Protecting the Internet from Dictators

Technical and Policy Solutions to Ensure Online Freedoms

Warigia Bowman

Clinton School of Public Service
University of Arkansas, USA

L. Jean Camp

School of Informatics and Computer Science
University of Indiana, USA

Protecting the Internet from Dictators: Technical and Policy Solutions to Ensure Online Freedoms

Warigia Bowman and L. Jean Camp

ABSTRACT

In this paper we explore the interaction between Internet communications, activists, and the state in Egypt, Syria, Libya, Uganda and northern Sudan. This paper addresses the following problem: Under what conditions are authoritarian regimes able to disrupt Internet traffic in situations of a popular uprising, and what can be done to prevent it? We illustrate that there are three critical variables in this interaction: redundancy in communications, distribution of power across organizations and individuals and geographic localities, and state regulation. We argue for a more resilient, redundant network. We propose policies that can be implemented in more open states with greater influence on the development of the network. We illustrate that the same investments that empower dissidents actually strengthen the Internet for commerce and government, and against unauthorized attacks.

Keywords: Internet traffic, Internet censorship, online freedom, network, Middle East.

Introduction

Internet censorship of political sites is the norm in many countries in the Middle East and Africa as well as large parts of Asia (York, 2011). Many countries— including Iran, and China— have behaved in a restrictive manner towards the Internet. In addition, some African countries, such as Ethiopia, and the Ivory Coast, filter websites. Yet, the drama of the Arab Spring focused the world's attention on the vulnerability of the Internet in countries governed by repressive regimes. Accordingly, we believe that this historical moment presents an opportunity to explore the following question: under what conditions are authoritarian regimes able to disrupt Internet traffic in situations of a popular uprising, and what can be done to prevent it?[1]

Egypt is not the only country in the Middle East or in Africa to cut its citizens off from Internet, although perhaps it presents one of the most dramatic recent examples. Shutting off access to the Internet is not a new tactic during civil unrest. According to the Open Net Initiative, similar blockades have been imposed by Burma, Nepal and China (ISOC, 2011; Johnson 2011; Richtel 2011)Still, the scope of efforts by Egypt, Libya and Syria to shut down the Internet and cellular telephony in an effort to suppress rebellion from 2011to 2013have been

[1]The authors are grateful for the helpful comments they received from the KictaNet list, the LiberationTech list, Milton Mueller, Nivien Saleh, and various anonymous reviewers. We would also like to acknowledge the Giganet Workshop at the American University in Washington, D.C. in April 2011, which forced us to formulate our thoughts on the topic.

unprecedented. These shutdowns raise an important question for academics, engineers, and activists about what steps should be taken to prevent future episodes of Internet shutdowns.

The paper will begin by examining the case of Egypt. Egypt has spent the past two years in a revolutionary transition from an authoritarian state. On January 27th, 2011, the Egyptian government—which was ruled at the time by Hosni Mubarak—shocked the world when it cut off internal access to the Internet and Internet connectivity from the outside into Egypt with the goal of repressing political activism. The Egyptian case highlighted some important technical considerations regarding ensuring, enabling or even expanding Internet access under official or unofficial attack by authoritarian regimes in crisis.

In addition to Egypt, this paper documents political controls and restrictions on the Internet in Syria, Uganda, and Libya experienced in the year of the Arab Spring 2011 and beyond. All of these countries are facing pressure from their citizens to remove dictators, dismantle semi-authoritarian governments, and to accelerate the democratization process. Citizens of all these nations all have experienced attempts by the ruling government to control, restrict and block access to the Internet in general, and Internet based social media applications such as Facebook, and Twitter in particular. Interestingly, these countries have had different outcomes with regard to activists' ability to use social media to organize. This paper contributes to the policy, political science, communications, and computer science literature by mapping the status of the Internet in these cases, and proposing innovative technical and policy solutions for protecting the Internet from dictators and repressive regimes throughout the world.

The Importance of Resilience and Redundancy

This paper derives its arguments regarding the importance of redundancy and resilience from work done in computer science and politics. We expand and broaden those arguments. In this paper, we introduce three more considerations relevant to this interaction: redundancy in communications, distribution of power across organizations, individuals and geographic locations, and state regulation.

Importantly, this literature notes that avoiding having one single point of failure can increase resilience. For example, in the context of domain name systems ("DNS"), domain names were long highly centralized in the root zone. An extremely limited number of computers in the world stored all the information about top-level domain names. As of a result of this centralization, these servers were repeatedly subject to a type of attack known as the "distributed denial of service" attack (Yogesh, 2006).Yogesh suggests that a scheme which avoids concentrating name resolution in a single server--i.e. spreading name resolution across multiple servers, increases resilience to attacks.

The current distribution of DNS servers has made the end points, not the center, more attractive as points of attack. The scale of DNS requires local copies of only a portion of the record, which is stored in a cache. As the nature of the Internet infrastructure has changed; the point of attack is altered even when overall resilience is increased. Securing networks against

disruption and censorship requires designing more resilient architectures and understanding the new vulnerabilities of these architectures.

In a similar vein, a standardized protocol DNS Security Extensions requires distributing authority over the DNS root zone (Kuerbis and Mueller, 2007). This type of protocol would also allow widespread encrypted communications, potentially enhancing security. This protocol would allow for multiple, but limited in number, non-governmental organizations to generate, sign and distribute root zone keys. This approach has multiple benefits, but embodies two politically important concepts. First, it distributes responsibility, taking advantage of decentralization. Second, it eliminates governmental organizations from the process of managing the root, thereby reducing the chances that governments will abuse their power to control the Internet. In technical terms, attacks that must subvert multiple keys or create multiple apparently valid but forged digital signatures are more difficult than attacks that must subvert a single key or signature. For example, the experience of "Flame" argues against reliance on a single signature. In a similar vein, Mueller argues for more competition among DNS roots, to reduce abuses of power (Mueller, 2001).

Laura DeNardis focuses on "critical Internet resources," including Internet Protocol addresses, (IP addresses) the Domain Name System (DNS) and Autonomous System Numbers (ASN's) (DeNardis, 2010). She notes that securing the naming, numbering, and control plan of the Internet infrastructure is one of the most critical areas of Internet governance. DeNardis highlights mounting concerns about government censorship and surveillance in the architecture itself, and also addresses techniques that repressive governments can use to suppress freedom of expression. Researchers of the University of Cambridge Computer Laboratory have also demonstrated that resilience, rather than potentially more brittle security, is an essential goal for the evolving Internet (Hall, Anderson, Clayton, Ouzounis, and Trimintzios, 2011).

Building upon this literature, we argue for a more resilient, redundant, and distributed network. We suggest that a critical aspect of Internet Governance is ensuring both infrastructure and critical Internet resources in countries ruled by authoritarian and semi-authoritarian governments. In addition, we propose policies suitable for politically more open states that could simultaneously positively influence the development of the global Internet network. We illustrate that the same investments that will empower dissidents strengthen the Internet for commerce and government, and against unauthorized attacks.

Methodology

This paper makes specific technical and policy recommendations to respond to an ongoing crisis in telecommunications in the Middle East and North East Africa. It relies on a careful and exhaustive analysis of primary source data, including newspaper interviews, interviews with activists and government officials, as well as participant observation by one of the authors during the January 25th Revolution in Egypt itself. In addition, this paper uses secondary sources, such as newsletters, emails by activists and academics, blogs and opinion pieces. This paper also builds on the authors' original qualitative research on the state of the telecommunications sector in Northern and Eastern Africa.

