The Communication Review, 14:216–232, 2011

ISSN: 1071-4421 print/1547-7487 online
DOI: 10.1080/10714421.2011.597254

Routledge
Taylor & Francis Group

When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media

PHILIP N. HOWARD, SHEETAL D. AGARWAL,
and MUZAMMIL M. HUSSAIN
Department of Communication, University of Washington, Seattle, Washington, USA

Although there have been many studies of the different ways regimes censor the use of social media by their citizens, shutting off social media altogether is something that rarely happens. However, it happens at the most politically sensitive times and has widespread—if not global—consequences for political, economic and cultural life. When do states disconnect their digital networks, and why? To answer this question, the authors build an event history database of incidents in which a regime went beyond mere censorship of particular websites or users. The authors draw from multiple sources, including major news media, specialized news services, and international experts, to construct an event log database of 566 incidents. This rich, original dataset allows for a nuanced analysis of the conditions for state action, and the authors offer some assessment of the effect of such desperate action. Comparative analysis indicates that both democratic and authoritarian regimes disable social media networks for citing concerns about national security, protecting authority figures, and preserving cultural and religious morals. Whereas democracies disable social media with the goal of protecting children, authoritarian regimes also attempt to eliminate what they perceive as propaganda on social media. The authors cover the period 1995–2011 and build a grounded typology on the basis of regime type, what states actually did to interfere with digital networks, why they did it, and who was affected.

For replication data, please visit http://faculty.washington.edu/pnhoward/

Address correspondence to Philip N. Howard, Department of Communication, University of Washington, 102 Communications Building, Box 353740, Seattle, WA 98195, USA. E-mail: pnhoward@uw.edu

Between January and April 2011, public demand for political reform cascaded from Tunis to Cairo, Sana'a, Amman, and Manama. This inspired people in Casablanca, Damascus, Tripoli, and dozens of other secondary cities to take to the streets to demand change. By May, the political casualties were significant: Tunisia's Ben Ali and Egypt's Mubarak, two of the region's most recalcitrant dictators, were gone; Libya was locked in a civil war; several monarchs had sacked their cabinets and committed to constitutional reforms (and some several times over). Governments around the region had sued for peace by promising their citizens hundreds of billions of dollars in new spending measures for infrastructure projects, family and unemployment benefits, free or subsidized food, salary increases for civil servants and military personnel, tax cuts, affordable-housing subsidies, and social security programs. Morocco and Saudi Arabia appeared to fend off serious domestic uprisings, but the outcomes for regimes in Bahrain, Jordan, Syria, and Yemen were far from certain. Democratization movements had existed long before technologies such as mobile phones and the Internet came to these countries. With these technologies, people sharing an interest in democracy built extensive networks, created social capital, and organized political action. With these technologies, virtual networks materialized in the streets. As a desperate measure, many states tried to choke off information flows between activists, and between activists and the rest of the world.

Mubarak tried to disconnect his citizens from the global information infrastructure in the last week of January 2011. It was a desperate maneuver with mixed effect. A small group of tech-savvy students and civil society leaders had organized satellite phone and dialup connections to Israel and Europe, so they were able to keep up strong links to the rest of the world. It appears that some of the telecommunications engineers acted slowly on the order to choke off Internet access. The first large Internet service provider (ISP) was asked to shut down on Friday, January 28, but engineers did not make the change until Saturday. Other providers responded quickly, but returned to normal service on Monday. The amount of bandwidth going into Egypt certainly dropped off for 4 days, but it was not the information blackout Mubarak had asked for. Taking down the nation's information infrastructure also crippled government agencies. The people most affected were middle-class Egyptians, who were cut off from Internet service at home. Some people certainly stayed there, isolated and uncertain about the status of their friends and family. In the absence of information about the crisis, others took to the streets, eager to find out what was going on.

This was not the first wave of incidents in which governments disconnected their citizens from global information flows. On Friday, June 12, 2009, Iran voted. When voters realized the election had been rigged, many took to the streets to protest. Social media such as Twitter, Facebook, and SMS messaging were actively used to coordinate the movements of protesters and to get images and news out to the international community. Compared

with protests that occurred the last time elections were stolen, the social movement lasted longer, it drew in millions more participants, and there were more witnesses to the brutal regime crackdown. Social media had a clear role in extending the life of civil disobedience. Although the theocratic regime did not fall, there were some important outcomes: the ruling mullahs were split in opinion about the severity of the crackdown. As part of the response, the regime attempted to disable national mobile phone networks. It disconnected the national Internet information infrastructure for several hours and installed a deep-packet inspection system that significantly slowed traffic.

