Issues in TECHNOLOGY Innovation

Number 13 October 2011

The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?

Philip N. Howard, Sheetal D. Agarwal, and Muzammil M. Hussain

EXECUTIVE SUMMARY

When do governments decide to interfere with the Internet, and why? While many observers celebrate the creative use of digital media by activists and civil society leaders, there are a significant number of incidents involving government-led Internet shutdowns. Governments have offered a range of reasons for interfering with digital networks, employed many tactics, and experienced both costs and benefits in doing so.

© Reuters/Steve Crisp

When and why do states disconnect their digital networks is a principle question we examine in this paper. To answer this question, we built an event history database of incidents in which a regime went beyond mere surveillance of particular websites or users, and actually disconnected Internet exchange points or blocked significant amounts of certain kinds of traffic. All in all, there were 606 unique incidents involving 99 countries since 1995: 39 percent of the incidents occurred in democracies, 6 percent occurred in emerging democracies, 52 percent occurred in authoritarian regimes, and 3 percent occurred in fragile states. 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. Finally, we developed a category for the impact of the interference.

Issues in Technology Innovation

The Center for Technology Innovation at Brookings has launched its inaugural paper series to seek and analyze public policy developments in technology innovation.

The Center for Technology Innovation

Founded in 2010, the Center for Technology Innovation at Brookings is at the forefront of shaping public debate on technology innovation and developing data-driven scholarship to enhance understanding of technology's legal, economic, social, and governance ramifications.

We find that overall more democracies participate in network interventions than authoritarian regimes. However, authoritarian regimes conduct shutdowns with greater frequency. After 2002, authoritarian governments clearly began using such interference as tool of governance. In recent years, even fragile states have interfered with domestic information infrastructure, usually as a last effort at maintaining social control.

Regime Responses to the Political Use of Social Media

Philip N. Howard is an associate professor in the Department of Communication at the University of Washington.

Sheetal D. Agarwal is a doctoral student in the Department of Communication at the University of Washington.

Muzammil M. Hussain is a doctoral student in the Department of Communication at the University of Washington.

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 constitutional 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. But with these technologies, pro-democracy agitators 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 impact. A small group of tech-savvy students and civil society leaders had organized satellite phones 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 was asked to shut down on Friday, January 28, but engineers didn't respond until Saturday. Other providers responded quickly, but returned to normal service on Monday. The amount of bandwidth going into Egypt dropped off for four 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. But 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.[1] 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 was actively used to coordinate the movements of protesters and to get images and news out to the international community.

For civil society actors around the world, digital media and online social networking applications have changed the way in which dissent is organized.

Compared to 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. While 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.[2] Even today, the Iranian regime claims to be building the capacity to completely disconnect its public from global digital infrastructure.[3]

For civil society actors around the world, digital media and online social networking applications have changed the way in which dissent is organized.[4] 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 networks.[5] 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? And when they do not have the capacity to control digital networks, how do states respond offline to dissent and criticism? What is the impact 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 impact 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.[6] 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, we are able 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 Internet Service Provider (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. Though 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 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 last 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 sub-networks of digital media, and sometimes even by disconnecting national information infrastructure from global networks.

Since 1995—the year the National Science Foundation effectively privatized the Internet—there have been at least 606 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 civil 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 impact on the national economy and because of international political pressure. Shutting off the Internet for a country's network also has an impact 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.[7]

