Journal of Strategic Security

Volume 5
Number 2 *Volume 5, No. 2: Summer 2012*

Article 6

The Iron Fist vs. the Microchip

Elizabeth I. Bryant
Georgetown University, elizabeth.i.bryant@gmail.com

pp. 1-26

Recommended Citation
Bryant, Elizabeth I.. "The Iron Fist vs. the Microchip." *Journal of Strategic Security* 5, no. 2 (2012) : 1-26.
DOI:
http://dx.doi.org/10.5038/1944-0472.5.2.1

Available at: https://scholarcommons.usf.edu/jss/vol5/iss2/6

The Iron Fist vs. the Microchip

Abstract

This article focuses on how information and communication technology (ICT) influences the behavior of authoritarian regimes. Modern information and communication tools can challenge authoritarian rule, but the same technology can be used by savvy regimes to buttress their own interests. The relationship of technology and political power is more accurately conceived of as a contested space in which competitors vie for dominance and as a neutral tool that is blind to value judgments of good versus evil. A realist understanding of the nature and limits of technology is vital in order to truly evaluate how ICT impacts the relative strength of intransigent regimes fighting to stay in power and those on the disadvantaged side of power agitating for change. This is particularly relevant when examining both regimes that have survived and those that have fallen in the wake of the Arab Spring. The cases of Saudi Arabia, Egypt, and Iran are used to demonstrate why some regimes fail in this pursuit, while others thrive.

Journal of Strategic Security
Volume 5 Issue 2 2012, pp. 1-26
DOI: 10.5038/1944-0472.5.2.1

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

The Iron Fist vs. the Microchip

Elizabeth Bryant
Georgetown University

Abstract

This article focuses on how information and communication technology (ICT) influences the behavior of authoritarian regimes. Modern information and communication tools can challenge authoritarian rule, but the same technology can be used by savvy regimes to buttress their own interests. The relationship of technology and political power is more accurately conceived of as a contested space in which competitors vie for dominance and as a neutral tool that is blind to value judgments of good versus evil. A realist understanding of the nature and limits of technology is vital in order to truly evaluate how ICT impacts the relative strength of intransigent regimes fighting to stay in power and those on the disadvantaged side of power agitating for change. This is particularly relevant when examining both regimes that have survived and those that have fallen in the wake of the Arab Spring. The cases of Saudi Arabia, Egypt, and Iran are used to demonstrate why some regimes fail in this pursuit, while others thrive.

Introduction

A divergence of academic and expert opinion exists on whether information and communication technology (ICT) is an inherent force for democratization, or whether it is merely another tool that authoritarian regimes manipulate to achieve their own ends. ICT, understood as electronically empowered communications, specifically Internet or cellular network–based communications and the social media tools it supports, has created a paradigm shift as political actors around the world have recognized the technology's political significance. In the context of the Middle East and particularly the Arab Spring, Western analysis initially hailed ICT as an

unstoppable force inherently on the side of freedom, yet hindsight tells a different story. The relationship of technology and political power is more accurately conceived of as a contested space in which competitors vie for dominance, as a neutral tool that is blind to value judgments of good versus evil. A realist understanding of the nature and limits of technology is vital in order to truly evaluate how ICT impacts the relative strength of intransigent regimes fighting to stay in power and those on the disadvantaged side of power agitating for change. This is particularly relevant when examining both regimes that have survived and those that have fallen in the wake of the Arab Spring.

As a starting point, it is helpful to explore how firmly rooted regimes in the Middle East assess how ICT can be both a threat and an asset. Answering how authoritarian regimes in the Middle East adapt to the challenges posed by the rise of ICT (or fail to do so) demands an examination of how states of particular relevance—Saudi Arabia, Egypt, and Iran—approach ICT from a security perspective. First, a functional summary of the ICT-related tactics being used by authoritarian regimes will be articulated. The tactics identified are then compared and contrasted within the framework provided by the case studies of Saudi Arabia, Egypt, and Iran. Finally, policy implications derived from the case studies will be explored.

Overview of the ICT Tactics Used by Authoritarian Regimes

Authoritarian regimes employ a wide array of tactics to maintain the commanding heights in ICT. This is not surprising, given the long-standing link between authoritarian rule and control of communication flows.[1] These tactics can be put into the general categories of filtering and surveillance, censorship, infrastructure control, and propaganda.

Filtering and Surveillance

Filtering normally refers to the technical approaches to blocking access to information on the Internet, but can also apply to mobile phone networks.[2] Internet filtering in particular restricts what websites can be accessed and what keywords can be searched. Filtering in the form of technical blocking can be achieved by Internet protocol (IP) blocking,[3] universal resource locator (URL) blocking via proxy,[4] and domain name system (DNS) tampering.[5] These methods are most often used when the blocking targets are out of the reach of domestic security services, that is, the offending source is hosted outside of the country. This is particularly

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

apparent when diaspora groups opposed to the current regime form advocacy groups and then remotely try to target audiences within their home countries using the Internet.

Another blocking technique uses keywords present in the website's URL. Particular keywords are entered as criteria for blocking; a common example would be to block search returns on words like "sex" or "porn."[6] A similar tactic is for search engines to agree to remove search results based on criteria provided by the government. This in turn makes the desired websites more difficult for Web surfers to find. As a result, security services get a double bonus: they deter more casual surfers from stumbling across something potentially inflammatory or sordid, and they can also identify the machines that doggedly pursue a particular forbidden topic.

Furthermore, techniques can be used to discover the identities of the users behind particular IP addresses. Machines are identified by unique IP numbers, so if a security service is able to analyze the activity of a machine and match it to the pattern of life for a targeted person or group, the target becomes particularly vulnerable. When security services reach this level of sophistication, activists lose the ability to assume that the Web offers any true mask of anonymity. If an activist is operating under the assumption of anonymity, while actually under the surveillance of an adversary's security service, he could incriminate not only himself but his compatriots as well.

Typically, filtering is a way for regimes to maintain cultural and political control over their populations. It can be used to ban access to sites that are deemed subversive, whether the sites clash with religious and cultural values, or are politically seditious in that they criticize or even call for violence against the regime. Filtering is a mechanism for the regime to send a clear signal to its population, because there is little method for making restrictions ambiguous. It is transparent to users what can and can't be accessed, and it does not take a great deal of imagination for users to see why this is so.[7]

Surveillance, in the context of ICT, can be much more subtle. It is approached in many different ways, but the goal is the same: to monitor the behavior and to assess the intent of citizens. Surveillance can involve the interception of wireless Internet traffic, monitoring packet-switched networks (email, chat, Voice over Internet Protocol), monitoring social networks, "wiretapping" phone conversations, and using geolocation technology to track cellphones.

