log post. The Guardian, 21 Mar. 2011. <http://www.guardian.co.uk/global-development/poverty-matters/2011/mar/21/social-networks-activists-achieve-change>.

Hindman, Matthew Scott. The Myth of Digital Democracy. Princeton: Princeton UP, 2009.

Hindman, Matthew. "AWhat is the Online Public Sphere Good For?" The Hyperlinked Society: Questioning Connections in the Digital Age. Ed. Joseph Turow and Lokman Tsui. Ann Arbor: University of Michigan, 2008.

Howard, Alex. "How Governments Deal With Social Media." *The Atlantic*. 9 Aug. 2011. <http://www.theatlantic.com/technology/archive/2011/08/how-governments-deal-with-social-media/243288/>.

Howard, Philip N., Sheetal D. Agarwal, and Muzammil Hussain. "The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?" Issues in Technology Innovation 13 (2011). Center for Technology Innovation at Brookings.

Iacucci, Anahi A. "The Search for Neutrality in Open Data and Crisis Mapping." *Diary of a Crisis Mapper*. 21 Feb. 2011. <http://crisismapper.wordpress.com/2011/02/21/the-search-for-neutrality-in-open-data-and-crisis-mapping/>.

ICT Policy Review. Arab Republic of Egypt Ministry of Communications and Information Technology. *ICT Policy Review Egypt*. Switzerland: UNITED NATIONS PUBLICATION, 2011.

"ICT." *Techterms.com*. <http://www.techterms.com/definition/ict>.

Imam, Yasser. "Mubarak Resigns As Egypt's President; Armed Forces To Take Control." *The Huffington Post*. TheHuffingtonPost.com, 11 Feb. 2011. <http://www.huffingtonpost.com/2011/02/11/mubarak-red-sea-egypt_n_821812.html>.

"Internet & Cyber Crime Terms and Definitions." *Pursuit Magazine*. <http://pursuitmag.com/cyber-crime-terms-and-definitions/>.

"INTERNET Security." *Network Security Articles for Windows Server 2003, 2008 & Vista*. 16 Oct. 2002. <http://www.windowsecurity.com/whitepapers/INTERNET_Security_.html>.

"Internet Gains on Television as Public's Main News Source." *Pew Research Center for the People and the Press*. 4 Jan. 2011. 06 May 2012. <http://www.people-press.org/2011/01/04/internet-gains-on-television-as-publics-main-news-source/>.

IRI Egypt Index. 20 June 2011. <http://www.iri.org/sites/default/files/2011%20June%205%20IRI%20Egypt%20Index,%20April%2014-27,%202011.pdf. >

Johnson, Bobbie. "How Twitter Could Unleash World Peace." *Bloomberg Businessweek*. 11 Apr. 2011. <http://www.businessweek.com/technology/content/apr2011/tc20110411_512316.htm>.

Jonasson, David. "Swedish Protection Does Not Apply to Wikileaks." *Stockholm News*. 7 Aug. 2010. <http://www.stockholmnews.com/more.aspx?NID=5771>.

Joyce, Mary C. "Activism, Repression, and ICT: What We Know Now." *The Meta-Activism Project*. 20 Jan. 2011. <http://www.meta-activism.org/2011/01/activism-repression-and-ict-what-we-know-now/>.

Joyce, Mary C. "Induction and Deduction in Digital Activism Research." *The Meta-Activism Project*. 24 July 2011. <http://www.meta-activism.org/2011/07/induction-and-deduction-in-digital-activism-research/>.

Joyce, Mary C. "Mobilizing Structures and a Dig at Gladwell." Web log post. The Meta-Activism Project. 6 Apr. 2011. <http://www.meta-activism.org/2011/04/mobilizing-structures-and-a-dig-at-gladwell/>.

Kahler, Miles. "Collective Action and Clandestine Networks." Networked Politics: Agency, Power, and Governance. Ithaca: Cornell UP, 2009.

Kahler, Miles. "Information Networks and Global Politics," in Christoph Engel and Kenneth H. Keller, editors, Understanding the Impact of Global Networks on Local Social, Political, and Cultural Values, (Baden-Baden: Nomos Verlagsgesellschaft, 2000), pp. 141-157

Kahler, Miles. "Networked Politics: Agency, Power, and Governance." Networked Politics: Agency, Power, and Governance. Ithaca: Cornell UP, 2009.

Kain, E. D. "The Mutual Knowledge Revolution." Forbes.com. Forbes, 18 Mar. 2011. <http://www.forbes.com/sites/erikkain/2011/03/18/the-mutual-knowledge-revolution/>.