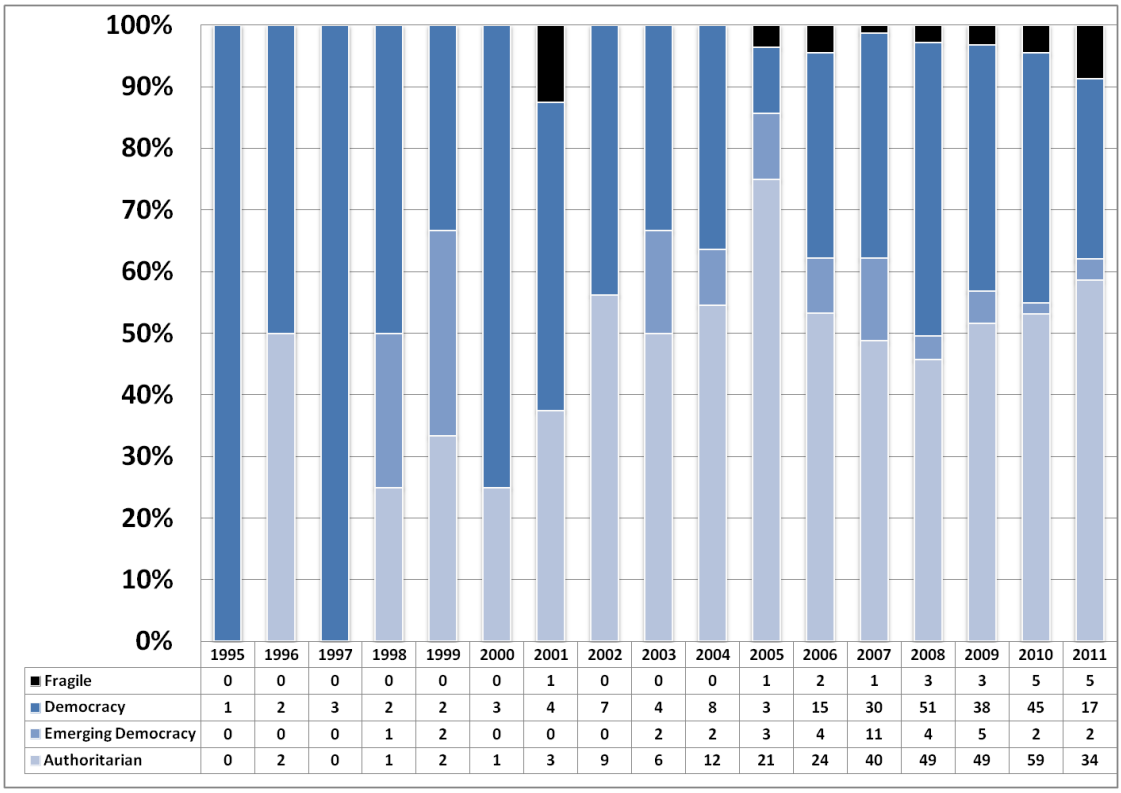
We conducted a comparative case analysis of the occasions in which regimes disconnected significant portions of their national digital infrastructure, including mobile phones and Internet access. Our goal is to define the range of situations in which states have actually disrupted large sections of their own national information infrastructure. Through a grounded comparison of incidents, we demonstrate the importance of understanding how information technologies have a role in political responses and counter-insurgency 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. While 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.

Surprisingly, while authoritarian regimes practice controlling full-networks, sub-networks, and nodes more than democracies, democracies are the most likely to target civil society actors by proxy by manipulating Internet service providers.

Rising Rates of Government Interference

Over time, the number of incidents involving state interference with Internet infrastructure has increased dramatically.[8] 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 citizens; by proxy, through controlling Internet service providers, forcing companies to shut down specific websites or denying access to disagreeable content; and, in the most extreme cases, shutting down access to entire online and mobile networks. Surprisingly, while authoritarian regimes practice controlling full-networks, sub-networks, and nodes more than democracies, democracies are the most likely to target civil society actors by proxy by manipulating Internet service providers. Governments exercised control by targeting full-networks (shutting down the Internet), sub-networks (blocking websites), network-nodes (targeting individuals), and by proxy (pressuring Internet service providers).

Figure 1: State Interference with Digital Networks, By Regime Type



	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Fragile	0	0	0	0	0	0	1	0	0	0	1	2	1	3	3	5	5
Democracy	1	2	3	2	2	3	4	7	4	8	3	15	30	51	38	45	17
Emerging Democracy	0	0	0	1	2	0	0	0	2	2	3	4	11	4	5	2	2
Authoritarian	0	2	0	1	2	1	3	9	6	12	21	24	40	49	49	59	34

Figure 1 reveals that until about 2002, the majority of states interfering with their domestic information infrastructure were democracies. After 2002, authoritarian governments clearly began using such interference as tool of governance. In recent years, even fragile states have interference with domestic information infrastructure, usually as a last effort at maintaining social control.

While 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 annually. 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 (since 2006), 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?

Governments have offered a wide range of reasons for interfering with digital media. Most commonly, states interfere with digital networks with the goal of protecting political authority or 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 sub-category oft attributed for intervention. For example, in 2007 Kazakh officials shut down opposition websites for three 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* sub-category 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 four years in prison for email discussions and postings in online forums and chat rooms related to democracy. The *mitigating dissidence* sub-category 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* sub-category include cases in which a regime acted in response to events surrounding elections. This sub-category 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.

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.

The second over-arching reason for disabling social media was to 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 sub-category 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 is from 2009, when Pakistan blocked access to 450 sites including Facebook and YouTube after an international event to draw the prophet Mohammed was organized on Facebook.

The lasting impact 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 non-governmental organizations and like-minded, in-country organizations. Certainly not all of these virtual communities are about elections, but their existence is a political phenomenon particularly 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 oppositions 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 means 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. This almost always means that target sites, such as YouTube, Facebook, and Twitter, are accessible through other means.