For civil society actors around the world, digital media and online social networking applications have changed the way in which dissent is organized (Bimber, 2005; Howard, 2010; Still, 2005). Social movement leaders from around the world use online applications and digital content systems to organize collective action, activate local protest networks, network with international social movements, and share their political perspective with global media systems (Byrne, 2007; De Kloet, 2002; Shumate, 2006). In the past, authoritarian regimes easily controlled broadcast media in times of political crisis; by destroying newsprint supplies, seizing radio and television stations, and blocking phone calls. It is certainly more difficult to control digital media on a regular basis, but there have been occasions in which states have disabled a range of marginal to significant portions of their national information infrastructure. What situational tendencies cause state-powers to exercise specific acts of blocking Internet access and disabling digital networks? When do regimes resort to the more extreme measures of shutting off Internet access? When they do not have the capacity to control digital networks, how do states respond offline to dissent and criticism? What is the effect of doing so, and who is most affected?

It is difficult to investigate patterns of state censorship. Many reports of censorship are essentially self-reports by technology users who assume there is a political reason behind their inability to connect to a digital network, whether they are mobile phone networks, gaming networks, or the Internet. Sometimes the state admits to acts of censorship, which makes it easier to learn why the government interfered and to what effect. Other times the state acts so clumsily or breaks the communication link between such large networks that many users can report being affected. While several researchers study the broad social effect of censorship, there are only a few who are able to provide evidence about both the shared perception that the state is surveilling its public and specific incidents of censorship that involve disconnections in digital networks (Deibert, Palfrey, Rohozinski, & Zittrain, 2010; Deibert, Palfrey, Rohozinski, Zittrain, & Stein, 2008). Drawing from multiple sources, however, it is possible to do a comparative analysis of the myriad incidents in which government officials decide to censor

their online publics. By collecting as many known incidents of state intervention in information networks, it is possible to map out the contours of crisis situations, political risks, and civic innovations to understand the new intersections between state power and civil society.

Not all incidents involve authoritarian regimes, and not all acts of state censorship are easy to describe and classify. One of the first incidents occurred on December 29, 1995, when German prosecutors demanded that an ISP block 4 million worldwide subscribers from reading sex-related information on portions of the Internet. This was the first instance of such drastic measures of state censorship, legislation, and regulation of information received online. Motivation for the shutdown came from a police investigation into child pornography in Bavaria, Germany. Although German officials were targeting 220,000 German subscribers when they asked for the block, CompuServe had no mechanism in place to limit just German users at the time, thus, they shut down service to all subscribers. In all, CompuServe restricted subscriber access to 200 newsgroups, specifically related to the site *Usenet*. Reaction to the censorship elicited varied responses from community and civic groups. The National Center for Missing and Exploited Children, for example, hailed it as a form of "electronic citizenship." Meanwhile, groups such as the Electronic Freedom Foundation indicated both concern and resistance to the notion of state control over individual rights online.

This early incident of state intervention with Internet connectivity brought forth questions that we still struggle to answer today: Who controls Internet content? What are the legitimate reasons for state interference with digital networks? Over the past 15 years, we find that states are increasingly willing to interfere with the links between nodes of digital infrastructure by shutting out particular users or shutting off particular servers, by breaking the links to subnetworks of digital media, and sometimes even by disconnecting national information infrastructure from global networks.

Recently, Research in Motion (RIM) was involved in a complex issue involving several states' requests to provide better access to the server nodes in Blackberry service networks. In the spring of 2010, a prominent political figure in the United Arab Emirates (UAE) used his Blackberry's mobile camera to record himself torturing a Bangladeshi migrant worker. The video was taken and posted online, causing outrage from human rights groups and embarrassing the country's ruling elites. The UAE's response has been to demand that RIM provide dedicated servers within their territory so that the regime could monitor traffic and disable services as needed. Eventually both Saudi Arabia and the UAE threatened to ban the use of the popular Blackberry smart phone. The UAE threatened to block access to text messages, e-mail, and web browsers if RIM did not allow government access for security investigations. The threat of censorship was still in place as of October 2010, potentially affecting more than half a million users of the most popular smart phone in the UAE.

In 2010, India followed suit, also citing national security as the impetus for demanding RIM stop encrypting data sent through their phones. This incident illustrates a growing tension between governments and mobile Internet users' privacy today. Increasingly, over the past decade private companies and ISP providers like RIM are caught in between meeting the security and information needs of their citizen users, and obeying imposed government regulations by nation states. Most recently, Vodafone was under pressure from both Mubarak's regime to shut off Internet access and civil society activists to keep the communication channels open. Concession by the ISPs is more valuable to these states than a block however, as a block will severely limit businesses run by citizens in these countries as well as those of visitors and tourists. After Vodafone complied with Mubarak's regime to turn off Internet access, it cost the national economy an estimated $90 million and the country's reputation as a safe and stable place for technology firms to invest.