Cases for Discussion

The cases of Egypt, Libya, Syria and Uganda are of great interest to political and telecommunications analysts. We specifically analyze these countries over a short time frame: one of great upheaval that took place during the Arab Spring from January 2011 to January 2013. All countries are in the process of initiating or deepening democratization. All countries examined in this document have experienced efforts by repressive governments to control the Internet to varying degrees in an effort to minimize dissent. Yet, although this thread of control runs through the narrative, these countries have had wildly varying degrees of success in their efforts.

In Egypt in the spring of 2011—almost exactly two years ago—, Mubarak was completely successful in shutting off multiple means of communication for nearly a week. Yet, after Mubarak's fall, the Internet, Facebook, Twitter and other social media have become vibrant tools for organizing and reporting, both inside and outside the country. In Syria, the government of Bashar al Assad has been fairly successful in limiting access to the Internet and social media, but the country has also experienced periods of liberalization. Libya during its rebellion represented a scenario, where the government had full control over means of communication, but the rebels' access to communication depended on their proximity to democratizing Egypt. Finally, Uganda represents the best-case scenario. There, Museveni's attempts to shut off Twitter and Facebook—even for 24 hours—failed.

Egypt

In a futile effort to cling to power and quell dissent, the failing Mubarak government used many avenues to restrict or control information during the January 25th Revolution, including shutting down Internet access on January 27th. By January 29th, 2011, 91% of Egypt's Internet networks were down (ISOC 2011; Richtel, 2011).

How was the Internet Taken Offline in Egypt?

The now deposed Mubarak government used multiple methods to take Egypt offline. To get access to the rest of the Internet, Egyptian Internet Service Providers (ISPs) need a "gateway": a physical link to other ISPs outside of Egypt, which ISPs lease from the Egyptian Government. First, the Egyptian government asked Internet Service Providers to disconnect their services or face long-term commercial risk (e.g., lose their licenses) or even face immediate personal risk (vividly illustrated by the arrest of Google's Wael Ghonim) (Richtel, 2011). As the ISPs complied with the government's order, network addresses within Egypt became unreachable.[2] Vodafone resisted, until, in the words of the New York Times, "it was obliged to

[2]One of the only websites still active in the entire country was the AUC website. AUC owns the IP prefix 213.181.237.0/24 announced by the AS8524. This connects with RAYA Telecom and Noor Data Networks. AUC was able to maintain very limited connectivity by switching between these two service providers.

comply" (Glanz and Markoff, 2011) More impressively however, Noor Group provided service for several more days after the 28th.

Had ISPs chosen not to comply, Telecom Egypt could have physically cut off the connection to the network at the gateway level, which would have severely disrupted traffic in other countries. In addition the government reportedly took down Egyptian country code Domain Name Servers,halting[3] all traffic to and from local sites. Finally, Internet Exchange Points (IXPs) were disabled, severing in-country connectivity (Johnson, 2011; ISOC, 2011; Fahim, 2011).

Impact of Internet Shutdown in Egypt

With the Internet down, Egypt seemed cut off from the world. The sense of disconnection was heightened because the government had shut off mobile texting and Twitter, pulled *Al Jazeera* Arabic TV (but not *Al Jazeera* English), and even stopped all mobile telephony and outgoing landline telephony for several days. Egyptian business was devastated, untold millions of dollars were lost from electronic transactions, and the banking system and stock exchange were crippled.

As its failure became more likely, the Mubarak government probably intended that shutting down the network would slow political agitation. In fact, turning off cell phones, and making the Internet go dark likely sped up the regime's fall. In the absence of new technologies, people were forced to rely on traditional means of communication, including knocking on doors, going to the Mosque (Bremer 2011), assembling in the street, or other central gathering places. Indeed, interviews conducted with Egyptian citizens indicate some revived traditional means of communication such as climbing palm trees to make announcements (Bremer, 2011).

Thomas Schelling (1960) won the Nobel Prize for discovering that in the absence of information, people will coordinate by selecting a focal point that seems natural, special or relevant to them. Given the protests, Tahrir was—and is—the obvious focal point. By blocking the Internet, Mubarak's government inadvertently fueled dissent while galvanizing international support for the people of Egypt.

[3]Domain Name Servers map the human-usable, common Domain (e.g., "soic.indiana.edu or http://scc.cu.edu.eg/) to an address that is usable by the network for connectivity, i.e., an IP address. It has been argued that these are inherently hierarchical and certainly the governance of these is implemented as a strict hierarchy. Just as the School of Computing controls soic.indiana.edu, Indiana University controls indiana.edu and EduCause manages .edu; the Scientific Computation Center controls scc.cu.edu.eg; University of Cairo controls cu; and the government of Egypt controls .eg. Therefore it very easy for a nation to cut off those organizations that are within the hierarchy of the county's county code domain name by simply refusing to map the domain names to the Internet addresses. However, since FaceBook and Twitter are .com addresses, simply bringing down the .eg hierarchy would not have affected that mapping.

Libya

Libya is an oil-rich nation in North Africa. Libya also faced a revolutionary political transition in the past two years. A revolt pushed Colonel Muammar El Qaddafi out of power after forty years of erratic and idiosyncratic rule. Demonstrations in Libya against the Qaddafi government began in February, 2011, as part of the wave of protest sweeping the Arab world. On February 22, Qaddafi initiated an armed crackdown—shooting two unarmed men at a rally—which would deteriorate into civil war. Activists on the Internet announced a "day of rage," in the capital Tripoli, echoing Egypt's revolutionaries.

Shortly after the Libyan demonstrations started, Internet access and cell phone access deteriorated sharply (Gonzales and Harting, 2011).Colonel Qaddaffi mimicked Mubarak's actions, creating an information blackout in Tripoli (Faheem and Kirkpatrick, 2011). Qaddafi reacted to the protests in Tripoli and elsewhere by tightly controlling the movements of foreign journalists, shutting down mobile phones and the Internet, and interfering with television transmissions. By late February, even the United Nations High Commissioner for Refugees was unable to communicate effectively with Libya. Even *Al Jazeera* experienced interference on the Arabsat satellite frequency shortly after civil war broke out in Libya.

Protesters and journalists were limited in large part to satellite phones to get the news out of the country (Ryan, 2011).Libyana, one of the country's two main mobile phone providers, was somehow able to stay online and provide free service throughout the uprising (Hill, 2011). According to Evan Hill of *Al Jazeera*, Qaddafi shut down the other provider, Al-Madar. Qadaffi further ordered the monopoly telecommunications company to switch off landline access and severed—physically cut— Libya's backbone fiber optic cable, which connected the phone and Internet in the eastern part of the country to those in the western part of the country.Libyana was able to stay online because it was less centralized and had key infrastructure and equipment in rebel held Benghazi. Despite local connectivity, callers had difficulty connecting beyond the country's borders, and calls often disconnected. The rebels were able to shuttle some communications equipment into the country as NATO allowed some rebel flights in to bring personnel, food, medicine and other key materiel. The situation was alleviated somewhat when a team arrived from the UAE with a large satellite dish, a modem, routers and other equipment, and was able to connect Libyana to Etilsalat, allowing connections to the rest of the world.

With the death of Colonel Muammar Qaddafi on October 20th, 2011, the nation of Libya transitioned to a new government controlled by former rebel forces. The provisional government, the Transnational National Council took charge of the levers of power. Militias have since made the centralization of power in the new country difficult. On July 7th, 2012, Libyans elected their first government under democratic rule. A coalition led by Mahmoud Jabril, a Western educated political scientist won the majority of the seats. There is currently not updated information on the status of telecommunications under the provisional government.