With Internet-associated surveillance, regimes can employ policies that restrict privacy to deter behavior, or utilize clandestine means for exploiting the perception of privacy. A deterrence approach might include requiring Internet cafes to keep records of their customers and what they access online, or requiring bloggers to register and get publishing licenses from the government. The exploitation aspect of surveillance often manipulates technology to gather information. These activities might include quietly observing and analyzing a dissident's political views, plans, and connections by hacking into social media accounts, installing keylogging software on a target's machine, or analyzing photographs and videos of a protest to identify the instigators. Another technique is deep packet inspection. Deep packet inspection (DPI) enables security services to monitor and gather information about users, as well as block certain communications.[8]

A variation on security through surveillance is banning software and hardware that make surveillance activities more difficult. The tactic of banning software and hardware in order to restrict access is observable across the Middle East. This tactic is not unfamiliar, since fax machines, satellite dishes, and even photocopy machines have at times been either banned or tightly controlled in the region.[9] It is also notable that past attempts to restrict equipment have often been overcome by widespread access to and use of the equipment, as in the case of satellite dishes for personal use in Iran. Although a ban may be in place technically, if the regime does not have the capability or will to enforce the ban, it is ultimately worthless.

Sometimes even the threat of a ban is enough for companies thirsting for market access in the Middle East to compromise the fidelity of their systems.[10] The most widely cited anecdote concerns the threatened ban of BlackBerry devices in Saudi Arabia in early August of 2010. The Saudi Arabian government had threatened to ban the devices on the grounds that the encryption could shield potential terrorist plots from the Ministry of the Interior, Saudi Arabia's main security service. The issue was eventually resolved when the producers of the BlackBerry, Canadian-based Research In Motion (RIM), agreed to share user data with the regime by placing a server in the Kingdom to service the Saudi Arabian BlackBerry market (BlackBerry servers up until this point had always been centralized in Canada). The companies involved called this outcome the "BlackBerry solution in Saudi Arabia."[11]

While historical examples of hardware bans may have proved effective, at least by making communication more difficult than necessary, the tactic is losing ground due to the sheer proliferation of electronics across the

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

The Iron Fist vs. the Microchip

region. Mobile phones in particular have become ubiquitous, even among poorer segments of society. Per the International Telecommunication Union (ITU), as of 2009 the rates of cellular subscriptions per 100 citizens were 67/100 in Egypt, 71/100 in Iran, and 174/100 in Saudi Arabia.[12]

Censorship

Censorship, in the context of this paper, is contrasted to filtering techniques insofar as it concerns activities undertaken in reaction to material already published and available for public consumption. Essentially, censorship entails extensive monitoring of online content, especially content that is deemed to be culturally offensive or politically subversive. As a result, it limits what users can produce and disseminate. Should a user post or publish content out of the range of what is acceptable, a site or post can be reported, flagged, and taken down. Often, the individual responsible for circulating the offending content will be tracked down and confronted by the regime. This confrontation might be a stern warning, or, in more extreme cases, beatings, imprisonment, and other forms of intimidation. These consequences, when both credible and severe, often persuade all but the most intrepid citizens to practice self-censorship.

Another approach to censorship is examining what methods regimes pursue to encourage citizens to self-censor. These methods are typically the confrontational approaches just discussed: if an author is fearful of being physically or legally harassed, he or she will be more careful in choosing what content to publish. If there is a perception that the regime is engaged is extensive surveillance activities, both on- and offline, the result is a chilling effect. Often, the fear of repercussion will result in authors venting frustrations through allegory. For example, in Egypt during the Mubarak era, it was popular to write "fiction" that was actually thinly veiled criticism of real events and policies.[13]

Infrastructure Control

ICT infrastructure includes fixed and mobile telephone networks, computer networks, and installed bases of computing hardware and software that support the Internet and telecommunications.[14] Other auxiliary components include Internet service providers and institutions such as cybercafes, schools, and companies that comply with national monitoring efforts. How a regime plans and implements control over physical IT infrastructure is indicative of a regime's overall control strategy. A patient and comprehensive approach is reflective of a highly strategic regime with the means for control. Hallmarks of a sophisticated infrastructure strategy include variations of "kill switches" to quickly disable Internet con-

nectivity or the ability of the regime to compel telecoms to temporarily shut down networks. The point about influence over local telecommunications companies is important, because a quick, unified shutdown requires obedience and responsiveness.

For example, in January 2011, Egypt effectively shut down in-country Internet access for a period of roughly five days.[15] This could be achieved because the Mubarak regime held sway over the major Egyptian telecoms. Another reason why Internet access in Egypt could be cut off in such a quick and complete manner is the limited number of telecoms in the country. In Egypt, just five companies represent the majority of the market. This is typical for less competitive markets, especially markets where the main competitor is wholly or partially state owned. By contrast, in the United States hundreds of companies, including heavyweights like Sprint, Verizon, AT&T, and T-Mobile, would have to comply in order to shut down the Internet in a similar manner.[16]

To limit access in a subtle manner, a regime may choose to engage in bandwidth throttling. Basically, throttling is a method to decrease the speed and performance of Internet connections. It can achieve an effect similar to that of shutting down the Internet by making the Internet so inconvenient and unreliable that it is no longer an effective tool to inform or organize the opposition. The upside of throttling from the perspective of a security service is that it is less likely to elicit a passionate backlash, as throttling can be carried out subtly and can be attributed to unintentional causes.

Propaganda

Propaganda, historically a favorite tool of authoritarian regimes, can be disseminated with stunning effectiveness electronically. A regime that is savvy enough to use the Internet as a propaganda mouthpiece is often also cunning enough to use ICT tools both to fend off criticism and to build support from citizens. One example is how authoritarian governments have created a veneer of government transparency by creating mechanisms online to receive feedback from citizens and to persuade the population that policy choices exist.[17] The result is a sense that the regime is receptive to the opinions of citizens. If input is received that is unsupportive, it can be easily ignored and erased, while positive statements can be gathered and promoted. This system also provides a means to identify subversive citizens for monitoring. For example, if the interface is a message board, the author of the negative message can then be watched as a potential adversary to the regime.

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

Propaganda, when done well, can be extremely effective. Propaganda that plays to the open nature of the Internet not only is persuasive to internal audiences, but is able to gain external sympathizers as well. Additionally, carefully orchestrated propaganda can be used to discredit movements against the regime. It is worth noting how Iran has seized on the idea of producing propaganda that appeals to both Iranian hearts and minds; it appeals to consumers by presenting plausible defenses of regime policy, and then exacerbates identity politics by fanning the flames of nationalism. It is starkly suspicious of the West, and seeks to stir up Iranian nationalism and promote in-group/out-group sentiments by claiming that Islam is under attack from the Western world.