Since 1995—the year the National Science Foundation effectively privatized the Internet—there have been at least 566 occasions in which governments intervened in the connections of a digital network. Of these, about half were enacted by authoritarian regimes. The three countries with the highest number of incidents, China, Tunisia, and Turkey, represent both authoritarian and democratic regimes. In times of political uncertainty, rigged elections, or military incursions, ruling elites are sometimes willing to interfere with information infrastructure as a way of managing crises. In many of these cases, the targets (victims) are active domestic civic society movements with international linkages. When these movements organize, authoritarian governments can react harshly and invasively by blocking access to the global Internet. Yet at the same time, these authoritarian regimes find that they cannot block Internet access for extended periods, both because doing so has an effect on the national economy and because of international political pressure. Shutting off the Internet for a country's network also has an effect on the capacity of the state to respond to the crisis—for example, Egyptian authorities did not expect that turning off Internet and SMS networks would draw out protesters in larger numbers to the street. Therefore, the decision tree for choking off Internet access also involves some willingness to incapacitate portions of the government's security apparatus. Increasingly, civil society groups find methods to circumvent the blocked social media. A significant corpus of literature has grown around the use of newer digital media by social movements against authoritarian regimes (Garrett, 2006; Marmura, 2008; McLaughlin, 2003). Although there is a healthy ongoing conversation by scholars on the issue of civil societies' uses of digital media for social and political mobilization, this investigation illuminates the impetuses, tactics, and effects of state responses to online engagement.

We conduct a comparative case analysis of the occasions in which regimes disconnected significant portions of their national digital infrastructure, including mobile phones and Internet access. Our goal is to define the range of situations in which states have actually disrupted large sections of their own national information infrastructure. Through a grounded comparison of incidence, we demonstrate the importance of understanding how information technologies have a role in political responses and counterinsurgency tactics of many kinds of regimes. Such comparative study will help explicate the meaning of contemporary state power in media systems of both advanced and developing countries. Although some have argued that the state no longer has strong control of media production and consumption systems, there are a range of occasions in which state power over digital networks is noticeably strong.

METHODS AND DATA

Event history analysis is a commonly used comparative method for understanding the real circumstances of political crises. More important, it is particularly useful for developing nuanced understanding of relatively new social phenomena, and for building typologies and categories of political action. Drawing on a range of sources, we built a unique collection of detailed event logs for major disruptions in digital networks of nations between 1995 and 2010. We collected information about incidents as reported in major news media, specialized news sources such as national security and information security blogs, and other online forums for discussing such topics. These sources include Google News, LexisNexis, Attrition.org, GlobalVoices.org, among others.

A case is defined as an occasion in which a government intervened in a digital network by breaking or turning off connections between national subnetworks and global information networks. Sometimes this meant blocking ports or access to a particular subnetwork of digital media, such as content at the domains Facebook.com or YouTube.com. In times of significant political or military crisis, such as war or contested elections, the governments might disconnect SMS messaging services or block the entire country's access to global networks. In addition, regimes may target individual actors in networks. However, these incidents are more than general government threats of surveillance or intimidation (which are also forms of censorship). These are distinct incidents where government officials made the specific decision to disable the links or nodes in the portions of the information networks they can control.

Because the literature on digital censorship often makes a distinction between democracies, emerging democracies and authoritarian regimes, we rely on the Polity IV data about regime type (Marshall & Jaggers, 2010). In

addition, since several of the governments appearing in the event log are too fragile to sensibly be given one of these three categories, we rely on Polity IV data for a category of fragile regimes. As per Polity IV coding, if a state was recovering from civil war or foreign military invasion, experiencing a complex humanitarian disaster, or had effectively failed for other reasons, we code this state as fragile. A state's regime type was set according to the Polity IV score for that state in the year of the reported incident. Several countries had several incidents, and it is possible that regime types changed over time.

All in all, there were 566 unique incidents involving 101 countries: 39% of the incidents occurred in democracies, 7% occurred in emerging democracies, 51% occurred in authoritarian regimes, and 2% occurred in fragile states. Each incident was coded for the name of the country in which a state agency intervened in digital networks, the year of the incident, the type of regime, and a precise date if available. We made general notes on the narrative of each incident, and mapped on the Polity IV score for the country in the year of the incident. Then we developed three standardized typologies for the kinds of incidents being reported. First, we developed a category that iteratively helped define the case, and a typology of actions that states take against social media. Second, we developed a category for why they took that action, sometimes relying on third-party reports if the state simply denied any interference. Last, we developed a category for the effect of the interference.