What lessons can be learned from the Libyan case? Importantly, in the case of Libya, the former dictator Qaddafi controlled the country's satellite and cell phone communications infrastructure. The lesson in this case is that having complete government control of a monopoly or duopolistic telecommunications infrastructure completely is risky. Because there was some

distribution of infrastructure, however, the natural diffusion of networking under the packet switched world was already a component of information availability during the transition. To this day, Egypt and Syria have only one Internet gateway, controlled by the government-owned monopoly telecommunications company. These highly centralized systems of control are extremely vulnerable to being shut down by dictators.

To the extent that the Libyan Internet remained resilient during the civil war, it did so because infrastructure was geographically distributed in areas out of control of the main government. The capacity for the connectivity within the regional network was in part a function of the manner of disconnection; there were apparently no disruption attacks beyond severing the connectivity through shutting down power or links. Inter-network connectivity was gained by the use of VSATs, although they provided limited bandwidth. Finally, the private sector bravely stepped in, in the form of Libyana and Etilsalat, to provide connectivity despite the risk of a military attack by Qaddafi. Accordingly, broad physical distribution of the network, and a combination of private sector and government control, will decrease network vulnerability in authoritarian settings. This case demonstrates how resilient networking protocols, which continue to function within isolated domains, are necessary for any situation of disruption: natural disaster, revolution, or scattered power failures.

Syria

Despite an ongoing rebellion that emerged out of the Arab Spring, Syria is still nominally ruled by the repressive—and extremely violent—government of President Bashar al-Assad, who inherited rule from his father, also a dictator. A series of protests began in Syria in March 2011. Al Assad began cracking down harshly in April of the same year. As the crackdown now enters its third year, soldiers have defected from the Syrian Army to fight alongside rebels. As of summer 2012, the rebel coalesced around a group called the Free Syrian Army. By the beginning of 2013, Syria had descended into civil war. Over 60,000 Syrians have died, mostly civilians. More than 400,000 Syrians have fled as refugees into neighboring countries. In late 2012, the United States formally recognized the National Coalition of Syrian Revolutionary and Opposition Forces as the country's legitimate representative.

Syria has long had strict controls on the Internet (York 2011). The ruling government in Syria still controls mobile telephony (Syriatel) as well (Stack, 2011). The Internet in Syria is mainly provided by the Syrian Telecom Establishment, the state owned Internet Service Provider (Renesys, 2011) In the past, Syria has blocked the sites of social media, as well as those of political opposition parties, in addition to filtering social content aggressively (York, 2011). In addition, the website of the banned Muslim Brotherhood has been blocked in Syria. Internet activists in Syria were able to circumvent some of these restrictions by using VPN based services, web-based proxies, and other anti-censorship tools. That citizens were banned for reading did not imply that the police were not. Indeed, while the ban on Blogspot was in place, four bloggers were arrested for content published on Blogspot blogs.

In February, 2011, Syria granted open access to Facebook, Blogspot, and YouTube for the first time since 2007. Yet, social media tools in Syria have certainly been used by the Al Assad government for surveillance of activists (York 2011). The US State Department has

mentioned its concern that the Syrian government may be using social media tools to monitor activists. Indeed, these concerns have a foundation. In Azerbaijan, the moderator of a Facebook page was arrested, and in Tunisia, dissidents' Gmail and Facebook accounts were hacked by the Government during the Jasmine Revolution. More recently, Moroccan activists have also had their Facebook accounts hacked. Tweets have highly identifiable information, which is a boon to security services looking for activists to arrest. Even if activists are anonymous, deep packet inspection, a technique common in Iran and China, can reveal the identities of activists.

By the end of May 2011, Syria had re-imposed restrictions on the Internet (Preston, 2011). The Syrian government has demanded that dissidents turn over their Facebook passwords, and has also turned off the mobile network intermittently. The Syrian government's approach was more subtle approach than that of the Egyptian government. For most of the conflict, instead of shutting down the entire Internet, as the Mubarak government did, the Syrian government turned off electricity and telephone in neighborhoods with many activists. Indeed, York's warnings that Facebook would prove to be a risk for dissidents have become true, as the Syrian government has used the application to monitor dissidents critical of the regime, confiscating laptops, and attacking opponents online.

On June 3, 2011, massive protests called for the resignation of President Bashar al Assad. In response, the government temporarily shut down the Internet access for those in Syria (Washington Post; Google 2011). For those outside of Syria, approximately two thirds of Syria's networks were no longer reachable from the global Internet (Renesys, 2011). Service was restored on June 4, 2011. This first major Syrian Internet shutdown caused a global furor. Online videos of protests and government crackdowns have been one of the only ways that the world has been able to stay informed about Syria's popular uprising. Due to the rolling Internet blackout in Syria, media activities have had to move to the border with Turkey to pick up a signal from Turkcell (Stack, 2011).

Syria is now embroiled in a deadly full-scale civil war, after government forces fired on protesters peacefully demonstrating in Damascus on July 15, 2011. The United States is currently mulling over what type of intervention is appropriate to help the Syrian people. In June 2012, the Wall Street Journal reported that the US military, the CIA and the State Department, in conjunction with Turkey, Saudi Arabia, Qatar and other allies of the rebels is providing the Syrian Free Army with logistical and communications support (WSJ, June 2012). Much of this support is flowing over the Turkish border, where branches of the Syrian Free Army are based. The Syrian conflict is not be as quickly resolved, or as decisive as the outcome in Libya. The current election outcomes in Egypt show that even that revolution may take years to resolve. Indeed, ensuring the freedom of the Internet in the region will not be a short-term project.

In late November 2012, the Syrian national Internet was shut down again, with analysts speculating that Assad had ordered the Internet and some cell phone connections switched off (Timberg, 2012).Further, in areas such as Deir al Zour, the Syrian government has maintained a sustained information outage. The Syrian government has placed sharp limits on the movement of independent journalists. The inability to get accurate information from traditional news sources has thus heightened the importance of social media as an information source.

First, the Syrian case illustrates that the use of authentication techniques that depend upon "who you know," also called social authentication, must be evaluated in terms of possible risks to dissidents (Kim, Tang, and Anderson 2012). For example, Facebook considered a protocol that required that you indicate the faces that you recognize to recover a lost password. Such an authentication approach, which asks dissidents to acknowledge their membership in a set of nine people, one of whom is known to be an associated with an identified enemy of a regime, will actually heighten the ability of repressive regimes to single out dissidents.

Second, the Syrian case demonstrates that neighboring countries with more open governments, such as Turkey Lebanon, and Jordan can, and have been providing crucial support for the beleaguered communication apparatus of the rebels. Indeed, the State Department has sent 2000 pieces of communication equipment, including satellite phones, to the rebels (Timberg, 2012) The United States government and other rebel sympathizers could enhance communications by providing technology such as Cells on Light Trucks in politically protected areas can enable connectivity to the outside world in conflict situations.

Uganda

Uganda is a semi-authoritarian state that nonetheless has some democratic aspects. President Yoweri Museveni came to power in a military coup 25 years ago. Uganda has both an elected Parliament and an elected President. Uganda held both parliamentary and presidential elections in February of 2011. Musevenihas in the past been considered a reformer, and has brought peace and stability to Uganda. However, he recently pushed a change to the Constitution through Parliament allowing him to run for a fourth presidential term. His government combines both democratic and authoritarian aspects.