Case Study: Saudi Arabia

Saudi Arabia, the Arab world's wealthiest and ostensibly most pious regime, has both the means and the motivation to put a premium on security and stability. The ruling Saud family has maintained power since the founding of the country in 1935, and survival of the monarchy is dependent on an aggressive and comprehensive security strategy. Religion also plays a role: tight control is exercised over anything that is seen as compromising to "Saudi Arabian values," specifically, anything that degrades Saudi Arabia's strict interpretation of Islam, or that questions the legitimacy of Saud family rule. To enforce cultural and religious norms, the Saudi government sponsors the *Mutawa'in*, or religious police. The *Mutawa'in* are under the auspices of the Committee for the Promotion of Virtue and the Prevention of Vice. This group has a central role in assessing the cultural impact of ICT on the cultural fabric of the Kingdom, and up until 2006 had almost unrestricted ability to interrogate, detain, or arrest citizens on the basis of moral infractions.[18]

The regime recognizes that the Internet can hamper cultural prerogatives, but that it can also be used to enhance them. Saudi Arabia sees the Internet as an opportunity for counterterrorism and counter-radicalization efforts.[19] For example, an online counter-radicalization program called the Sakinah Campaign works to attract would-be radicals seeking religious guidance. Workers for the Sakinah Campaign then will engage these seekers of religious enlightenment in one-on-one online chats to redirect them from more violent Islamist groups. The Sakinah Campaign is popular because it is not affiliated directly with the government, yet it enjoys the full support of both the Ministry of the Interior and the Ministry of Islamic Affairs.

Filtering and Surveillance

To counter culturally and politically threatening content, the Saudi government has implemented a technically complex and expensive system to cut off internal access to sites determined to be unfavorable.[20] Culturally, the Kingdom is dedicated to ensuring strict reverence for Islam, enforcing narrow codes for male/female interactions and even "protecting" the populace from the influence of Western vices.[21]

Also, the Saudi royal family is quite sensitive to criticism and political opposition, and will block political opposition sites. While censorship limits what can be produced internally, filtering techniques are used to limit access to sites that are hosted outside of the country (and therefore out of the reach of censors). Two examples of major opposition groups subject to filtering are the Committee for the Defense of Legitimate Rights (CDLR) and the Movement for Islamic Reform in Saudi Arabia (MIRA). Both are groups that are blocked for trying to influence public sentiment against the regime in Saudi Arabia.[22] The example of MIRA is interesting on two levels: the first is because MIRA draws international attention, and the second is the continuous cat-and-mouse game played between MIRA and the Saudi filterers. On the first point, MIRA draws scrutiny from not just Saudi Arabia, but the Western security community as well. The group, which is now based in London, has been added to the United Nations Security Council 1267 list of terrorist individuals and organizations, ostensibly because of affiliations with al-Qaida and other like-minded groups. The second is that MIRA has been able to beat the filtering system for short intervals of time by simply changing their Web address, which then allows their site to slip past the filters.

Additionally, Saudi Arabia's vast financial resources enable it to be a voracious consumer of filtering technology.[23] The interest for new and better technology is high, and many Western companies recognize the Saudi appetite as an opportunity to develop and sell their technologies. Examples include Narus, a deep-packet-inspection–technology provider (and wholly owned subsidiary of Boeing) that counts the Kingdom among its Middle Eastern clientele.[24]

The responsibility for filtering in the Kingdom falls to the Communications and Information Technology Commission (CTIC), which is Saudi Arabia's main regulating body for information and communication technology.[25] In contrast to other actively filtering countries, such as China, Saudi Arabia is quite open and transparent regarding what is filtered. Users that encounter a restricted page are given the opportunity to dispute the blocking of certain IP addresses. Any user wishing to lodge a

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

complaint should be aware that Saudi ISPs are required to maintain records on the identities of their users, and will have to provide those records to the authorities if requested to do so.[26]

Another notable Saudi security tactic is to use the Internet to facilitate information gathering. For example, the Saudi Arabian government launched YaHajj.com, a trip-planning website for devout Muslims to use when planning their Hajj to Mecca. It helps foreign Muslims plan their travel to Saudi Arabia, but it also allows the Saudi government to enhance their database of passport information and other identifiers of foreigners wishing to enter the country.[27] This, in addition to visa applications and other procedures necessary to enter the country, creates a robust picture of foreign travel to and from the Kingdom.

To enhance the ability of Saudi security to intercept electronic communications, the regime pays close attention to the capabilities of devices and software available to its citizens. Thus, the "BlackBerry Solution in Saudi Arabia," or the acquiescence of the makers of BlackBerry to allow the Saudi government to bypass BlackBerry's encryption and access user data, is unsurprising. The Kingdom represents a large and important market for companies operating in the Middle East, and even a company like BlackBerry could be persuaded to compromise user privacy to maintain a foothold in the wealthy nation. The BlackBerry case is also interesting because the Saudi government has a legitimate concern regarding encrypted communications and threats to national security.

Censorship

Saudi Arabia's emphasis on upholding Islam informs the Kingdom's approach to censoring content on the Internet. But censorship isn't just limited to cultural material. As with filtering, content that is deemed to be politically subversive is also highly controlled. The threshold for unacceptable political speech is quite low. The royal family is highly sensitive to criticism and dissent in general, and content that is negative regarding the royal family is aggressively monitored and eliminated.

The Internet Service Unit (ISU), a department of the King Abdulaziz City for Science and Technology, leads censorship efforts.[28] It is the main government authority for the Internet in Saudi Arabia. The ISU is not only in charge of selecting and implementing censorship technology, but also employs professional censors to comb the Saudi Internet for illegal material.[29]

The formal security service isn't the beginning and end of censoring work on the Web; pious volunteers spend countless hours patrolling chat rooms, YouTube, Twitter, blogs, and other forms of social media for offensive content. These unpaid volunteers then "flag" the offending sites, giving them the nickname "flaggers."[30] This could be viewed as a form of digital activism, but an activism of the kind that actually feeds paranoia and repressive actions by the government.

In addition to the flaggers, Saudi Arabia also keeps close tabs on content published online. As of January 1, 2011, all news media blogs are required to register with the Saudi Ministry of Culture and Information. Legally, this online content is regulated in the same manner as print media. The Ministry must approve editors for online news sites in the same manner in which they approve editors for paper newspapers.[31] Furthermore, only Saudi nationals with high school degrees who are at least twenty years of age are able to gain the needed license to report news.[32]

Infrastructure Control

Saudi Arabia built their Internet infrastructure in a highly centralized fashion. The Saudi Internet is connected to the global Internet by only two nodes, and all Internet service providers engaged in the Saudi market must connect through those two nodes.[33] These gateways, administered by the ISU, are then defended by multiple, redundant firewalls to maintain the desired level of filtering.