Although we might expect authoritarian regimes to more aggressively interfere with their digital infrastructure than other types of regimes, Figure 1 reveals that democracies also substantively disconnect their communication networks. In recent years, there have been at least 80 incidents a year. Only a fraction of these involve emerging democracies, but Figure 1 only begins the analysis. Over time, it appears that all types of regimes have become more and more willing to interfere with information access. As social media have diffused, they have become a fundamental infrastructure for collective action. Even though democracies appear just as aggressive as authoritarian regimes in disconnecting digital networks, are there differences in the ways in which such states intervene? What are the different reasons for such drastic interventions?

ANALYSIS: DECISION PATHS AND OPPORTUNITY STRUCTURES

Civil society is often defined as the self-generating and self-supporting community of people who share a normative order and volunteer to organize political, economic or cultural activities that are independent from the state (Diamond, 1994). Civil society groups are a crucial part of all elections because they represent diverse perspectives and promote those perspectives

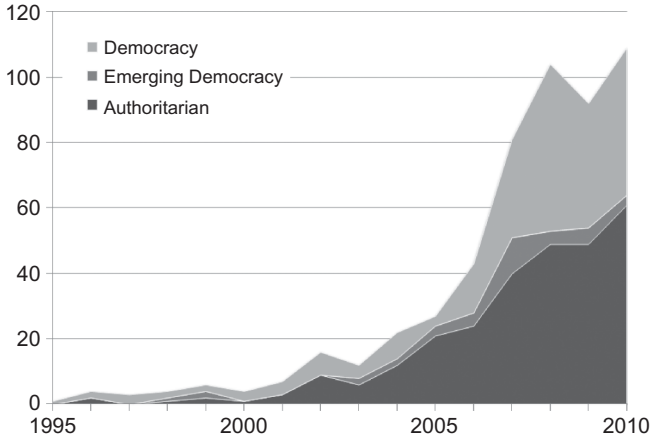

FIGURE 1 Number of Major Incidents of State Intervention in Digital Networks, By Regime Type, 1995–2011 ($N = 566$). Current as of April 2011. Regime Type Attributed to the Specific Year in Which Incident Was Recorded.

through communications media. Moreover, a key tenet of the shared normative order is that no one group can claim to represent the whole of society. Democracy is best served by a multitude of groups that contribute in different ways to conceiving public policy options and national development goals. Some governments work hard to censor digital media, but even in such countries the Internet is difficult to control. Governments might own nodes in the network, but rarely can they completely choke off network connections. This means that tools like YouTube, Twitter, Facebook, and e-mail are useful, and at sensitive times, critical, organizational tools. In some of the toughest authoritarian regimes, these tools are crucial because face-to-face conversations about political life are so problematic. For civil society groups—these tools are often content distribution systems largely independent of the state.

The Internet has become an invaluable logistical tool for organization and communication for civil society groups. It is an information infrastructure mostly independent of the state, and since civil society groups are by definition social organizations independent of the state, the Internet has become an important incubator for social movements (radical and secular) and civic action. The Internet has altered the dynamics of political communication systems in many countries, such that the Internet itself is the site of political contestation between the state and civil society.

How Do States Interfere With Digital Networks?

We find that states interfere with digital networks using many tactics, with various levels of severity: online, by shutting down political websites or portals; offline, by arresting journalists, bloggers, activists, and

TABLE 1 How Do States Disconnect Their Digital Networks? Incidents, by Regime Type ($N = 754$)

	Democracy	Emerging democracy	Authoritarian	Fragile	Total
Complete network shutdown (full networks)	13	3	30	3	49
Specific site-oriented shutdowns (subnetworks)	140	25	210	8	383
Individual users (Nodes)	82	16	125	3	226
By proxy through Internet service provider	47	4	41	4	96

Note. Incident types are not mutually exclusive, given that some incidents involved combinations of state tactics against social media use.

citizens; by proxy, through controlling ISPs, forcing companies to shut down specific websites or denying access to disagreeable content; and, in the most extreme cases, shutting down access to entire online and mobile networks. Surprisingly, we find that while authoritarian regimes practice controlling full-networks, subnetworks, and nodes more than democracies, democracies are the most likely to target civil society actors by proxy by manipulating ISPs. Table 1 presents cases where governments exercised control by targeting full-networks (shutting down the Internet), subnetworks (blocking websites), network-nodes (targeting individuals), and by proxy (pressuring ISPs).