Voting during the February 2011 elections in Uganda was largely peaceful. However, discontent simmered under the surface as Dr. Kizza Besigye tried to unseat President Yoweri Museveni.Besigye has unsuccessfully contested the presidency in Uganda in the past three elections. Museveni won the past election with 68 percent of the vote. Besigye has a significant political following. As voting during this February's presidential election occurred, the government sought to censor text messages deemed to have the potential to incite unrest, such as those containing the words "Egypt, or "bullet." (Gettleman and Kron, 2011)

There is credible evidence that Museveni did try to block the Internet and other forms of media to control political activism. Uganda has implemented a new type of control on the Internet for activists, blocking websites temporarily around a protest or some other political event (York, 2011). The opposition, led by Besigye, implemented "Walk To Work" protests against high food and fuel prices in Uganda in mid-April (Onyango-Obbo, 2011).TheUgandan Communication Commission allegedly ordered Ugandan ISPs to block Facebook and Twitter for 24 hours. The sites were apparently unavailable for a short time period on Uganda Telecom (*The Observer,* 2011). In a move that echoed the Mubarak government's attempt to usher in an alternate reality by not covering protests in Tahrir, while broadcasting only happy scenes of soldiers giving candy to children on TV during the Revolution, the Ugandan government ordered NTV not to broadcast the major Walk to Work protest live on television.

These largely unsuccessful efforts to control political information were accompanied by a violent and brutal police arrest of the leader of Uganda's main opposition party (Freedom of Expression Clearing House). On April 20, 2011, Ugandan soldiers and police fired teargas to disperse protesters demonstrating against the arrest of Besigye. Interestingly, the attack on Besigye went viral on YouTube and resulted in an enormous number of political tweets against Museveni in Uganda (Onyango-Obbo, 2011).

What is truly intriguing about the Ugandan case, then, is not that the Museveni government attempted to control Twitter and Facebook but that it was *unsuccessful*. The inability of the government to silence the Internet for even 24 hours stands in stark contrast to Egypt, Syria, and Libya. In Egypt, the Mubarak Government asked providers to stop sending data over their ISPs. They complied. In Libya, the backbone was actually severed. In Syria, the government has almost total control of the infrastructure. By contrast, in Uganda, ISPs declined to turn off access to Facebook and Twitter. Only Uganda Telecom—the government owned telecommunications company—complied and then, only briefly. This is attributable to several differences between Uganda and the other cases. Three key differences distinguish Uganda from Libya, Syria and Egypt. First, Uganda is fairly democratic, and it has a very active parliament, and several political parties. Second, Uganda's press is quite free, and third, Uganda's telecommunications sector is one of the most of the most competitive in the entire region.

Among the semi-authoritarian states analyzed here, Uganda stands out as the most liberal. Uganda was a one-party state for a while, but has recently moved towards multiparty politics. Even as a one party state, the Parliament of Uganda had the power to curb the actions of President Museveni. In other words, Uganda has long had some semblance of substantive democracy. Second, Uganda's press is quite free. It has eight television stations, twenty-eight radio stations, and the newspaper sector, which is published in multiple languages, is openly critical of both the President and members of Parliament.

Finally, Uganda's telecommunications sector has been privatized and liberalized since the late 1990s (Bowman, 2007). The telecommunications agency was privatized (becoming UTL), with the Ugandan government retaining 49% strategic stake and 51% being sold to a strategic investor from a South African consortium. A second national operator, MTN, was licensed immediately. The third operator, Celtel, came in soon after. The Ugandan parliament explicitly wanted to encourage investment and also aimed for full liberalization. By 2009 Uganda had the most competitive telecommunications sectors in the East African Community (Bowman, 2009). In 2011, two years later, Uganda has five telecommunications providers, and at least nine Internet Service Providers.[4] More than thirty-five operators in Uganda are licensed to handle voice and data (UCC, 2011).

The Aftermath: Recent Efforts to Limit Political Expression

The Egyptian and Syrian shutdowns represent a political reference point with regard to suppression of speech on the Internet. The government of Sudan (North) responded to ongoing and wide scale student protests against Omar al Bashir's recent austerity measures by tightening

[4]Although Egypt has five ISPs as well, Egypt is three times the size of Uganda in terms of population.

state control over foreign and domestic news sources. (Zhang, June 2012) Protesters have been beaten and tear gassed, detained and arrested. Foreign news reporters have been barred from entering and reporting on the revolts. (Global Voices 2012) Nonetheless, according to the Electronic Frontier Foundation, in late June of 2012, there were rumors of an impending Internet shutdown in Sudan. (York, 2012) the Sudanese government stopped short of shutting down the Internet. Patrick Meier of Qatar Foundations' Social Research Institute states that the Bashir government used Facebook to call for a fraudulent protest, where would be protesters were then arrested, and allegedly even tortured to reveal their Facebook identities. (Meier, 2011) The Sudanese example, nearly a year after the advent of the Arab Spring, teaches us two lessons. First, Sudan demonstrates that repressive governments are learning from previous nation's experiences about how to utilize technology to increase surveillance and control of activists. Second, Sudan demonstrates that even repressive governments may think twice about the economic and political risks of a full Internet shutdown.

Social Media: Tools of Revolution?

One of the primary motivations in cracking down on the Internet in the four cases under discussion has been the government's fear of social media. What is the role of social media in organizing protest? Why is it important to protect the access of activists and organizers to social media? It is worth briefly establishing the value of social media as a tool of protest, because that can help motivate academics, engineers, and activists to ensure its availability where possible.

First, social media speed communications. They make it easy to communicate quickly with groups at remote geographical distances. In fact, some suggest that the upheavals may have spread more quickly due to the instantaneous nature of modern communications (AP, 2011). For example, activists in Jordan, Libya, Yemen, Sudan, Uganda, Bahrain, and Morocco were encouraged by the successes of their counterparts in nearby Egypt and Tunisia that they witnessed in ubiquitous news coverage on the web (Harsch, 2011).

Second, social media can be used to help ensure the accountability of regimes. This effect was seen in the summer of 2009 when Iranian activists were able to use Twitter and Facebook to send pictures to the outside world and alert them that the election was being thrown. Further, activists such as Rami Nakhle operating out of Beirut are using social media to publish news and images of the protest movement against the Syrian government. Election results in Kenya's highly contested 2010 Constitution were transmitted by SMS. Voters in Uganda were able to ask questions of candidates via Facebook during the February parliamentary and presidential elections in that country.

Third, social media shift power away from conventional media, making the position of citizen journalists more important. In cases such as Libya and Syria, where the official media do not accurately portray reality, social media are an important mechanism of getting some news, creating a public sphere outside the control of the state (Tufecki, 2011).

Fourth, and most importantly, social media facilitate organizing. Juris argues that social media help coordinate actions, build networks, and coordinate actions. Juris makes the important

point that social media "complement and facilitate face to face interaction, rather than replacing them." This point has been powerfully illustrated by the Tahrir Square protests taking place on July 15, 2011, where Tahrir and January 25th on Twitter are a key means for relaying information both within and outside Egypt regarding the ongoing protests in Tahrir Square. Social media in Egypt are being used to "publicize demands, call demonstrations and win support from broader sectors of the population" (Harsch, 2011) Shutting down the internet is not only limits political "expression" but also reduces channels and quality of political participation.

Yet, as Tarak Barkawi of the University of Cambridge and Lisa Anderson of American University have elegantly pointed out, social media do not cause revolutions, human agency does.Barkawi points out that revolutionaries in France, Haiti, and the US received news of each other's activities by ship in the late 1700s, learned from mistakes, plotted strategy, and "improved on their repertoires of revolt and resistance." Anderson notes that revolutions in Tunisia, Libya and Egypt took place in 1919, and the news spread swiftly by telegraph. Further, as Esther Dyson reminds us, the speed, and immediacy of the Internet should not lull us into the false illusion that the struggles for freedom will not be long, and hard fought.