The Saudi government introduced their public to the Internet in a deliberately cautious fashion. It was not until 1999 that public access was made available.[34] Up until the early 2000s, the Saudi government intentionally kept access costs high, conceivably because they were anxious to see how the experiment of introducing the Internet would play out.[35] However, limited access during this time did not cause distress among the young and wealthy. Saudis of means had already been accessing the Internet via Bahrain for years. By pursuing this strategy, the Saudi government is preventing the perfect from being the enemy of the good: those truly determined to bypass the filters and censors can do so, yet the obstacles still are successful in deterring more casual users from using the Internet in a way that conflicts with the desires of the regime. The widespread use of proxy servers also calls into question the notion that limited nodes for external connections are fully effective.

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

Propaganda

Much of Saudi Arabia's ICT-restriction activities are carried out on the grounds of protecting Islam and the culture of the Kingdom. Perfidious sites such as those featuring child pornography or those that promote violence against the government are used as justification for broader restrictions. Also, Saudi Arabia has embraced e-governance tools. On the surface, this is quite positive. Interfacing with the government via the Internet makes citizens feel that the government is accessible and responsive. However, these tools also enable the government to keep an ever-tighter watch on citizens and to improve their ability to spot and neutralize potential political instigators.

Case Study: Egypt

Egypt is valuable as a case study for numerous reasons: it is heavily populated and relatively poor, and many citizens outside of the large urban areas are illiterate. It is also quite possibly the most visible country radically affected by the Arab Spring. The now-deposed ruler Hosni Mubarak managed his power on the basis of military control and populist rhetoric for approximately thirty years. President Mubarak's power seemed entrenched until a swift popular uprising in January 2011 overwhelmed the government in both velocity and numbers. This uprising embraced the Internet as a tool to organize and promote a message of regime change, and was able to create a shallow but swift movement that accomplished in eighteen days what was thought impossible for nearly thirty years.

Political power in Egypt has long been rooted in control of the security apparatus; a hybrid approach of populism and military rule allowed for Mubarak's lengthy rule. It is important to note how Egypt is different from the other cases presented in this article. Unlike its neighbors on the Arabian Peninsula, it is not a resource-rich country. Egypt also does not have a significant middle class that is well educated. The means for population control are quite limited; Egypt does not have the resources to achieve high ratios of law enforcement personnel per citizen, nor does it have the capability to economically co-opt Egyptian citizens. This plays out in how Egypt has approached communications technology. Telecoms are generally allowed to flourish, and in many cases the telecoms are the business enterprises of those holding political power. Filtering has not been pursued by the regime, but surveillance techniques of the low-tech variety are adapting to high-tech modes of communication.

Another point of interest in the case of Egypt is how the revolution has drawn attention to communications technology. While social media was utilized during the revolution, it is helpful to remember that Facebook penetration in January 2011 was only at 5 percent. By April 2011, the revolution had caused a surge in the popularity of the platform, and the percentage of Facebook users by population experienced a 42 percent increase within the span of four months.[36] Another notable statistic regarding ICT saturation in Egypt is the vast number of mobile phone users. Out of a population of approximately 82.1 million,[37] 55 million Egyptians are cell phone users. By contrast, only 20 million are identified as Internet users.[38]

Filtering and Surveillance

Egypt shows little evidence of employing a filtering strategy. By contrast, the Egyptian security apparatus had (and has) an extensive surveillance regime. In Egypt, it is not a question of what can be accessed, but what a citizen is observed accessing, and especially what they might be saying. Speech that is critical of the security services (including the military) and Islam is closely monitored. Surveillance is often followed up with beatings, arrests, and other forms of intimidation.

During the January 2011 revolution, authorities arrested thirty-year-old Google executive Wael Ghonim. His crime? Running a popular Facebook page called "We are all Khaled Said," which brought attention to systematic brutality against citizens by the Egyptian police forces.[39] Ghonim's appeal as an idealistic, educated activist quickly made him a cause célèbre in the West. He was detained by the police for twelve days, and was eventually released. Blogger Maikel Nabil Sanad was not as fortunate. He was arrested in April 2011 for criticizing the lack of transparency in the Egyptian armed forces (among other things). His punishment? A three-year prison sentence.[40]

Another characteristic of Egypt's relationship with ICT is that the lines between commerce and security are often blurred. For example, Skype, a VoIP-based service that allows customers to make calls cheaply over the Internet, has experienced headwinds entering the Egyptian market. This is because Skype poses a two-fold problem for Egypt: Skype's encryption makes it extremely difficult to monitor conversations for security purposes, and Skype cuts into profit margins for telecoms by providing a lower-cost option for long-distance and international phone calls.

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

The BBC reported in the spring of 2011 that documents had been discovered indicating Gamma International, a UK-based encryption firm, allowed Egypt to experiment with a technology called Finfisher to counter the Skype surveillance problem.[41] Finfisher operates as spyware: by posing as a download for a popular application like iTunes, Finfisher can be inadvertently installed on a target's machine. The technology can then clandestinely record Skype conversations and route the data back to another machine.

Censorship

Censorship, defined by this article as a retroactive activity taken in response after offending content is posted, has not been extensively employed in Egypt. Rather, the threats of beatings or intimidation for content critical of the regime and of the security services have encouraged citizens to engage in self-censorship.

What is remarkable about the spring 2011 revolution is that the more people shunned self-censorship, the more burgeoning bloggers and protestors felt empowered to take to their keyboards, as well as the streets. The sharp uptick of participants in the movement quickly overwhelmed the security force's capability to respond. People were still being harassed, beaten, and arrested, but the sheer velocity of citizens joining the protest soon made the final outcome inevitable.

Infrastructure Control

Historically, Egypt has allowed a modified free-market approach to building out ICT infrastructure. Egypt, lacking the oil resources of Iran and Saudi Arabia, felt economic pressures to allow the Internet and mobile communications to grow swiftly throughout the regimes. The Egyptian military and security services, which are also heavily engaged in Egyptian business enterprises, found the economic benefit of ICT proliferation enticing. They did not foresee any major sociopolitical issues with the increasing adoption of the new technologies; instead they saw the technology for its potential economic benefit. Case in point: in 2002 the regime launched the "free Internet" initiative, which allowed any citizen with a phone line and a computer to get online for the price of a phone call.[42]

Although Egypt was not equipped to delay the velocity of events in 2011 in the same way that Iran was with its Green Revolution in June 2009, there was a significant event on January 27, 2011. Egypt pulled a desperate but a technically impressive move: by strong-arming Egyptian telecoms and

ISPs, Internet and mobile phone services were taken offline for a period of five consecutive days.[43] Renesys, an Internet analytics firm, observed how the major telecoms in Egypt cut access almost simultaneously on January 27, 2011, at the height of the protests.[44] This incident demonstrates both what an authoritarian government can and will do if they are backed into a corner,[45] and the speed at which they are able to achieve their immediate aims.