The most extreme form of network control is when states shut down access to the Internet. Authoritarian regimes did so significantly more than fragile states and emerging democracies, and also twice as more as democracies. A clear illustration of this was when China shut down Internet services in the Xinjiang region after ethnic riots erupted in 2006. The riots resulted in 140 fatalities, and the state has since blocked access to Twitter and other social networking sites to control the conflict and dissent. More recently, Pakistan severely restricted the Internet after a US-based cartoonist organized an "Everybody Draw Mohammed Day." After the event attracted 43,000 fans from around the world, the Pakistan government went into 'banning mode' because the event invited members to draw and post pictures of the revered prophet. Similarly, emerging democracies, like Haiti and Thailand, have engaged in shutting down main ISPs, or entire online networks like YouTube, respectively. Thousands of Haitians lost Internet access in 1999 when the government attempted to allegedly silence dissent and consolidate power under the guise of punishing Alpha Network Communications for selling telephone cards and providing international telephone services. More recently, Bangladesh blocked YouTube and most other file sharing services after recordings of a meeting between the Prime Minister and army senior officers were leaked onto YouTube. Thailand, also an emerging

democracy with a record of political online censorship, maintains a block on entire Internet services such as YouTube. Bangladesh, a democracy, also blocked entire networks when a political crisis over the murder of a prominent lawyer raged on the WordPress network. These examples suggest that although complete network shut-downs are least common, they tend to materialize when states face national controversies and moments of severe social and political unrest, often (but by no means exclusively) in authoritarian regimes.

Unlike the most extreme measure of shutting down entire online networks, states are most likely to target individual websites (online) or their producers and users (offline). Democracies are much more likely to engage in online content censorship than other tactics, although they also frequently target civil society members offline. The earliest case of a democracy shutting down online subnetworks was in 1995 when German authorities removed access to over 200 Internet newsgroups deemed indecent and offensive. In 1996, German authorities again removed access to banned material, such as a Netherland's online magazine. More recently, advanced democracies such as Australia, as of July 2010, is considering a mandatory Internet filter to censor a list of URLs associated with child sexual abuse, bestiality, sexual violence, crime, violence, drug use, and content advocating violence and extremism.

While socially questionable material and content promoting criminal activities are commonly cited reasons for blocking content in democratic states, some states have also used this as a tactic for foreign policy disputes. In August 2010, South Korea engaged in an online dispute with North Korea over social media when South Korean citizens were threatened with arrests for accessing North Korea's Twitter feed. However, despite attempting to reroute requests from North Korea's Twitter page to a warning page, more than 9,000 followers had accumulated.

In instances such as this, when unable to block online content effectively, states are forced to go directly towards censoring individuals. Authoritarian states do this most often, and in many cases, with more severity. Bloggers, journalists, and social activists are the most common individual targets of offline censorship, often facing arrests and fines. For example, an Egyptian blogger was sentenced to 4 years in prison for insulting the Egyptian President Hosni Mubarak. Following Thailand's coup d'état in 2006, two cyber dissidents were arrested for comments made about the monarchy in online discussion boards, and now face a minimum sentence of 15 years in prison. Another example of online activities leading to offline government reactions is Cuba's arrests of two online journalists working for CubaNet in 2005 and 2007. These journalists were arrested for engaging in "subversive propaganda" and "precriminal social danger." With authoritarian regimes, it is generally the case that criticisms of political elites are

often dealt with the imposition of fines, searches, seizure of equipment, and imprisonment.

Although democracies also engage in a good amount of censoring individual users, paralleling the conditions of authoritarian regimes, they also have a unique tendency to target individuals providing the infrastructure. Democracies have a slightly higher rate of blocking content and controlling civil society actors through indirect measures, such as targeting Internet ISPs. Turkey and Italy, both democracies, have legally pursued charges against ISPs and their users. In March 2010, an Italian court convicted three Google executives for not removing violent video content that appeared on their online services. In August 2009, Malawi approved legal measures to pressure ISPs in monitoring social networking sites such as Twitter and Facebook. Hungary and Belgium have also shared experiences where ISPs have received pressures to approve "notices of takedown" procedures from their governments. It is surprising to note that although authoritarian regimes frequently fine and imprison civil society actors directly for criticizing the regime and its elites, democracies have more examples of regimes using legal frameworks and roundabout measures for targeting ISPs and their users.

Why Do States Interfere With Digital Networks?