Next Steps: Technological Solutions for Protecting the Internet

A) Recommendations for Local Activists

Both technological and policy solutions were urgently needed to respond to the autocratic blackouts imposed by Qaddafi and Al Assad. From a technological standpoint, the cases in this essay teach us that activists in countries likely to experience similar problems should mobilize well-wishers around the world, who have sufficient funds (George Soros OSI) to invest in "redundancy" as well as "distribution." Redundancy is an information concept that emphasizes building multiple lines of communication, should one line fail. Distribution is the idea that more independent means of communication should be used, and should be distributed throughout multiple users, not centralized. Four fibers in four different conduits provide redundancy. If all four of these fibers are controlled by the same institution, however, this structure does not provide distribution. Distribution is the organizational mirror of the technical practice of redundancy. The result of infrastructure which is redundant, well-distributed, and well designed is a resilient network.

A blend of old and new information technologies is best for maintaining true connectivity. "Pen and paper" lists of staff, friends, landlines, mobiles, home addresses and other key information should be maintained to prevent isolation even if the Internet goes down. Further, robust and tested methods, such as FM and shortwave radio are an outstanding means to communicate with the outside world. Indeed an ancient form of community communication - the call to prayer - played a critical role in organizing cities and towns in Egypt.

B) Recommendations to NATO/ International Organizations

In the case of Libya, where Qaddafi controlled the country's satellite and cell phone communications infrastructure, Dan Gonzales and Sarah Harting have recommended that NATO deploy cell phone base stations on aircraft or tethered balloons. Calls could then be routed to

Navy ships and a commercial operator could foot the bill, as Etilsalat has done (Gonzales and Harting, 2011). Offering unused bandwidth on pre-existing backplane infrastructure approaches being costless, and could increase the reputation and appeal of a commercial operator. However, getting the communication to the backplane can be difficult

In terms of the cellular network for areas when there is limited cellular capacity (Cells on Wheels) COWs and *COLT*s (Cells on Light Truck) are common industry terms. These are used for sudden spikes in usage (e.g., festivals) and in disaster response. The advantage of investing in these platforms over a response by the US Military is three fold. First, the technology could remain in country after any resolution of conflict. Second, local expertise in cellular technology could be created or leveraged, and this human capital could remain when any conflict is over. Third, no one can be as responsive as the people on the ground themselves in terms of knowing when there is sudden need.

COWS, COLTS, and the inherent transfer of towers when there is transfer of territory offers a possible solution to the problem of rapid response from isolation. Ad-hoc networking offers realm of possibilities; however, ensuring that there are individuals who can utilize their computers as networking nodes is critical. The expansion of training for members of NGOs, such as that supported primarily by the Open Society Institute, can be expanded to autocratic areas as long as the framing is capacity building. Ironically, much technical training is now embedded in military aid so that those least likely to need to leverage this technology against the government are the most likely to have the skills. Given the role of gender in the revolution in Egypt, targeting civilian women for technical training has the advantage of being capacity-building in the absence of any conflict, and empowering for any conflict.

Cellular networks will connect to the larger Internet through the national telephony and Internet provider networks. Thus these networks can be constructed quickly and support local communication. However, connection to the outside could remain nonexistent. In technical as well as political terms, these concentrations of connectivity remain single points of failure.

In Libya, the area held by the rebellion was safe from the air. This was not the case in Syria. Syria, like Uganda, is a large nation. Mesh networking, discussed below, would be limited. Small wireless devices, with the addition of directional antennae, are still limited to single digit miles. With this constraint, there are not network protocols that have been shown to be able to function with the hundreds of “hops” that are needed to reach the border. When there are pockets of isolated parties, and long distances to borders, satellite uplinks are nearly inevitable. Yet satellite uplinks by definition announce themselves, drawing bombing and allowing the oppressive regime to spy on rebels. Rebels and revolutionaries need a combination of mobile uplinks and grid or mesh protocols that can respond to the movement of critical nodes.

In none of the cases examined in this paper have the governments engaged in disabling attacks. However, when the relatively naïve approaches of shutting off gateways and cutting cables fails, most governments have the capacity to inject malicious content into the current control plane of the Internet. Most famously, Pakistan hacked YouTube for a significant portion of the globe in an internal censorship effort that became inadvertent attack (Hunter, 2008) and

China Telecom can accidentally hijack the traffic intended for the US Department of Defense, Apple, Cisco, DE Shaw, HP, Symantec and Yahoo! There is a problem (Rahul, 2012).

For commercial reasons providers can choose their own networks even if the path is inferior. This is problematic. AT&T rerouted traffic to China Telecom while Level3 did not. There were not internal controls or indicators of trust that distinguished Department of Defense traffic going to China Telecom from AT&T as at all unusual. These incidents illustrate the need for a global infrastructure that is more resilient against distribution of network routing misinformation. Traffic or prefixes (corresponding to specific networks) within the network can be labeled as more or less critical, with changes requiring potentially even human interaction.

C) Recommendations to Local NGOs

January 27th teaches us that a move away from centralization, particularly in the presence of autocratic governments, is crucial. Universities and NGOs who can afford to do so should invest in Very Small Aperture Terminals (VSATs). VSATs provide independent wireless link connectivity through satellite, not cable connections. VSATs can only be forced to stop operation through physical destruction. VSATs are increasingly affordable and increasingly mobile. Mobile VSAT systems provide alternatives for communication that are low bandwidth but easy to defend because they are quick to move in rural areas and potentially easy conceal (except from the sky) in urban ones. It is easy to imagine a SDN configuration combining very many mobile devices, a smaller number of laptops or desktops, with mobile VSATs as the critical link to the outside world.

D) Recommendations to Local ISPs

One potential argument is that ISPs should secure satellite links, or find other means to create non-vulnerable gateways. ISPs decide at what point they choose to cooperate with government repression, and at what point they resist. Libanya resisted and kept mobile telephony operational in much of Libya until Etilsalat could restore a link to the outside world. In order to have a decision, there must be investment before a crisis that enables a meaningful technical alternative.

While the shutdown of January 27th suggests the market will reward those who take efforts to keep the network up, the reality is that even the most resistant provider eventually complied in Egypt. Demanding that ISPs withstand governmental pressure aligns the technology against the centers of regulatory power. In contrast, demanding a more resilient control plane (so that events such as the instant removal of effectively every point inside of Egypt via routing announcement) aligns the interests of the ISPs with a network that is less vulnerable to errors and attacks with the interest in being less easy to manipulate by abuse of authority. This was the case in Libya, where alternate infrastructure was located in rebel held Benghazi. Ensuring local network connectivity in cases of disconnection from the larger network is valuable for the ISP and for every nation in the world, as each region has its own meteorological storms regardless of the existence of political turbulence.

January 27th illustrates the distinction between security and resilience, and close examinations can critically inform the development of border gateway protocols [5]over the next year. There is no question, for example, that public key infrastructure solutions would depend upon some centralized governmental or government-licenses authorities for domestic routers. Solutions, which call for agreement for the construction and removal of routes, may prove promising or problematic, depending on the point at which approval is made (Zhang, 2011).

