COLUMBIA UNIVERSITY
JOURNAL OF POLITICS & SOCIETY

Web Feature: Tuesday, April 15, 2014
Editor: Robert Baldwin, Editor in Chief
Author: Yunjing Li, Emory University

Political Monitoring in Cyberspace

As digital communication technologies rapidly develop, many types of Internet control mechanisms have been institutionalized to monitor and regulate the cyberspace. Digital activism has been influenced by a multitude of economic, social, and political elements. The political element is particularly important in the case of social activism (Joyce, 2010). While social activists are quickly learning to leverage various online platforms to organize activities, governments from around the world are also upgrading their monitoring tools to increase surveillance, passing new laws to restrict online content, and even arresting social media users. Since governments frequently collect communication data on their citizens, it is important to examine the effect of governments' digital surveillance on changes in social activists' online behaviors. The theory and hypotheses of this paper are developed based on different countries' Internet freedom measures and digital social activism records.

Digital media and online social networking applications have changed the way that dissent is organized (Bimber, 2005; Howard, 2010; Still, 2005). Activists are using the Internet to raise awareness, coordinate campaigns, and manage their community. As social media has become an inexpensive and fast coordinating tool for nearly all social activism, governments are trying to monitor and prevent activities that can threaten their regime. In June 2013, a former NSA contractor, Edward Snowden, revealed evidence of the U.S. government's secret surveillance program and received international media attention. The PRISM program collects stored Internet communications generated by companies such as Google Inc. According to Google's official blog for its transparency report, government requests for user information double over three years. Astoundingly, the top five countries

requesting user information from Google are all democratic governments. Although this leak caused outrage amongst the public, it is unlikely to reduce the monitoring level of the U.S. government.

Previous studies have explored the purposes of digital monitoring. One study indicated that both democratic and authoritarian regimes monitor their network for two main reasons: protecting political authority and preserving the public good (Howard & Agarwal & Hussain, 2011). Governments provide several explanations for requesting social media information: protect political leaders, state institutions, election processes, eliminate propaganda, and mitigate dissidence and national security. Throughout the literature base, national security was the most commonly cited reason for surveillance (P. N. Howard et al. 2010).

The second reason, preserving the public good, is a more challenging issue. The cyberspace is a "flowing" public good that cannot be easily tracked or defined. Symantec Corporation's 2013 Internet Security Threat Report shows that the United States is ranked first in the number of Internet attacks (22.7%), followed by China (11.0%), India (6.5%), Brazil (4.0%), and Germany (3.4%). Although the United States is perceived as the country with the highest level of security technology, it is also the number one target for cybercriminals. Steven Salbu argues that a standardized monitoring system must be developed in order to monitor access to the Internet. However, Salbu's research does not discuss monitoring of Internet content, which is a more difficult issue than the monitoring of Internet access. Joss Hands created the idea of "quasi-autonomous recognition network," which captures the practices of micro-coordination and the role of communicative action in the context of the fluidity and dynamics of cooperative activism

(Hands, 2011). Because Internet use spans the globe, cyberspace monitoring needs to be addressed in an international context. In spite of this, current laws regarding regulation of Internet usage are still determined by individual nations.

GOVERNMENTAL MONITORING IN CYBERSPACE

The primary aim of this paper is to learn about the ability of government monitoring to change digital activists' behaviors and hinder movement outcomes. My theory proposes that the government can use digital monitoring tools to influence the outcome of digital activism within the country. The presence of digital monitoring can change activists' behaviors because it can expose their agenda. The word "digital activism" encompasses all social and political campaigning practices that use digital network infrastructure. However, my theory mainly focuses on political practices. The most important question in understanding digital activism is whether governmental monitoring makes people's attempts at social activism any different than before the age of the Internet. For example, if a million people are following a campaign's Twitter account, what effect will government monitoring have on this account? Does governmental monitoring encourage/depress the correct people to hear and react to the digital message?

According to Sandor Vegh (2003), the types of Internet activism fall into three general areas: awareness/advocacy, organization/mobilization, and action/reaction. In order to assess the changes in activism, this paper will measure the outcomes of digital activism. The outcome measurement includes not only the successfulness of a case, but also the likelihood of mobilized offline action triggered by digital activism.

