



# NATIONAL DEFENSE RESEARCH INSTITUTE

CHILDREN AND FAMILIES  
EDUCATION AND THE ARTS  
ENERGY AND ENVIRONMENT  
HEALTH AND HEALTH CARE  
INFRASTRUCTURE AND  
TRANSPORTATION  
INTERNATIONAL AFFAIRS  
LAW AND BUSINESS  
NATIONAL SECURITY  
POPULATION AND AGING  
PUBLIC SAFETY  
SCIENCE AND TECHNOLOGY  
TERRORISM AND  
HOMELAND SECURITY

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

This electronic document was made available from [www.rand.org](http://www.rand.org) as a public service of the RAND Corporation.

Skip all front matter: [Jump to Page 1](#) ▼

## Support RAND

[Purchase this document](#)

[Browse Reports & Bookstore](#)

[Make a charitable contribution](#)

## For More Information

Visit RAND at [www.rand.org](http://www.rand.org)

Explore the [RAND National Defense  
Research Institute](#)

View [document details](#)

## Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND electronic documents to a non-RAND website is prohibited. RAND electronic documents are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.



# Internet Freedom



# Political Space



Olesya Tkacheva, Lowell H. Schwartz,  
Martin C. Libicki, Julie E. Taylor,  
Jeffrey Martini, Caroline Baxter



NATIONAL DEFENSE RESEARCH INSTITUTE

**Internet  
Freedom**



**Political  
Space**

Olesya Tkacheva, Lowell H. Schwartz,  
Martin C. Libicki, Julie E. Taylor,  
Jeffrey Martini, Caroline Baxter

Prepared for the U.S. Department of State

The research described in this report was prepared for the U.S. Department of State. The research was conducted within the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

#### Library of Congress Cataloging-in-Publication Data

Tkacheva, Olesya.

Internet freedom and political space / Olesya Tkacheva, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, Caroline Baxter.

pages cm

Includes bibliographical references.

ISBN 978-0-8330-8063-9 (pbk. : alk. paper)

1. Internet—Social aspects. 2. Internet—Political aspects. 3. Internet—Government policy. I. Title.

HM851.T56 2013

302.23'1—dc23

2013033674

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

**Support RAND**—make a tax-deductible charitable contribution at [www.rand.org/giving/contribute.html](http://www.rand.org/giving/contribute.html)

**RAND**® is a registered trademark

*Cover design by Dori Gordon Walker*

*Cover images by Thinkstock*

© Copyright 2013 RAND Corporation

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of RAND documents to a non-RAND website is prohibited. RAND documents are protected under copyright law. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see the RAND permissions page ([www.rand.org/pubs/permissions.html](http://www.rand.org/pubs/permissions.html)).

RAND OFFICES

SANTA MONICA, CA • WASHINGTON, DC

PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA

DOHA, QA • CAMBRIDGE, UK • BRUSSELS, BE

[www.rand.org](http://www.rand.org)

## Preface

---

Over the past decade, the Internet has become a battleground between repressive governments that would censor content and those who advocate free access for all. In 2011 the Bureau of Democracy, Human Rights and Labor (DRL) at the Department of State asked RAND to assess the effect of Internet freedom on the relationship between civil society and elected officials worldwide, and to examine such questions as: Does Internet freedom make government more accountable to the people? If, so by which mechanisms? How does expanding freedom online affect political space offline, and in which countries will these effects be most visible? How can DRL maximize the impact of its ongoing Internet freedom initiatives?

This study was conducted during 2011–12 and focuses on the role of the Internet and social media during popular protests in 2011 in Egypt, Syria, China, and Russia. We compare the ways that different political contexts and informational environments altered the opportunities for online mobilization and how, subsequently, online activism grew into offline mobilization. We also studied Radio Free Europe and Radio Liberty, aimed at the Soviet Union and Eastern Europe during the Cold War as a way of grounding Internet freedom within the broader context of information freedom. The goal of the study is to identify the mechanisms by which the freedom to browse, post, and share information online may transform state-society relations in nondemocratic regimes.

This analysis highlights several mechanisms through which open and free Internet can trigger political transformation. In fully authori-

tarian regimes that outlaw opposition and elections, Internet freedom promotes the expansion of social space and, in so doing, transforms political space. The Internet can also undermine the stability of a non-democratic regime by triggering an information cascade that mobilizes civil society; free Internet can also make political coalitions more inclusive by opening deliberations that cut across socioeconomic cleavages, thereby spreading information to people who do not usually interact on a daily basis. The expansion of online freedoms does not automatically translate into visible political outcomes, however, because such factors as fragmentation of the elite, support of international allies, and socioeconomic status of netizens affect how authorities respond to online mobilization.

This analysis will be of interest both to policymakers seeking to understand how digital media can advance U.S. policy goals worldwide and to scholars working on the Internet-democracy nexus. The research was sponsored by the DRL and conducted within the International Security and Defense Policy (ISDP) Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis on defense and national security topics for the U.S. and allied defense, foreign policy, homeland security, and intelligence communities, as well as foundations and other nongovernmental organizations that support defense and national security analysis.

For more information on ISDP, see <http://www.rand.org/nsrd/about/isdp.html> or contact the director (contact information is provided on the web page).

# Contents

---

<b>Preface</b> .....	iii
<b>Figures and Tables</b> .....	ix
<b>Summary</b> .....	xi
<b>Acknowledgments</b> .....	xxi
<b>Abbreviations</b> .....	xxiii

## CHAPTER ONE

<b>Introduction: The Autocratic Challenge and Internet Freedom</b> .....	1
Political Space and the Internet .....	4
Styles of Repression .....	7
Introduction to Internet Freedom Programs .....	12
Organization of the Report .....	14

## CHAPTER TWO

<b>The Internet and Political Process in Different Regimes</b> .....	17
Is the Internet Transforming Politics? Where and How? .....	19
Cyberactivism in Democratic and Nondemocratic Regimes .....	24
How and Where Can Internet Freedom (Technologies) Transform Political Space? .....	28
Political Communication and Social Mobilization .....	29
Internet Freedom and Framing Process .....	32
Key Actors in Cyberspace .....	32
Bloggers, Netizens, and Political Space .....	35
Web 2.0 Users and Political Space .....	35
Online Activists and Political Space .....	37
Internet Freedom and the Modes of Transformation of Political Space ...	38
Conclusion .....	41



CHAPTER THREE

**Cyberactivists, Social Media, and the Anti-Mubarak Protests**

**in Egypt**..... 43

Social Media’s Significance: The Debate ..... 47

    Cyberenthusiasts ..... 48

    Cyber-Killjoys ..... 49

How Social Media Bridged Egypt’s Mobilization Gaps ..... 55

    Social Media Was the Opposition’s Only Tool for Reaching and  
    Mobilizing a Mass Base ..... 55

    No Other Opposition Force Would Confront the State with Mass  
    Action ..... 65

    Military Considered Defection Only After Demonstrations Grew  
    and It Was Forced to Either Shoot or Remove Mubarak ..... 68

Conclusion: What This Means for the Study of Social Media ..... 70

CHAPTER FOUR

**Internet Freedom and Political Change in Syria**..... 73

Internet Usage by the Numbers ..... 74

Internet Censorship ..... 77

Use of the Internet in the Syrian Uprising ..... 79

    Circumvention Technologies During the Protests ..... 82

    Regime Adaptation ..... 83

    External Dimensions ..... 87

How Internet Freedom Affected Political Change in Syria ..... 89

CHAPTER FIVE

**The Internet in China: Threatened Tool of Expression and**

**Mobilization**..... 93

Netizens and Authorities in Cyberspace..... 95

Censorship and Circumvention Methods..... 96

Online Activists and Authorities in Political Space ..... 101

Online Mobilization and Policy Outcomes ..... 103

    Wenzhou Train Crash..... 104

    Dalian Chemical Plant..... 107

    Internet and Popular Mobilization in Rural Areas ..... 110

Ethnic Riots and the Internet ..... 112

Internet Freedom Technologies: Tools for the Motivated Elites or Mass-Use Technologies? .....	116
---	-----

#### CHAPTER SIX

<b>Fighting Electoral Fraud in the 2011 Russian Election with Internet and Social Media</b> .....	119
Critical Information and Postelection Protests .....	120
RuNet: Russian Internet .....	124
Russian Authorities and Cyberactivists .....	127
Golos and Online Election Fraud Reporting .....	130
Golos and Citizens' Whistle-Blowing .....	133
Electoral Fraud, Social Media, and Post-Election Protests .....	139
Social Media and Voter Mobilization .....	141
Conclusion .....	145

#### CHAPTER SEVEN

<b>Information Freedom During the Cold War: The Impact of Western Radio Broadcasts</b> .....	149
Short-Term and Long-Term Objectives of RFE/RL .....	150
Measuring the Size of RFE/RL Audiences and Determining Its Effectiveness .....	157
The Role of RFE/RL in Social Unrest .....	162
Learning from the Cold War Experience: Lessons and Analysis from Communist Archives for Promoting Internet Freedom .....	171
What Impact Did U.S. Policymakers Hope to Achieve Through Their Efforts to Improve Communist Citizens' Access to Outside Information? .....	171
How Could RFE/RL Safely Assist Opposition Figures and Parties to the Communist Regime? How Did this Assistance Affect the Political Space? .....	173
What Did Communist Authorities Hope to Achieve Through Jamming Western Radio Broadcasts? How Did Western Broadcasters Attempt to Overcome Jamming? Did Jamming Alter the Impact of Western Radio Broadcasts? .....	176
Who Was the Target Audience for Western Short-Wave Broadcasts? How Confrontational Toward Communist Authorities Should the Broadcasts Be? .....	179

How Did U.S. Policymakers Measure Success in the Medium and Long Term of Western Radio Broadcasts? .....	182
<b>CHAPTER EIGHT</b>	
<b>Internet Freedom: Measure and Countermeasure</b> .....	185
The Struggle for Internet Freedom: A Multiplayer Strategic Competition .....	190
Countermeasures and Counter-Countermeasures .....	192
No or Expensive Internet .....	192
Halal Internet .....	193
Site and Content Blocking .....	194
Green Dam .....	196
Pwning Dissident Computers .....	196
Finding and Targeting Dissidents Through Their Internet Use .....	197
DDOS Attacks .....	198
50-Cent Party .....	199
Exceptional Violence .....	199
Greater Surveillance of Mobile Communication .....	200
The Future Architecture of the Internet .....	201
<b>CHAPTER NINE</b>	
<b>Key Findings and Policy Implications for Internet Freedom</b>	
<b>Programs' Design</b> .....	203
Summary of Case Studies: The Relationship Between Internet Freedom and Political Space .....	204
Impact of Opportunity Structures on the Outcomes of Online Mobilization .....	211
Implications for the Design and Implementation of Internet Freedom Programs .....	213
Leveraging Internet Freedom Programs: Maximizing Their Impact and Understanding Their Limitations .....	216
<b>APPENDIX</b>	
<b>Electoral Fraud Variable and Summary Statistics for the Russia Case Study</b> .....	223
<b>Bibliography</b> .....	231

# Figures and Tables

---

## Figures

1.1.	Components of Political Space.....	5
3.1.	Frequency of Google Search Queries for Key Word “Khaled Said” in Egypt.....	61
3.2.	Number of Connections from Egypt to the Tor Network.....	65
4.1.	Syria’s Internet and Mobile Penetration.....	76
4.2.	Number of Connections from Syria to the Tor Network.....	86
5.1.	Number of Connections from China to the Tor Network ...	99
5.2.	China Internet Penetration Rate .....	111
5.3.	Deletion Rates by Province .....	113
6.1.	Important Source of Political Information, March 2011 ....	125
6.2.	Number of Connections from Russia to the Tor Network....	127
6.3.	Frequency of Searches for “Falsifications,” 2011 .....	140
6.4.	Frequency of Searches for “Facebook” and “vKontakte,” 2011 .....	143
A.1.	Distribution of Voter Turnout in Selected Russian Regions.....	224

## Tables

2.1.	The Internet as a Mobilization Tool in Different Regimes....	25
6.1.	Correlates of Whistle-Blowing in the 2011 Election in Russia.....	136
6.2.	Facebook and Demonstrations for Clean Elections .....	142
A.1.	Kolmogorov-Smirnov Statistics .....	225
A.2.	Summary Statistics .....	229



## Summary

---

Since 2008, the Department of State has spent \$100 million to promote Internet freedom worldwide. These efforts included increasing public awareness of online censorship, developing and providing circumvention technologies that allow users access to blocked sites and censored information, protecting sites from distributed denial of service (DDOS) attacks, and offering Internet literacy training for civil society groups.<sup>1</sup> This report examines whether and how furthering the “freedom to connect” can empower civil society vis-à-vis public officials, make the government more accountable to its citizens, and integrate citizens into the policymaking process<sup>2</sup>—and if so, through which mechanisms? To answer these questions, we examined how access to information online may affect freedom of assembly, freedom of expression, and the right to cast a meaningful vote—the three dimensions that define political space.<sup>3</sup> Using Egypt, Syria, China, and Russia as case studies, we examined how online freedoms altered state-society relations in those countries. We focused on three types of actors who may benefit from Internet freedom: Internet users, netizens, and cyberactivists. The first category comprises those for whom conventional media is the primary

---

<sup>1</sup> Fergus Hanson, “Internet Freedom: The Role of the U.S. State Department,” in *Baked in and Wired: eDiplomacy @ State*, Brookings, October 25, 2012.

<sup>2</sup> The term “freedom to connect” was first used by Hillary Rodham Clinton, Secretary of State, “Remarks on Internet Freedom,” speech at Newseum, Washington, D.C., January 21, 2010.

<sup>3</sup> By “political space” we mean a metaphorical arena in which input from citizens is continually being received and taken into account by the governing authorities.

source of information and who only occasionally browse the web and rarely check their emails. The second category, referred to as “netizens,” comprises those for whom the Internet has become an integral part of daily activities; they browse online news sources daily and actively engage in online discourse. The third category, cyberactivists, are those who employ the Internet to mobilize others behind a specific cause or to advance a specific agenda. In our case studies, we examined how enhancing online freedoms can affect political processes. In addition to contemporary cases, we included a case study of the effects of Radio Free Europe (RFE) and Radio Liberty (RL) on political opinion and civil society development within the Soviet Union and Eastern Europe, as a way of grounding Internet freedom within the broader context of information freedom.