Kalathil, Shanthi, and Taylor C. Boas. Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule. Washington, D.C.: Carnegie Endowment for International Peace, 2003.

Kanalley, Craig. "Egypt Revolution 2011: A Complete Guide To The Unrest." *The Huffington Post*. TheHuffingtonPost.com, 30 Jan. 2011. <http://www.huffingtonpost.com/2011/01/30/egypt-revolution-2011_n_816026.html>.

Kanalley, Craig. "Egypt's Internet Shut Down, According To Reports." *The Huffington Post*. TheHuffingtonPost.com, 27 Jan. 2011. <http://www.huffingtonpost.com/2011/01/27/egypt-internet-goes-down-_n_815156.html>.

Kanalley, Craig. "New Egypt Government To Be Appointed, But President Mubarak Refuses To Step Down." *The Huffington Post*. TheHuffingtonPost.com, 28 Jan. 2011. <http://www.huffingtonpost.com/2011/01/28/new-egypt-government-to-b_1_n_815682.html>.

Kaplan, Andreas M., and Michael Haenlein. "Users of the World, Unite! The Challenges and Opportunities of Social Media." *Business Horizons* 53 (2010): 59-68.

Kang, Cecilia. "Haystack Stops Tests of Iran Anti-censor Software amid Security Concerns." *The Washington Post*. 14 Sept. 2010. Web. <http://www.washingtonpost.com/wp-dyn/content/article/2010/09/13/AR2010091305827_pf.html>.

Karaganis, Joe. Structures of Participation in Digital Culture. New York: Social Science Research Council, 2007.

Kavanaugh, Andrea. "Between a Rock and a Cell Phone : Social Media Use during Mass Protests in Iran , Tunisia and Egypt." *Media* 1.212 (2011). *Mendeley Research Networks*. 2011. <http://www.mendeley.com/research/between-rock-cell-phone-social-media-during-mass-protests-iran-tunisia-egypt/>.

Kedzie, Christopher, and Janni Aragon. "Coincident Revolutions and the Dictator's Dilemma." Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age. Ed. Juliann Emmons Allison. Albany: State University of New York, 2002.

Kellow, Cl, and Hl Steeves. "The Role of Radio in the Rwandan Genocide."*Journal of Communication* 48.3 (1998): 107-28.

Kelly, John. *PRIDE OF PLACE: Mainstream Media and the Networked Public Sphere*. Berkman Center for Internet and Society at Harvard University, 2008.

Keohane, Robert O., and Joseph S. Nye. "Power and Interdependence in the Information Age." Foreign Affairs 77.5 (1998).

"Key Global Telecom Indicators for the World Telecommunication Service Sector." INTERNATIONAL TELECOMMUNICATION UNION, 16 Nov. 2011. Web. <http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html>.

Kirkpatrick, David. "Tunisia’s Inner Workings Emerge on Twitter." *The New York Times*. 22 Jan. 2011.

Kohlmann, Evan F. "The Antisocial Network." *Foreign Policy*. 23 May 2011. <http://www.foreignpolicy.com/articles/2011/05/23/the_antisocial_network>.

Kokolis, Kalliope. "Media (R)evolutions: Global Internet Use." Blog.worldbank.org. World Bank, 04 Apr. 2012. <http://blogs.worldbank.org/publicsphere/node/5950>.

Kopytoff, Verne G. "Sites Like Twitter Absent From Free Speech Pact." *The New York Times*. The New York Times, 07 Mar. 2011. <http://www.nytimes.com/2011/03/07/technology/07rights.html?_r=1>.

Kwak, Haewoon, Changhyun Lee, Hosung Park, and Sue Moon. "What Is Twitter, a Social Network or a News Media?" Proc. of International World Wide Web Conference Com- Mittee, Raleigh, North Carolina. 2010.

L, G. "Http://www.economist.com/blogs/democracyinamerica/2011/10/social-media-and-wall-street-protests." *The Economist*. The Economist Newspaper, 11 Oct. 2011. <http://www.economist.com/blogs/democracyinamerica/2011/10/social-media-and-wall-street-protests>.

Lake, David A., and Wendy H Wong. "The Politics of Networks: Interests, Power, and Human Rights Norms." Networked Politics: Agency, Power, and Governance. Ithaca: Cornell UP, 2009.

Lee, Amy. "Cisco Said To Aid China In Installing Massive 'Peaceful Chongqing' Surveillance System." *The Huffington Post*. TheHuffingtonPost.com, 05 July 2011. <http://www.huffingtonpost.com/2011/07/05/cisco-china-peaceful-chongqing-surveillance_n_890382.html>.