Offline participation must be included to measure the success of activism. Anastasia Kavada suggests that greater ease and speed of online communication does not

necessarily lead to durable and stable activist networks (Kavada, 2010). In order to make activist networks last, regular organization of face-to-face meetings, maintenance of stable online spaces, and cooperation around well-defined projects are necessary (Kavada, 2010). Hence, it is necessarily to promote offline interactions for an activist group to succeed. In addition to sustaining a network, activists often combine online tools with physical meetings for decisions that require lengthy discussion or negotiation among numerous participants (Kavada, 2010).

In the *2009 Digital Activism Survey Report*, Brodock, Joyce, and Zaeck identified the survey respondents who were involved in offline mobilization (2009). They report that older activists in the respondent group are most likely to use digital technology to increase the efficiency of offline activities, such as training and evidence collection, and are less likely to utilize online tools such as posting original content on web sites (Brodock, Joyce, and Zaeck, 2009).

Activism is a collective action taken by a civic group. Despite the increasing usage of online communication tools, Michael Ayers' study on collective identity in online and offline feminist activists shows that forming a collective identity in cyberspace can be difficult because of the distance between group members (2003). A strong collective identity can help a social movement maintain itself and build strength over time. Based on this theory, we can explore whether governmental monitoring in cyberspace can prevent activist groups from building a collective identity. If a country with strict digital control can discourage offline mobilization, we will conclude that this monitoring mechanism constrains activists' ability to build a strong collective identity, which would ultimately hurt the final success of activism.

HYPOTHESES

A higher level of governmental monitoring technology enables a regime to control activism on the Internet. Monitoring is a precondition for the government to gain greater Internet control. Social activism can disturb the political environment and lead to instability. In this paper, I assume that governments want to pursue a stable political environment in the nation, so they want to watch activism movement as closely as possible, especially if the activist movement stands against the regime in power.

To determine the degree of government monitoring in the digital space, it is important for us to associate government monitoring with any changes in activism. The most direct way to determine the success of a social movement is to look at its outcomes. There are two types of metrics used in digital activism: tactical and strategic. Tactical metrics refer to the number of individuals who have taken some action related to a specific campaign, while strategic metrics refer to actually contributing a win or a loss (Karpf, 2010, 153).

Hypothesis One: The greater the governmental monitoring on the Internet, the higher the participation rate in offline mobilization.

Offline mobilization is a tactical outcome of digital activism. If an initiator cannot carry out actions online, the only alternative to its activity is to mobilize offline. Those who are likely to engage in online social movements are already active supporters; those who need to be persuaded are often not even using the medium or are not following the issues. Therefore, offline mobilization is a useful measurement to examine digital activists' behavior. These offline actions include protest, demonstrations, marches, riots, flash mobs, one-person protest, occupations, land seizure, sit-ins, walk-outs, public

meetings and speeches, withholding of fees, lobby, teach-ins, and boycotts that are carried out offline. Based on the available data, we can see that across different countries, there are clear variations in the ratios of activisms' offline mobilization across different countries.

Hypothesis Two: The final outcome of a digital action, whether all demands are achieved, is negatively associated with the level of Internet control.

To take this study further, it is important to judge all forms of activism at the strategic level. After we find out whether governmental monitoring changes activists' mobilization behavior, we want to know the effect of monitoring on digital activism's success. While the availability of digital engagement platforms leads to a wide variety of communication techniques, it does not guarantee the success of a social movement. We must explore the relationship between government monitoring and the success rate of a digital activism. It is rational to assume that in order to sustain social movements, most people are trying to avoid the risks of explicitly opposing the regime. Most people use online tools to hide their identities from authority. One of the biggest benefits of digital communication is that governments cannot easily identify a participant's identity. If a government has a stricter monitoring mechanism, it increases the risks of identity exposure, which can hinder the success of a movement. Stricter government monitoring can also increase the probability of dissidents being caught and banned from the Internet, which can lead to a lower success rate. Internet monitoring enables governments to interfere and discontinue social activists' agendas.

THE DATA

An ideal research design for the study of the effect of Internet monitoring on digital activism would classify digital social activism on a case-by-case basis, would analyze the specific monitoring mechanisms in every activism case, and would consider the monitoring cost and outcome of each case. Google's Transparency Report about governments' access to its own search engine has shed light on how laws and policies affect the flow of information online from around the world (2013). This report directly provides information on how closely governments watch Internet users. Nevertheless, the dearth of detailed records of governmental action on each case makes direct observation on the effect of monitoring difficult.

