Cyber Dimensions of State Repression

Meredith Blank
Political Science
University of Michigan

Anita Ravishankar
Public Policy & Political Science
University of Michigan

Amir Rahmati
Computer Science & Engineering
University of Michigan

Abstract

The Internet has long been considered a democratizing force, empowering citizens through unparalleled access to information. However, as citizens have adapted to and employed this new technology in protests against the state - in China, Syria, Egypt, and elsewhere - the state has fought back with their own effective strategies. Using cyber tools to carefully police online activity, halt protests, identify and arrest rebels, and block access to objectionable foreign websites, states have proven adept at advancing the technology of repression. This project will outline the dimensions of the cyber repression problem, offer context for cyber repression tactics in the broader realm of state repression, present examples of state-challenger cyber interactions, and conclude with a discussion of the relevant international human rights norms and initial policy solutions.

Recent state responses to popular challenges in Ukraine, China and Russia suggest the rise of a new tactic by the state - cyber repression. In the Ukraine, the government attempted to suppress popular protests by sending a threatening text message to individuals located within the protest vicinity [Hollister, 2014, Kramer, 2014][1]. After pro-Uigher demonstrations

[1]The text message read "Dear subscriber, you are registered as a participant in a mass disturbance." A detailed description of the event is available online at: `http://www.theverge.com/2014/1/21/5332726/ukraine-government-texts-ominous-orwellian-message-directly-to-cell`

in 2009, the Chinese government shut down the Internet in the Xinjiang province for ten months [MacKinnon, 2011]. Similarly, the Russian government has been accused of using youth organizations to run distributed denial-of-service attacks against oppositional newspapers [Carr, 2011]. Governments appear to be going online as a new way to control and coerce their populations.

Given the growth in government cyber activities, we explore what it means for state actors to engage in cyber repression. We also provide a framework of repression that incorporates digital coercion and intimidation. While cyber repression requires a better understanding of digitally-based capabilities, we argue that existing theories of state repression remain just as relevant as ever before – potentially more so as the cost of intimidation and coercion may be decreased.

1 Defining Cyber Repression

Traditional theories of state repression focus on government coercion or intimidation against their citizens [Davenport, 2007, Davenport and Armstrong, 2004, Poe and Tate, 1994]. Robert Goldstein [Goldstein, 1978] provides the most commonly used definition, describing it as:

> "The actual or threatened use of physical sanctions against an individual or organization, within the territorial jurisdiction of the state, for the purpose of imposing a cost on the target as well as deterring specific activities and/or beliefs perceived to be challenging to government personnel, practices or institutions" — Goldstein 1978, p. xxvii.

Goldstein's widely used characterization of state repression focuses on physical actions or threats of physical actions by the government. Repressive actions commonly include extrajudicial killings, political imprisonments and torture [Davenport, 2007]. In this regard, state repression literature to date is heavily framed within the realm of "physical integrity rights" or "the rights not to be tortured, extra-judicially killed, disappeared, or imprisoned for political beliefs" [Cingranelli and Richards, 2010]. Cyber-based coercion or intimidation, like in the case of the Ukraine or China, does not directly lead to physical harm of the target. A protest participant might receive a text or no longer have Internet access, but does not incur bodily harm

at the hands of the state or a state-sponsored actor. Yet, online actions like those conducted by the Ukraine or China are still for the purposes of "deterring specific activities and/or beliefs perceived to be challenging to the government" [Goldstein, 1978].

In this regard, cyber repression appears to achieve coercion and intimidation through limiting certain online behavior and imposing costs on the exercise of civil liberties.[2] For example, when the Chinese government decides to "turn off" the Internet for a specific region, it effectively imposes a number of costs on that population. More broadly, state Internet censorship restricts online association, assembly and speech. State-initiated cyber attacks or censorships can also undermine public trust in opposition groups [Carr, 2011]. Third, cyber repression may impose indirect or direct financial costs on its targets, particularly if it prevents the local population's engagement in economic exchanges. For example, the Xinjiang province reportedly experienced a drop in exports of 44% during its Internet shut down [The Economist, 2013]. Similarly, oppositional newspapers in Russia that suffered from DDOS attacks incurred the cost of downtime, the cost of recovery and mitigation in addition to overall loss in confidence [Carr, 2011]. While individual challengers to the state may remain physically unharmed, they incur meaningful costs because of their opposition.