Lessig, Lawrence. The Future of Ideas: The Fate of the Commons in a Connected World. New York: Random House, 2001.

Libicki, Martin C. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND, 2009.

Lohmann, Susanne. "The Dynamics of Informational Cascades: The Monday Demonstrations in Leipzig, East Germany, 1989-91." *World Politics* 47.1 (1994): 42-101. *JSTOR*.

Lynch, Marc. "Tunisia and the New Arab Media Space." *Foreign Policy*. 15 Jan. 2011.

Mackey, Robert. "Victory for WikiLeaks in Iceland' s Parliament." *The Lede Blog*. 17 June 2010. <http://thelede.blogs.nytimes.com/2010/06/17/victory-for-wikileaks-in-icelands-parliament/>.

MacKinnon, Rebecca. Consent of the Networked: The World-wide Struggle for Internet Freedom. New York: Basic, 2012.

Maginnis, Robert. "China Cyber-Stealing Its Way to Super Power Status." 10 Nov. 2011.

Maoz, Zeev. Networks of Nations: The Evolution, Structure, and Impact of International Networks, 1816-2001. Cambridge: Cambridge UP, 2011.

Mathews, Jessica T. "Power Shift." Foreign Affairs (1997). <www.foreignaffairs.com/articles/52644/jessica-t-mathews/power-shift?page=show>.

Mbeke, Peter O. *The Role of the Media in Conflict and Peace Building in Kenya*. Nairobi, 2009.

Meier, Patrick. "Changing the World, One Map at a Time." Lecture. TEDxKC. *PeaceMedia*. <http://peacemedia.usip.org/resource/patrick-meier-changing-world-one-map-time-%E2%80%93-tedxkc>.

Meier, Patrick. "Changing the World, One Map at a Time." *Slideshare.net*. 15 Apr. 2011. <http://www.slideshare.net/iRevolution/meier-re-publica-2011>.

Meier, Patrick. "What Is Crisis Mapping? An Update on the Field and Looking Ahead." *IRevolution*. 20 Jan. 2011. <http://irevolution.net/2011/01/20/what-is-crisis-mapping/>.

Michael, Maggie. "Mubarak Faces Egypt Protests On 'Day Of Rage'" *The Huffington Post*. TheHuffingtonPost.com, 25 Jan. 2011. <http://www.huffingtonpost.com/2011/01/25/mubarak-faces-egypt-prote_n_813572.html>.

Miel, Persphone, and Robert Faris. *NEWS AND INFORMATION AS DIGITAL MEDIA COME OF AGE*. Berkman Center for Internet and Society at Harvard University, 2008.

Mobile Giving Survey 2011. 14 Oct. 2011.

Morozov, Evegeny. "Political Repression 2.0." The New York Times. 1 Sept. 2011. <http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html>.

Morozov, Evgeny. "Facebook and Twitter Are Just Places Revolutionaries Go." Web log post. The Guardian. 7 Mar. 2011. <http://www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians>.

Morozov, Evgeny. "Iran Elections: A Twitter Revolution?" *Washington Post*. The Washington Post, 17 June 2009. <http://www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html?hpid=topnews>.

Morozov, Evgeny. "On the Irresponsibility of Internet Intellectuals." Foreign Policy. 13 Sept. 2010. <http://neteffect.foreignpolicy.com/posts/2010/09/13/on_the_irresponsibility_of_internet_intellectuals>.

Morozov, Evgeny. "The Great Internet Freedom Fraud." Foreign Policy. 16 Sept. 2010. <http://www.foreignpolicy.com/articles/2010/09/16/the_great_internet_freedom_fraud>.

Morozov, Evgeny. "Why the Internet Is a Great Tool for Totalitarians." Wired. 27 Dec. 2010. <http://www.wired.com/magazine/2010/12/st_essay_totalitarians/>.

Morozov, Evgeny. The Net Delusion: The Dark Side of Internet Freedom. New York, NY: PublicAffairs, 2011.

Moses, Asher. "Fighting China's Golden Shield: Cisco Sued over Jailing and Torture of Dissidents." *Smh.co.au*. The Sydnet Morning Herald, 16 Aug. 2011.

Mueller, Milton. Networks and States: The Global Politics of Internet Governance. Cambridge, MA: MIT, 2010.

Mulrine, Anna. "Pentagon Papers vs. WikiLeaks: Is Bradley Manning the New Ellsberg?" *The Christian Science Monitor*. The Christian Science Monitor, 13 June 2011. <http://www.csmonitor.com/USA/Military/2011/0613/Pentagon-Papers-vs.-WikiLeaks-Is-Bradley-Manning-the-new-Ellsberg>.