Looking across all of the incidents, we identified twelve categories represented two broader themes—protecting political authority and preserving the public good. The first broad theme of protecting leadership and state institutions included several kinds of reasons for state interference in public access to social media. These reasons include: protecting political leaders and state institutions; election crisis; eliminating propaganda; mitigating dissidence; and national security. *National security* was the most commonly cited reason under this theme, where officials cited "terrorism threats" and preventing the spread of "state secrets" as reasons to intervene with Internet access. Information that undermined protection of authority figures in any way was another subcategory oft attributed for intervention. For example, in 2007 Kazakh officials shut down opposition websites for 3 days, because of published transcripts and recordings related to a public battle between authoritarian President Nazarbayev and his estranged son-in-law. The *eliminating propaganda* subcategory included incidents where intervention occurred because of the spread of information aimed at serving an agenda undermining the standing regime. For example, China in 2003 sentenced an individual to 4 years in prison for e-mail discussions and postings in online forums and chat rooms related to democracy. The *mitigating dissidence* subcategory captures those cases in which intervention was attributed to an attempt to reduce dissident civic action, such as the U.S. arresting two individuals who tweeted about police locations during

G20 protests in Pittsburgh, Pennsylvania in 2009. Incidents included under the *election crisis* subcategory include cases in which a regime acted in response to events surrounding elections. This subcategory included times when the regime intervened prior to, during, or after elections. For example, in the aftermath of the highly contested Iranian elections in 2009, the regime first slowed and then shut down access to the Twitter network, which was heavily used by protestors to coordinate and share information about the contested elections.

The second over-arching theme for why states disabled social media was in claiming an urgent need to preserve the public good. Sub-categories of this theme include: preserving cultural and religious morals; preserving racial harmony; protecting children; cultural preservation; protecting individuals' privacy; and dissuading criminal activity. *Preserving cultural and religious morals* was the most cited reason for intervention across all themes and categories. This subcategory was used in incidents when officials attributed intervention to preventing the spread of blasphemous or offensive information that challenged the religious and cultural morality of the state. An overwhelming number of these cases involved targeting websites and individuals who accessed or distributed anti-Islamic or pornographic material (not including child pornography, which was captured in a separate category). An illustration of such an incident was from 2009, when Pakistan blocked access to 450 sites including Facebook and YouTube after an international event to depiction the prophet Mohammed was organized on Facebook.

Cultural preservation, included incidents in which interventions were attributed to the need to expel outside influence or threats to national interests were cited (but not related to terrorism or national security threats, which were captured by a separate category). In December 2006, Iran shut down access to websites such as YouTube and Amazon in order to "purge the country of Western influence." Though we encountered only a few cases that cited *preservation of racial harmony* as the impetus for action, these incidents are useful to recognize separately from other categories as they focus intervention on protecting the public specifically from ethnic or racially motivated violence. For example, in 2008 Germany convicted a blogger for inciting hatred by denying the Holocaust.

Dissuading the public from *criminal activity* is another reason often cited by officials. Incidents under this category include arresting individuals for copyright infringement, distributing illegal information, and participating in activities deemed illegal by the state, such as online gambling. Cases in this subcategory included the arrests or criminal prosecutions of individuals whom authorities claimed were breaking the law. An example of such a case was when Polish authorities arrested the creators of a peer-to-peer portal and shut down the site in 2009, citing copyright infringement as the reasoning.

Protecting children as a subcategory included incidents where officials explicitly sited threats to children and minors as reasons for intervention. While many of these incidents related to pornographic material, only those cases that specifically included reference to child pornography were included under this subcategory. States often adopted Internet laws and policies to protect children; an illustration includes Brazil's adoption of policies that require ISPs to provide lists of the websites they host to a child protection agency and put a button on their website that says "Pedophilia is a crime, denounce it."

Last, only four yet thematically distinct cases represented the final subcategory under this theme: *protecting individuals' privacy*. This subcategory included incidences in which authorities determined that an individual's privacy was jeopardized by content posted on the Internet. Perhaps the most clear example of such a case was when Tunisian official jailed and fined an individual for "causing harm by means of telecommunication networks" because he did not obtain an official permit or consent of the individuals he filmed for an online video.