In all of these counties there is widespread use of feature phones. These phones have the potential to provide autonomous networking. Previous work on so-called "smart dust" (e.g., Khan, 200) and processing-intensive sensor networks offers algorithms and models for using these phones themselves as platforms for communication over short distances. Next generation networking and the previous generation of research on mesh networking offer the capacity to add software (based on conditions) that enables "short-hop" communications in rapidly changing networks. Cooperative and autonomous sensing, communication, and highly distributed computing networks have been theorized for more than a decade. The Arab Spring suggests the global potential of such technology. Issues of trusted nodes, levels of trust, and priority of service have been addressed in the literature (*cf.* Camp). However, the models of trust may be inadequate. Encryption of only critical components of a message may be feasible using smart phones; but clearly public key remains beyond the processing capacity of the devices currently in most hands. What were theoretical constructs of highly distributed sensors in the past decade have arguably been realized

Next generation networking and the previous generation of research on mesh networking offer the capacity to add software based on conditions. It may be that outside connectivity or internal connectivity is critical. Borders may be a few miles away, or a few hundred. Resilience and flexibility can also assist in disaster recovery, and first response in stable regimes, as well as serving the needs of rebels in moments of political crisis.

Looking back, the failing Mubarak regime in Egypt made a careful, systematic isolation of Internet connectivity; allowing only the routes for the Egyptian stock market to remain active. The regime also ensured that traffic which was passing through, but not terminating in, Egypt was not altered. This points out to the sensitivity of the regime to the economic consequences of large-scale disruption of global connectivity. It is arguable, even likely, that a design for more secure BGP may have resulted in an even more controlled takedown. The political and technical coordination of the regime from January 27th can serve as a case in the study of the political fragility of BGP. A more resilient control plane would be more resilient to all dimensions of political attack, from dissidents as well as autocrats, and thus may be welcomed. January 27th illustrates that need for a network that is less focused on hardening and control, and more on fault tolerance and survivability. By focusing development of the next generation of BGP or

[5]BGP is the Border Gateway Protocol, which is how one network discovers a path to another network. Currently it works on announcements which are presumed to be trustworthy no matter how unlikely they may appear, such as April 2010 when a Chinese ISP announced it held 37,000 primarily subnetworks including those of the American government or in 2008 when Pakistan accidentally internationally announced that it was YouTube. BGPSEC is a set of proposals that are under examination by the IETF in order to either make the Internet more secure, more resilient, more controlled, or some combination of these.

SDN on graceful degradation, route evaluation, and survivability the timing of Arab Spring could prove timely in informing technical evolution, although in political and human terms it was inarguably long-delayed.

All the technical solutions to the autocrat are technical solutions to other threats. The same "announce and trust" foundation of routing that allowed Egypt to disappear from the virtual realm enables malicious attacks, and cascading errors. The construction of mobile alternatives to static state networks is valuable for climatic disasters (e.g., flooding, mudslides) as well as effective responses to autocratic decree. The investments in mobile response, resilience, and redundancy ironically not only enhance the ability to communicate in case of revolution, these also improve the ability to respond to crisis and reliable communication. The technologies themselves will be designed for reasons other than revolution. But without changes in policy, diffusion of these technologies will be thwarted.[6]

Policy Solutions

Western governments can also play an important role in ensuring Internet Freedoms. Export controls put in place by the Department of Commerce and the Department of Treasury "restrict the free flow of information online."As York has pointed out, the US government should ease controls on the export of Google Earth, or Microsoft to repressive regimes. Further, public statements matter. Vice President Joe Biden proclaimed that Mubarak was not a dictator, although he was forcibly quashing protests, and had cut off the Internet as well as mobile telephony in Egypt the week of January 25, 2011.

Unfortunately, companies from America manufacture the filtering products that limit access to the Internet in many countries. China prefers Cisco to censor Internet communications. Other countries in the Middle East including Tunisia, Saudi Arabia, the UAE, Bahrain and Kuwait, also use filtering technology.Websense was used in Yemen to control the Internet, whereas Qatar and the UAE are fond of Netsweeper. McAffee's Smart Filter technology is used to censor the Internet in Middle Eastern countries including Bahrain, Saudi Arabia, Oman, Sudan and Kuwait. The same TCP reset that is a foundation of the Great Firewall of China is used by American ISPs to prevent customers who seek to connect to peer-to-peer systems.

The US Department of State, as well as ministries of foreign affairs in European countries and the EU foreign policy tsar should seek to make sure that their statements in support of Internet freedoms in the Middle East and Africa are actually in line with legislation, export controls, and manufacturing efforts by American companies. Why, for example, does the US have a policy restricting the purchase of official copies of Microsoft products by Syrians, but

[6]Next generation Internet leaves open questions. Technologies that promise more consistency can threaten even current resilience against political attacks. Software defined networks and OpenFlow consider external errors and not purposeful shutdown as threats. Not only efforts to secure the control plane of the current Internet (i.e., BGP) but also the designs for the next generation of networks have been under-theorized and under-examined for threats by trusted third parties and operators.

allows the export of tools to filter the Internet in numerous repressive countries? Ironically, the US State Department has an Internet freedom agenda, which funds technology to circumvent the filtering systems built and exported by American companies. This illustrates a glaring conflict between American export policy, and diplomatic policy.

A final policy issue points not to domestic manufacturing policy, but instead to domestic law enforcement policy in the West. While the US Government cannot and should not set larger corporate standards; the US Government sets requirements for assistance to law enforcement for surveillance. Western law enforcement focuses on ease of access and certainty of availability with respect to citizens' communication. American legislation assumes respect for rule of law and demands hard-wired, usable access to Americans' communication. American router companies insisted on an the IETF standard that enabled built-in IP-based interception technologies; and it was the flagship founder of American communication - AT&T - that copied every communication through its routing center to law enforcement. A fundamental change in Western policy would be to invest in the technical training of law enforcement, so that alterations in the interest of filtering, throttling, and observation of traffic under the color of law required significant skill on the part of law enforcement. It is very easy to export a highly usable interaction for observation or destruction of communications. When that expertise is embedded in the institutions and human beings who cannot be so easily exported, the network and the globe it encircles are made both more resilient and more reliable. Constructing software such that wiretapping, surveillance, and access of stored data require multiple parties and technical expertise is the single most critical change in American policy and practice for protecting communications of dissidents abroad. Currently the surveillance is designed in, and the governance is bolted on, so to speak. This is not technical necessity; rather it is political choice. In addition to strengthening global transparency; such changes would also increase resilience of domestic networks.

Consider, for example, deep packet inspection as an innovation that has been focused on the protection of the copyrighted material in the United States. The same technology is being used to identify activists in repressive regimes. Support for ubiquitous encryption, with https as the default not the exception and with encryption enabled by default in email, would fundamentally alter the calculus of privacy and online autonomy. The focus on the putative bottom line by owners of copyright for mass-produced high-value digital entertainment information is the responsibility of those corporations. American policy makers could reasonably be expected to have a more global view. Again the conflict between immediate domestic policy (with transparency and rule of law assumed) versus immediate and long-term (global and domestic) policy is visible.

Encryption does not prevent targeted investigations of nations with rule of law, as indicated by the fact that the 2010 US Wiretap Report showed that encryption did not prevent the collection of evidence in even a single case. This is because the cryptographic keys are usually subject to technical and legal recovery on a computer such that the key can usually be recovered with targeted investment. What cryptography can do, and do well, is prevent widespread mass interception as might be used to discover activism (or even crimes) by those who would otherwise not be suspect. Embracing cryptography also limits the activities of online criminals by securing networks, as criminals and autocrats tend to be less than discriminating in their

targets. The past decades have shown that cryptography has not hindered targeted, criminal investigations.