Because it is nearly impossible to figure out the difference of governmental monitoring among individual cases of Internet activism, it is instead desirable to investigate the variance of governmental monitoring among countries. Governments use different monitoring mechanisms on the Internet, so it is relatively easier to observe the level of each state's Internet control. To do this, this paper will include one of Freedom House's datasets, which collects information on countries' laws and practices relevant to the Internet, accessibility of activism websites, and the government's reaction in individual cases. Matching each country's governmental control and its activism success rate may help assess the impact of government monitoring on social activism.

A digital activism campaign is defined as an organized public effort making collective claims of target authority in which civic initiators or supporters use digital media (Joyce, 2010). The term "activism" used in this paper includes campaigns that are directly against prevailing authority, private groups like business corporations, and

individual targets. The digital actions classified in this study meet the following requirements:

1) Digital involvement
2) Organized public effort
3) Collective goals made on behalf of a group of citizens
4) Claims (goal must propose a solution to the injustice so that the success of failure of the campaign may be evaluated)
5) Target (the people seeks to influence an entity of authority perceived as having the ability to implement the goal.)
6) Civic group

The data analyzed in this paper come from two datasets: "Freedom on the Net" report and "The Global Digital Activism Data Set". While "Freedom on the Net" offers Internet freedom scores of countries across the globe, "The Global Digital Activism Data Set" features coded cases of online digital activism from 151 countries. The two datasets were merged using "country" as their common variable.

The rate of offline mobilization and final outcome are dependent variables in this paper, and come from "The Global Digital Activism Data Set". The unit of observation is the digital activism case study. To be selected, the case studies were required to exhibit either at least one digital tactic or an instance of online discourse aimed at achieving social or political change, and needed to be recorded by a reliable third party source. All the digital activism must be initiated by a traditional civil society organization. The data were aggregated by a team of volunteers who searched websites for information on global digital activism. Researchers also collected data from peer reviewed journal articles that included digital activism case studies. The entire data set includes 1180 coded cases of digital activism from 151 countries and dependent territories, from 1982 through 2012.

For the purpose of this paper, there are 256 available activism cases from 46 countries that correspond to 2009, 2011, and 2012. In order to provide a clear picture of

the geography of these cases, the researchers only identified cases' primary countries. The offline mobilization rate was calculated based on the percentage of offline participation cases in each country. The dataset includes a variable called "participants in offline mobilization" that indicates the number of participants in the campaign's offline mobilization, defined as one or more initiators or supporters occupying a physical space. I coded all results with participant number greater than 0 as cases with offline mobilization. The dataset also provides a categorical variable describing the type of campaign outcomes including "all demands achieve," "goal partially achieved," and "campaign has had no effect". For the accuracy of outcome, I only considered campaigns that achieve all their demands as successful. The campaign success rate was calculated based on the percentage of successful cases in the total cases of a country.

My independent variable measures the degree of government online surveillance. In order to illustrate trends and opportunities for Internet freedom, Freedom House has developed a comprehensive and comparative set of indicators for monitoring and analyzing internet freedom. "Freedom on the Net" reports Internet freedom scores for 15 countries in 2009, 37 countries in 2011, 47 countries in 2012, and 60 countries in 2013 (2010 report is not available). This methodology applies basic standards of free expression that "everybody has the right to hold opinions without interference and to see, receive, and impart information and ideas through any media regardless of frontiers" to all countries irrespective of geographical location, ethnic or religious composition, or level of economic development. The final freedom score of a country consists of three components: obstacles to access, limits on content, and violations of user rights. The "obstacles to access" variable, which ranges from 0-25 points, measures infrastructural and economic barriers to

access, legal and ownership control over Internet service providers, and independence of regularity bodies. The "limits on content" variable, which ranges from 0-35 points, measures the degree of legal regulations on content, blocking of websites, self-censorship, vibrancy of online new media, and use of information communication technologies for civic mobilization. The "violations of user rights" variable measures surveillance, privacy, and repercussions like imprisonment. The last variable ranges from 0-40 points, and is weighted the most in the evaluation of Internet control. A total score (0-100 points) of all three measurements will be the final freedom score. A country with a high Internet freedom score has more obstacles to access, limits on Internet content, and violations of user rights. A country with a low freedom score has imposed less Internet control, which means it has a lower monitoring level in the cyberspace.