As digital repression does appear to impose costs on targets (whether discriminately or indiscriminately), we suggest a slight refinement to the classical definition of repression. Rather than confining state repression to physical sanctions, we suggest also including the use of psychological sanctions or civil liberty-based restrictions against an individual or organization. Government digital restrictions and cyber attacks do not necessarily lead to physical harm. However, these actions are no less deleterious.

Similar to physical repression, cyber repression can consist of a variety of tactics such as online censorship or cyber attacks. China's Great Firewall and Russian's state-owned Internet pipelines provide clear examples of how governments can control online access and online content [Rid, 2013, MacKinnon, 2011]. Through limiting content online, the government may limit the spread of certain challenging ideologies or political perspectives. Governments in Thailand and China have both been revealed to manipulate

[2]From a human rights perspective, civil rights and liberties are defined as "the rights to free speech, freedom of association and assembly, freedom of domestic movement, freedom of international movement, freedom of religion, and freedom to participate in free and fair elections for the selection of government leaders" [Cingranelli and Richards, 2010]

online political discussions [MacKinnon, 2011, Sinpeng, 2013]. In addition, the government can attempt to intimidate opposition groups through conducting denial-of-service (DDOS) attacks against them, throttling their Internet connection or by simply removing their online access [Carr, 2011]. As the digital environment presents new opportunities for state challengers (or "hacktivists"), the state too can leverage cyber capabilities to achieve certain political and security-related goals.[3]

2 Citizen and State Use of Technology

Although cyberspace is considered a new frontier in the citizen vs. state conflict, many of the tactics used by both side in their traditional interaction also applies to cyberspace. The ever-increasing access to mobile communication and connection to the Internet and social networks in particular has made communication and coordination easier for the citizens but has also created new possibilities for states to monitor and potentially crackdown on their citizens. Besides tracking, various governments have tried to limit the use of these technologies by promoting propaganda, employing intimidation tactics, censorship, and other repressive tactics.

2.1 Citizen use of technology

The citizens primarily use cyberspace, and the basic level of anonymity it provides to its users, for communication. Communication in cyberspace can take different shapes, which are briefly discussed below. Each of these methods has their own benefits and shortcomings that make them appropriate for different situations.

- VOIP: Voice over IP services such as Skype [4] and Oovoo [5] provide secure audio and video communication between different users. These tools are especially used for citizens communication with people in the outside world.

- Instant Messaging: Very much similar to text messages in cell phones, instant messaging (IM) provides a quick and easy line of communication

[3] For a review of hacktivists, see [Wong and Brown, 2013]

[4] `http://www.skype.com`

[5] `http://oovoo.com`

for citizens in the cyberspace. Instant messaging can be used between multiple known individuals or unknown individuals with pseudonyms in chat rooms and IRC channels. The main benefit of instant messaging compared to VOIP services is its low bandwidth requirement, which makes communication possible even with minimum connectivity, and also the relatively higher anonymity it provides.

- Email: Email is the oldest form of communication in the cyberspace. It provides individuals with a secure channel of communication. Email is especially desirable for sharing thoughts and ideas in an environment were regular channels of communication of individuals are monitored by the state.

- Blog: A blog is website typically used for information publishing or discussion. Each blog consists of a series of posts. Blog posts are written either by an individual or a group of authors and provide citizens the ability to share their viewpoints and writings with one another.

- Microblog: Microblogging is a service which allows users to create quick and short miniposts (typically known as tweets). Similar to correlation between IM and Email, Microblogging creates a faster and more interactive channel of communication for an individual compared to traditional blogs. Twitter is the most well known of these services.

- Video sharing: Video sharing services provide citizens with the opportunity to post videos online. These videos can either show events from the viewpoint of independent citizens, or provide individuals to broadcast their ideas to a wide audience. Youtube [6] and Vimeo [7] are the two of the better-known websites in this space.

The rise of blogging, microblogging, and video streaming have created a phenomenon known as "Citizen Journalism" [Deutsch Karlekar and Radsch, 2012] in which individuals take up the task of reporting news and events in situations where traditional news media do not have access because of state limitations. Besides using cyberspace for communication, citizens use cyberspace to access uncensored reporting and viewpoints that are otherwise suppressed by the state. Furthermore, citizens have grown to use various anonymity

[6] `http://www.youtube.com`
[7] `http://www.vimeo.com`

and censorship circumvention tools such as TOR [8] to escape state spying and limitations.