## **Summary of Case Studies: The Relationship Between Internet Freedom and Political Space**

In our first case study, which focused on Egypt, we found that the Internet and social media compensated the opposition for the shortfalls in the traditional organizational resources. The social groups that formed the core of the protesters lacked both the backing of the religious organizations and the Muslim Brotherhood’s support, especially during the initial stages of the revolution. In this case, social media compensated for such asymmetry in resources by first fostering the creation and the diffusion of frames (or action maps) that appealed to a sufficiently wide population and then by coordinating popular mobilization. The protests began with Facebook users circulating photos documenting a mid-2010 incident of police brutality against Khaled Said; this rapidly grew into a “We Are All Khaled Said” frame—violence against one is repression against all—that cut across social and economic cleavages. Social media introduced new voices into Egypt’s political space that were not affiliated with either of the existing opposition parties. The number of protesters who came out on the streets on January 25, 2011, caught the regime off guard and triggered a domino effect that led key supporters to defect from President Hosni Mubarak.

In Syria, our second case study, the mobilizing potential of the Internet was severely curtailed by the regime's tight censorship of online content, the ban on Facebook, and repressive measures against civil rights activists. In this case we found little evidence that the Internet had any visible impact on political freedoms on the eve of the civil war outbreak. However, the Internet was indispensable for attracting international attention to the protests and to subsequent atrocities committed by the regime during the violent conflict. This publicity increased the political costs to Russia and other states of supporting Bashar al-Assad, although to date that has not yet led them to abandon the regime. We also found that as the civil conflict unfolded, more and more netizens turned to anonymizing tools, such as Tor, to conceal their behavior from officials and to access censored information.

In our third case study, China, we found that the expansion of social space online, coupled with the growth of the middle class, facilitated social mobilization in situations that sought to improve the quality of service provision rather than challenge the regime's authority. Online mobilization was feasible in spite of excessive censorship because the spontaneity of online mobilization caught the Chinese authorities off guard and they failed to block the online discourse early enough to prevent mobilization. This case study also provided evidence for the limitations of this form of mobilization. In China, the empowerment provided by the Internet was not uniform across different segments of the society. Chinese authorities were more likely to respond to social pressures from better-educated and more-affluent Chinese citizens, while ignoring similar demands from poorer, rural citizens. In Dalian, protesters angry about pollution and safety concerns persuaded the local authorities to shut down a chemical plant, whereas local officials were not swayed by citizens of Yunnan—a poorer, less-developed province—who raised similar environmental concerns and advocated stricter law enforcement against a polluting plant. Perhaps Internet freedom may lead to uneven expansion of voice, vote, and assembly across different segments of society because more influential groups will be also more likely to have connection to the Internet.

Turning to Russia, protests in the aftermath of the 2011 elections to the national assembly (Duma) illustrated how online mobilization



manifested given a relatively high level of Internet penetration and a relatively open political space. In an environment with tight government control over traditional media, nongovernmental organizations (NGOs) can use the Internet to reach out to voters and to collect evidence challenging the validity of the frame put forward by the authorities. The Internet was the only channel through which voters in Russia could expose electoral violations that took place on Election Day and during ballot counting. By documenting irregularities at polling stations and distributing them via YouTube, and by analyzing statistical data and posting the results, netizens were able to persuade many voters that election results were rigged. Social media subsequently facilitated the coordination of protests throughout the country by providing information on scheduling, location, names of the opposition leaders who would head the demonstrations, and the expected number of social media users who would show up.

Unlike China, Russia already had an active civil society that can help organize protests. Opposition parties, NGOs, and online activities before the elections had established positive reputations, making them more effective in contesting the frame put forward by the government. The role of the Internet in Russia was to strengthen the links among the civil society, NGOs, and the opposition parties—whereas personal networks helped with offline mobilization, especially among white-collar, college-educated, middle-class, urban residents.

In the historical case study of RFE and RL in the Soviet Union and Eastern Europe, we drew parallels between the goals and constraints faced by U.S. policymakers during the Cold War and the challenges entailed in implementing Internet freedom programs. Both the RFE and RL broadcast alternative information to people living behind the Iron Curtain in the hope that this would bring about political change, either in a piecemeal or revolutionary fashion. The program exploited ideological vulnerabilities of the Soviet regime by appealing to the intelligentsia and youth who aspired to be part of a global cultural community. The goal of the program was to provide alternative frames for understanding the Western culture and policies that would compete with those propagated by the Soviet officials in the mainstream media and educational institutions. These programs played

an important role in disseminating information about social protests, major environmental disasters, and *samizdat* literature—that is, dissident literature suppressed by the government. Although these programs did not directly alter the internal dynamics of the Soviet system, they did contribute to the rise of an alternative culture based on values inconsistent with the Soviet ideology.

## Findings and Policy Implications

Our analysis yields six important results.

- **The channels by which Internet freedom can expand political space depend on the level of Internet penetration, the reach of those programs, and regimes' repressive capacity.** Since not all Internet users take equal advantage of the Internet and Internet freedom programs, we distinguish among occasional Internet users, netizens, and cyberactivists. Most occasional Internet users lack information technology (IT) proficiency to configure their browsers, clean cookies, or install circumvention software, or they may find using circumvention tools too costly. Netizens use the Internet to engage in frequent online discussions with online communities. Online activists employ the Internet to mobilize others behind a specific cause or to advance a specific agenda. Each of these actors plays a distinct part in online mobilization. Netizens attract Internet users' attention to the specific government action or policy and build consensus among Internet users on the appropriate course of action. Online activists bridge online discourse with offline organizational resources and civil society groups without whose support online mobilization cannot manifest itself offline. Internet users disseminate narrative through their online and offline social networks. Internet freedom programs, by design, target either online activists and netizens or all Internet users. Since coercive measures used by nondemocratic governments narrow the range of available options and make

online mobilization more costly, the menu of actions available to these actors for online mobilization depends on the regime type.

- **The expansion of social space online may lead to the expansion of political space even if netizens do not start out using the Internet for political purposes.** As our China and Russia cases studies show, political online mobilization grew out of non-political uses of the Internet. In China, rapid economic changes brought about a sweeping social transformation that contributed to the rise of new social identities. The Internet facilitated interaction among these new social groups and enabled them to challenge the state by fostering cooperation among netizens from across the socioeconomic spectrum. In Russia, the growing ranks of enterprises that use the Internet for business have improved Russian citizens' information technology skills; these skills were then used to document electoral violations after the 2011 legislative elections.
  - A similar synergy between social and political space emerges from the historical case study of the Radio Free Europe and Radio Liberty programs in the Soviet Union and Eastern Europe, which explicitly tried to preserve the ethnic identities of minorities while promoting the growth of civil society within communist states. These efforts turned out to be pivotal in the democratization process that occurred in Eastern Europe and the Soviet Union after the fall of communism.
- **Online information can undermine the stability of non-democratic regimes by triggering an information cascade.** The impact of protests is frequently proportional to the number of protesters who appear on the streets. The Internet can facilitate social protests by enabling citizens to anonymously express their true opinions and coordinate collective action, which can create a domino effect. Online mobilization in both Egypt and Russia triggered a wave of protests with long-term consequences—most notably the stunningly swift collapse of the Mubarak regime. Although social media in Egypt did not cause the popular uprising that came to center in Tahrir Square, it substantially increased the number of people who participated in the first demonstration.

The size of the crowd in the Square caught Egyptian authorities by surprise and triggered the defection of some high-ranking army officials. In Russia, the information about electoral fraud triggered a wave of online mobilization that manifested itself in a series of mass demonstrations. Syria's activists used the Internet to publicize elite defection from the regime, albeit with more limited success against a brutal and determined foe.

- **The Internet can make political coalitions more inclusive by opening up deliberations that cut across socioeconomic cleavages, thereby spreading information to people who do not normally interact on a daily basis.** This conclusion emerges primarily from the review of theoretical literature on the diffusion of information online and the literature on social movements. While weak ties facilitate the diffusion of information online, strong ties create peer pressure that contributes to offline social mobilization.
- **Online mobilization is more likely to manifest itself on the streets when targeted against a specific policy outcome than against the regime.** This conclusion is largely based on the case study of China, where online activists benefited from intraparty competition between the progressive and old guard factions, coupled with the vertical competition between the national and regional officials. Party officials, seeking to advance their policy agenda, capitalized on online mobilization when netizens were dissatisfied with the specific policy outcome.
- **Technological empowerment has not been uniform.** The Internet has benefited the middle class more than it has less-affluent individuals. In Russia, the majority of protesters in 2011 were white-collar professionals who are also active users of the Internet. In China, the authorities were more responsive to the middle class' online and offline mobilization than to similar demands from poorer, rural residents. In Egypt, secular students and recent college graduates in cities formed the core of the protesters who participated in the first demonstration.

### Measure and Countermeasure

Politics is the struggle for power, and the expansion of political space would inevitably alter the rules for that struggle. Autocratic regimes have power, want to keep it, do not respect the norms of liberal democracy, and prefer to restrict the political space for its citizens. They also want the scope to carry out policies without the constraints that an aroused citizenry would impose. Therefore, they frown on any of the following:

- circulation of bad news from the inside
- circulation of good news from the outside
- delegitimization of fraudulent elections
- spreading dangerous images
- mobilization of opposition
- organization of opposition.

Regime tactics include blocking the Internet entirely or making access prohibitively expensive, setting up a so-called Halal Internet (a national Internet with few, if any, links to the outside), blocking sites or content, creating Green Dam software that can block content, pwning (taking over) activists' computers, targeting activists through the Internet use, launching denial-of-service attacks, unleashing fifty-cent trolls (government-paid shills who post pro-government material and try to intimidate legitimate opposition voices), and, on the most extreme end of the spectrum, targeting violence at activists.

Some countermeasures arise spontaneously. Moore's Law holds that the price of the Internet will come down over time. Attempts to build a Halal Internet that provides different services to businesses than individuals can be short-circuited by exploiting little-known network connections. Civil activists can carve out their own space in much in the way that jihadists do on today's Internet. Site and content blocking can be offset in some cases by clever users who, for example, use substitute words such as "stroll" for "protest" or resort to audio or video transmissions to get around programs designed to block certain words. Other techniques include circumvention software such as Tor or Ultra-surf. Pwning computers is difficult to counter, but care in download-

ing, platform choice, and technological approaches can help. A range of techniques exists to deal with DDOS attacks, including rehosting servers or repairing vulnerabilities.

### **Implications for Internet Freedom Programs**

What factors correlate with more effective Internet freedom programs?

Our research suggests that regime type is key. Hybrid states (e.g., Russia) have an active civil society, one that Internet freedom tools can further empower. Civil society groups can be trained to quickly respond to circumstances when Internet access is blocked. These groups can also be assisted when their websites come under DDOS attack by rehosting them on servers that are harder to choke. As the recent Russian parliamentary election suggests, Internet freedom programs can affect elections by making it harder to harass voters or engage in outright fraud, and make it easier for domestic and international audiences to monitor election results.

However, hybrid regimes do have other ways to shut down or curtail the Internet impact of civil society groups. In response to social protests, Russia's parliament created new laws that would shut down sites; its security services continue to harass and punish opponents of the regime. However, the greater visibility and the harsher repression required to control civil society groups in Russia will, over time, erode the regime's domestic and international acceptance.

For authoritarian regimes, broadening the use of circumvention is key. Chinese and Iran-style regimes have undertaken vast efforts to filter the information their citizens can access and prevent dangerous information from being created and posted. These regimes do this to maintain the frame that authorities want their citizens to have about the society they live in and to eliminate their citizens' contact with any information that might allow them to start forming alternative views. Circumvention tools weaken this process by providing people with access to outside information that could rebut the frame of authoritarian regimes. Such tools also help citizens of autocracies communicate without fear of being monitored; they thus contribute to the development of social space. While forming any civil society group inside an

authoritarian state is difficult, circumvention tools that provide anonymity allow for at least its rudiments.

Internet freedom tools can improve the lives of citizens of non-democratic states. They let people highlight such unaddressed issues as environmental dangers or shoddy infrastructure. Corrupt local officials can be exposed anonymously with less fear of retribution. Other officials can be held more accountable for their actions. Internet freedom tools generally allow users to explore the virtual world unencumbered by ideological restrictions.

## Acknowledgments

---

We would like to thank the U.S. State Department Bureau of Democracy, Human Rights, and Labor for providing the funding for our research. It has been a pleasure to work with the DRL team: Katharine Kendrick, Christopher Riley, Ian Schuler, and John Tye, who provided invaluable input at the conceptual stage of this project and assisted us on a number of occasions in thinking through the best ways to frame the problem.

We also benefited enormously from discussions with our RAND colleagues and individuals working on Internet freedom issues both overseas and in the United States. We are grateful to the many government officials, NGO staff, and civil society activists who took the time to share their knowledge and opinions with us. We also appreciate the helpful suggestions from Philip Howard, Warren Bass, Dalia Dassa Kaye, Andrew Scobell, and Andrew Weiss, who read through early drafts of the report and helped us refine and improve it significantly. We are also grateful to Kirill Kalinin for sharing precinct-level election data for Russia. We also wish to thank our RAND colleague Ryan Henry for his work on the initial stages of this project and his helpful insights and suggestions on our work. Finally, we owe thanks to Olga Oliker, Seth Jones, and James Dobbins at RAND for their generous support of this project.