There were certain types of cases that were difficult to categorize. There include reports of some incidents where there was not enough information to assert the reasons for the intervention. This includes cases in which officials simply did not cite a reason for intervention, or when our primary texts did not provide enough insight into why the intervention took place. These incidents categorized as *unknown/other*. In addition, there were cases in which officials simply denied any responsibility for censorship or claimed it was a technical issue, thus we are unable to attribute reasons for the intervention. These cases are captured in the subcategories, *censorship denied* and *alleged system failure*. While it may not be surprising that authoritarian regimes invoke intervention policies to protect state authorities and institutions, Table 2 reveals that democratic regimes exercise intervention efforts at nearly the same level for these same reasons, which severely limits civil society groups from participating in the foundational democratic practices of the regime.

The advantage of a comparative approach is that it allows us to avoid and move beyond organizational and technological determinism (Howard, 2002). It does so by allowing us to build grounded typologies of real government responses to the development of new media, and particularly social media.

The lasting effect of a temporary disconnection in Internet service may actually be a strengthening of weak ties between global and local civil society networks. When civil society disappears from the grid, it is noticed. What lasts are the ties between a nation's civic groups, and between international nongovernmental organizations and like-minded, in-country organizations. It is certain that not all of these virtual communities are about elections, but their existence is a political phenomenon particularly

TABLE 2 Why Do States Disconnect Their Digital Networks? Reasons, by Regime Type ($N = 556$)

	Democracy	Emerging democracy	Authoritarian	Fragile	Total
Protecting authority					
Protecting political leaders and state institutions	30	7	23	1	61
Election crisis	4	3	9	0	16
Eliminating propaganda	5	1	24	0	30
Mitigating dissidence	8	5	11	3	27
National security	29	6	34	0	69
Preserving the public good					
Preserving cultural and religious morals	27	4	37	6	74
Preserving racial harmony	9	0	1	0	10
Protecting children	30	0	2	0	32
Cultural preservation	2	0	19	0	21
Protecting individual's privacy	3	0	2	0	5
Dissuading criminal activity	29	3	18	1	51
Alleged system failure, neither denied nor admitted	4	4	9	0	17
Censorship denied by state	3	1	11	0	15
Unknown, other	40	4	90	4	138
Total	223	38	290	15	566

Note. Reasons for intervention are mutually exclusive.

in countries where state and social elites have worked hard to police offline communities. Thus, even the bulletin boards and chat rooms dedicated to shopping for brand name watches are sites that practice free speech and where the defense of free speech can become a topic of conversation. The Internet allows opposition movements that are based outside of a country to reach in and become part of the system of political communication within even the strictest authoritarian regimes. Today, banning political parties could simply mean that formal political opposition is now organized online, from outside the country. It could also mean that civil society leaders turn to other organizational forms permitted by network technologies. When states disconnect particular social media services, student and civil society leaders develop creative workarounds and relearn traditional (offline) mobilization tactics. Thus, target sites, such as YouTube, Facebook, and Twitter, are almost always accessible through other means.

CONCLUSION: THE CAUSES AND CONSEQUENCES OF DIGITAL INTERVENTIONS

When a political, military, or other security crisis is over, what remains is the lasting effect of a temporary outage in digital network connectivity. The

Internet has become a crucial component of political communications during elections—even rigged ones. It has also become a crucial component of political communication during other kinds of regime transition, such as executive turnover, foreign military intervention, natural disasters, and social protests that challenge a regime's legitimacy. Information infrastructure is not simply part of the general context of contemporary social mobilization. Indeed, social computing is a defining feature of elections these days. Digital media such as mobile phones and the Internet now help incubate civic conversations, especially in countries that heavily censor the national print and broadcast media.

Internet access is often limited to wealthy social elites, but these elites have a key role in either accepting or rejecting the outcome of an election. The Internet has become a necessary infrastructure for the development of civil society and election season is often the time for civic groups to be most active. Most (although not all) of the regimes studied in this event catalogue are authoritarian, or were when the decision to disconnect from global information networks was taken. For authoritarian regimes, the single greatest threat to stability is often internal: elite defection. When the cohort of wealthy families, educated and urban elites, and government employees decide they no longer wish to back a regime, it is most likely to fail. In most of the countries studied here, only a small fraction of the population has Internet access through computers and mobile phones. However, this small population is the one that authoritarian regimes work hard to broker information for.

It is not Twitter, blogs, or YouTube that cause social unrest. Today, successful social movement organizing and civic engagement is difficult to imagine without them, even in countries such as Iran and Egypt. Many people in these countries have no Internet or mobile phone access. Nevertheless, the people who do—urban dwellers, educated elites, and the young—are precisely the population with the capacity to enable regime change, or tacitly support electoral outcomes. These are the populations who support or defect from authoritarian rule, and for whom connections to family and friends have demonstrably changed with technology diffusion. Comparative analysis reveals the degree to which different regimes feel threatened by social media, whether such tools are actively used to organize dissent, or passively used for producing and consuming culture.