Murphy, Zoe. "China Struggles to Censor Train Crash Coverage." *BBC News*. 28 July 2011. <http://www.bbc.co.uk/news/world-asia-pacific-14321787>.

Nagan, Winston P., and Craig Hammer. "The Changing Character of Sovereignty in International Law and International Relations." *University of Florida Levin College of Law*.

"News and Information as Digital Media Come of Age." *Berkman Center for Internet & Society*. 18 Dec. 2008. <http://cyber.law.harvard.edu/node/4904>.

"New Study on the Use of Social Media in Fighting Corruption." Civil Society Against Corruption, 1 Feb. 2012. Web. <http://www.againstcorruption.eu/story/new-study-on-the-use-of-social-media-in-fighting-corruption>.

Nordenson, Bree. "Overload! Journalism's Battle for Relevance in an age of Too Much Information." *Columbia Journalism Review*. Dec. 2008.

Nye, Joseph S. The Future of Power. New York: PublicAffairs, 2011.

Nye, Joseph. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, 2010.

"NYPD: Arrests In 'Occupy Wall Street' Protest Justified." *CBS New York*. 24 Sept. 2011. <http://newyork.cbslocal.com/2011/09/24/police-make-arrests-in-wall-street-protest/>.

O'Connor, Rory. "#january25 One Year Later: Social Media & Politics 3.0." *Huff Post Media*. 25 Jan. 2012.

Olivarez-Giles, Nathan. "Tunisia Protesters Use Facebook, Twitter and YouTube to Help Organize and Report." *Los Angeles Times*. 14 Jan. 2011.

Osiander, Andreas. "Sovereignty, International Relations, and the Westphalian Myth." *International Organization* 55.2 (2001): 251-87. *Labmundo.org*. <http://www.labmundo.org/disciplinas/OSIENDER_sovereignty_international_relations_and_the_westphalian_myth.pdf>.

Peckham, Matt. "Facebook and Twitter Will Say No to Social Media Blocking in Wake of Riots." *Time*. 24 Aug. 2011.

Press, Andrea Lee., and Bruce Alan. Williams. The New Media Environment: An Introduction. Chichester, West Sussex, U.K.: Wiley-Blackwell, 2010.

Preston, Jennifer. "Protesters Look for Ways to Feed the " *The New York Times*. The New York Times, 25 Nov. 2011. <http://www.nytimes.com/2011/11/25/business/media/occupy-movement-focuses-on-staying-current-on-social-networks.html>.

Rauhala, Emily. "What Uprising? China Censors News From Egypt." *TIME.com*. 31 Jan. 2011. <http://newsfeed.time.com/2011/01/31/what-uprising-china-censors-news-from-egypt/>.

Reagle, Joseph M. "‘‘Be Nice’’: Wikipedia Norms for Supportive Communication." *New Review of Hypermedia and Multimedia,* 16.1 (2010): 161-80.

Republic of the Philippines Department of Science and Technology. Publication. 2003.

Roberts, Chris. "Gatekeeping Theory: An Evolution." *The University of South Carolina* (2005). <http://www.chrisrob.com/about/gatekeeping.pdf>.

Rosen, Jeffrey. *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*. Governance Studies at Brookings, 2011.

Rosenau, James, and David Johnson. "Information Technologies and Turbulence in World Politics." Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age. Ed. Juliann Emmons Allison. Albany: State University of New York, 2002.

Ross, Alec. "Digital Diplomacy and US Foreign Policy." *The Hague Journal of Diplomacy* 6 (2011): 451-55.

Ross, Alec, and Michael H. Posner. "Briefing on Internet Freedom and 21st Century Statecraft." *U.S. Department of State*. U.S. Department of State, 22 Jan. 2010. Web. <http://www.state.gov/j/drl/rls/rm/2010/134306.htm>.

Rushe, Dominic. "Icelandic MP Fights US Demand for Her Twitter Account Details." *The Guardian*. Guardian News and Media, 01 July 2011. <http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages>.

Russian Invasion of Georgia. 10 Nov. 2008.

Sabbagh, Dan. "Tories Torn over Regulating Social Media." *The Guardian*. Guardian News and Media, 24 Aug. 2011. <http://www.guardian.co.uk/uk/2011/aug/24/cameron-twitter-regulation>.

Sanderson, Thomas, David Gordon, and Guy Ben-Ari. *International Collaborative Online Networks*. Washington, D.C.: CSIS, 2008.

Schachtman, Noah. "26 Years After Gibson, Pentagon Defines 'Cyberspace'."*Wired.com*. 23 May 2008. Web. <http://www.wired.com/dangerroom/2008/05/pentagon-define/>.