Conclusion and a Research Agenda

The Egyptian January 25th Revolution has powerfully demonstrated that social networks and the Internet can play a powerful role in empowering people and promoting democracy (Abdel Baky, 2011). Yet, the Egyptian January 27th Internet shutdown, and the Libyan and Syrian shutdowns that followed, demonstrate the fragility of access, particularly in countries with high governmental control. Efforts should be made to expand connectivity and computer access in rural, poor and remote areas throughout Egypt, the Middle East and Africa, so that future political movements can empower and mobilize the grassroots through effective internal communication.

Alternative private sector gateways should be a standard for every nation, so that the government no longer has the power to shut down the only gateway. The experience of Russia, Armenia and Georgia (which lost Internet connectivity for five hours when a single elderly woman sought copper) argues that this duplication of resources is in the national interest. In addition, current efforts to secure the control plane should be informed by the range of technologies used to isolate and destroy Internet connectivity; focusing on more survivable and reliable routing as opposed to more secure, and potentially more fragile, technological future.

As hardware and communications facilities may change hands in the case of warfare, the implications of the next generation of networks for these potentially sudden changes should be considered. Already the challenges of running trustworthy networking on untrustworthy hardware are being considered with Software Defined Network (SDN). SDN has been focused on data centers and large ISPs, yet the use of cheap hardware as secure routers has unexplored potential for underground networks as well.

Former Secretary of State Hilary Clinton's U.S. International Strategy for Cyberspace was a bold step towards supporting Internet Freedom. As Kornbluh and Weitzner have argued, "collective action is needed to safeguard this global treasure."The US government must align export policy, diplomatic policy, the power of standards, and a technical research community that shapes the globe. Future research should explore how political participation theories may enlighten our understanding of activism using the Internet and social media. Finally, activists and policy people should demand that rights to telephony and Internet connectivity be incorporated into freedom of information guarantees.

About the Authors:

Warigia Bowman, Ph.D. earned her doctorate in public policy at the John F. Kennedy School of Government at Harvard University. She currently teaches as an Assistant Professor at the Clinton School of Public Service at the University of Arkansas. She taught as a Visiting Professor at the American University in Cairo, in the School of Global Affairs and Public Policy in 2011. She

was in Cairo during the Egyptian Revolution, and was online when the Internet was shut down. Her current research focuses on the Internet in North Africa and East Africa. She can be contacted at: warigia@gmail.com

L. Jean Camp, Ph.D. is a Full Professor in the School of Informatics and Computer Science at the University of Indiana, Bloomington. She has published books with MIT Press, Kluwer Academic, and Springer. She taught for eight years at Harvard's Kennedy School. She can be contacted at: ljcamp@indiana.edu

References:

Abdel-Baky, Mohamed. 2011.Cyber-Revolution. *Al Ahram Weekly*, February 16.Accessed March 29, 2013 at: http://weekly.ahram.org.eg/2011/1034/sc30.htm

Anderson, Lisa. 2011. Demystifying the Arab Spring, parsing the differences between Tunisia, Libya and Egypt. *Foreign Affairs*, 90(3) (May/June).

Barkawi, Tarak. 2011. World Politics and the Revolution in Libya,*Aljazeera.Net*, July 3. Accessed July 15, 2011, at:http://english.aljazeera.net/indepth/opinion/2011/07/201173113123144759.html

Booth, W. 2011. Libyan Rebels Hampered by Lack of Weapons. *The Washington Post*, July 15.

Bremer, Jennifer. 2011. Lagaan Shabaaya focus group with residents of Bulaq Dakran, Egypt. (Conducted April 17, 2011). On file with American University in Cairo, Department of Public Policy.

Bremer, Jennifer. 2011. Lagaan Shabaaya interview with residents of Beni Suef and Kajania, Egypt (conducted April 15, 2011). On file with American University in Cairo, Department of Public Policy.

Bowman, Warigia.2007. Interview with Patrick Mwesigwa. Kampala, Uganda Communications Commission.

_____. 2009."Digital Development: Technology, Governance and the Search for Modernity in East Africa." *PhD diss. Harvard University.*

_____. 2011. Email communication with Badru Ntege, CEO and Systems Engineer, one2net, Uganda. February 16.

_____. 2011.Email communication with L. Jean Camp, Professor of Informatics, University of Indiana, February 2.

_____. 2011.Email communication with Timothy McGinnis, African Internet

Infrastructure Consultant and Ambassador to the World Summit on Information Society, February 18.

Camp, L. Jean. 2011. Email communication with Warigia Bowman, Assistant Professor of Public Policy at American University in Cairo. February 2.

Cowie, James. 2011.Syrian Internet Shutdown. *Renesys Blog*. June 3. Accessed July 4, 2012, at: http://www.renesys.com/blog/2011/06/syrian-internet-shutdown.shtml

DeNardis, Laura. 2010. The Emerging Field of Internet Governance. *Yale Information Society Project Working Paper Series*. Accessed March 29, 2013 at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343

Dyson, Esther. 2011. Illusions of Democracy on the Internet. *Al Jazeera.Net*, May 28. Accessed July 3, 2011, at: http://english.aljazeera.net/indepth/opinion/2011/05/20115231423151984 25.html.

El-Sanosi, Maha. 2012. Sudan: Unshackling the Sudanese Revolution. *Global Voices*, June 24. Accessed July 4, 2012, at: http://globalvoicesonline.org/2012/06/24/sudan-unshackling-the-sudanese-revolution/

Fahim Kareem and David Kirkpatrick. 2011. Qaddafi's Grip on the Capital Tightens as Revolt Grows. *The New York Times*, February 22.

Flock, Elizabeth. 2011. Syria Internet Services Shut Down as Protesters Fill Streets. *Washington Post*, June 3. Accessed March 29, 2013 at: http://www.washingtonpost.com/blogs/blogpost/post/syria-internet-services-shut-down-as-protesters-fill-streets/2011/06/03/AGtLwxHH_blog.html

Gettleman, Jeffrey and Josh Kron. 2011. Uganda Carries Out Its Elections in Largely Peaceful Fashion. *The New York Times*, February 18.

Glanz, James and John Markoff. 2011. Egypt Leaders Found "Off" Switch for Internet. *The New York Times*, February 15.

Golooba-Mutebi, Frederick. 2011. As the Arabs Rise Up and Conquer Fear, Black Africa Looks On in Gloomy Envy, *The East African*, February 14.

Gonzales, Danand Sarah Harting. 2011. Can you hear Libya Now? *The New York Times*, March 4.

Hall, Chris, Ross Anderson, Richard Clayton, Evangelos Ouzounis, and Panagiotis Trimintzios. 2013 Resilience of the Internet Interconnection Ecosystem. Pp. 119-149 in *Economics of Information Security and Privacy III*. New York: Springer Verlag.

Harsch, Ernest. 2011. Cyber-activists Lend Savvy to North African Revolutions. *Africa Renewal*(United Nations), March 23. Accessed March 29, 2013, at: http://allafrica.com/stories/201103231054.html

ISOC Monthly Newsletter, (2011) Egypt Internet Shutdown Q & A. February 2. Accessed October 9, 2011, at: http://isoc.org/wp/newsletter?/p=3100

Hill, Evan. 2011. How Rebel Phone Network Evaded Shutdown. *Aljazeera.Net*, April 23. Accessed, July 3, 2011 at: http://english.aljazeera.net/indepth/features/2011/04/20114233530919767.html

Kim, Hyoungshick, John Tang, and Ross Anderson. 2012. Social Authentication: Harder Than It Looks. Pp. 1-16 in Angelos Keromytis (Ed.), *Proceedings of Financial Cryptography*. London, UK: Springer Verlag.