2.2 State use of technology

In reaction to citizen use of cyber technologies, states have also moved to monitor and control cyberspace. State control over communication infrastructure enables it to track citizen activity on the web to a great extent. In cooperation with domestic internet service providers, the states can track communications and pages visited by individual users. States have also tried to infiltrate secure communications between citizens by initiating man-in-the-middle attacks, as in the case of Diginotar in Iran [Prins, 2011].

In addition to monitoring and tracking, states also respond to and interfere with citizen activity in cyberspace in a variety of ways:

Internet Censorship Censorship is the primary tool used by states to slow down the dissipation of information and communication between citizens. It is estimated that over 500 million Internet users reside in countries that engage in the systematic filtering of online content. [OpenNet Initiative, 2012]. Censorship can take the from of blocking websites not aligned with states ideology, or blocking services such as Skype. In Iran, "The Committee for Determining Offensive Contents" plays this role, while in China the State Council Information Office and the Chinese Communist Party?s Propaganda Department? take on these efforts. For more in-depth analysis of censorship technologies in these countries, we direct the reader to [Simurgh Aryan, 2013]

Falsification of information One of the shortcomings of citizen journalism is the difficulty for third parties to independently verify the details. In such an atmosphere, the state has the ability to falsify the information by either distributing propaganda through official news sources or relying on government supporters to disseminate news that support the state's view.

Intimidation Just like outside of the cyber domain, intimidation is one of the key ways state can put pressure on its opposition. This can be done officially by passing laws against anti-government propaganda on the web and

[8] `https://www.torproject.org`

prosecuting dissidents, or unofficially by threatening activists and dissidents against taking actions.

Retaliation Where intimidation does not deter activists, the state may take various retaliatory actions, ranging from prosecution and imprisonment to assassination. These actions are usually directed by a branch of security force dedicated to Cyber crimes among which China Internet Police and Iran Cyber Police are the most notorious. In Nov 2012 Iran Cyber police allegedly tortured and killed a blogger they had in custody [Dehghan, 2012].
Though international norms against traditional state repression tactics (e.g., violation of physical integrity rights) are fairly well established, there is no clear consensus regarding the sort of cyber repression tactics discussed above. The following section attempts to map existing international norms and laws to the cyber dimension.

3 International Human Rights Norms and Laws

In the context of the existing international human rights framework, cyber repression primarily concerns violations of the rights to privacy and freedom of opinion and expression. These rights are enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention on the Rights of the Child, and the International Convention on the Protection of All Migrant Workers and Members of Their Families [Human Rights Council, 2013]. A number of regional charters also enumerate these rights [Human Rights Council, 2013]. Although they are broadly acknowledged, how exactly these rights translate to the cyber sphere remains unclear. A recent report by the Human Rights Council of the United Nations General Assembly characterizes the problem as follows:

> Despite the widespread recognition of the obligation to protect privacy, the specific content of this right was not fully developed by international human rights protection mechanisms at the time of its inclusion in the above-mentioned human rights instruments. The lack of explicit articulation of the content of this right has contributed to difficulties in its application and enforcement [UNESCO, 2012]. As the right to privacy is a qualified right, its interpretation raises challenges with respect to what

> constitutes the private sphere and in establishing notions of what constitutes public interest. The rapid and monumental changes to communications and information technologies experienced in recent decades have also irreversibly affected our understandings of the boundaries between private and public spheres.

The absence of specific guidelines delineating what rights citizens have online leaves states extensive room to pursue essentially whatever practices best suit their interests. Resolving this issue requires developing and institutionalizing updated norms of privacy and expression that reflect the contemporary cyber capabilities of both citizens and the state. The Haifa Center of Law and Technology offers the following definition of the right to privacy:

> The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner, and timing of the use of those parts we choose to disclose [Onn, 2005].

This right encapsulates both access and control of information, and is an enabling condition for the exercise of freedom of expression and opinion, which Amnesty International defines as the "right to seek, receive, and impart information and ideas without fear or interference." [Amnesty Int., 2014]

As discussed in the previous section, there has been no shortage of state-challenger interactions in which the rights to privacy, expression, and opinion have been violated. Though it may be unsurprising that many of these abuses take place in those states with past records of human rights violations, recent revelations of state surveillance activities within the United States suggest that even states with highly embedded democratic ideals and civil liberties provisions are also willing to engage in activities that violate these rights as defined above. Further, where traditional repressive tactics may be more overt and attributable, cyber repression activities offer governments the added incentive of plausible deniability. Given the difficulties of monitoring and enforcement in the cyber realm, developing effective policy prescriptions for responding to and preventing cyber repression presents a tremendous challenge. In addition, as much of the relevant infrastructure is owned and operated by the private sector, initiatives that do not partner with these

entities can achieve limited success at best. Preliminary efforts to address this problem are briefly discussed below.