Conclusion: Sensible Foreign Policy Objectives for the West

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. For these reasons, foreign policy objectives must include some sensible information infrastructure aspects.

Increasingly, Western governments are advocating for open access to the Internet as a key element in foreign policy, and investing in online tools for promoting democratic values. For example, the U.S. State Department has allocated some $28 million to Internet Freedom programs around the world. Still, there are several kinds of sensible foreign policy recommendations that could support the information infrastructure of civil society actors and allow people around the world access to international news content. Policy goals could include:

- Support net neutrality by enforcing and promoting policies for equal access and non-discrimination both at home and abroad.
- Hold open conversations with U.S.-based firms that export censorship software, build kill-switches, or design user-policies that have an impact on how civic leaders organize popular democracy movements.
- Support freedom of expression, particularly by having U.S. diplomats advocate for individual journalists—or citizen journalists—who have been arrested or harassed by repressive regimes.

- Avoid using information sanctions as a policy mechanism for punishing states. Civil society actors also suffer when foreign governments impose restrictions on the flow of information.
- Invest in broad digital literacy and technology development programs in developing countries, by supporting programs that educate citizens that support local sustainable innovation in communities.

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 impact 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.

Acknowledgements

For questions about this research, please contact Philip N. Howard, Department of Communication, University of Washington, 102 Communications Building, Box 353740, Seattle, WA, 98195 or by email at pnhoward@uw.edu. The authors gratefully acknowledge support from the Project on Information Technology and Political Islam (www.pitpi.org), funded by the National Science Foundation under awards #IIS-0713074 and #IIS-1144286. 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.

The Center for Technology Innovation
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
http://www.brookings.edu/techinnovation

Editor
Christine Jacobs

Production & Layout
John S Seo

Tell us what you think of this *Issues in Technology Innovation*.

E-mail your comments to techinnovation@brookings.edu

Endnotes

[1] Philip N. Howard, *Digital Origins of Dictatorship and Democracy: The Internet and Political Islam* (Oxford University Press, 2010).

[2] Philip N. Howard, "Revolution in the Middle East Will be Digitized (Maybe Next Year)," *Miller-McCune* 2, no. 7 (2009).

[3] "'It Is Possible to Pull the Plug'," *Spiegel Online*, February 9, 2011, World, http://www.spiegel.de/international/world/0,1518,783662,00.html.

[4] Bruce Bimber, "Reconceptualizing Collective Action in the Contemporary Media Environment," *Communication Theory* 15(4) (November 1, 2005): 365-388; Brian Still, "Hacking for a Cause.," *First Monday* 10(9) (September 5, 2005).

[5] Jeroen De Kloet, "Digitisation and its Asian discontents: The Internet, Politics and Hacking in China and Indonesia.," *First Monday* 7(9) (September 2, 2002); Dara Byrne, "Public Discourse, Community Concerns, and Civic Engagement: Exploring Black Social Networking Traditions on BlackPlanet.com," *Journal of Computer- Mediated Communication* 13(1) (October 1, 2007): 319-340; Michelle Shumate, "Trouble in a Geographically Distributed Virtual Network Organization: Organizing Tensions in Continental Direct Action Network.," *Journal of Computer-Mediated Communication* 11(3) (April 2006): 802-824.

[6] Ronald J. Diebert and Rafal Rohozinsk, *Access Denied* (MIT Press, 2008); Ronald J. Deibert et al., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, 1st ed. (MIT Press, 2010).

[7] R, Kelly Garrett, "Protest in an Information Society: A Review of Literature on Social Movements and the New ICTs.," *Information, Communication & Society* 9(2) (April 2006): 202-224; Stephen Marmura, "A Net Advantage? The Internet, Grassroots Activism and American Middle-Eastern Policy," *New Media & Society* 10(2) (April 1, 2008): 247-271; W. McLaughlin, "The Use of the Internet for Political Action by Non-State Dissident Actors in the Middle East.," *First Monday* 8(11) (November 3, 2003).

[8] 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, Lexus Nexus, Attrition.org, GlobalVoices.org, among others.

A case is defined as an occasion where a government intervened in a digital network by breaking or turning off connections between national sub-networks and global information networks. Sometimes this meant blocking ports or access to a particular sub-network 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. Additionally, regimes may target individual actors in networks. But 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.

Since 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. 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 606 unique incidents involving 99 countries: 39 percent of the incidents occurred in democracies, 6 percent occurred in emerging democracies, 52 percent occurred in authoritarian regimes, and 3 percent 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. Finally, we developed a category for the impact of the interference.