Schmidt, Eric, and Jared Cohen. "The Digital Disruption: Connectivity and the Diffusion of Power." Foreign Affairs. 2010. <http://www.foreignaffairs.com/articles/66781/eric-schmidt-and-jared-cohen/the-digital-disruption>.

Schmitt, Michael. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: National Academies, 2010.

Sheridan, Mary B. "Autocratic Regimes Fight Web-savvy Opponents with Their Own Tools." The Washington Post. 22 May 2011. <http://www.washingtonpost.com/world/autocratic-regimes-fight-web-savvy-opponents-with-their-own-tools/2011/04/19/AFTfEN9G_story.html>.

Shirky, Clay. "The Political Power of Social Media: Technology, the Public Sphere, and Political Change." Foreign Affairs (2011). <http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media>.

Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs*. Jan.-Feb. 2011. <http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media>.

Sikkink, Kathryn. "The Power of Networks in International Politics." Networked Politics: Agency, Power, and Governance. Ithaca: Cornell UP, 2009.

Silverman, Justin. "BART Phone Blackout: Did the S.F. Transit Agency Violate Free Speech Protections?" *Citizen Media Law Project*. 25 Aug. 2011. <http://www.citmedialaw.org/blog/2011/bart-phone-blackout-did-sf-transit-agency-violate-free-speech-protections>.

Singh, J. P. "Multilateral Approaches to Deliberating Internet Governance." Policy & Internet 1.1 (2009): 91.

Sinnreich, Aram, Nathan Graham, and Aaron Trammell. "Weaving a New 'Net: A Mesh-Based Solution for Democratizing Networked Communications." The Information Society 27.5 (2011): 336-45..

Slaughter, Anne-marie. "A New Theory for the Foreign Policy Frontier: Collaborative Power." The Atlantic, 30 Nov. 2011.

<http://www.theatlantic.com/international/archive/2011/11/a-new-theory-for-the-foreign-policy-frontier-collaborative-power/249260/>.

Slaughter, Anne-Marie. "America's Edge: Power in the Networked Century." Foreign Affairs (2009). Foreign Affairs. <http://www.foreignaffairs.com/articles/63722/anne-marie-slaughter/americas-edge?page=show>.

"Mubarak Tells Egypt He Will Not Seek Re-Election." *The Huffington Post*. TheHuffingtonPost.com, 01 Feb. 2011. <http://www.huffingtonpost.com/2011/02/01/mubarak-tells-egypt-he-wi_n_817132.html>.

"Sovereignty." *Stanford Encyclopedia of Philosophy*. 31 May 2003. <http://plato.stanford.edu/entries/sovereignty/>.

Standby Volunteer Task Force, and UN OCHA. *Libya Crisis Map Deployment*. 2011.

Steele, Cherie, and Arthur Stein. "Communications Revolutions and International Relations." Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age. Ed. Juliann Emmons Allison. Albany: State University of New York, 2002.

Stelter, Brian. "Twitter Feed Evolves Into a News Wire About Egypt." *Media Decoder Blog*. The New York Times, 13 Feb. 2011. <http://mediadecoder.blogs.nytimes.com/2011/02/13/twitter-feed-evolves-into-a-news-wire-about-egypt/>.

Stremlau, Nicole, Matthew Blanchard, Yusuf A. Gabobe, and Farhan A. Ahmed. *The Role of the Media in the Upcoming Somaliland Elections: Lessons from Kenya*. Stanhope Centre for Communications and Policy Research, 2009.

"Stuxnet." *The New York Times*. 15 Jan. 2011. <http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html>.

Swaine, Jon. "Georgia: Russia 'conducting Cyber War'" *Telegraph.co.uk*. 11 Aug. 2008. Web. <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>.

Tanenbaum, Andrew S. *Computer Networks*. Upper Saddle River, NJ: Prentice Hall PTR, 2003.

Taliaferro, Jeffrey. *GLOSSARY OF KEY TERMS IN INTERNATIONAL RELATIONS*. 27 Oct. 2008. Medford, MA.

Tehranian, Majid. "GLOBAL COMMUNICATION AND INTERNATIONAL RELATIONS: CHANGING PARADIGMS AND POLICIES." The International Journal of Peace Studies 2.1 (1997). <http://www.gmu.edu/programs/icar/ijps/vol2_1/Techrenian.htm>.

"The Economic Impact of Shutting down Internet and Mobile Phone Services in Egypt." *OECD.org*. OECD, 4 Feb. 2011. <http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html>.