4 Targeting the Technology

Given the difficulties associated with attribution, responses to cyber repression that target the technology may be an effective alternative to directly sanctioning states that engage in these activities. After all, cyber repression is enabled by cyber technologies, much of which is developed by private entities. Several recent reports document the use of surveillance technology "produced by Western companies" to identify, detain, and torture protestors in Iran, Syria, Bahrain, and Tunisia [National Public Radio, 2011]. One current proposal comes from the 41-country Wassenaar Arrangement, the "key international instrument that imposes controls on the export of conventional arms and dual-use goods and technologies." This group recently initiated efforts to impose export controls on these technologies [Page, 2013]. Though this is far from a comprehensive solution to the cyber repression problems set forth in this report, it marks an important initial step in the process to define and curtail these widespread and insidious abuses.

5 Conclusion

This report endeavored to outline the dimensions of the cyber repression problem, offering context for cyber repression tactics in the broader realm of state repression, presenting examples of state-challenger cyber interactions, and concluding with a discussion of the relevant international human rights norms and possible policy solutions. Though many challenges remain, this preliminary report offers a starting point for further research on cyber repression.

References

[Amnesty Int., 2014] Amnesty Int. (2014). Freedom of expression.

[Carr, 2011] Carr, J. (2011). Inside cyber warfare: Mapping the cyber underworld.

[Cingranelli and Richards, 2010] Cingranelli, D. and Richards, D. (2010). Human rights quarterly.

[Davenport, 2007] Davenport, C. (2007). State repression and political order.

[Davenport and Armstrong, 2004] Davenport, C. and Armstrong, D. (2004). Democracy and the violation of human rights: A statistical analysis from 1976 to 1996.

[Dehghan, 2012] Dehghan, S. K. (2012). Iran accused of torturing blogger to death.

[Deutsch Karlekar and Radsch, 2012] Deutsch Karlekar, K. and Radsch, C. C. (2012). Adapting concepts of media freedom to a changing media environment: Incorporating new media and citizen journalism into the freedom of the press index.

[Goldstein, 1978] Goldstein, R. J. (1978). Political repression in modern america: from 1870 to the present.

[Hollister, 2014] Hollister, S. (2014). Ukrainian government texts ominous orwellian message directly to cell phones of protestors.

[Human Rights Council, 2013] Human Rights Council (2013). Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression.

[Kramer, 2014] Kramer, A. E. (2014). Ukraine's opposition says government stirs violence.

[MacKinnon, 2011] MacKinnon, R. (2011). China's networked authoritarianism.

[National Public Radio, 2011] National Public Radio (2011). The technology helping repressive regimes spy.

[Onn, 2005] Onn, Y. (2005). Privacy in the digital environment.

[OpenNet Initiative, 2012] OpenNet Initiative (2012). Global internet filtering in 2012 at a glance.

[Page, 2013] Page, K. (2013). International body moving to restrict export of surveillance systems used to commit human rights abuses.

[Poe and Tate, 1994] Poe, S. and Tate, N. (1994). Repression of personal integrity rights in the 1980s: A global analysis.

[Prins, 2011] Prins, J. R. (2011). Diginotar certificate authority breach operation black tulip.

[Rid, 2013] Rid, T. (2013). Cyberware and peace: Hacking can reduce real-world violence.

[Simurgh Aryan, 2013] Simurgh Aryan, Homa Aryan, J. A. H. (2013). Internet censorship in iran: A first look.

[Sinpeng, 2013] Sinpeng, A. (2013). State repression in cyberspace: The case of thailand.

[The Economist, 2013] The Economist (2013). Turning off the entire internet is a nuclear option best not exercised.

[UNESCO, 2012] UNESCO (2012). Global survey on internet privacy and freedom of expression.

[Wong and Brown, 2013] Wong, W. H. and Brown, P. A. (2013). E-bandits in global activism: Wikileaks, anonymous, and the politics of no one.