However, by the time Egyptian officials had decided to shut down the Internet, it was too late for Mubarak. The movement was well past its nascent stages, and at this point the Internet was the equivalent of training wheels, which the movement no longer needed for effectiveness. When the Internet shut down, the reaction of the people was not to stay inside or to isolate themselves from the surrounding events. Instead, thousands of Egyptians poured into the streets to collect "ground truth" as to what was really going on. Furthermore, the shutdown incurred an economic price tag as well. An intergovernmental think tank, the Organization for Economic Co-operation and Development (OECD), estimated the cost of the shutdown at approximately 90 million U.S. dollars.[46]

What is more difficult to say is how the outcome of events would have been affected had the means for mass communication been altered at an earlier juncture. There is no satisfying way to prove the counterfactual, but the likely conclusion would be that any alteration of a common good or service, be it communication or trash collection, would result in strained relations between the government and the citizens dependent on those services.

Case Study: Iran

Of the three cases presented in this paper, Iran has the most extensive and sophisticated strategy to counter disruptive information and communication technologies. The regime, relative to Saudi Arabia and Egypt, is the most paranoid and the most skeptical of foreign influence via the Internet and cultural media such as music and movies. Also, Iran uses a full spectrum approach to ICT domination. Iran demonstrates competency in all the tactics presented within the scope of this article. The regime takes a comprehensive approach, and commits many resources to staying one step ahead of perceived internal and external enemies.

The issue of ICT in Iran is highlighted by the protests following the 2009 elections. The protests, fueled by widespread allegations among the educated middle class that the winning party had engaged in large scale vote-

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

rigging and fraud, were well documented by Iranian participants on social media sites such as Twitter and Facebook.[47] When the protests turned violent and citizens were beaten and killed, graphic images made their way outside of Iran via the Internet. The video of the shooting death of a young Iranian woman, Neda Agha-Soltan, by a member of the Basij quickly went viral on YouTube.[48, 49] The video, shot by a bystander on a cell phone, shocked the Western world and became a rallying cry for the movement.[50] The protests were relatively short lived, but many Western commentators quickly dubbed the movement the "Twitter Revolution" in reaction to the widespread documentation of the protests on social media. Westerners anxious to see Iran liberalize fervently hoped that ICT would add to the momentum needed to vanquish a repressive regime hostile to the United States.

For as much excitement the Green Movement generated for the West, in reality, it was never that widely based among the Iranian population.[51] The misperception of the movement's popularity may have arisen because the regime had silenced foreign reporting, and as a result citizen-reported media sprang up to fill the vacuum of non-state-generated news. The citizens, using Twitter, YouTube, and other media to get their message out, represented the young, educated, and wired supporters of Mir Hossein Mousavi and other reformists.[52] The Iranian Diaspora, as well as many Western reporters, played up the protests as something that could potentially topple the regime.

In the end, communication technologies failed to help the movement reach critical mass in terms of committed participation. Ultimately, old repression tactics of intimidation used against the protestors proved to be enough to squash the movement. Authorities raided dorms, made mass arrests, fired upon protestors, and rounded up, detained, and even tortured instigators.[53] After the brutal crackdown, the Green Movement receded back into the private hopes of reformist citizens and like-minded supporters abroad.

Filtering and Surveillance

Iran is a practitioner of pervasive filtering, and is aggressive in seeking out and improving upon technologies that allow Iran to achieve its internal security objectives.[54] Filtering is typically carried out through a centralized system, and the technology used is produced within the country, making it more difficult for Western Internet-freedom promoters to circumvent. Another key factor is that the government enjoys a monopoly

over Iran's telecommunications industry. As a result, the government faces little resistance when mandating filtering requirements for major Iranian ISPs.

Filtering activities have extensive legal cover in Iran. An official policy established in 2001 by the Supreme Council of the Cultural Revolution requires all access service providers to be capable of blocking access to "immoral" and opposition websites. The content bans detailed by the policy are sweeping. It is forbidden to insult Islam, the Supreme leader, or the Grand Ayatollahs, or to "distort" Islamic instructions. Online activities degrading or critiquing Khomeni's political views that founded the 1979 revolution are also subject to blocking. But blocking does not stop at religious content. During the 2009 protests, access to websites supporting the political opposition was denied.[55]

Censorship

Despite the frailties of the Green Movement, it still caused a tremendous reaction from the regime, even well after the movement had subsided. The threat to regime stability resulted in the Iran Revolutionary Guard Corps' (IRGC) taking a greater interest in preventing the Internet from being a tool that could foment unrest against the regime. In the months after the June 2009 protests, the regime assembled a twelve-person team tasked with unearthing "insults and lies" on Iranian websites. But the effort didn't stop there. Once subversive content was discovered, its authors were identified and arrested. Additionally, the Internet was used to compile photos and videos of protest participants. These select images were posted online in publications read by regime supporters, and the police requested help in identifying the would-be revolutionaries. This open-source policing effort proved effective: one major push on a pro-Ahmadinejad website produced tip-offs that led to at least forty arrests.[56]

Infrastructure Control

Iran has built extensive control mechanisms into their Internet architecture, often at the expense of the performance of ICT tools in the country. Iran built its Internet in such a way that traffic coming in and out of the country goes through a single gateway. As such, the structure is centralized, and security measures can be applied uniformly across the country, rather than in a piecemeal fashion.[57] Furthermore, the single gateway can serve as a choke point, and the regime can control the flow of communications traffic should popular movements against the regime ignite. Allowing high-speed access for households has been a contentious issue, and

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

the notoriously sluggish household access speeds rarely top 128 kilobytes per second. This in turn limits the ability of users to enjoy streaming audio and video, as well as other multimedia downloads.[58]

Iran's infrastructure is tightly controlled, but officials are prepared to take it one step further with the implementation of a "halal" Internet. This would be a closed network (intranet) exclusively available in Iran, and would be the only public Internet the Iranian public could access. The intent of this new network would be to isolate Iranians from Western influences. Iranian officials cite China as the inspiration for this project, and indicate that they will be using "foreign consultants" to build the intranet.[59]