Kornbluh, Karen and Daniel Weitzner. 2011. Foreign Policy of the Internet. *The Washington Post*, July 14. Accessed March 29, 2013, at: http://articles.washingtonpost.com/2011-07-14/opinions/35237279_1_internet-global-consensus-foreign-policy

Kuerbis, Brendan and Milton Mueller. 2007. Securing the Root: A Proposal for Distributing Signing Authority. *Internet Governance Project*, Syracuse University. Accessed March 30, 2013, at http://www.internetgovernance.org/wordpress/wp-content/uploads/SecuringTheRoot.pdf

Johnson, Bobbie. 2011. How Egypt Switched off the Internet.*Gigaom.com*, January 28.Accessed on July 3, 2011, at: http://gigaom.com/2011/01/28/how-egypt-switched-off-the-internet/

Juris, Jeffrey. 2005. The New Digital Media and Activist Networking within Anti-Corporate Globalization Movements, *Annals of the American Academy of Political and Social Science*, 597: 189-208.

Macleod, Hugh and Annasofie Flamand. 2011. Tweeting the Police State. *AlJazeera.Net* English, April 9. Accessed April 1, 2013 at: http://www.aljazeera.com/indepth/features/2011/04/20114814358353452.html

Meier, Patrick. 2011. How to Use Facebook if you are a Repressive Regime. *Blog: iRevolution*: February 10. Accessed April 2, 2013, at: http://irevolution.net/2011/02/10/facebook-for-repressive-regimes/

Mwenda, Andrew. 2011. Can't Walk, Drive or Fly? So Why Is Besigye's Star Rising? *The East African*, May 9. Accessed July 13, 2011, at http://www.theeastafrican.co.ke/magazine/Cant-walk-drive-or-fly-So-why-is-Besigyes-star-rising/-/434746/1158320/-/view/printVersion/-/10xi20e/-/index.html

Mueller, Milton. 2002. Competing DNS Roots: Creative Destruction or Just Plain Destruction? *Journal of Network Industries*, 3(3).

N. A. (No Author). 2011. Total Internet Blackout in Egypt. *Al Jazeera.Net*. February 1. Accessed July 20, 2011 at: http://english.aljazeera.net/news/middleeast/2011/02/2011210459908692.html

N.A. 2011. Libya: A State of Terror. *Al Jazeera Net*. March 3. Accessed July 15, 2011, at: http://english.aljazeera.net/programmes/general/2011/03/2011338154221771.html.

N.A. 2011. "A Continent's Discontent,"*AlJazeera.Net.* April 12. Accessed July 13, 2011,at:http://english.aljazeera.net/indepth/features/2011/04/201141014942125983.html.

N.A. 2011. Authorities arrest Opposition, Battle Journalists and Protesters, April 20. *International Freedom of Expression Exchange Clearing House*, Accessed July 13, 2011, at http://allafrica.com/stories/201104210226.html

N.A. 2011.Arab Spring hardens into summer of stalemates as challenge of changing regimes becomes clearer. *USA Today*, July 17. Accessed July 15, 2011,at http://usatoday30.usatoday.com/news/world/2011-07-16-arab-spring-stalled_n.htm

Odera-Outa, G. 2011. Kenya: Use Social Media to Bring Change. *Nairobi Star*, July 8. Accessed July 13, 2011, at: http://allafrica.com/stories/201107110066.html

Onyango-Obbo, C. 2011. Museveni's Crackdown on Besigye Brings Tough Integration Issues Into the Open. *The East African*, May 16. Accessed April 5, 2013 at: http://www.theeastafrican.co.ke/news/-/2558/1162724/-/o2n541z/-/index.html

Parfitt, T. 2011. Georgian woman cuts off web access to whole of Armenia. *The Guardian*, April 6. Accessed July 12, 2011, at: http://www.guardian.co.uk/world/2011/apr/06/georgian-woman-cuts-web-access

Preston, J. 2011. Seeking to Disrupt Protesters, Syria Cracks Down on Social Media. *The New York Times*, May 22.

Richtel, Matt. 2011. Egypt Cuts Off Most Internet and Cell Service. *The New York Times*, January 28.

Ryan, Yasmine. 2011. Breaking the Sound Barrier on Libya.*AlJazeera.Net*, February 21. Accessed April 2, 2013, at: http://www.aljazeera.com/indepth/features/2011/02/2011221171619799536.html

Squarcella, C. 2011.Three Case Studies on the Egyptian Disconnection. Roma Tre University. *RIPE Labs*. Accessed July 19, 2011 at: https://labs.ripe.net/Members/csquarce/three-case-studies-egyptian-disconnection

Stack, Liam. 2011. Activists Using Video to Bear Witness in Syria, *The New York Times*, June 18.

Timberg, Craig and Babak Dehghanpisheh. 2011. Syria's Internet Shutdown Leaves Information Void. *The Washington Post*, November 29. Accessed December 7, 2012, at: http://articles.washingtonpost.com/2012-11-29/world/35585439_1_syrian-people-hama-opposition-coalition

Tufecki, Zeynep. 2011. As Egypt Shuts Off the Net, Seven Theses on the Dictator's Dilemma. *Blog: Technosociology*: our tools ourselves. Accessed August 27, 2011, at: http://technosociology.org/?p=286

Uganda Communications Commission. 2011. *Licensed Communications Service Providers*. Accessed September 12, 2011, at http://www.ucc.co.ug/#

Zhang, Xin, Hsu-Chun Hsiao, Geoffery Hasker, Haowen Chan, Adrian Perrig and David Andersen. 2011. "SCION: Scalability, Control, and Isolation on Next-Generation Networks". *Proceedings of IEEE Symposium on Security and Privacy* (Oakland), May.

York, Jillian. 2011. Unblocking Syria's Social Media. *Al Jazeera.Net English*, February 12, 2011. Accessed July 12, 2011,at: http://www.aljazeera.com/indepth/opinion/2011/02/2011212122746819907.html

_____. 2011.Africa's Cascade of Internet Censorship.*AlJazeera.Net English*, May 12. Accessed July 13, 2011, at: http://www.aljazeera.com/indepth/opinion/2011/05/2011512134039497302.html

_____. 2011. The Booming Business of Internet Censorship. *Al Jazeera.Net English*, March 29. Accessed July 12, 2011, at: http://www.aljazeera.com/indepth/opinion/2011/03/2011329113450125509.html

_____. 2011. The Dangers of Social Media Revolt. *Al Jazeera.Net English*, March 9. Accessed July 12, 2011, at: http://www.aljazeera.com/indepth/opinion/2011/03/20113713105997823.html

_____. 2011. Grasping the New Online Reality. *Al Jazeera.Net English*, February 23. Accessed July 12, 2011, at: http://www.aljazeera.com/indepth/opinion/2011/02/2011223124335266961.html

_____. 2011. Will Sudan Pull A Mubarak? *Electronic Frontier Foundation*, June 22. Accessed July 15, 2012,at: https://www.eff.org/deeplinks/2012/06/will-sudan-pull-mubarak

Yogesh, P. and A. Annan. 2006. Alternate Architecture for Domain Name System to foil Distributed Denial of Service Attack. *Journal of Internet Banking and Commerce*, 11(1). Accessed April 2, 2013 at: http://www.arraydev.com/commerce/JIBC/2006-04/Alt%20Architecture%20for%20DNS.html