The International Criminal Court and Post-Election Violence in Kenya. Internews, 2010.

"The Meaning of Stuxnet A Sophisticated "cyber-missile" Highlights the Potential—and Limitations—of Cyberwar." *The Economist*. 30 Sept. 2010. <http://www.economist.com/node/17147862>.

Schaffer, Jan. *The Role of Cell Phones in Carrying News and Information*. Publication. Washington, D.C.: Center for International Media Assistance, 2008.

"The Web's New Walls." *The Economist*. 2 Sept. 2010.

Thomson, Janice E. "State Sovereignty in International Relations: Bridging the Gap Between Theory and Empirical Research." *International Studies Quarterly* 39 (1995): 213-33.

"Tor: Overview." Tor Project. Web. <https://www.torproject.org/about/overview.html.en>.

"Treaty of Westphalia." *The Avalon Project*. <http://avalon.law.yale.edu/17th_century/westphal.asp>.

Tufecki, Zeynep. "As Egypt Shuts off the Net: Seven Theses on Dictator's Dilemma." Web log post. Technosociology. 28 Jan. 2011. <http://technosociology.org/?p=286>.

Ungerleider, Neal. "Here's a Map of the Humanitarian Crisis Hotspots in Libya (Don't Tell Gaddafi)." *Fast Company*. 3 Sept. 2011. <http://www.fastcompany.com/1736822/libya-crisis-map-united-nations>.

United Nations ICT Task Force. Internet Governance: A Discussion Document. By George Sadowsky, Raul Zambrano, and Pierre Dandjinou. New York, USA, 2004.

United Nations, Charter of the United Nations, 1945, 1 UNTS II, available at: http://www.un.org/en/documents/charter/chapter2.shtml [accessed 9 April 2012]

United States of America. Department of State. United States Advisory Commission on Public Diplomacy. *A NEW DIPLOMACY FOR THE INFORMATION AGE*. Washington, D.C., 1996.

"Ushahidi." Web. <http://ushahidi.com/>.

Vaisman, Andries. "Ushahidi Helps Bring Crowdsourcing Technology to 132 Countries Worldwide." *Knight Foundation*. 9 Aug. 2011. <http://www.knightfoundation.org/blogs/knightblog/2011/8/9/ushahidi-helps-bring-crowdsourcing-technology-to-132-countries/>.

Vallance, Chris. "Wikileaks and Iceland MPs Propose 'journalism Haven'" *BBC News*. BBC, 02 Dec. 2010. <http://news.bbc.co.uk/2/hi/8504972.stm>.

Van Noort, Carolijn. *Social Media Strategy: Bringing Public Diplomacy 2.0 to the next Level*. San Francisco, 2011.

Walker, Christopher, and Robert W. Orttung. "Lies and Videotape." *The New York Times*. The New York Times, 23 Apr. 2011. <http://www.nytimes.com/2011/04/23/opinion/23walker.html?ref=media>.

Wang, Ching-ning. "Communication Technology and the Retreat of the State." *Http://besser.tsoa.nyu.edu/*. <http://besser.tsoa.nyu.edu/impact/f99/Papers/wang.html>.

Wasik, Bill. "Gladwell vs. Shirky: A Year Later, Scoring the Debate Over Social-Media Revolutions." Wired. 27 Dec. 2011. <Gladwell vs. Shirky: A Year Later, Scoring the Debate Over Social-Media Revolutions>.

Wawro, Alex. "What Is Deep Packet Inspection?" *PCWorld*. 1 Feb. 2012. <http://www.pcworld.com/article/249137/what_is_deep_packet_inspection.html>.

Webster, Frank. "Globalization, Information, and Change." Technology, Development, and Democracy: International Conflict and Cooperation in the Information Age. Ed. Juliann Emmons Allison. Albany: State University of New York, 2002.

Weinberger, David. "Gladwell Discovers It Takes More than 140 Characters to Overturn a Government." Web log post. Joho the Blog. 2 Oct. 2010. <http://www.hyperorg.com/blogger/2010/10/02/gladwell-discovers-it-takes-more-than-140-characters-to-overturn-a-government/>.

Wellman, Phillip W. "Facebook Becomes Divisive in Bahrain | Middle East | English." *Voice of America*. 17 Aug. 2011. <http://www.voanews.com/english/news/middle-east/Facebook-Becomes-Divisive-in-Bahrain-127958073.html>.

Whittaker, Zack. "Two-thirds of Brits Support Facebook, Twitter Shutdown in Future Riots." Weblog post. *ZDNet*. 8 Nov. 2011.

"Who Are the Tier 1 ISPs?" *DrPeering*. <http://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php>.