Propaganda

In Iran, there is a unit within the national police force launching a counter campaign to the perceived dangers of Facebook, Twitter, and other Web applications produced by the West. The campaign is focused on students and young people, and the deliberate message is that these Western sites endanger both the user and Iran. There is a distinct level of paranoia visible within the structure of the campaign, as leaders claim that Western sites that appeal to Iranians are deliberately crafted by the West to influence internal Iranian affairs.[60] That message is also often coupled with filtering procedures that block access to Western news outlets such as the BBC, Voice of America, the Guardian, Fox News, and CBS.[61]

The Iranian regime is also aggressive in using scapegoat techniques in attempts to deflect criticism for controversial events. The media is then used to spread and reinforce messages supporting the regime's version of how events occurred. For example, with the shooting death of protester Neda Agha-Soltan, the regime came out with several story lines placing blame on foreign terrorist organizations, and even the CIA. The fabricated versions of events were then repeated both in Iranian media and in interviews with foreign press.[62] Pressure was put on Agha-Soltan's mother to accept payment in exchange for reinforcing the story line that the Iranian forces were not responsible for the death of her daughter.[63]

Also, the regime is highly skilled in using the communicative power of ICT to counteract the messaging of protestors. For example, texting is used to broadcast the regime's version of public service announcements. One regime-generated text carried the following message during the Green Movement protests: "Dear citizen, according to received information, you have been influenced by the destabilizing propaganda which the media affiliated with foreign countries have been disseminating." As in the cam-

paign to shield impressionable students from the "dangers" of Western influence via the Internet, foreign governments are cited as the cause for political disruptions. Furthermore, the rest of the text continues by saying, "In case of any illegal action and contact with the foreign media, you will be charged as a criminal consistent with the Islamic Punishment Act and dealt with by the Judiciary."[64] Note that punitive action is threated should an Iranian choose to embrace anti-regime sentiments. This is something of a hallmark of the regime's propaganda: denounce anti-regime opinions as the result of foreign influence, and if that is not enough to deter budding protesters, threaten severe consequences for opposing the regime.

U.S. Policy Implications

In light of the stark realities presented thus far, it is important to restate what ICT can and cannot do. ICT is a tool capable of increasing the velocity of communications and bringing networked populations greater access to information. The Internet itself is open and decentralized, but it is also highly malleable. It would be incorrect to characterize the approach of authoritarian regimes as one of "controlling" information and communication technology. It would be more accurate to say that success achieved by authoritarian regimes comes from an ability to wield the communicative power of ICT. Cunning regimes also find ways for the technology to serve their interests, such as using ICT to exploit communications, spread propaganda, and gather intelligence on perceived enemies.

The position of the State Department, as articulated by Secretary Hillary Clinton in a February 15, 2011, speech, is that U.S. policy should support international political freedom of expression on the Internet. This is not a new position, but the way in which Internet freedom should be promoted has changed. The foreign policy approach of the U.S. government has begun to sober to the limits and realities inherent to ICT. In the late 2000s, enthusiasm for the democratizing powers of the Internet was at its zenith. Visionaries thought if protesters were trained in the arts of modern communication strategies and given the right tools to circumvent filters and censors, the possibilities would be limitless. To frame this point, consider how in the midst of the 2009 Iranian protests promoters for democracy and human rights were anxious to send in tools to help the protesters circumvent the Iranian regime. When the movement was crushed, many ICT idealists were left dazed. The fervor for tools has not gone away, but the enthusiasm for technical answers to sociopolitical

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

problems has become more tempered. State Department official Michael Posner neatly summed up this sentiment by saying, "Facebook does not foment dissent; people do."[65]

The instrumental approach of providing circumvention technology to actors behind a "digital iron curtain" is well meaning but historically has failed to meet its objectives. As Clay Shirky advocates in a 2011 *Foreign Affairs* article, the United States should distance itself from the instrumental approach of relying on purely technological solutions to help activists, as it can often harm as much as it can help.[66] Take for example the Haystack technology provided in the wake of the 2009 elections in Iran.[67] Haystack is a technology that emerged in the midst of the 2009 Iranian protests. Its objective was to mask political websites with innocuous identifiers and to break through Iranian firewalls. The technology was not as secure as it was thought to be, and it actually gave the Iranian government the ability to track down individual Haystack users.[68]

Also, more care should be taken in understanding how authoritarian regimes conceptualize security, and how that informs their approach to Internet and communications technology. This is an important point to understand, especially when the security priorities of an authoritarian regime and the United States converge (for example, in counterterrorism efforts in Saudi Arabia). If in the rush to promote Internet freedom the United States forgets to examine the full context of the security environment, well-intentioned policy may result in negative unintended consequences. That is not to make a value judgment on the policy of Internet freedom, which is perfectly in line with the freedoms the United States upholds, but it is to caution that sometimes values and security objectives can conflict.

From the U.S. perspective, it remains important to acknowledge the commercial potential of the Internet and view Internet freedom as a mechanism to enhance global prosperity. On the other hand, export-control policy helps to slow down the transmission of technology to regimes that are at odds with U.S. policy objectives. For example, certain encryption technology has the computing capability necessary to defeat strong encryption and often needs U.S. government approval to be sold overseas. But the challenge is that the United States does not have a monopoly on tools that can be used to buttress regimes at odds with U.S. policy. Repressive regimes can be served by alternate suppliers or devise ways such as alternate transshipment routes to acquire the technology desired.[69] Additionally, U.S. sellers often track their equipment through the initial, legal sale and have no further influence as to subsequent trans-

fers of their technology after that point. At present, U.S.-produced Web surveillance technology ostensibly sold to law enforcement bodies overseas is not subject to end-user monitoring agreements.

Ultimately, the realm of ICT is best understood as a contested space in which the advantage will go to the most adaptive competitor. ICT is not inherently on the side of freedom or tyranny. How the United States or any other responsible party chooses to behave in that space does have consequences. That is not to say that the best approach is to do nothing and let trends take their courses, but that the outcomes to actions taken to invigorate online activity can and do have consequences, both good and bad.

Conclusion

In essence, authoritarian regimes survive the information age by using new tactics to support old strategies. That is, the most successful authoritarian regimes in the information age are the regimes that are able to wield information and communication technology to support positive and negative inducements aimed at their citizens. For example, regimes have long engaged in propaganda to blunt reformists and outside influence, but savvy regimes are able to use ICT to amplify propaganda that serves its interests. A negative inducement is creating an environment of paranoia, thereby convincing citizens that any effort against the regime is being watched and will bear consequences.