When digital networks are reactivated, personal networks that cross international boundaries also reactivate. Digital outages have become sensitive moments in which student leaders, journalists, and civil society groups experiment with digital technologies. Even if their favorite candidates are not elected, the process of experimentation with digital media is important because it results in infusing more information habits and news diets independent of the state into their daily engagement with public life.

The political climax of uprising takes the form of state crackdowns or major concession to popular demands that can include executive turnover. Stalemates between protesters and ruling elites can result in protracted battles. However, in each country, the political climax of uprising can also be marked by a clumsy attempt by the state to disconnect its own people from digital communications networks. Banning access to social media websites, powering down mobile phone towers, or disconnecting the Internet exchange points in major cities are an authoritarian government's desperate strategies for asserting control. And there are serious economic consequences to disconnecting a nation from global information infrastructures, even temporarily. Interrupting digital services cost Egypt's economy at least $90 million, and their reputation among technology firms as a stable place for investment. In Tunisia it was activist hackers—*hacktivists* as many call themselves—who did the most economic damage by taking down the stock exchange. For the most part, it is recalcitrant authoritarian governments who make the decision to interfere with their country's digital networks.

Most technology users in most countries do not have the sophistication to work around state firewalls or keep up anonymous and confidential communications online. In each country, a handful of tech-savvy students and civil society leaders have these skills, and used them well during the Arab Spring. Learning from other democracy activists in other countries, these information brokers used satellite phones, direct landline connections to ISPs in Israel and Europe, and a suit of anonymization software tools to supply the international media with pictures of events on the ground—even when desperate dictators attempted to shut down national ISPs.

Information infrastructure *is* politics. And the political culture that we now see online during elections comes not just from political elites, but from citizens: using social media, documenting human rights abuses with their mobile phones, sharing spreadsheets to track state expenditures, and pooling information about official corruption. Perhaps the most lasting effect of digital media use during crises is that people get accustomed to being able to consume and produce political content. When regimes disconnect from global information infrastructure, they employ a range of stop-gap measures that usually reinforces public expectations for global connectivity.

ACKNOWLEDGMENTS

The authors gratefully acknowledge support from the World Information Access Project (www.wiaproject.org), funded by the National Science Foundation under award "Human Centered Computing: Information Access, Field Innovation, and Mobile Phone Technologies in Developing Countries" (Award #0713074). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not

necessarily reflect the views of the National Science Foundation. Replication data used in this research is available on the project website.

REFERENCES

Bimber, B. (2005). Reconceptualizing collective action in the contemporary media environment. *Communication Theory*, *15*, 365–388.

Byrne, D. (2007). Public discourse, community concerns, and civic engagement: Exploring Black social networking traditions on BlackPlanet.com. *Journal of Computer-Mediated Communication*, *13*, 319–340.

De Kloet, J. (2002). Digitisation and its Asian discontents: The Internet, politics and hacking in China and Indonesia. *First Monday*, *7*(9). Retrieved from http://www.firstmonday.dk/issues/issue7_9/Kloet/index.html

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J. L., & Stein, J. G. (2008). *Access denied: The practice and policy of global internet filtering*. Cambridge, MA: The MIT Press.

Diamond, L. (1994). Rethinking civil society: I. Toward democratic consolidation. *Journal of Democracy*, *5*, 4–17.

Garrett, R. (2006). Protest in an information society: A review of literature on social movements and the new ICTs. *Information, Communication & Society*, *9*, 202–224.

Howard, P. N. (2002). Network ethnography and the hypermedia organization: New media, new organizations, new methods. *New Media & Society*, *4*, 550–574.

Howard, P. N. (2010). *Digital origins of dictatorship and democracy: The Internet and political Islam*. New York, NY: Oxford University Press.

Marmura, S. (2008). A net advantage? The Internet, grassroots activism and American Middle-Eastern policy. *New Media & Society*, *10*, 247–271.

Marshall, M., & Jaggers, K. (2010). *Polity IV: Political regime characteristics and transitions, 1800–2009*. College Park, MD: Center for International Development and Conflict Management.

McLaughlin, W. (2003). The use of the Internet for political action by non-state dissident actors in the Middle East. *First Monday*, *8*, 1. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1791/1671

Shumate, M. (2006). Trouble in a geographically distributed virtual network organization: Organizing tensions in continental direct action network. *Journal of Computer-Mediated Communication*, *11*, 802–824.

Still, B. (2005). Hacking for a cause. *First Monday*, *10,* 1. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1274/1194.