# Abbreviations

---

Amcomlib	American Committee for Liberation from Bolshevism
CEC	Central Election Commission
CIA	Central Intelligence Agency
DDOS	distributed denial of service
DRL	Bureau of Democracy, Human Rights, and Labor
DoS	Department of State
FEC	Free Europe Committee
FOM	Public Opinion Fund
FSB	Federal Security Service
GDP	gross domestic product
ICT	information and communications technologies
IP	Internet providers
ISDP	International Security and Defense Policy
ISP	Internet service provider
IT	information technology
MIT	Massachusetts Institute of Technology
NDP	National Democratic Party
NGO	nongovernmental organization
PX	paraxylene
RFE	Radio Free Europe

RIAS	Radio in the American Sector
RL	Radio Liberty
SORM	System for Operative Investigative Activities
SPC	Supreme People's Court
VOA	Voice of America
VPN	virtual private network
VTsIOM	Russian Public Opinion Research Center

## Introduction: The Autocratic Challenge and Internet Freedom

---

The struggle between freedom and autocracy has been going on for hundreds of years and shows no sign of resolution. Since the 1970s, what has been called the third wave of democratization has transformed a number of Asian, African, European, and Western Hemisphere societies from authoritarian to more democratic forms of government. This trend slowed over the past decade (and even reversed in some regions), even as popular uprisings challenged—and in several cases ousted—long-established authoritarian regimes in Arab world.<sup>1</sup> During 2011, for instance, a wide range of countries—including Russia, China, Iran, Ukraine, and Ethiopia—all saw significant declines in their levels of freedom. Scholars point to several factors that likely accounted for such erosion of democratic advances as has occurred outside the Arab world: the global financial crisis, which discredited the West; the increasing power and influence of Russia and China regionally and globally; the erosion of U.S. and European Union leverage over nondemocratic states; and the growing ability of regimes to protect themselves from the Internet.<sup>2</sup>

---

<sup>1</sup> Freedom House, *Freedom in the World 2012: The Arab Uprisings and Their Global Repercussions*, Washington, D.C., undated; Economist Intelligence Unit, *Democracy Index 2011: Democracy Under Stress*, London, December 16, 2011.

<sup>2</sup> Larry Diamond, “Democracy’s Third Wave Today,” *Current History*, Vol. 110, No. 739, November 2011, pp. 299–307. For more on how powerful authoritarian regimes can mitigate democratization efforts, see Gary Clyde Hufbauer et al., *Economic Sanctions Reconsidered: History and Current Policy*, Washington, D.C.: Institute for International Economics, 1991. Regarding the important role that U.S. and Western leverage plays in democratization, see

Human beings are naturally political animals, as the ancient Greeks taught, but it is in the very nature of autocracy to try to suppress the inclination of people to engage in their own governance. This engagement has two components: vote and voice. The vote is what defines democracy, if one assumes that the voting is free and fair. But participation also requires voice—the ability to express and exchange political opinions. Absent voice, voting is an empty exercise. Indeed, absent voice, all other forms of political participation become empty exercises as well.

The Internet, putatively, should be a great boon for exchange. In most places, people gravitate to its low cost, instant speed, near-infinite reach, and multiple forms (from mainstream media to blogging and social media). One no longer needs a printing press to enjoy freedom of the press, so to speak. Yet, precisely because of the Internet's power, nondemocratic regimes have concluded that a free and unregulated Internet constitutes a threat to their survival. At the same time, with rare exceptions, they understand that the Internet is increasingly unavoidable for participation in the world economy. They are assertively intervening in cyberspace, seeking to manage online activities and expression. The types and forms of these interventions widely vary. Factors that influence how regimes attempt to manage and control the Internet include the overall level and style of regime repression of society, the technical sophistication of the regime, the regimes' strategy for holding on to power, and the level of resources the regime can mobilize to control the Internet.

The strategies and tactics that regimes use to suppress Internet freedom are also closely linked to the internal and external structures that maintain the regimes' hold on power. For example, the security services can leverage their extensive human network of sources to manage the use of Internet cafés. The police may require café owners to establish the identity of users, report on the material they are accessing, and allow the security services to monitor the Internet activities of their patrons directly. The same restrictive legal and regulatory mechanisms used to control other types of media can be extended to the

Web. For example, regimes can require websites to register with the government. This allows the government to hold websites accountable for what appears on them and to make it a crime to post material that is not approved.

Nondemocratic regimes have also grown to appreciate how the Internet can be used to entrench their hold on power.<sup>3</sup> Increasingly, regimes are using the Internet to conduct surveillance of dissidents and democracy movements. Regimes have developed sophisticated means to digitally track their citizens' activities, including networks of personal contacts. The Internet also plays a critical role in improving the effectiveness of the regimes' propaganda campaigns. Modern propaganda can be easily distributed in highly personal and targeted ways to citizens' mobile devices and email accounts.

Internet censorship contradicts core U.S. values, and since 2008 the State Department has allocated \$100 million to increase popular awareness of the state of Internet freedom, to educate civil society about potential vulnerabilities to regime surveillance, and to provide venture capital to develop tools to enhance online anonymity.<sup>4</sup> Since anonymization tools and information technology (IT) literacy programs are apolitical in nature and are available to Internet users regardless of their political orientation, it merits asking whether enhancing Internet freedom can have any effect on state-society relations or if the effects of these programs are limited only to the Internet itself. Put another way, even if one could expand the "freedom to connect" for tech-savvy Internet users, would political space expand as a result? How does online freedom affect state-society relations? Furthermore, in what context should we expect Internet freedom programs to have the most visible impact? By answering these fundamental questions, this manuscript focuses on the relationship between online freedoms and the political process offline.

---

<sup>3</sup> Evgeny Morozov, *The Dark Side of Internet Freedom: The Net Delusion*, New York: Perseus Books Group, 2011.

<sup>4</sup> Fergus Hanson, "Internet Freedom: The Role of the U.S. State Department," in *Baked in and Wired: eDiplomacy @ State*, Brookings, October 25, 2012.

## Political Space and the Internet

The concept of political space has become more important in both policymaking and academic circles. The State Department's Human Rights and Democracy Fund, which is part of the Bureau of Democracy, Human Rights, and Labor (DRL), lists "opening up political space in struggling or nascent democracies and authoritarian regimes" as one of its critical objectives. DRL sees increasing political space as directly connected with promoting human rights and democracy worldwide, and as a vital step in bring about positive transnational changes in hybrid and authoritarian states.<sup>5</sup>

The concept of political space resists easy definition. In terms of classic political philosophy, the state is created (or at least legitimized) when a community of people hand authority over themselves to a political system that governs and regulates their behavior.<sup>6</sup> This does not mean, though, that individuals give up their rights to engage in the political process. Political space is the arena in which input from citizens is continually being received and taken into account by the governing authorities. In a fully democratic society, political space is an area where unconstrained articulation and organization can occur and where political authority using the structures of the state cannot arbitrarily control or inhibit the will of the people. By the norms of liberal political theory, ignoring the will of the people—or, worse, repressing the expression of that will—violates the social contract. In extreme cases, the authorities' right to govern can be revoked if citizens feel their basic liberties are being violated.

Political space can be defined as constituting three spheres of activities, as illustrated in Figure 1.1. One sphere is the ability to freely assemble. How easily can citizens hold public meetings on issues of political concern? How willing is the government to let them form associations? A second sphere is citizens' abilities to express themselves.

---

<sup>5</sup> U.S. State Department, *Bureau of Democracy, Human Rights, and Labor (DRL) Programs* web page, undated.

<sup>6</sup> On social contract theory, see John Locke, *Second Treatise of Government*, London, 1690; David Hume, *A Treatise of Human Nature*, London, 1740.

**Figure 1.1**  
**Components of Political Space**



RAND RR295-1.1

Can citizens hold and voice opinions without interference from the government? Can they seek, receive, and impart information and ideas through any media source? A third sphere is the ability to participate in the selection of governing authorities through a free and fair electoral process. Do voters have a franchise? Can they exercise it without intimidation? Will votes be accurately counted? Can everyone campaign on a relatively even footing? Maintaining political space in this sphere goes well beyond merely having an election. It encompasses the degree that those outside the governing party can vigorously compete for political power.

The Internet has clearly introduced new ways for citizens to enter the political space and exercise their basic rights, notably their “Free-



dom to Connect.”<sup>7</sup> Exercising Internet freedom can be defined by several actions individuals undertake online. The three activities listed below are ranked by the degree of political activism involved in undertaking each one of them.

The most common activity that citizens can engage in on the web is *browsing*. This requires an Internet connection and the freedom to navigate to any site. The second is *sharing* information with others. This often involves taking information you have discovered online and providing it to others who might be interested in it. It can range from directly texting or emailing information to specific individuals to sharing information with a much wider circle through blogs, discussion groups, and social media. The third—and the one with the highest degree of political activism—is *creating and posting information* online. This is closely connected with freedom of expression online. Citizens create content for the Web through different types of media (including text, graphics, audio, and video) and then place it online so other people can view it. The unique priorities of the Internet allow people to rapidly express and share their points of view with a wide audience.

Not all Internet users take equal advantage of the opportunity to browse, post, and share. In this report we distinguish among three types of users. The first category comprises occasional users of the Internet for whom conventional media is the primary source of information and they only occasionally browse the web and rarely check their emails. Such users generally lack IT proficiency to configure their browsers, clean cookies, or install circumvention software. Although in some countries this category may encompass an overwhelming majority of Internet users, these actors are only marginally important for our analysis because they are least likely to use the existing circumvention technologies. The second category comprises those for whom the Internet has become an integral part of daily activities. They browse online news sources daily and actively engage in online discourse. We refer to

---

<sup>7</sup> Hillary Rodham Clinton, Secretary of State, “Remarks on Internet Freedom,” speech at the Newseum, Washington, D.C., January 21, 2010; Hillary Rodham Clinton, Secretary of State, “Internet Rights and Wrongs: Choices and Challenges in a Networked World,” speech at George Washington University, Washington, D.C., February 15, 2011.

such users as “netizens.”<sup>8</sup> The third category comprises cyberactivists; i.e., those who employ the Internet to mobilize others behind a specific cause or to advance a specific agenda. Our analysis will focus on netizens and cyberactivists, and we will seek to examine how enhancing these actors’ ability to browse, post, and share can affect political space.

## Styles of Repression

Since Internet penetration has been growing rapidly, especially in non-democratic regimes, our analysis focuses on the complex interplay between styles of repression and the expansion of online communication and mobilization channels. Styles of repression vary across non-democratic regimes, which have been categorized based on institutional, ideological, and pluralistic attributes. This study focuses on two categories of nondemocratic regimes, authoritarian and hybrid.<sup>9</sup>

Authoritarian regimes have a long historical lineage, but hybrid regimes appear to be a new style of regime that has emerged since the Cold War. The term “hybrid” (or competitive authoritarianism) reflects

---

<sup>8</sup> This term has different connotations depending on the culture. In the United States, it is used to highlight civic engagement aspects of citizenship and to underscore the value of collective work and the communal aspects of public communications. In China, this term is used to highlight libertarian aspects of citizenship and an individual’s freedom to pursue life without state intervention. See Michael Hauben, Ronda Hauben, and Thomas Truscott, *Netizens: On the History and the Impact of Usenet and Internet*, Los Alamos, Calif.: IEEE Computer Society Press, 1997; Brian Fung, “‘Netizen’: Why Is This Goofy-Sounding Word So Important in China?” *Atlantic*, October 11, 2012.

<sup>9</sup> Within the authoritarian category there is an important subcategory of regimes labeled “totalitarian” by political scientists. Totalitarian regimes such as Nazi Germany and the Soviet Union under Stalin sought to exert total control over societies, including establishing and maintaining a monopoly over all communications. These types of regimes rejected the idea that individuals should be allowed even a social space free from government control. The regime in North Korea is the only one today that fits the classic definition of a totalitarian state and, unsurprisingly, it allows almost no public access to the Internet. The classic works on what delineates a totalitarian regime from other types of authoritarian regimes are Hannah Arendt, *The Origins of Totalitarianism*, Orlando, Fla.: Houghton Mifflin, 1976; and Carl J. Friedrich and Zbigniew K. Brzezinski, *Totalitarian Dictatorship and Autocracy*, Cambridge, Mass.: Harvard University Press, 1956.

the fact that some regimes holding regular elections may lack other important attributes of democratic government.<sup>10</sup> Some political scientists believe that hybrid regimes are a transitional category and that a small push from outside forces can steer them toward democracy.<sup>11</sup> Others assert that a hybrid regime can remain in its current political configuration for a sustained period of time.<sup>12</sup> Levitsky and Way developed a topology of authoritarian and hybrid regimes based on the following dimensions:

1. status of core democratic institutions
2. status of opposition
3. level of uncertainty over election outcomes.<sup>13</sup>

In authoritarian regimes, uncertainty about the successor is low either because the power is transferred without holding elections or because elections are uncontested since opposition parties are banned or severely suppressed. Hybrid regimes hold competitive elections (as opposed to, say, plebiscites)—but those elections are not always free or fair due to instances of voter harassment and fraud. The political playing field is not always level; pro-regime candidates have vastly greater resources at their disposal, influence over major media outlets, and the support of biased election officials working the rules in their favor.

Another important difference between authoritarian and hybrid regimes is the way they manage civil liberties such as freedom of expression and freedom of assembly. In democratic states, freedom of expression and freedom of assembly are legally protected and an independent

---

<sup>10</sup> Larry Diamond, “Thinking About Hybrid Regimes,” *Journal of Democracy*, Vol. 13, No. 2, 2002, pp. 21–35.

<sup>11</sup> Samuel Huntington, *The Third Wave: Democratization in the Late 20th Century*, Norman, Okla.: University of Oklahoma Press, 2011.

<sup>12</sup> Thomas Carothers, “The End of the Transition Paradigm,” *Journal of Democracy*, Vol. 13, No. 1, 2002, pp. 5–21; Levitsky and Way, 2010.

<sup>13</sup> Levitsky and Way, 2010. Although totalitarian regimes comprise an important conceptual category and are distinct from authoritarian ones, we focus on authoritarian regimes because North Korea is the only one today that fits the classic definition of a totalitarian state.

judiciary ensures that the government does not violate these rights. In authoritarian states, civil liberties are not even minimally protected. Independent political organizations—and, in extreme cases, all independent organizations—are forbidden by the state. All political groups are sponsored by the state and controlled by the government. Freedom of political expression is severely curtailed and public criticism of national leaders or government policy is illegal. In authoritarian states, most opposition activity is driven underground or exiled.

Hybrid regimes have a different relationship with civil society than authoritarian ones do. In hybrid regimes, civil liberties are nominally guaranteed and at least somewhat respected. Freedom of assembly is allowed to some degree, with civic and oppositional groups meeting and organizing openly. Opposition groups are even allowed to protest against the government. Some independent media exists and, for the most part, it reports freely on government activities.