We should be cautious when using the freedom score. Monitoring technologies like filtering are prone to being either too sensitive or not sensitive enough. Current technology is not able to accurately identify and target specific categories of content on the Internet. Underblocking leads to the failure of filtering to block access to all the content targeted for censorship. On the other hand, filtering technologies often block content they do not intend to block (OpenNet 2013). The final freedom score does not precisely reveal each country's intention.

INITIAL ASSESSMENT OF INTERNET INTERVENTION

I conducted an initial assessment of how different levels of governmental Internet control affect the rate of offline mobilization and rate of successful campaign among countries. To directly compare total freedom scores to campaign outcomes, I first divided countries into three Internet freedom statuses: free (0-30 Points), partially free (31-60

points), and not free (61-100 points). The average number of cases studies for a "free" country is 5.0, versus 1.9 case studies for a "partially free" country and 2.4 case studies for a "not free" country. There are more available cases for countries with a lower governmental Internet control. This can be caused by two reasons: more information is available in a more open digital environment and more cases of social activism occur in these countries. Table 1 presents the average offline mobilization rates and average success rates corresponding to country statuses. When compared across statuses, average offline mobilization rates do not reveal a clear pattern. Although countries with "not free" status have a higher average offline mobilization rate, "free" and "partially free" countries do not show substantial differences in this outcome category. This is not sufficient to support my hypothesis that countries with higher Internet control encourage people to participate offline mobilization. Average success rates across the three status groups do not show a clear pattern either. While "free" countries and "not free" countries on average have the same success rate of 31.2%, "partially free" countries have a slightly lower average success rate of 30.9%. Therefore, neither offline mobilization nor success rate are proportional to the range of freedom score assigned to each status. These findings are not consistent with my second hypothesis that tighter Internet control hinders activism's success rate in a country.

However, the first assessment is only based on the total freedom score for each country. Deeper analysis is necessary to learn about the influence of the three components in the total freedom score. Table 2 presents a breakdown of the average Internet freedom score for each status. The values of obstacles to access, limits on content, and violations of

user rights follow the direction of expectations, and freer countries tend to have a lower Internet freedom score.

In order to evaluate the influence of each component on the rate of offline mobilization and success rate, I ran two regression models to figure out whether there is a linear relationship between governmental control and campaign outcome. The three components are the independent variables in my regression models. By putting all of them into the same model, I was able to hold them constant while testing the relative impact of other components. Table 3 presents the correlation coefficient and significant level of each freedom score component in the regression model for the rate of offline mobilization. The results show that the components neither follow the direction of expectation nor are statistically significant. Based on the overall summary of fit, the r-square result for this model is only 0.001. Hence, the relationship between the three measures of government control and offline mobilization is not significant. Table 4 presents the regression results for the rate of successful outcome with the three components as independent variables. Again, the results show that none of the components neither follow the direction of expectation nor are statistically significant. The r-square result for this model is 0.052, which indicates no significant relationship between these three government control variables and rate of successful outcome.

Despite the different measures of online activism outcome, my initial results are not consistent with theoretical expectations concerning the relationship between the level of governmental monitoring and online activism outcome. I have looked into the three dimensions of government monitoring in a vacuum. I did not consider the increasing blurring between offline and online life, since people are now increasing using the web to

organize offline protest as well. Up to this point, my analysis has only looked at monitoring in individual countries. What are other possible explanations are there for the success rate of digital activism? There are social, cultural, and institutional factors influencing the outcome of online activism in countries. Although I do not have data on each country's social and cultural context, I can find out each country's regime type and use this information as an additional control variable.

OTHER INSITUTIONAL FACTORS

In addition to the freedom score variables in previous regression models, I added regime type as a control variable to my study. I classified countries into four groups: authoritarian, transitional government, emerging democracy, and democracy. A transitional government is a government temporarily set up to prepare the way for a permanent government. An emerging democracy refers to the rise of political structures without central planning, but organized by many individual participants. Table 5 shows that regime type has a significant impact on the outcome of digital activism. The results for regime type show a strong pattern in activism outcome (see table 6), but the results for the freedom score still do not follow a pattern. Table 6 and 7 show that countries with a higher level of democracy tend to have less government control on the Internet.