Evgeny Morozov, author of *The Net Delusion* and self-proclaimed "cyber realist," assesses the current information environment in one pithy statement: "technology changes over time … human nature, hardly ever."[70] With that in mind, observers of events unfolding in the Middle East must assess the social context of information and communications technology, and be wary of its limits. To quote Morozov again, "Internet-centrism is akin to agreeing to box blindfolded. Sure, every now and then we may still strike some powerful blows against our authoritarian adversaries, but in general this is a poor strategy if we want to win."[71] Technology may act as a vanguard, but in reality is not loyal to one side over another. Rather, the information environment is best understood as a contested space, and the commanding heights will go to those who understand information and communications technology in technical, social, economic, political, and security-related dimensions.

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

About the Author

Ms. Bryant is currently affiliated with The Chertoff Group, a strategic security consulting firm based in Washington, DC. She began her career working in the personal office of U.S. Senator Chuck Grassley, and furthered her congressional experience with the Congress and U.S. Foreign Policy program at the Council on Foreign Relations (CFR). At CFR, she assisted in strategic outreach to connect CFR resources with members of Congress and their staffs. Ms. Bryant received a Bachelor of Arts in International Studies and Political Science from the University of Iowa. She received her Master of Arts in Security Studies from Georgetown University in December 2011. The views in this article are the author's own, and are not reflective of The Chertoff Group.

References

1 Grey Burkhart and Susan Older, *The Information Revolution in the Middle East and North Africa* (Santa Monica RAND, 2003), xii.

2 "About Filtering," *The OpenNet Initiative*, available at: *http://opennet.net/about-filtering*.

3 IP blocking is achieved by setting up a block specific to a website or a machine's Internet Protocol (IP) address. An IP address is a series of numbers that acts as a unique identifier for a website or machine online.

4 A URL is a string of text that identifies a specific web page, for example *http://georgetown.edu*. A weak URL block can be circumvented by typing in an IP number instead of the URL. URL blocking via proxy prevents this strategy from being successful.

5 DNS tampering prevents an Internet domain name from resolving to its proper IP address.

6 "West Censoring East: The Use of Western Technologies by Middle East Censors 2010–2011," *The OpenNet Initiative*, available at: *http://opennet.net/sites/opennet.net/files/ONI_WestCensoringEast.pdf*.

7 The OpenNet Initiative creates data sets on filtering and Internet censorship by testing the accessibility of certain IP addresses from within target countries. Using this method, researchers are able to systematically map out and test the accessibility of online content by country. Information is available at: *http://opennet.net/sites/opennet.net/files/ONIDatareadme_Nov%202011.pdf*.

8 Christopher Rhoades and Loretta Chao, "Iran's Web Spying Aided by Western Technology," *The Wall Street Journal*, June 22, 2009, available at: *http://online.wsj.com/article/SB124562668777335653.html*.

9 Mahmoud Fandy, "Technology, Trust, and Social Change in the Arab World," *Middle East Journal* 54:3 (2000): 378–394.

10 Cecily Hilleary, "BlackBerry Ban a Hot Issue in the Middle East," *Voice of America*, August 11, 2010, available at: *http://tinyurl.com/caneh64 (www.voanews.com/content/heart-of-blackberry-issue-in-uae-100465634/172241.html)*.

11 "Zain Saudi Arabia, Alcatel-Lucent and RIM Launch the BlackBerry Solution in Saudi Arabia," RIM press release, September 14, 2009.

12 The country with the highest cell phone penetration in the region is the UAE, which has 232.07 subscriptions for every 100 Emirates. This data is drawn from the International Telecommunication Union's 2009 ITU World and Telecommunications/ICT Indicators Database.

13 Fandy, "Technology, Trust, and Social Change in the Arab World."

14 Burkhart and Older, *The Information Revolution in the Middle East and North Africa*, 7.

15 "Egypt Returns to the Internet," *Renesys Blog*, February 2, 2011, available at: *http://tinyurl.com/4hhp9r5 (www.renesys.com/blog/2011/02/egypt-returns-to-the-internet.shtml#latest)*.

16 "Internet Blackouts: Reaching for the Kill Switch," *The Economist*, February 10, 2011, available at: *http://www.economist.com/node/18112043*.

17 Burkhart and Older, *The Information Revolution in the Middle East and North Africa*, 32.

18 "Arab Political Systems: Baseline Information and Reforms—Saudi Arabia," *Carnegie Endowment for International Peace*, March 6, 2008: 13, available at: *http://www.carnegieendowment.org/files/Saudi_Arabia_APS.doc*.

19 Christopher Boucek, "The Sakinah Campaign and Internet Counterradicalization in Saudi Arabia," *CTC Sentinel*, August 2008, available at: *http://carnegieendowment.org/files/CTCSentinel_Vol1Iss9.pdf*.

20 Burkhart and Older, *The Information Revolution in the Middle East and North Africa*, 43.

21 Access to sites facilitating gambling or the viewing of pornography is strictly forbidden.

22 Taylor Boas, "Weaving the Authoritarian Web," in John Zysman and Abraham Newman (eds.), *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology* (Stanford, CA: Stanford Business Books, 2006), 14.

23 Joshua Teitelbaum, "Dueling for Da'wa: State vs. Society on the Saudi Internet," *Middle East Journal* 56:2 (2002): 222–239.

24 Narus company website, available at: *http://www.narus.com/index.php/partners/global-partners*.

25 *http://www.citc.gov.sa/English/AboutUs/AreasOfwork/Pages/default.aspx*. The CTIC is also responsible for granting licenses to telecoms and Internet service providers; without the CTIC license business cannot be done in the Kingdom.

26 Boas, "Weaving the Authoritarian Web," 21.

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

27 Burkhart and Older, *The Information Revolution in the Middle East and North Africa*, 44.

28 Ibid., 43.

29 Ibid.

30 Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011), 215.

31 Joshua Teitelbaum, "Saudi Arabia Contends with the Social Media Problem," Jerusalem Center for Public Affairs, February 8, 2011, available at: *http://tinyurl.com/6n8uzzf (jcpa.org/article/saudi-arabia-contends-with-the-social-media-challenge/).*

32 Neal Ungerleider, "Saudi Arabia Now Forcing News Bloggers to Obtain Licenses, Promote Islam," *Fast Company*, January 12, 2011, available at: *http://tinyurl.com/4r224wp (www.fastcompany.com/1716303/saudi-arabia-forcing-news-bloggers-to-obtain-licenses-promote-islam).*

33 Teitelbaum, "Saudi Arabia Contends with the Social Media Problem."

34 Boas, "Weaving the Authoritarian Web," 14.

35 Teitelbaum, "Dueling for Da'wa," 236.

36 Dubai School of Government, "Civil Movements: The Impact of Facebook and Twitter," *Arab Social Media Report* 1:2 (May 2011), available at: *http://www.dsg.ae/portals/0/ASMR2.pdf*.