Yet hybrid regimes frequently violate civil liberties and curtail the influence of civil society organizations. They tend to use more subtle methods to achieve their aims. Legal instruments such as tax, libel, and defamation laws are often used to harass and punish opponents. Laws are followed selectively and in a partisan manner to go after opposition groups or figures. Independent human rights activists, media groups, and reporters are threatened legally and sometimes physically for their reports. There is limited use of violence, which is generally carried out by criminal elements not provably associated with the regime.

Civil society actors in hybrid regimes, unlike in full authoritarian regimes, continue to contribute to the political space even with harassment. Yet, by raising the cost of opposition activities, hybrid regimes seek to manage political activity so as to avoid serious threats to their power. As with holding elections, maintaining some civil liberties helps hybrid regimes resist domestic and international pressure for political change while maintaining their grip on power. The existence of an independent media, opposition political parties, and political nongovernmental organizations (NGOs) allows rulers to argue to the international community that they are upholding civil liberties within their country. For citizens upset with the government, these organizations provide an outlet for their anger that is not particularly dangerous or

threatening. In a globalized world with intense competition for talent, creative individuals are the least likely to want to live in very repressive authoritarian states. By maintaining some degree of civil liberties and a public space, hybrid states give themselves a better chance of holding onto some of their most economically productive citizens.

In the post–Cold War period, hybrid regimes proliferated because many incumbents decided that holding elections was a useful way of resisting domestic and international pressure for political change while maintaining their grip on power. Elections, even if only marginally competitive, allowed rulers to assert their legitimacy to the international community. In addition, the domestic power and legitimacy of rulers are enhanced when leaders and ruling parties can argue that elections have provided them with a popular mandate for their actions.

To illustrate how different styles of repression can alter the pathways by which Internet freedom can transform political space, our analysis juxtaposes two authoritarian regimes—China and Syria—with two hybrid regimes—Egypt under Hosni Mubarak and Russia shortly before Vladimir Putin’s election to a third presidential term. We selected these countries because of their relevance to U.S. national interest, their level of Internet censorship, and the type of political oppression they face.

Both China and Syria tightly censor the Internet. They have appeared on the top of the “Internet Enemies” list put together by Reporters Without Borders and were also ranked in 2012 as “not free” by the Freedom House in its report on the state of Internet freedom. On the political dimension as well, Freedom House ranked both countries as “not free” due to gross violations of human rights and civil liberties. Prior to the outbreak of the protest in Syria, the regime of Bashar al-Assad relied on ambiguity in the penal code, the Emergency Law, and a 2001 Publications Law to justify repression against journalists, writers, bloggers, intellectuals, and university professors. Since 2006, any gatherings of more than five people in public have been banned, only state-friendly NGOs working on apolitical issues have been allowed to exist, and all political organizations were required to be affiliated with the Baath Party. The legal system was highly politicized. The rights of

Kurdish and other minorities were heavily suppressed.<sup>14</sup> China received a similar rating by the Freedom House index due to the long history of repression of civil society by the Communist Party. In 2011, the party responded to the growing popular unrest against corruption and injustice by strengthening its security forces and intelligence agencies, and further tightening its grip over civil society and the Internet.<sup>15</sup> Both China and Syria (during the Assad rule) constitute textbook examples of authoritarian regimes, albeit with different levels of Internet penetration, which was as high as 38 percent in China and only about 19 percent in Syria in 2011.

We juxtapose these two cases with Russia during the Medvedev presidency and Egypt under the Mubarak regime, both of which were ranked as having slightly more political rights and civil liberties than China and Syria, but still “not free.” This Freedom House ranking captures more-intense intra-elite contestation, especially during elections in which multiple parties can nominate candidates and opposition parties win small shares of seats in the national legislatures. Electoral fraud and selective harassment of opposition candidates reduces opposition chances of success—and on several occasions, the opposition boycotted the elections as not fair. Both regimes tightly censor traditional media but in 2011 still refrained from directly censoring the Internet. Instead, they used selective repression through the prosecution of bloggers and cyberactivists, other administrative and legal means, and cyberattacks upon selected sites to manage the Internet’s political influence. Their combination of *de jure* provisions for multicandidate elections coupled with *de facto* restrictions on how those elections were held make Egypt (under the Mubarak regime) and Russia examples of competitive authoritarianism (or hybrid regimes). The two countries differ in the level of Internet penetration. In 2011, almost 45 percent of

---

<sup>14</sup> Freedom House, *Freedom on the Net 2012*, September 4, 2012b; Freedom House, *Freedom in the World: Syria*, web page, 2011b.

<sup>15</sup> Freedom House, 2012b, pp. 126–152; Freedom House, *Freedom in the World: China*, web page, 2011a.

the Russian population had access to the Internet, compared with only 26 percent in Egypt.<sup>16</sup>

We also would have liked to include a totalitarian regime as a case study, but the only country that qualified, North Korea, has almost no Internet. We conducted a historical case study of Radio Free Europe and Radio Liberty programs in the Soviet Union, in part, to explore how access to uncensored information can transform political space in a totalitarian regime.

## Introduction to Internet Freedom Programs

Initial U.S. Internet freedom efforts began in the early 2000s and largely focused on circumventing censorship, particularly in China and Iran.<sup>17</sup> However, since 2008, the State Department has broadened its efforts with programs encompassing privacy protection and online security, Internet for training journalists and civil society actors, and the development of organizational and advocacy skills based on information and communications technology (ICT). Since 2008, Congress has appropriated approximately \$100 million for the State Department's Internet freedom programs. The Secretary of State has requested \$27.5 million for these activities for fiscal year 2013.<sup>18</sup>

U.S. Internet freedom activities can be divided into six sets of activities:<sup>19</sup>

1. developing and providing circumvention technologies that allow users access to blocked sites and censored information

---

<sup>16</sup> Internet World Stats, *Internet Users in the Middle East and the World*, web page, June 30, 2012c; Internet World Stats, *Internet Users in Europe*, web page, June 30, 2012b.

<sup>17</sup> For information on the Bush administration's policies toward Internet freedom, see Paula Dobriansky, Under Secretary of State for Democracy and Global Affairs, "Global Internet Freedom Task Force," presentation, Washington, D.C., December 20, 2006.

<sup>18</sup> Thomas Lum, *China, Internet Freedom, and U.S. Policy*, Washington, D.C.: Congressional Research Service, Report R42601, July 13, 2012.

<sup>19</sup> This list draws upon Lum, 2012.

- largely by routing through proxy servers, as well as enhancing online anonymity
2. developing and providing software that protect sites from distributed denial of service (DDOS) and other cyberattacks from repressive governments or other organizations
  3. training civil society groups—including human rights activists, journalists, and other NGOs—to communicate and operate better in repressive environments
  4. providing rapid response to emerging situations when Internet access for civil society groups is threatened
  5. funding research that explores global Internet freedom conditions to increase public awareness about how nondemocratic regimes are encroaching on Internet freedom
  6. advocating for Internet freedom as a basic human right on a national and international basis, including advocacy for the principles of Internet freedom in multinational form such as the United Nations, publicly highlighting violations of Internet freedom within nondemocratic states, and encouraging private technology companies to utilize best practices in countries that repress Internet freedom.

This report scrutinizes a core assumption for the Internet freedom programs: that expanding opportunities to browse, post, and share information online can visibly and tangibly expand other basic freedoms. Our report seeks in general terms to assess whether and under what circumstances enhancing “freedom to connect,” especially for a handful of tech-savvy individuals, can expand political space. We answer this question by scrutinizing the existing literature and collecting original qualitative and quantitative evidence to identify the channels by which the Internet can promote self-expression and mobilization. The Internet freedom programs are unlikely to achieve the desired outcomes if the underlying premise about the Internet and civil society empowerment turns out to be false. Therefore, this study is dedicated to examining when and how the Internet can foster online mobilization and greater citizen engagement in political processes, and understanding the conditions under which online mobilization can move



offline and transform political space. The goal of the analysis is not to quantify the number of netizens who benefit from Internet freedom programs, but rather to uncover mechanisms that enable online activists to succeed.

## Organization of the Report

Our analysis begins in Chapter Two with a summary of academic literature on the role the Internet plays in politics and society. The chapter briefly reviews recent scholarship regarding which groups within society are most empowered by the Internet and the opportunity structures that shape how the Internet is utilized in democratic and non-democratic regimes. The chapter then investigates a critical theoretical question about how the Internet may transform the political space in nondemocratic regimes. Considerable scholarly debate has taken place on how the rapid expansion of the Internet in nondemocratic countries alters the balance between civil society and the state. Far less work has analyzed the mechanisms through which this change might take place. The chapter concludes by identifying causal mechanisms that translate online activities to outcomes in the three spheres of political space (collective action, voice, and vote).

Chapters Three through Seven present case studies. Our contemporary cases were chosen to explore how the Internet and the political space interact, particularly during the periods of social stress and upheavals. They focus for the most part on two questions:

- How does improving Internet freedom for netizens affect the political space?
- For Internet freedom policy, what are the trade-offs between concentrating on deepening Internet freedom for committed users vs. broadening Internet freedom so it encompasses the less-networked pieces of society?

Chapter Three explores the role that the Internet and social media played in the successful uprising in Egypt that resulted in Mubarak's

downfall. It discusses the competing viewpoints that have emerged on how critical a role social media played in the revolution, and concludes that social media was the only force in the country able to mobilize and organize young, urban, and secular activists into action.

Chapter Four is on Syria, a counterexample to Egypt. It shows how a determined regime that employs high levels of Internet censorship and a powerful and organized internal security service can neutralize netizens' attempts to challenge the existing status quo, at least for a time. Syria, however, does show that the Web has some utility—even in the most challenging environments—as a platform for attracting international attention to the events.

Chapter Five focuses on China. It analyzes how, even in an authoritarian regime with intensive Internet control, the Web can become a tool for self-expression and collective mobilization. Internet activity associated with the Wenzhou train crash and the protests about the Dalian chemical plant are examined as examples of how social mobilization sometimes emerges inside China.

Chapter Six looks at Russia, where the Internet remained free until recently, particularly in contrast to more traditional media. Russia is a hybrid state. In the face of electoral fraud, civil society groups have attempted to use the freedom provided by the Internet to fight back against the state, notably in the disputed Russian parliament elections of December 2011. We conclude that the Internet can facilitate both the diffusion of information about electoral fraud and social mobilization offline. The Internet has helped to inspire the most sustained protest movement in Russia since Putin took power in 2000.

In Chapter Seven, we analyze the long-term influence of Radio Free Europe and Radio Liberty on political opinion and civil society development within the Soviet Union and Eastern Europe. Historical information is used to shed light on the potential impact that Internet freedom programs may have on hybrid and authoritarian states today. Drawing on external and internal audience surveys, testimony from people such as former President Vaclav Havel, and the magnitude of communist regimes' countermeasures against the broadcasts, the chapter documents the impact that outside forces can have on political development inside authoritarian states.

Chapter Eight explores the various measures governments take against Internet freedom, and how the forces fighting for Internet freedom attempt to counter them in turn. It concludes that the struggle for Internet freedom is a complex and dynamic one that will ebb and flow as the architecture of the Internet continues to develop.

The final chapter draws on the existing literature in the field and the empirical evidence gathered in the case studies to reach some initial conclusions about the relationship between Internet freedom and political space. We then explore the implications of these conclusions for the design and implementation of Internet freedom programs. Finally, we identify areas where U.S. Internet freedom programs are likely to have the greatest impact and leverage and some of the inherited limitations of such programs.

## The Internet and Political Process in Different Regimes

---

Social media and the Internet are ubiquitous. A billion people are already on Facebook; every day a half million more come onboard. YouTube has 490 million unique users who visit the site every month and view 92 billion pages each month. Every minute, 3,000 images are uploaded to Flickr. Twitter handles 1.6 billion queries per day, and 11 new accounts are created per second. When new social media technologies appear, they attract millions of users in a blink of an eye. It took Google+ less than three weeks to attract 10 million users.<sup>1</sup> The majority of Internet users, however, reside in countries that restrict the right to vote, the freedom to assemble, and the freedom to speak and write.<sup>2</sup> This rapid expansion of the Internet in nondemocratic countries has prompted the debate about a democratizing potential of new technologies. Some scholars perceive the Internet as a panacea for political repression.<sup>3</sup> Others, to the contrary, portray the Internet as a tool capable of strengthening nondemocratic rulers.<sup>4</sup>

This chapter joins this debate by focusing on two questions: (1) Who are key players in cyberspace? (2) When and how does online

---

<sup>1</sup> Jeffbullas.com, *20 Stunning Social Media Statistics Plus Infographic*, web page, undated.

<sup>2</sup> China has the largest number of Internet users in the world by far, although large non-democratic states such as Russia, Iran, and Vietnam also have significant numbers of users.

<sup>3</sup> Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations*, New York, N.Y.: Penguin Group, 2008; Philip Howard, *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*, Oxford, England: Oxford University Press, 2010.

<sup>4</sup> Morozov, 2011.

activism can transform political space? The answers would help illuminate the relationship between the Internet and democratization by examining the complex interaction between virtual and offline communities. This chapter argues that bloggers and cyberactivists have a distinct impact on political space different from other actors because online networks that foster cyberactivism do not mirror ties that contribute to offline mobilization. Community activists rely on face-to-face contacts with their colleagues, neighbors, church members, friends, family, and other people with whom they share strong ties. Since strong ties evolve as a result of repeated interactions, they are shaped by existing socioeconomic cleavages. Bloggers and cyberactivists are interlinked with netizens and other Internet users via weak ties, which are best suited for rapid diffusion of information across a wide range of different communities. Thus, weak ties can deliver information in communities that are not interlinked with each other by strong ties. The expansion of political space takes place when civil society actors who have organizational resources decide to act upon information that went viral in cyberspace.