Wines, Michael, and Sharon LaFraniere. "In Baring Facts of Train Crash, Blogs Erode China Censorship." *The New York Times*. The New York Times, 29 July 2011. <http://www.nytimes.com/2011/07/29/world/asia/29china.html>.

Wolf, Naomi. "The Shocking Truth about the Crackdown on Occupy." *The Guardian*. Guardian News and Media, 25 Nov. 2011. <http://www.guardian.co.uk/commentisfree/cifamerica/2011/nov/25/shocking-truth-about-crackdown-occupy?fb=optOut>.

Yelaja, Prithi. "U.K. Riots Reveal Social Media Double Standard." *CBCnews*. CBC/Radio Canada, 10 Aug. 2011. Web. <http://www.cbc.ca/news/world/story/2011/08/10/social-media-riots.html>.

York, Jillian. "Freedom Fail." Foreign Policy 29 Apr. 2011. <http://www.foreignpolicy.com/articles/2011/04/29/freedom_fail>.

Zetter, Kim. "Did a U.S. Government Lab Help Israel Develop Stuxnet?" Wired. 17 Jan. 2011. <http://www.wired.com/threatlevel/2011/01/inl-and-stuxnet/>.\

Zetter, Kim. "Son of Stuxnet Found in the Wild on Systems in Europe." *Wired.com*. 18 Oct. 2011. <http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild/>.

Zittrain, Jonathan, and John Palfrey. "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet." *OpenNet Initiative*. <http://opennet.net/sites/opennet.net/files/Deibert_06_Ch05_103-122.pdf>.

Zittrain, Jonathan. The Future of the Internet: And How to Stop It. London: Allen Lane, 2008.

Zuckerman, Ethan. "Internet Freedom: Beyond Circumvention." Web log post. My Heart's in Accra. Ethan Zuckerman, 22 Feb. 2010.

<http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/>.

Zuckerman, Ethan. *INTERNATIONAL NEWS: Bringing About the Golden Age*. Berkman Center for Internet and Society at Harvard University, 2008.

Interviews

Al Omran, Ahmed. NPR, Social Media Production Assistant. 15 March 2012. Personal Interview.

Atshan, Sa'ed. Tufts University, Lecturer. 21 March 2012. Personal Interview.

Bestavros, Azer. Boston University, Professor. 19 March 2012. Personal Interview.

Bociurkiw, Michael. Senior Vice President of Partnership for HUM News. 6 March 2012. Personal Interview.

Ambassador Brian Carlson. Former U.S. State Department Official. 16 March 2012. Personal Interview.

De, Subrata. NBC, Executive Producer. 23 March 2012 Personal Interview.

El-Ghobashy, Tamer. Wall Street Journal, Reporter. 22 March 2012. Personal Interview.

Garden, Ken. Tufts University, Professor. 6 March 2012. Personal Interview.

Gittleson, Ben. Center for Arabic Study Abroad, Student. 1 March 2012. Personal Interview.

Harding, Joel. Information Operations Holistic Organizers. 15 March 2012. Personal Interview.

Howitt, Aliza. Occupy Boston, Member. 6 November 2011. Personal Interview.

Irizarry-Gerould, Yamila. Center for Arabic Study Abroad, Student. 29 February 2012.

Iskandar, Adel. Georgetown University, Adjunct Professor. 19 March 2012. Personal Interview.

Jemmali, Montassar Anas. Tunisian Youth Patriots. 23 February 2012. Personal Interview.

Khalil, Ashraf. Freelance Journalist. Author of Liberation Square. 27 March 2012. Personal Interview.

Lewis, James. CSIS, Director of the Technology and Public Policy Program. 23 March 2012. Personal Interview.

Litvin, Margaret. Boston University, Assistant Professor. 12 March 2012. Personal Interview.

Martel, William. Fletcher School, Professor. 12 March 2012. Personal Interview.

Mehta, Jigar. #18DaysInEgypt, Co-Creator. 23 February 2012. Personal Interview.

Meier, Patrick. Ushahidi, Co-Founder. Lincoln Labs, Ushahidi Director. 19 March 2012. Personal Interview.

Nassar, David. Hotspot Digital, Founder. 18 November 2010. Personal Interview.

Nawara, Wael. Arab Alliance of Freedom and Democracy, President. 24 March 2012. Personal Interview.

Perino, Kate. Standby Task Force Report, Team Coordinator. 7 March 2012. Personal Interview.

Perino, Kate. Occupy Boston, Member. 6 November 2011. Personal Interview.

Rageh, Rawya. Al Jazeera English, Reporter. 18 March 2012. Personal Interview.