Despite the strict digital control by their governments, countries with a transitional government have the highest average rate of offline mobilization and the highest average rate of success rate. The nature of the political environment in these countries probably encourages governments to change in order to meet demands of activism. Ian Angus stresses the increasing importance of what he calls "emerging publics," which are generated out of social movements (Angus, 2001, 55). He claims that "it is with the social

movements of our time that the future of democracy rests," in that these movements create new publics that challenge existing power structures, and "this public questioning of relations of power is emergent in so far as it proposes to change the society as a whole" (Angus, 73). When a government is in transition, it is more prone to becoming a target of activism. Because the government's power lacks the stability of other regime types, its public can have stronger power to push for changes.

CONCLUSION

This paper studies the different measures of governmental monitoring and outcomes of social activism. Readers should recognize that although the cases in this study do provide some insight into how activism occurs, they collectively reveal only a partial range of possibilities. Context is very important to understand digital activism. Due to the limits of available data, this paper only touches the surface of governmental monitoring. More direct measures of government monitoring should be considered to better evaluate changes in activists' behaviors.

Although I do not find that government monitoring has an effect on the outcome of digital activism, I conclude that regime type matters more in determining the success of activism. In an environment where political leaders and state institutions understand both the power of digital activism and the opportunity it presents for doing tasks differently, digital activists will likely be able to play a significant role (Glaisyer, 2010). Digital activists are especially important in a country with a government in transition. Under an authoritarian regime where open dissent is unwelcome, digital activism will almost certainly be repressed. The contest between the surveillance and counter surveillance

technologies will continue as long as governmental monitoring exists and impacts people's Internet usage.

Future research can also examine digital monitoring by other actors. If we specify the actors in this paper, the results might be different. In addition to political activism, non-political activism cases also have a lot of potential for future studies. As more organizers emerge from outside the social movement tradition, we will see trends that are distinct from protests in the past; specifically, private collective actions will become more frequent (Earl & Kimport, 2011). After the PRISM incident, many Internet companies are trying to strengthen their commitment to the open exchange of information. Similar to Google, Twitter has also published a report that highlights trends in government requests for account information, content removal, and copyright notices. How does this monitoring information change the way people use the Internet? Today, the web is a highly centralized, commercial, winner-takes-all environment (Scholz, 2010). Current literature on cyberspace monitoring places considerable emphasis on governments' interaction with social activists. The interactions between governments and commercial actors are waiting to be explored.

APPENDIX

Table 1
Outcomes of Internet Freedom Status

Country Status	Number of Countries	Outcome Type: Average Offline Mobilization Rate	Outcome Type: Average Success Rate
Free (0-30)	25	53.4%	31.2%
Partially Free (31-60)	41	52.0%	30.9%
Not Free (61-100)	21	62.4%	31.2%

Table 2
A Breakdown of Internet Freedom Score

Country Status	Freedom Score Component: Average Score of Obstacles to Access	Freedom Score Component: Average Score of Limits on Content	Freedom Score Component: Average Score of Violations of User Rights
Free	5.3	6.9	11.1
Partially Free	11.6	12.4	19.8
Not Free	18.5	25.9	32.5

Table 3
Regression Results for the Rate of Offline Mobilization

Independent Variables	Correlation Coefficient	Standard Error	Prob>|t|
Intercept	0.588	0.109	<.0001
Obstacles to Access	0.002	0.012	0.866
Limits on Content	-0.001	0.011	0.973
Violation of User Rights	-0.002	0.001	0.868
		R-Square	0.001
		Observations	87

Table 4
Regression Results for the Rate of Successful Outcome

Independent Variables	Correlation Coefficient	Standard Error	Prob>|t|
Intercept	0.257	0.099	<.011
Obstacles to Access	0.017	0.010	0.105
Limits on Content	-0.018	0.010	0.073
Violation of User Rights	0.005	0.009	0.543
		R-Square	0.052
		Observations	87

Table 5
Fit Model with Regime type and Freedom Score

Independent Variables	Correlation Coefficient	Standard Error	Prob>|t|
Impact on Offline Participation			
Intercept	0.588	0.168	<.001
Total Freedom Score	0.001	0.003	0.903
Authoritarian	-0.119	0.099	0.232
Democracy	-0.067	0.096	0.487
Emerging Democracy	0.082	0.080	0.3106
		R-Square	0.0470
		Observations	87
Impact on Outcome Success			
Intercept	0.445	0.151	<.005
Total Freedom Score	-0.00159	0.0029	0.591
Authoritarian	-0.033	0.089	0.718
Democracy	-0.092	0.087	0.294
Emerging Democracy	-0.161	0.072	0.029*
		R-Square	0.09
		Observations	87

Note: * indicates significant result.