We also show that the menu of actions available to cyberactivists for online mobilization depends on the regime type because coercive measures used by nondemocratic governments narrow down the range of available options and make online mobilization more costly. Nondemocratic rulers attack bloggers and cyberactivists in both physical and cyberspace by interchangeably using physical violence and DDOS attacks, hacking and pwning activists' computers,<sup>5</sup> and censoring online content. Cybermeasures increase the cost of operating online for both activists and those Internet service providers (ISPs) that offer web-hosting services. On the demand side, censorship increases the time it takes Internet users to browse and share information posted by bloggers and cyberactivists, and it limits the number of Internet users capable of accessing information posted by cyberactivists because not all Internet users know how to circumvent censorship. On the supply side, repressive measures and cyberattacks increase the cost of maintaining online visibility for activists and bloggers, thus driving down the volume of politi-

---

<sup>5</sup> "Pwn" is hacker jargon for compromising or controlling another system (without authorization).

cal discussion. The range of tools available to cyberactivists depends on the overall level of repression both offline and online.

This theoretical discussion shows that online activists and civil society actors are complementary, and the channels that foster offline mobilization serve as an important intervening variable that affects the relationship between online activism and the expansion of political space. Furthermore, since the range of tools for online mobilization is specific to the regime, the expansion of Internet freedom will affect political space via different channels; thus, similar Internet freedom programs may have varied results.

We begin our analysis by reviewing the existing literature on the Internet-democracy nexus and focus on cross-regime differences in the political uses of the Internet. We then explain the nature of political communication and its impact on social mobilization, and propose our own conceptual framework that examines how bloggers, netizens, and cyberactivists can create narratives that facilitate social mobilization and trigger subsequent transformation of political space. By focusing on how narratives emerge and diffuse online, we seek to understand who is empowered by access to the Internet and related technologies, how social groups can take advantage of online networking, and under what circumstances cybermobilization, which could bring about political change, may arise.

## **Is the Internet Transforming Politics? Where and How?**

To understand the relationship between Internet freedom and political processes in nondemocratic societies, it is helpful to examine first the mechanisms by which the Internet may have affected democratic processes in the United States and in other democracies. The theoretical and empirical literature on this subject has not reached an unambiguous answer because empirical findings are not always consistent with theoretical predictions and empirical results are also sensitive to such contextual factors as the level of development, diffusion of other technologies, and political culture. This section highlights the most important theoretical and empirical findings.

In democracies, the Internet affects political processes by lowering the cost of acquiring information. Since more-informed citizens are more engaged in politics, it was initially believed that the digital revolution would increase the political participation of marginalized groups who would take advantage of virtual and offline opportunities for political engagement.<sup>6</sup> The literature that emerged later, in the early 2000s, began emphasizing polarizing effects of online discourse. Since individuals only consume news that is consistent with their point of view, the Internet can produce “echo chambers” that reinforce existing differences in opinion, further polarizing the American public.<sup>7</sup>

However, empirical tests did not reveal the Internet having any large effects on attitudes or on behavior. The small difference in political attitudes between Internet users and nonusers found by earlier studies disappears when one accounts for the selection problem that arises because individuals who oppose the regime use Internet more frequently—perhaps because they do not believe news reported by the traditional media, which is tightly controlled by the government.<sup>8</sup> Thus, a positive correlation between anti-regime attitudes and Internet use disappears when statistical models account for nonrandom exposure to the Internet. Therefore, microlevel studies frequently fail to find differences in political attitudes. Similarly, studies that focused on political engagement did not find any differences between Internet users and nonusers.<sup>9</sup>

---

<sup>6</sup> Lawrence K. Grossman, *Electronic Republic: Reshaping American Democracy for the Information Age*, New York: Penguin Books USA Inc., 1995; Rabia Karakaya Polat, “The Internet and Political Participation: Exploring the Explanatory Links,” *European Journal of Communication*, Vol. 20, December 2005, pp. 435–459.

<sup>7</sup> Cass R. Sunstein, *Republic.com*, Princeton, N.J.: Princeton University Press, 2002; Eli Pariser, *The Filter Bubble: What Is the Internet Hiding from You?* New York: Penguin Press, 2011.

<sup>8</sup> Richard Davis and Diana Owen, *New Media and American Politics*, Oxford, England: Oxford University Press, 1998; Diana Owen, “The Internet and Youth Civic Engagement in the United States,” in Sarah Oates, Diana Owen, and Rachel Kay Gibson, eds., *The Internet and Politics: Citizens, Voters and Activists*, New York: Routledge, 2006.

<sup>9</sup> Shelley Boulianne, “Does Internet Use Affect Engagement? A Meta-Analysis of Research,” *Political Communication*, Vol. 26, No. 2, May 2009, pp. 193–211.

Another line of inquiry examined how the Internet can lead to sudden mobilization in nondemocratic regimes. The Internet can help foster “information cascades,” during which large segments of population change their attitude toward the regime. Such cascades occur because individuals hide their true preferences toward the regime, fearing repression. They become more willing to reveal those preferences when external shocks to the system provoke protests, which subsequently snowball as more and more individuals walk out on the streets.<sup>10</sup> The Internet can accelerate this snowball effect by increasing the speed with which information about protests is circulated.<sup>11</sup>

In addition to “information cascades,” the Internet can reduce the persuasiveness of the traditional state-oriented media. Persuasion occurs when individuals change their attitudes after receiving political messages. More-knowledgeable individuals are less likely to be persuaded because they apply critical analysis to the news reported by the state controlled media.<sup>12</sup> The Internet can undermine a regime’s ability to persuade citizens by making citizens more sophisticated consumers of news reported by state-controlled media.

The Internet also can make political space more inclusive by reducing the cost of mobilization. The success of social movements depends on mobilizing structures, opportunity structures, and the framing process. Mobilizing structures encompass mechanisms that facilitate the collective action. The Internet can reduce the cost of recruiting new members by enabling rapid diffusion of information about group activities. The Internet can also facilitate mobilization by promoting common identity among social media users, creating common points of reference, and reducing dependence on the traditional media for publicity.

---

<sup>10</sup> Timur Kuran, “Now Out of Never: The Element of Surprise in the East European Revolution of 1989,” *World Politics*, Vol. 44, No. 1, October 1991, pp. 7–48.

<sup>11</sup> David M. Faris and Patrick Meier, “Digital Activism in Authoritarian Countries,” in Aaron Delwiche and Jennifer Jacobs Henderson, eds., *The Participatory Cultures Handbook*, Oxford, England: Routledge: Taylor and Francis, Inc., 2012, p. 200.

<sup>12</sup> Barbara Geddes and John Zaller, “Sources of Popular Support for Authoritarian Regimes,” *American Journal of Political Science*, Vol. 33, No. 2, May 1989, pp. 312–347.



The effect of the Internet depends on opportunity structures that shape the social groups' ability to influence political processes. Opportunity structures encompass such factors as openness of the policymaking process, availability of allies, elite fragmentation, and repressive capacity of the regime.<sup>13</sup> An open political system presents multiple opportunities for state-society interaction and, thus, increases the probability that online mobilization has an impact on policy outcomes. Intra-elite competition might also affect a state's response to online mobilization because competing factions within the ruling coalition may join online activists to advance their own agenda within the regime. Domestic or international allies can supply online activists with organizational support and financial resources required for orchestrating effective collective action offline.

Quantitative studies support the hypothesis that opportunity structures affect how online mobilization manifests itself offline by showing how the relationship between the Internet and democratization is nonlinear. For example, earlier studies measured democratization using the Freedom House index or Polity scores, and found positive correlations between a country's level of democratization and the rate of Internet penetration.<sup>14</sup> These studies also showed that the strength of this relationship depends on the region of the world or the level of development. In more recent analysis, Meier focused on the number of political protests in 38 countries between 1990 and 2003 and found that the Internet is positively correlated with protests only in countries with a high rate of mobile phone usage.<sup>15</sup>

---

<sup>13</sup> R. Kelly Garrett, "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs," *Information, Communication and Society*, Vol. 9, No. 2, 2006, pp. 202–224; Patrick Meier, *Do "Liberation Technologies" Change the Balance of Power Between Repressive States and Civil Society?* Ph.D. thesis, Fletcher School of Law and Diplomacy, 2011, Chapter Two; Doug McAdam, John D. McCarthy, and Mayer N. Zald, eds., *Comparative Perspectives on Social Movements*, Cambridge, UK: Cambridge University Press, 1996.

<sup>14</sup> Michael L. Best and Keegan W. Wade, "The Internet and Democracy: Global Catalyst or Democratic Dud?" *Bulletin of Science, Technology and Society*, Vol. 29, No. 4, September 30, 2005, pp. 255–271; Jacob Groshek, "The Democratic Effects of the Internet, 1994–2003," *Communication Gazette*, Vol. 71, No. 3, April 2009, pp. 115–136.

<sup>15</sup> Meier, 2011, Chapter 3, footnote 16.

Although these studies are an extremely useful first step toward understanding the relationship between the Internet and democracy, they do not establish causality. The correlation between Internet penetration and democratization may be spurious if the factors that promote the diffusion of new technologies, such as a high standard of living, also promote democratization.

Philip Howard developed the most comprehensive account of nonlinear impact of the Internet in countries with a large Muslim population by examining the complex interplay among socioeconomic conditions and the rise of citizen journalism, online mobilization by political parties, and satellite. Howard distinguishes between democratization, which is equivalent to the collapse of an authoritarian regime, and democratic consolidation that occurs in the aftermath of the breakdown of an authoritarian regime and manifests itself in the deepening of democratic values and processes. He shows that a small country size and a relatively large active online civil society are favorable conditions for democratization, whereas the expansion of telecommunication infrastructure and diversification of economy that reduces a country's dependence on natural resources favor democratic consolidation.<sup>16</sup>

In a sequel study that focuses on the Arab Spring, Howard and Hussain argue that to understand the impact of new technologies on political processes, one should examine the factors that contribute to sudden politicization of these tools. They show that proliferation of mobile phones and expansion of Internet service contributed to the rise of vibrant online civic society in the Arab countries. The most active participants of this society were young residents of urban centers who rapidly became politicized after the success of Tunisia's revolution. The advent of new technologies forced the traditional media to reinvent itself to maintain the customer base; subsequently, al-Jazeera began disseminating news that contradicted the official policy line. The changes in the media and technological environment, combined with such socioeconomic characteristics as average per capita income,

---

<sup>16</sup> Howard, 2010.

unemployment rate, and the share of mobile phone users, all contributed to the wave of protests in the Arab region.<sup>17</sup>

A microlevel study by Nisbet et al. provides further evidence that the effect of the Internet is conditional on country-specific factors. Their analysis is based on survey data from 28 African and Asian countries and focuses on the level of support for democratic values. Using a multilevel model, they found that the difference in political attitudes between Internet users and others is greater in democratic countries and in countries with higher rates of Internet penetration.<sup>18</sup>

Large-N studies, overall, suggest that the relationship between the Internet and democratization is highly sensitive to a country's political, economic, and cultural environment. We then take this a step further by examining how opportunity structures affect the nexus between the Internet and political space.

## Cyberactivism in Democratic and Nondemocratic Regimes

The growing tendency of states to regulate online traffic, coupled with their use of traditional methods of coercion, produced subtle differences in political uses of the Internet between democratic and nondemocratic regimes. Table 2.1 compares liberal-type democracies with hybrid regimes such as Mubarak's Egypt and Russia, and then with the more authoritarian regimes as China, Syria, or Iran. Hybrid regimes, although they vary in the degree of openness and contestation, hold regular elections in which multiple parties compete for office, allow diversity of opinions, and pay lip service to democratic values. Authoritarian regimes exhibit much lower levels of contestation because political opposition is outlawed and no channels exist for meaningful citizens' participation in the policymaking process.

---

<sup>17</sup> Philip N. Howard and Muzammil M. Hussain, *Democracy's Fourth Wave? Digital Media and the Arab Spring*, Cambridge, Mass.: Cambridge University Press, 2013.

<sup>18</sup> Erik C. Nisbet et al., "Internet Use and Democratic Demands: A Multinational, Multi-level Model of Internet Use and Citizen Attitudes About Democracy," *Journal of Communication*, Vol. 62, April 2012, pp. 249–265, footnote 7.

**Table 2.1**  
**The Internet as a Mobilization Tool in Different Regimes**

Activity	Democratic Regime	Competitive Authoritarian or Hybrid Regime	Authoritarian Regime
<b>Participation Levels</b>			
Participation costs	Internet reduces recruitment and publicity costs for the opposition; online activism overlaps with other forms of political participation	Opposition's online presence is vulnerable to DDOS attack, and dissemination of information about events is limited to a narrow circle of online activists	Opposition is outlawed, information is circulated among atomized individuals; online activism rarely translates or overlaps with other forms of political participation; anonymity is required for self-expression
Collective identity	Internet fosters shared awareness among online group members	Internet encourages both shared awareness and counterculture	Internet fosters counterculture that uses the same symbols and terms of references
<b>Contentious Activity</b>			
Dissemination of information	Internet is used to circulate information to all users	Information is available to those who use circumvention technologies	Same as hybrid
<b>Organizational Issues</b>			
Decentralization of organizations	Internet makes existing social movements less hierarchical, allows for grassroots initiatives	Social movements originate online and then might migrate into the real world	Internet fosters spontaneous mobilization of tech-savvy Internet users
Movement entrepreneurs	Leaders' reputation stems from real-world activities	Leaders cultivate their reputation in the virtual world	Same as hybrid
<b>Framing Process</b>			
Create publicity and news coverage	Internet creates uniform opportunities for everyone to express views outside the mainstream	Internet provides alternative to the state-controlled media's point of view	Internet enables a handful of individuals to bypass state-controlled media

The categories in Table 2.1 follow the literature on social mobilization and focus on mobilization and framing stages of protests. In democratic societies, the Internet fosters the formation of new groups by making it easier to share information, enabling contributions at various effort levels, and reducing the need for organizational hierarchy.<sup>19</sup> Online groups evolve around information circulated via social media. These groups do not require large amounts of financial resources and can be sustained by modest levels of effort. Even small individual contributions can have a big impact because existing social tools effectively aggregate them into coordinated action.

In hybrid regimes, the opposition's online activities are vulnerable to DDOS attacks and surveillance by the authorities. In authoritarian regimes, the opportunities for online circulation of information are more limited because of filtering of online content. Further, coercion of activists narrows the set of actors who can use the Internet for political mobilization. Coercion encourages self-censorship. This shifts online discourse away from political matters toward other subjects.