Redmond, Scott Douglass. Clever Industries, President. 2 March 2012. Personal Interview.

Sachs, Marcus. Verizon National Security Policy. 15 March 2012. Personal Interview.

U.S. State Department Official. 28 March 2012. Personal Interview.

U.S. State Department Official. 5 April 2012. Personal Interview.

U.S. State Department Official. 19 March 2012. Personal Interview.

York, Jillian. Electronic Frontier Foundation, Director for International Freedom of Expression. 21 March 2012. Personal Interview.

Appendix A

Relevant Blogs

#18DaysInEgypt(http://beta.18daysinegypt.com/)
3Arabawy (http://www.arabawy.org/)
The Arabist (http://www.arabist.net/)
Ashraf Khalil (http://www.ashrafkhalil.com/)
The Big Pharaoh (http://www.bigpharaoh.org/)
Clay Shirky's Internet Writings (http://www.shirky.com/)
CrisisCommons(http://crisiscommons.org/blog/)
Deanna Zandt (http://www.deannazandt.com/blog/)
Dispatches from Tahrir (http://www.ashrafkhalil.com/2011/11/13/dispatches-from-tahrir/)
Empathetics: Integral Life (http://empathetics.org/2009/01/)
EngageJoe Wiki (http://www.engagejoe.com/)
Evgeny Morozov (http://www.evgenymorozov.com/writings.html)
Google Public Policy Blog (http://googlepublicpolicy.blogspot.com/)
IdealWare (http://www.idealware.org/blog)
Inanities (http://inanities.org/)
Internet.artizans (http://www.internetartizans.co.uk/)
iRevolution: From Innovation to Revolution (http://irevolution.net/)
Jadaliyya (http://www.jadaliyya.com/)
Jillian C York (http://jilliancyork.com/)
Musings of a Computer Scientist (http://blogs.bu.edu/best/)
New Diplomacy Platform (http://www.newdiplomacyplatform.com/)
OpenNet Initiative (http://opennet.net/blog)
Rantings of a Sand Monkey (http://www.sandmonkey.org/)
RConversation (http://rconversation.blogs.com/)
Tactical Technology Collective (http://www.tacticaltech.org/)
Technosociology: our tools, ourselves (http://technosociology.org/)
Traveler in an Antique Land (http://travelerinanantiqueland.blogspot.com/)
Unsettling the Dust (http://translatingrev.wordpress.com/)
The Ushahidi Blog (http://blog.ushahidi.com/)
Whimsley: Technology and Politics (http://whimsley.typepad.com/whimsley/)

Relevant Institutions

American University Center for Social Media
American University's School of International Service International Communication Program
Berkley Electronic Press
Brookings Institute
Carnegie Endowment for International Peace
Center for Strategic and International Studies
Center for Democracy and Technology
Center for Future Civic Media at MIT
Comparative Media Studies Program at MIT
Council on Foreign Relations
Fletcher Hitatchi Center for Technology & International Affairs
George Washington University Institute for Public Diplomacy and Global Communication
Harvard Berkman Center for Internet & Society
Harvard Institute of Politics

"Harvard-MIT-Yale" Cyberscholar Working Group
International Center on Nonviolent Conflict
London School of Economics Media and Communications
MacArthur Foundation
MIT Media Lab
Open Net Initiative
Public Diplomacy Council
Princeton Center for Information Technology Policy
The Information Society
University of Southern California Center on Public Diplomacy
United States Institute of Peace
Yale Law School Information Society Project

Relevant Publications
Harvard Journal of Law and Technology
Yale Journal of Law and Technology
Richmond Journal of Law and Technology
UCLA Journal of Law and Technology
Virginia Journal of Law and Technology
Information, Communication & Society Journal
Global Media Journal

Acronyms

DNS	Domain Name System
CSO	Civil Society Organization
DPI	Deep Packet Inspection
IANA	Internet Assigned Numbers Authority
ICANN	International Corporation for Assigned Names and Numbers
ICI	Information and Communication Infrastructure
ICT	Information and Communication Technology
IDS	Intrusion Detection Software
IETF	Internet Engineering Task Force
IGO	Intergovenmental Organization
IP	Internet Protocol
IR	International Relations
ISP	Internet Service Providers
IT	Information Technology
LAN	Local Area Network
RIR	Regional Internet Registries
RMA	Revolution in Military Affairs
SBTF	Standby Task Force
SCADA	Supervisory Control and Data Acquisition
SMS	Short Messaging Service
TCP	Transmission Control Protocol
TNC	Transnational Corporation
U.S. SD	United States State Department