37 Central Intelligence Agency, "Egypt," *The World Factbook*, available at: *https://www.cia.gov/library/publications/the-world-factbook/geos/eg.html*.

38 "Internet blackouts: Reaching for the Kill Switch."

39 Khaled Said was a young Egyptian who was beaten to death by two policemen on a public street in 2010. "We Are All Khaled Said," available at: *https://www.facebook.com/elshaheeed.co.uk*.

40 Freedom House, "Country Report: Egypt," *Freedom on the Net 2011*, April 11, 2011, available at: *http://tinyurl.com/75qfars (www.freedomhouse.org/sites/default/files/inline_images/Egypt_FOTN2011.pdf)*

41 Gamma International denies having any part in providing surveillance technology to Egypt. See Stephen Grey, "UK Firm Denies 'Cyber-Spy' Deal with Egypt," *BBC*, September 20, 2011, available at: *http://www.bbc.co.uk/news/technology-14981672*; Evgeny Morozov, "Political Repression 2.0," *New York Times*, September 1, 2011, available at: *http://tinyurl.com/3pfa5wp (www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html?_r=1).*

42 Freedom House, "Country Report: Egypt."

43 It has been reported that all it took to shut down the Internet in Egypt was six phone calls from Hosni Mubarak to the major Egyptian telecoms. See John Palfrey's opening statement in the Economist's online debate on Internet Democracy: John Palfrey and Evgeny Morozov, "Internet Democracy: This House Believes That the Internet Is Not Inherently a Force for Democracy," *The Economist*, February 23, 2011, available at *http://www.economist.com/debate/days/view/662*.

44 "Egypt Leaves the Internet," *Renesys Blog*, January 27, 2011, available at: *http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml*.

45 Note that before the January 2011 Internet shutdown in Egypt, the last event of that scale was the complete cutting off of Internet access in Burma during the Saffron Revolution in September 2007; see Mridal Chowdhury, " The Role of the Internet in Burma's Saffron Revolution," Berkman Center Research Publication No. 2008–8, September 1, 2008, available at: *http://tinyurl.com/83edcaq (cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Chowdhury_ Role_of_the_Internet_in_Burmas_Saffron_Revolution.pdf_0.pdf).*

46 "Internet blackouts: Reaching for the Kill Switch."

47 Hadi Soharbi-Haghighat and Shohre Mansouri, "WHERE IS MY VOTE? ICT Politics in the Aftermath of Iran's Presidential Election," *International Journal of Emerging Technologies and Society* 8:1 (2010):25.

48 The Basij is a volunteer paramilitary organization under the control of the Iranian Revolutionary Guard Corps.

49 Saeed Kamali Dehghan, "How Film about Iranian Protester Neda Agha-Soltan Went Viral," *The Guardian*, June 4, 2010, available at: *http://www.guardian.co.uk/world/video/2010/jun/04/neda-agha-soltan-iran*.

50 Ali Jahanii, "Neda Agha Soltan killed 20.06.2009, Presidential Election Protest," YouTube video, available at: *http://www.youtube.com/watch?v=76W-0GVjNEc&skipcontrinter=1*.

51 Morozov, *The Net Delusion*, 1.

52 "New Media Pack Political Punch," *Oxford Analytical Daily Brief*, July 2, 2008, 1.

53 Hillary Clinton, "Internet Rights and Wrongs: Choices and Challenges in a Networked World," speech, George Washington University, February 15, 2011.

54 "Iran," *OpenNet Initiative*, June 16, 2009, available at: *http://opennet.net/research/profiles/iran*.

55 Soharbi-Haghighat and Mansouri, "WHERE IS MY VOTE? ICT Politics in the Aftermath of Iran's Presidential Election," 28.

56 Morozov, *The Net Delusion*, 10.

57 Rhoades and Chao, "Iran's Web Spying Aided by Western Technology."

58 Amir Baherpour and Roya Soleimani, "Oppression 2.0: Iranian Discontent in Cyberspace," *PBS Frontline*, July 2011, available at: *http://tinyurl.com/3rwlrvc (www.pbs.org/wgbh/pages/frontline/tehranbureau/2011/07/oppression-20-iranian-discontent-in-cyberspace.html).*

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1

59 Neil Ungerleider, "Iran Cracking Down Online with Halal Internet," *Fast Company*, April 18, 2011, available at: *http://www.fastcompany.com/1748123/iran-launching-halal-internet*.

60 Rhoades and Chao, "Iran's Web Spying Aided by Western Technology."

61 Ronald Diebert, *Casting a Wider Net: Lessons Learned in Delivering BBC Content on the Censored Internet*, Canada Centre for Global Security Studies and Citizen Lab at Munk School of Global Affairs, University of Toronto, October 11, 2011, available at: *http://munkschool.utoronto.ca/downloads/casting.pdf*.

62 Andrew Malcom, "Top of the Ticket: Iran Ambassador Suggests CIA Could Have Killed Neda Agha-Soltan," *Los Angeles Times*, June 25, 2009, available at: *http://tinyurl.com/nax2s7 (latimesblogs.latimes.com/washington/2009/06/neda-cia-cnn-killing.html)*.

63 Monica Gamsey, producer, "A Death in Tehran," *PBS Frontline*, November 17, 2009, available at: *http://www.pbs.org/wgbh/pages/frontline/tehranbureau/deathintehran/*.

64 Morozov, *The Net Delusion*, 11.

65 Michael Posner, "Internet Freedom and Human Rights: The Obama Administration's Perspective," remarks to the New America Foundation's 'Future Tense' conference, Washington, DC, July 13, 2011, available at: *http://www.state.gov/g/drl/rls/rm/2011/168475.htm*.

66 Clay Shirky, "The Political Power of Social Media," *Foreign Affairs*, January/February 2011, available at: *http://tinyurl.com/28r09cl (www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media)*.

67 Morozov, *The Net Delusion*, 207.

68 "Worse Than Useless," *The Economist*, September 16, 2010, available at: *http://www.economist.com/node/17043440*.

69 Take for example Blue Coat, a California firm that inadvertently supplied Syria with filtering and monitoring tools. Blue Coat claimed that their product was shipped to the Middle East with the Iraqi government as the intended recipient, and reported the improper transfer when they discovered the technology was being used in Syria. See: *http://tinyurl.com/3dnz222 (online.wsj.com/article/SB10001424052970203687504577001911398596328.html)*.

70 Morozov, *The Net Delusion*, xvii.

71 Ibid.

Journal of Strategic Security

https://scholarcommons.usf.edu/jss/vol5/iss2/6
DOI: http://dx.doi.org/10.5038/1944-0472.5.2.1