Molding group identity is another channel by which the Internet can foster social mobilization. Unlike news stories told by professional journalists and carefully selected by editors, the language and the content of blog posts resonate well with social media users who are younger than newspaper audiences. Similarities between writers and readers contribute to common identities and facilitate a further discussion of the subject and information sharing. It thereby fosters common identity that makes collective action easier.<sup>20</sup> In authoritarian regimes, the Internet encourages the emergence of counterculture that serves as a surrogate to group membership, rather than promoting formation of groups. This counterculture can emerge as an attempt to circumvent censorship. For example, such euphemisms as "stroll" instead of "protest" or "May 35" for "June 4," 1989 (the date of the Tiananmen Square protest) became conventional in the lexicon of Chinese bloggers.

Contentious activity is another important strategy used by online activists. Participants of social movements can rely on sit-ins, demon-

---

<sup>19</sup> Shirky, 2008.

<sup>20</sup> Shirky, 2008, footnote 21.

strations, automobile rallies, and other forms of protests. Both in democratic and nondemocratic states, the Internet can expand the menu of protest methods available to activists. For example, social boycotts initiated offline can be made more effective by circulating information about them through email and Skype, and using mapping platforms to map affected areas.<sup>21</sup> In nondemocratic regimes, the likelihood that an online movement can evolve to offline protest is lower due to a higher probability of repression and the state's co-opting of movement leaders.<sup>22</sup>

The Internet can also transform the relationship between movement entrepreneurs (would-be leaders) and followers—again, depending on the regime's character. In democracies, social movement leaders frequently cultivated their reputation outside cyberspace by actively engaging in public life. Their name recognition offline provides credibility for their mobilization online. The opposite often holds in quasidemocratic regimes. Since opportunities for political participation are restricted, movement entrepreneurs frequently develop their reputation in cyberspace and use it for online and offline mobilization. For example, Alexey Dymovsky (the founder of White Ribbon, an anti-corruption movement in Russia) was an obscure police officer; he became an internationally known anti-corruption fighter after posting a YouTube video in which he accused his superiors of endemic corruption. Alexey Navalny (a leader of the 2011–2012 post-election protests in Russia) was initially renowned among only Russian bloggers. He cultivated his offline name recognition by running a series of online anti-corruption forums. Thus, cyberspace in hybrid states can become an incubator for future elites who lack access to the traditional media or who lack the financial resources to start a formal organization.

In authoritarian regimes, the cultivation of an online reputation is hindered by the anonymity of online discussion. Even as anonym-

---

<sup>21</sup> *Civil Resistance 2.0*, Google document, undated.

<sup>22</sup> See, for example, Floriana Fossato and John Lloyd with Alexander Verkhovsky, *The Web that Failed: How Opposition Politics and Independent Initiatives Are Failing on the Internet in Russia*, Oxford, England: Oxford University Press, Reuters Institute for the Study of Journalism, 2008.

ity protects online activists from being arrested by the authorities, it increases the cost of joining the protest. Authorities can use social media to attract the opposition, then cull it. For example, shortly after the outbreak of protests in Egypt, the Sudanese government put up a Facebook site calling for a demonstration in Khartoum; they then arrested everyone who appeared in the designated place and time.<sup>23</sup>

So, the relationship between the Internet and social mobilization depends on the governing environment. The tighter the state's control of the Internet and the more repressive the regime, the less likely it is that these technologies will have the same effect on political space as in a democratic regime. In a highly controlled environment, although the Internet can foster political discourse, fewer can participate in it. The more repressive the environment, the more tech-savvy those individuals must be. Online discussion in nondemocratic states will also take on a more mundane and private character, rather than a political or public one. Opportunities to cultivate name recognition online will be hindered by the anonymity required for surviving in the repressive environment.

Cross-regime comparison of online mobilization suggests that the menu of choices available to the opposition will be affected by the state's responses. Therefore, the debate about the effect of the Internet on political space should take into account the political context in which the Internet is used because context determines which functions can be used.

## **How and Where Can Internet Freedom (Technologies) Transform Political Space?**

In more pluralistic regimes, the Internet would foster social mobilization by enabling civil society activists to cultivate their reputation online, by expanding the menu of contentious activities, and by disseminating information that delegitimizes the regime. This section therefore examines in a greater depth the type of actors who might

---

<sup>23</sup> Meier, 2011, Chapter 4.

employ the Internet to bring about political change. These actors seek to promote a diverse set of objectives by capitalizing on online mobilization tools. This section examines how the diffusion of information online among these actors can bring about political change. We begin our analysis with the discussion of how and why information disseminated online may contribute to social mobilization. The literature on framing of political communication serves as the building block for our subsequent discussion of social mobilization.

### **Political Communication and Social Mobilization**

Public officials need media to project their power into society. In the United States, the President, administration members, and Congress members turn to media outlets to mobilize citizens behind their vision of the issues. In nondemocracies, incumbents rely on media to disseminate propaganda and limit the ideological boundaries of public deliberation. In both types of regimes, the mainstream media serves as a conduit of such political messages to the public. As Robert Entman illustrates, political communication occurs in cascades. News originates from the administration and passes down to an inner circle of the elite who share it with the mainstream media, which disseminates the news further to the general public. Each round of diffusion is shaped by the competition for frames.<sup>24</sup>

Framing affects how people perceive events. It entails “selecting and highlighting some facets of events or issues, and making connections among them so as to promote a particular interpretation, evaluation, and solution.”<sup>25</sup> For example, a public protest can be cast as “free speech” or a “threat to public order.” Frames affect an individual’s perception of events by evoking familiar images and concepts that simplify the cognitive process required for absorbing a message.<sup>26</sup> The diffusion of a political message from a state’s leaders to other tiers depends

---

<sup>24</sup> Robert M. Entman, *Projections of Power: Framing News, Public Opinion, and U.S. Foreign Policy*, Chicago: University of Chicago Press, 2004, p. 5.

<sup>25</sup> Entman, 2004.

<sup>26</sup> For a review, see Dennis Chong and James N. Druckman, “Framing Theory,” *Annual Review of Political Science*, Vol. 10, 2007, pp. 103–126.



on the congruence between the message frame and interpretive heuristics used by actors in each step down.<sup>27</sup>

Frames also perform an important function in social mobilization because they contribute to consensus building on movement goals. This process entails constructing “action-oriented sets of beliefs and meanings that inspire and legitimate the activities and campaigns of a social movement organization.”<sup>28</sup> These frames promote the common understanding of social conditions that need changing, social groups that would benefit from such changes, and proposed course of action.

Not all frames are equally persuasive and thus equally capable of attracting a large number of followers. The appeal of a frame depends on its consistency, empirical validity, and credibility, as well as the saliency of its issue. People tend not to resonate with frames based on claims that are internally inconsistent, cannot be substantiated by real-life examples, or made by speakers who are not perceived as trustworthy.<sup>29</sup>

Political competition between incumbents and opponents in democratic societies entails articulating competing frames with the goal of expanding popular support for their point of view. Mainstream media facilitates the diffusion of these competing messages.

Although social mobilization requires frames that resonate with the public, it still faces the ubiquitous collective action problem. Individuals, as rational actors, make their decisions based on a cost-benefit calculus. They participate in political rallies, sign petitions, volunteer

---

<sup>27</sup> Interpretive heuristics are cognitive shortcuts that individuals use to make sense of new information. Individuals compare any news to events they experienced in the past and rely on preexisting experience and knowledge to form opinions about new events. Accounts of events that use familiar reference terms are more likely to resonate with individuals than those that rely on concepts unfamiliar to the audience. Since socioeconomic status, race, gender, religious, and cultural background frequently influence interpretive heuristics, the government officials do not always select frames that can appeal to all citizens. The mainstream media facilitates the diffusion of government’s message by modifying the frames used by the state leaders to make them more congruent with the audience’s background. Entman, 2004.

<sup>28</sup> Robert D. Benford and David A. Snow, “Framing Process and Social Movements: An Overview and Assessment,” *Annual Review of Sociology*, Vol. 26, August 2000, p. 614.

<sup>29</sup> Benford and Snow, 2000.

at the polling stations, and even show up at the polls only when the benefits outweigh the costs. Social movements are hindered by the collective action problem because they seek to achieve collective goods that will be available to all movement members regardless of whether they marched in rallies, contacted their representatives, or donated money—hence, the proverbial free-rider problem.<sup>30</sup>

Individuals can be induced to participate in a collective action through pressure from their family members, friends, and neighbors. Peer pressure is an important factor in an individual's decision to vote, express voice, and engage in collective action because individuals care about how their behavior is perceived by people in their social networks.<sup>31</sup> Social networks are composed of different types of ties. Ties between close friends are considered to be stronger than the ones between colleagues or neighbors. Ties are formed and developed in the process of interpersonal interactions or as a result of membership in the same organization.

Not all ties have the same effect on political mobilization. People who belong to civic organizations are more likely to be persuaded to participate in a collective action by other association members than they are by their friends.<sup>32</sup> Those who do not belong to any organizations will be influenced by those with whom they have strong ties.<sup>33</sup>

---

<sup>30</sup> Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Goods*, Cambridge, Mass.: Harvard University Press, 1965.

<sup>31</sup> Alan S. Gerber, Donald P. Green, and Christopher W. Larimer, "Social Pressure and Voter Turnout: Evidence from a Large-Scale Field Experiment," *American Political Science Review*, Vol. 102, February 2008, pp. 33–48.

<sup>32</sup> Chaeyoon Lim, "Social Networks and Political Participation: How Do Networks Matter," *Social Forces*, Vol. 82, No. 2, December 2008, pp. 961–982.

<sup>33</sup> Henry E. Brady, Kay Lehman Schlozman, and Sidney Verba, "Prospects for Participants: Rational Expectations and the Recruitment of Political Activists," *American Political Science Review*, Vol. 93, No. 1, March 1999, pp. 153–168; Donatella della Porta, "Recruitment Process in Clandestine Political Organizations: Italian Left-Wing Terrorism," in Bert Klander-mans, ed., *International Social Movement Research*, Vol. 1, Greenwich, Conn.: JAI Press, 1999, pp. 155–169.

In democratic societies, interpersonal contacts have a larger impact on nonelectoral activities than on electoral ones.<sup>34</sup>

Social networks evolve around people with similar religious, cultural, ethnic, and socioeconomic backgrounds. Homophily, the tendency of like to gravitate to like, affects the strength of the ties between people in a network, with stronger ties likely among individuals with similar backgrounds.<sup>35</sup> Since strong ties increase the effectiveness of interpersonal communication, homophily implies that political mobilization will take place among people from similar social or economic strata.

### **Internet Freedom and Framing Process**

In the introductory chapter we defined Internet freedom as an unrestricted ability to post, to browse, and to share information in cyberspace. Understanding how these freedoms can transform political space requires identifying the causal mechanisms by which online mobilization translates into an action in political space. The relationship between these two may not have a single cause. As Henry Ferrell notes, anyone “who assumes a simple relationship between new technologies and political outcomes may be making very serious mistakes” because of “different mechanisms that might intervene between forms of communication such as the Internet and final political outcomes.”<sup>36</sup> Therefore we begin our analysis by defining those actors who post, browse, and share information online on a daily basis and then explaining when and how mobilization in cyberspace can evolve into collective action offline.

### **Key Actors in Cyberspace**

In countries where the Internet is unrestricted, any Internet user can browse, post, and share online information. Not everyone takes advan-

---

<sup>34</sup> Chaeyoon Lim, “Mobilizing on the Margin: How Does Interpersonal Recruitment Affect Citizen Participation in Politics?” *Social Science Research*, Vol. 39, No. 2, March 2010, pp. 341–355.

<sup>35</sup> For review, see Miller McPherson, Lynn Smith-Lovin, and James M. Cook, “Birds of a Feather: Homophily in Social Networks,” *Annual Review of Sociology*, Vol. 27, August 2001, pp. 415–444.

<sup>36</sup> Henry Farrell, “The Consequences of the Internet for Politics,” *Annual Review of Political Science*, Vol. 15, June 2012, p. 38.

tage of these freedoms because posting requires crossing the chasm from quietly consuming information to publicly sharing it. An individual's varied willingness to take advantage of the possibilities presented by the Internet and Web 2.0 technologies allows us to distinguish three sets of actors: bloggers, cyberactivists, and netizens.

Bloggers are those Internet users who crossed the chasm from quiet consumption to self-expression online on a myriad of topics ranging from cooking to political campaigning. Some of them discuss political issues, perhaps spending most of their time reposting and commenting on news published elsewhere. In so doing, they help Internet users navigate gigabits of data posted daily online and, at the same time, assure the factual accuracy of statements made in the mainstream media.<sup>37</sup>

A blogger's visibility is measured by the number of permanent hyperlinks between his or her blog and other blogs (hyperlinks are similar to citations in the printed media); the more frequently authors are cited, the more their name is recognized. Shirky, and more recently Farrell and Drezner, showed that ranking of blogs by hyperlinks follows a power law distribution. A handful of blogs attract a large share of links to emerge as information powerhouses; most blogs have few hyperlinks.<sup>38</sup>

Blogs also vary by their intended audience. As Ethan Zuckerman notes, some blogs have more links to the outside world than to the local online community. For example, bilingual blogs—such as one run by the prominent Tunisian blogger Subzero Blue and another called NoToTerrorism.com—bridge the Arabic blogosphere to the English-speaking community. Statistics on such “bridgeblogs” are not being collected, though.<sup>39</sup>

Since blogging takes time and is rarely paid for, some blogs are maintained collectively as a way of spreading the cost of updating them and providing opportunities for collective public self-expression and col-

---

<sup>37</sup> Laura McKenna and Antoinette Pole, “What Do Bloggers Do? An Average Day on an Average Political Blog,” *Public Choice*, Vol. 134, Nos. 1–2, January 2008, pp. 97–108.

<sup>38</sup> Shirky, 2008; Henry Farrell and Daniel W. Drezner, “The Power of Politics of Blogs,” *Public Choice*, Vol. 134, Nos. 1–2, 2008, pp. 15–30.