Table 6
Outcomes Based on Regime Type

Regime Type	Number of Countries	Average Freedom Score	Outcome Type: Average Offline Mobilization Rate	Outcome Type: Average Success Rate
Authoritarian	24	69.4	49.6%	30.2%
Transition	7	54.9	**71.4%**	**64.3%**
Emerging Democracy	20	45.1	68.8%	21.3%
Democracy	36	28.4	53.3%	30.8%

Note: Bold Entries represent cases in which the value is the biggest in the category.

Table 7
A Breakdown of Internet Freedom Score based on Regime Types

Regime Type	Average Score of Obstacles to Access	Average Score of Limits on Content	Average Score of Violations of User Rights
Authoritarian	17.3	22.6	29.5
Transition	15.1	13.6	26.1
Emerging Democracy	11.5	13.7	19.9
Democracy	6.9	8.7	13.3

REFERENCES

Angus, Ian. 2001. *Emergent Publics*. Winnipeg: Arbeiter Ring.

Ayers, Michael. 2003. "Comparing Collective Identity in Online and Offline Feminist Activists." McCaughey, Martha & Ayer Michael, ed. *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge, 145-164.

Bimber, Bimber. 2005. "Reconceptualizing Collective Action in the Contemporary Media Environment." *Communication Theory* 15:4, 365-388.

Brodock, Katharine, Mary Joyce, and Timo Zaeck. 2009. *Digital Activism Survey Report 2009*. July. http://creativecommons.org/licenses/by-nc-sa/3.0/us. (November 2, 2013)

Glaisyer, Tom. 2010. "Political Factors: Digital Activism in Closed and Open Societies." Joyce Mary, ed. *Digital Activism Decoded: the New Mechanics of Change*. New York: International Debate Education Association, 85-98.

Google. 2013. "Official Blog: Government Requests for User Information Double Over Three Years." http://googleblog.blogspot.com/2013/11/government-requests-for-user.html (December 07, 2013)

Hands, Joss. 2011. *@ is for Activism: Dissent, Resistance and Rebellion in a Digital Culture.* New York: Pluto Press.

Howard, Philip N. 2011. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. New York: Oxford UP.

Joyce, Mary, & Philip Howard. 2013. *Global Digital Activism Data Set Version 2.0.* August 20. Seattle: University of Washington. http://digital-activism.org/download/1191/ (November 1, 2013).

Joyce, Mary, ed. 2010. *Digital Activism Decoded: The New Mechanics of Change*. New York: International Debate Education Association.

Karpf, Dave. 2010. "Measuring the Success of Digital Campaigns." Joyce Mary, ed. *Digital Activism Decoded: the New Mechanics of Change*. New York: International Debate Education Association, 150-161.

Kavada, Anastasia. 2010. "Activism Transforms Digital." Joyce Mary, ed. *Digital Activism Decoded: the New Mechanics of Change*. New York: International Debate Education Association, 100-118.

Kelly, Sanja, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, and Ashley Greco-Stoner. 2013. *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media*. October. http://www.freedomhouse.org/report-types/freedom-net (November 1, 2013).

McCaughey, Martha, & Michael D. Ayers. 2003. *Cyberactivism: Online Activism in Theory and Practice*. New York: Routledge.

OpenNet Initiative. 2013. "About Filtering." https://opennet.net/about-filtering (December 01, 2013)

Philip N. Howard , Sheetal D. Agarwal & Muzammil M. Hussain. 2011. "When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media." The Communication Review 14:3, 216-232. (November 19, 2013)

Salbu, Steven. 1998. "Who Should Govern the Internet? Monitoring and Supporting a New Frontier." *Harvard Journal of Law & Technology* 11:2, 429-480.

Scholz, Trebor. 2010. "Infrastructure: Its Transformations and Effect on Digital Activism." Joyce Mary, ed. *Digital Activism Decoded: the New Mechanics of Change*. New York: International Debate Education Association, 17-31.

Still, Brian. 2005. "Hacking for a Cause." First Monday, September 5. http://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/1274/1194 (November 15, 2013)

Symantec. 2013. Internet Security Threat Report 18 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (December 13, 2013)

Vegh, Sandor. 2003. "Cyberactivism: Classifying Forms of Online Activism: the Case of Cyberprotests against the World Bank." McCaughey, Martha & Ayer Michael, ed. *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge, 71-98.