<sup>39</sup> Ethan Zuckerman, “Meet the Bridgebloggers,” *Public Choice*, Vol. 134, Nos. 1–2, 2008, pp. 47–65.

laboration on topics of similar interests. Collective blogging has been very popular in Iran; some blogs were launched by journalists whose newspapers were banned by the authorities.<sup>40</sup> Others were launched by feminist NGOs.<sup>41</sup> Still others emerged spontaneously as a result of coordination among bloggers who shared interests in sports, arts, or politics.<sup>42</sup>

The literature on the Internet frequently draws parallels between the blogosphere and what Jürgen Habermas called the “public sphere.” Habermas’s critical theory argues that the legitimacy of public institutions is rooted in citizens’ perception of them, and how that perception evolves during face-to-face deliberation of public matters. This theory influenced the first wave of political science literature on blogging and prompted arguments that online discourse approximates the Habermas deliberation process.<sup>43</sup> Later studies, however, began questioning similarities between these two by arguing that rather than bring diverse people together, the Internet actually encourages segregation and polarization through the formation of echo chambers in which discourse takes place among likeminded people.<sup>44</sup> This polarization hypothesis is not supported by empirical findings. Several studies showed that, in the United States, the Internet is better than face-to-face discussion at exposing people to dissenting points of view.<sup>45</sup> Studies of the Russian blogosphere also found a high level of interaction between users belonging to different ideological camps.<sup>46</sup>

---

<sup>40</sup> Emrooznews.blogspot.com, Arabic website, undated; Rooydadnews.blogspot.com, Arabic website, undated; Baamdadnews.blogspot.com, Arabic website, undated.

<sup>41</sup> Herlandmag.net, web blog, undated.

<sup>42</sup> Annabelle Srenberny and Gholam Khibany, *Blogostan: The Internet and Politics in Iran*, London and New York: I.B. Tauris, 2010, pp. 50–57.

<sup>43</sup> A. Michael Froomkin, “Habermas@Discourse.Net: Toward a Critical Theory of Cyberspace,” *Harvard Law Review*, Vol. 116, No. 3, January 2003, pp. 749–873.

<sup>44</sup> Cass Sunstein, “Neither Hayek nor Habermas,” *Public Choice*, Vol. 134, 2008, pp. 87–95.

<sup>45</sup> Matthew Gentzkow and Jesse M. Shapiro, *Ideological Segregation Online and Offline*, Cambridge, Mass.: National Bureau of Economic Research, NBER Working Paper No. 15916, 2010.

<sup>46</sup> Bruce Etling et al., *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization*, Cambridge, Mass.: Harvard University’s Berkman Center for the Study of

### **Bloggers, Netizens, and Political Space**

Bloggers can transform the information environment from one dominated by the elite to one in which information diffuses from the bottom: e.g., via posts of eyewitness accounts of events that rapidly spread throughout the blogosphere. The speed with which such news can be circulated destroys the government's first-mover advantage. In so doing, it attenuates persuasiveness of authorities' message as people delay forming opinions in the face of conflicting messages.<sup>47</sup>

The mainstream media frequently responds to such bottom-up information, particularly when it comes from prominent blogs. The bloggers' influence on the mainstream media stems from their expertise on the topic, professional connections to journalists, and their online reputation for providing impartial and accurate analysis.<sup>48</sup> Such bloggers can undermine the persuasiveness of official political communication and can affect the content of the mainstream media news.

### **Web 2.0 Users and Political Space**

Web 2.0 technologies such as Facebook, Flickr, and YouTube increased the role that a random Internet user can play in disseminating information. The distribution of links in social networks resemble hyperlinks among bloggers. Only a handful of users have a very high number of friends, and they become key nodes through which information is disseminated among other network members. These highly connected nodes shorten information paths and enable rapid diffusion of information among members who belong to different clusters and are not directly connected to each other.<sup>49</sup>

---

Internet and Society, October 2010.

<sup>47</sup> Lilach Nir and James N. Druckman, "Campaign Mixed-Message Flows and Timing of Vote Decision," *International Journal of Public Opinion Research*, Vol. 20, No. 3, August 2008, pp. 326–346.

<sup>48</sup> Nic Newman, "The Rise of Social Media and Its Impact on Mainstream Journalism: A Study of How Newspapers and Broadcasters in the UK and U.S. Are Responding to a Wave of Participatory Social Media, and a Historic Shift in Control Toward Individual Consumers," Reuters Institute for the Study of Journalism Working Paper, September 2009.

<sup>49</sup> Alan Mislove et al., "Measurement and Analysis of Online Social Networks," IMC 2007, San Diego, Calif., October 24–26, 2007.

Social media creates the illusion of face-to-face communication even as it enables strangers to share information. Unlike face-to-face discussion that takes place among friends, information pathways in cyberspace follow weak ties. As Eytan Bakshy notes, Facebook users are ten times as likely to forward a newsfeed to their Facebook friends when the link to this newsfeed comes from a weak tie. In contrast, when the link is shared by a strong tie, Facebook users are only six times as likely to share the link with others. Thus, news is shared primarily among those who do not regularly communicate with each other.<sup>50</sup> Social media creates another way for information to be disseminated, particularly among people from different strata who do not belong to the same social network. In so doing, it reduces some socioeconomic and cultural barriers to the diffusion of information.

Social media promotes the consensus-building that usually has to precede social mobilization. It changes the way frames are constructed by reducing the role of the leadership and by increasing people's input in identifying victims of policies, collecting empirical evidence, and narrowing the gap between frames and daily experience. YouTube and Flickr, along with such crowdsourcing platforms as Ushahidi (originating in Kenya), enable rapid collection and distribution of large volumes of data supporting movement causes. Frames that emerge during online discussion resonate better with daily experience of social media users than those constructed by movement leaders.

With social media, movements need not depend so much on mainstream media for coverage. When the mainstream media covers events, it can create a counterframe to make a movement's message less persuasive. Social media helps movement leaders reach potential followers directly.

Because online discussion can yield multiple frames, the skewed distribution of links in the blogosphere facilitates convergence to a single one. Farrell and Drezner note that heavily hyperlinked bloggers can facilitate coordination on a common frame by becoming "focal points" for blog readers.<sup>51</sup> In Schelling's classic formulation of the con-

---

<sup>50</sup> Eytan Bakshy, "Rethinking Information Diversity in Networks," Facebook web page, January 17, 2012.

<sup>51</sup> Farrell and Drezner, 2008.

cept, in the absence of information, two people seeking each other out at a time and location undefined in New York City will naturally gravitate toward noon at Grand Central Station as a logical place to meet up.<sup>52</sup> Netizens are more likely to adopt frames articulated on popular blogs because they expect other Internet users to do the same.<sup>53</sup>

### **Online Activists and Political Space**

Online activists can use the Internet to ignite political transformation. Unlike bloggers or social media users, who may not even vote or participate in demonstrations, political activists turn to the Internet to attract popular attention to an action aimed at unseating the incumbent regime. In Egypt and Syria, these actors fought a war on two fronts: the one in the cybersphere with their mobile phones and digital cameras, the other on the streets of Damascus or Cairo.<sup>54</sup> They crossed the line between the virtual and the real world.

Online activists frequently turn to the Internet to increase popular awareness of their cause, especially when the mainstream media are silent about their activities. Online activists usually serve as “political entrepreneurs” who undertake offline mobilization and reach out to the population not connected to the Internet. They are usually affiliated with opposition parties, NGOs, or civil society organizations and are willing to undertake popular mobilization to win a public office or attain some other payoff that exceeds the costs and risks associated with social mobilization.

---

<sup>52</sup> Thomas Schelling, *The Strategy of Conflict*, Cambridge, Mass.: Harvard University Press, 1960.

<sup>53</sup> Farrell and Drezner, 2008, pp. 15–30.

<sup>54</sup> Luke Harding, “Syria’s Video Activists Give Revolution the Upper Hand in Media War,” *Guardian*, August 1, 2012.



## Internet Freedom and the Modes of Transformation of Political Space

In the introductory chapter we defined political space as an arena in which input from citizens is continually being received and taken into account by the governing authorities. We also showed how the size of a society's political space is defined by the right to vote along with freedom of expression and assembly. Political space becomes broader when more people can exercise these rights. Free voting means a secret ballot, a meaningful alternative to the incumbent and fair elections. Freedom of assembly may be guaranteed in law but effectively curtailed by requirements to obtain authorization to hold a meeting. Similarly, government's censorship of traditional media, coupled with targeted repression of independent journalists, can curtail freedom of expression guaranteed by one or another constitution. Political space deepens with enhancements in how people can exercise these freedoms—e.g., enabling a meaningful vote not only in the national elections but also in local ones, not only recognizing freedom to assemble but also fostering the development of such institutions as political parties and competitive elections that facilitate preference articulation.

Broadening and deepening political space requires the coordination of activities among activists, bloggers, and netizens in cyberspace and concurrent coordination of events offline. Offline mobilization, however, depends on structural factors such as the fragmentation of the elite, economic conditions, the distribution of power between the regime, and the society. The opportunities for social mobilization will be affected by the openness of the political system, fragmentation within the elite, and the state's ability to repress protesters. These factors affect people's cost-benefit calculus when it comes to deciding whether to join or merely watch protesters on the streets.

Internet freedom cannot eliminate these structural constraints directly, but it can broaden the coalitions of actors who vote, sign petitions, join protest rallies, and participate in other offline events. Information online is more likely to be spread among people who are linked by weak ties, which can broaden the coalitions of actors involved in a political action by more widely accessing and sharing information.

Information flows more quickly among people who belong to different clusters, both offline and online. Such information can spark online deliberation that cuts across traditional offline divides; it can thus contribute to the evolution of frames that resonate with a broader set of actors, who in their turn will pass those frames to their friends during face-to-face discussions. In so doing, the Internet and social media can broaden political space by facilitating consensus, thereby building on movement goals. Online discourse enables multiple actors to engage in narrative formation. Frames that emerge as a result of this deliberation will resonate with a broader set of actors. Social media also increases the speed with which these frames can be circulated online and then diffused face-to-face within the same social network. Offline interpersonal communication affects an individual's decision to vote, to sign petitions or file complains, to join social movements or protest rallies. Thus, offline and online social networks complement each other. The latter are more valuable for reducing socioeconomic, religious, or ethnic barriers to diffusing the information and creating frames that resonate with a broader set of actors. Offline social networks affect whether frames that originate online bring about a visible political action.

The type of political regime and the level of Internet penetration will influence the synergy between online mobilization and offline political action. The more the Internet is restricted to those of the same social actors, the narrower the set of actors becomes who can be mobilized by social frames that originated online. In countries with limited Internet, there will likely be some disconnect between movement frames that originated online and interpretive heuristics used by those without Internet access. Thus the narrative will resonate with fewer people.

Regime type can affect how online mobilization translates into outcomes in political space by shaping offline strategies. The suppression of political parties, interest groups, and civil society that takes place in an authoritarian regime deprives online activists of a power base from which to launch offline mobilization. It forces them to rely on clandestine networks and other informal institutions, such as ethnic-based groupings, private social networks, and religious organizations to mobilize people. Tight state censorship of the traditional media either completely blocks coverage of events that could ignite online dis-

course or it changes reference frames to minimize their popular appeal. At the same time, filtering of online traffic lowers the probability that links to the political discourse can reach the sites of prominent bloggers because authorities can block frames that challenge the validity of the official storyline before they are acquired by too many netizens. The authorities can also coerce those who started this discourse. These constraints make the relationship between online and offline mobilization more tenuous, and it makes political action more spontaneous by dint of being less organized.

Repressive measures affect the probability of success with which voice, vote, or assembly spheres can be expanded. The transformation of political space along these three dimensions therefore will not be symmetric. For instance, in Iran, the Internet strengthened voice for some social groups without transforming other dimensions. Feminist movements, for example, have successfully used the Internet to attract public attention to domestic violence, to build coalitions against the law allowing temporary marriages, and to lobby for changes in the birthrights to citizenship law. The rise of blogosphere also fostered the growth of a popular culture inconsistent with traditional Islamic norms.<sup>55</sup> The effect of the Internet on voting in Iran has been more controversial. Although it helped the Green Movement to circulate images documenting police brutality against detainees that delegitimized the regime, protests failed to make elections fairer or more competitive. Greater scrutiny of online traffic in the aftermath of the protests made anti-state online activism less feasible.<sup>56</sup>

Similarly, in China the Internet contributed to the expansion of voice rather than vote or freedom of assembly. Yongnian Zheng shows that online movements were more successful in China when citizens spoke against specific government actions rather than for the overthrow of the Communist Party. This outcome was due to internal competi-

---

<sup>55</sup> Srenberny and Khibany, 2010, pp. 35–41.

<sup>56</sup> Saeld Golkar, “Liberation or Suppression Technology? The Internet, the Green Movement, and the Regime in Iran,” *International Journal of Emerging Technologies and Society*, Vol. 9, No. 1, 2011, pp. 50–70; Babak Rahimi, “The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran,” *Communication Review*, Vol. 14, No. 3, 2011, pp. 158–178.

tion between the party's soft- and hard-liners. When online movement challenged the nature of the regime, these two wings of the party united to fight the challenger. When online movement did not threaten the survival of the party, the liberal faction strategically exploited popular discontent to advance its own agenda within the party.<sup>57</sup>

The dimensions along which the Internet can transform political space will depend on the distribution of power between the society and the regime, the extent of fragmentation within the regime, and other opportunity structures. The expansion of voice and assembly spheres is frequently associated with liberalization; e.g., the process by which individuals and social groups become better protected from arbitrary or illegal rights committed by the state or the third parties. The expansion of the vote may bring democratization that is accompanied by the expansion of rules and procedures of citizenship to a larger set of actors.

## Conclusion

This chapter showed that when discussing the Internet-democracy nexus, it is important to keep in mind that the set of actors who browse, share, and post information online is heterogeneous. Online mobilization entails coordinated action on the part of bloggers and netizens, cyberactivists, and Web 2.0 users or Internet users. Bloggers and netizens are those Internet users who crossed the line from passively consuming online information to actively producing it. They contribute to online mobilization by attracting Internet users' attention to the specific government action or policy and to build online consensus about the nature of problem, its causes, and the most suitable course of action. Cyberactivists are those who employ the Internet to mobilize others behind a specific cause or to advance a specific agenda. These actors frequently participate in construction of narrative and also bridge online discourse with offline organizational resources and civil society groups without whose support online mobilization

---

<sup>57</sup> Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China*, Stanford, Calif.: Stanford University Press, 2008.

cannot manifest itself offline. Internet users and Web 2.0 users contribute to online mobilization by disseminating narrative through their online and offline social networks.

The range of mobilization options available to cyberactivists depends on the oppressiveness of the regime. The more oppressive the regime and the tighter the Internet censorship, the narrower the set of netizens that can be reached by cyberactivists and the more difficult it is for cyberactivists to mobilize the society because they frequently lack organizational resources. The probability that online mobilization will manifest itself offline also depends on the structural constraints that shape state-society interaction and can include such factors as intra-elite fragmentation, support of other nondemocratic allies, and pressure from the international community.

## Cyberactivists, Social Media, and the Anti-Mubarak Protests in Egypt

---

A mass uprising in Egypt started on January 25, 2011, and in just 18 days brought an end to the 30-year rule of President Hosni Mubarak. The media quickly dubbed the uprising “the Facebook Revolution,” after the social media website on which many of the young activists met and organized their activities.<sup>1</sup> Many analysts argued that the Internet had provided an essential space for activists to circumvent state repression, become informed about the regime’s crimes, and build a community of like-minded individuals who, by coming together, gained the confidence needed to take risks collectively that they had been unwilling to run individually. These cyberenthusiasts point out that Mubarak demonstrated the degree to which he felt threatened by social media by incurring the steep economic costs associated with closing the Internet. At the time, Egyptian activists also attributed much of the credit for their success to communications technologies,<sup>2</sup> although they were themselves surprised by the huge response to their call for protests. As one prominent activist blogged, “This is becoming the region’s first telecommunication civil war. Our Internet and smartphones are weapons [the government] won’t allow us to have.”<sup>3</sup>

---

<sup>1</sup> Abigail Houslohner, “Is Egypt About to Have a Facebook Revolution?” *Time*, January 24, 2011.

<sup>2</sup> Xiaolin Zhuo, Barry Wellman, and Justine Yu, “Egypt: The First Internet Revolt?” *Peace Magazine*, Vol. 27, No. 3, July–September 2011, p. 4.

<sup>3</sup> Maryam Ishani, “Foreign Policy: Scramble to Silence Partner Protests,” *NPR*, January 28, 2011.

After the revolution, many cyberenthusiasts began pointing to Egypt as a powerful example of what Internet freedom could achieve in the right circumstances. Cyberenthusiasts, noting what had been achieved in Egypt, began to advocate for additional U.S. Internet freedom efforts in the region. They believed that the peaceful toppling of the regime in Egypt could be duplicated elsewhere if the power of social media were harnessed wisely. In addition, the impact of social media in Egypt seemed to vindicate an Internet strategy focused on deepening the abilities of already well-connected netizens. It seemed that even in Egypt, a country with little Internet penetration, social media was able to help galvanize a large and successful public uprising.

Critics of the cyberenthusiasts and their interpretation of the Egypt case emerged quickly after the revolution. These critics questioned the centrality of social media to the revolution's success, warning that cyberenthusiasts were hyping its importance. Some discounted the mobilizing role of technologies altogether, pointing out that people, not tools, make revolutions. MSNBC correspondent Richard Engel reflected this sentiment, stating: "This didn't have anything to do with Twitter and Facebook. . . . This had to do with people's dignity, people's pride."<sup>4</sup> Other skeptics claimed that social media played a fairly unimportant role in comparison to other factors, such as the Muslim Brotherhood's participation, the enthusiasm generated by the preceding revolution in Tunisia, the military's disillusionment with Mubarak, and the impact of other mobilization tools such as SMS (short messaging services) and satellite media.<sup>5</sup> Other naysayers were even more critical, arguing that social media may have harmed the revolution by letting the government monitor activists and by permitting Facebook users a free ride and the feeling that they were participating without incurring the costs of civil disobedience.<sup>6</sup>

---

<sup>4</sup> Frank Rich, "Wallflowers at the Revolution," *New York Times*, February 6, 2011.

<sup>5</sup> William Rugh, *Arab Mass Media: Newspapers, Radio, and Television in Arab Politics*, Westport, Conn.: Praeger, 2004.

<sup>6</sup> Navid Hassanpour, "Media Disruption Exacerbates Revolutionary Unrest: Evidence from Mubarak's Natural Experiment," paper presented to the American Political Science Association Conference, August 7, 2011.

This chapter agrees with cyberenthusiasts. Without social media, Mubarak's overthrow would not have occurred. That does not mean other factors were not significant or necessary; they most certainly were. Yet we do not see social media as just one of many important tools. Social media was key because it was the only means for the largely young, urban, and secular activists who organized the January 25 revolution to mobilize mass action, maintain a sustained connection with a mass audience, and circumvent a state security crackdown. This factor is significant because, despite the fact that the Muslim Brotherhood was the largest and most organized opposition group, it was unwilling to mobilize mass action against the state, as were most of the officially recognized, yet often weak, secular parties. This young, liberal opposition was the only group (or more accurately, "grouping") willing to call for massive protests. Their ability to use the Internet to place a large cadre of committed, cyberconnected supporters on the streets was critical for inspiring unconnected and depoliticized Egyptians to join the demonstrations. The secularists lacked other venues for organization, such as mosques, which have historically allowed the Muslim Brotherhood to mobilize supporters without the use of social media. So while one can imagine a revolution starting somewhere else without Facebook, it is hard to see how the one that happened in Egypt could have developed absent that technology.

The mobilizing success of the revolution was not due to activists' efforts alone. It was helped by the permissive Internet environment that the Mubarak regime established to connect Egypt to the global economy. As discussed in the next chapter on Syria, the far more brutal and organized Assad regime has been able to blunt the impact of social media through high levels of Internet censorship and a much greater willingness to use violence to repress cyberactivism and other types of political activism. In Egypt, on the other hand, the Internet before the revolution was not filtered, and the regime lacked technical mechanisms to selectively target particular websites and users. Only at the last moment, when the regime realized that it was in grave danger, did it take the extreme steps of shutting off the Internet entirely and blocking mobile servers.



To fully appreciate the critical role of social media, it is important to understand how it was responsible for causing the first domino to fall in a series of events that brought down the regime. Social media was the key to secularist mobilization; only after the secularists mobilized large numbers of Egyptians on the first day of protests was the Muslim Brotherhood pressured to join the uprising. Without the Brotherhood, building a sustained, cross-cutting movement with an organized ground game would have been nearly impossible for the young organizers, who had little more than a cyberconnection with their core constituency. And finally, it was only when confronted by sustained and growing opposition that the Egyptian military began to consider defection, the coup de grace for the Mubarak regime.<sup>7</sup> In sum, while the role of the military, the actions of the Muslim Brotherhood, and the participation of a large swath of the Egyptian public were all critical to the removal of Mubarak, this chapter will argue that the forging of these necessary conditions would not have been possible but for the use of social media by the largely liberal organizers of the January 25 demonstrations.

This chapter begins by describing some common arguments concerning the significance of social media in the Egyptian Revolution. The following section will then lay out and provide detailed support for the three propositions on which the chapter's argument is based:

- that social media was the only method available to liberal protest organizers that could bring out a huge number of Egyptians for the January 25 demonstrations
- that the young, secular opposition was the only force willing and able to foment such a large and direct challenge to the state
- that the army let Mubarak fall because the demonstrations were large, widespread, and sustained, thus demonstrating that remaining with Mubarak would result in major reputational costs to the military.

---

<sup>7</sup> Maha Azzam, "Egypt's Military Council and the Transition to Democracy," *Middle East and North Africa Programme, Briefing Paper 2012/02*, London: Chatham House, May 2012, p. 2.

The chapter concludes with a restatement of the main argument and the analytic contribution that this case study makes for the consideration of Internet freedom policy.

## Social Media's Significance: The Debate

For a country where nearly 30 percent of the population is illiterate,<sup>8</sup> and 22 percent live below the national poverty line,<sup>9</sup> Egypt's rapid adoption of cybertechnology has been impressive. Internet access did not become available in Egypt until 1993, first to members of Egypt's academic community, then to the public at large in 1995.<sup>10</sup> Usage expanded significantly after 2002 when government initiatives subsidized computer costs and introduced cheaper dial-up rates: Only 2.72 percent of the population used the Internet in 2002, but the penetration rate had grown to 11.7 percent by 2005.<sup>11</sup> According to Egyptian government statistics, Internet penetration rates nearly doubled between 2007 and 2010, from 13.75 percent to 30 percent, due in large part to greater mobile Internet access.<sup>12</sup> A month prior to the uprising, it was estimated that 8.6 million users were accessing the Internet through mobile devices.<sup>13</sup>

Social media use has expanded rapidly as well, especially after the introduction of Arabic Facebook in 2009. Between January 2009 and

---

<sup>8</sup> U.S. Central Intelligence Agency (CIA), *The World Factbook—Literacy*, web page, statistics for 2010, undated.

<sup>9</sup> World Bank, World Development Indicators and Global Development Finance, web page, 2011.

<sup>10</sup> Sanja Kelly and Sarah Cook, eds., *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*, Freedom House, 2011, p. 119.

<sup>11</sup> International Telecommunications Union, *Reports* web page, undated.

<sup>12</sup> United Nations Conference on Trade and Development, *ICT Policy Review: Egypt, Switzerland*, United Nations Publication, 2011, p. 2.

<sup>13</sup> United Nations Conference on Trade and Development, 2011, p. xiii.

late 2010, Facebook went from 900,000 users to nearly 5 million.<sup>14</sup> Today, Egypt ranks 19th in the world Facebook ranking, with 11.5 million users (more than 14 percent of the population). Twitter use is nearly impossible to verify, given that many users do not provide location information to avoid surveillance. One estimate placed the total number of Egyptian users in the first quarter of 2011 at 1,131,204, although only a small portion of these are active posters.<sup>15</sup>

### Cyberenthusiasts

Cyberenthusiasts quickly dubbed the overthrow of Mubarak as the “Facebook Revolution.” They attributed a wide variety of important communication and associational functions to social media, which they claimed resulted in a mass uprising against the Egyptian regime. Most of these assumed functions are very difficult to verify and are derived from theories proliferating in the literatures on collective action and social movements. Some claim that social media was important because it provided a source of information outside of state controls that raised awareness about regime corruption and police brutality. This information circulated widely on Facebook, YouTube, and Twitter, but some cyberenthusiasts downplay this function, pointing out that the media was comparatively free in Egypt, and, as summarized by sociologist Zeynep Tufekci, “People already know whether they’re happy or unhappy, the problem is collective action.”<sup>16</sup> To this end, many cyberenthusiasts emphasize the significance of social media’s ability to facilitate communication among large groups of people. There is general agreement within the cyberenthusiast camp that possibly the greatest impediment to collective action is the isolation of would-be participants. They base their decision to publicly oppose the regime on their assessment of how many other people feel

---

<sup>14</sup> Merlyna Lim, “Clicks, Cabs, and Coffee Houses: Social Media and Oppositional Movements in Egypt, 2004–2011,” *Journal of Communication*, Vol. 62, No. 2, 2012, pp. 231–248.

<sup>15</sup> Racha Mourta and Fadi Salem, “Civil Movements: The Impact of Facebook and Twitter,” *Arab Social Media Report*, Dubai School of Government, Vol. 1, No. 2, 2011, p. 16.

<sup>16</sup> Andy Greenberg, “Mubarak’s Digital Dilemma: Why Egypt’s Internet Controls Failed,” *Forbes*, February 2, 2011.

the same way and their willingness to take similar actions.<sup>17</sup> Only then can potential participants roughly gauge the government's ability to suppress.<sup>18</sup> An Egyptian activist highlighted this point, stating, "Before this social media revolution, everyone was very individual, very single, very isolated and oppressed in islands . . . But social media has created bridges, has created channels between individuals, between activists, between even ordinary men, to speak out, to know that there are other men who think like me. We can work together, we can make something together."<sup>19</sup> Finally, other social media proponents point out that while communication is important, it was social media's ability to form shared identities, or a socially connected Internet public,<sup>20</sup> that created the motivation and durable bonds needed for Egyptians to break the fear barrier and engage in risky collective action.<sup>21</sup>

### Cyber-Killjoys

What brought Hosni Mubarak down was not Facebook and it was not Twitter. It was a million people in the streets, ready to die for what they believed in.

— *New York Times* columnist Thomas Friedman<sup>22</sup>

A persistent refrain in the "Facebook Debate" is that social media does not make revolutions, people do.<sup>23</sup> The prevalence of this argument is

<sup>17</sup> Kuran, 1991, pp. 7–48.

<sup>18</sup> Zeynep Tufekci, "As Egypt Shuts Off the Net: Seven Theses on Dictator's Dilemma," Technosociology website, January 28, 2011.

<sup>19</sup> John Pollock, "Streetbook: How Egyptian and Tunisian Youth Hacked the Arab Spring," *MIT Technology Review*, September/October, 2011.

<sup>20</sup> Lim, 2012, p. 234.

<sup>21</sup> Dave Parry, "It's Not the Public Internet, It Is the Internet Public," Profound Heterogeneity website, February 4, 2011.

<sup>22</sup> Thomas Friedman, commencement speech delivered at Tulane University, New Orleans, May 12, 2011.

<sup>23</sup> See Adam Ostrow, "What the Egyptian Revolution Taught al-Jazeera About Digital," *Mashable Social Media*, March 5, 2011; Tarak Barkawi, "The Globalisation of Revolution,"

curious since it is a false dichotomy: Twitter and Facebook do not act independent of people, and the significance of social media and the actions and motivations of Egyptians are not mutually exclusive. What may account for the prevalence of black-and-white thinking concerning social media's impact is that people do not want to credit a medium typically used to spread frivolous gossip and funny cat videos with shaping an event as historic as the downfall of a dictator. While we may never know why the contributions of protesters and social media are presented as an either/or proposition, it has been clear that the more Western-media touted Egyptian activists as cyber-rock stars, and the more that the number of martyrs grew, so too did public pressure to disassociate social media from explanations for the revolution. Even demonstration organizers who had previously stated that social media was key to the uprising's success backed off of these claims in later months and shifted the spotlight to the sacrifice of the martyrs.

Yet below the surface of this starkly presented dichotomy lies a more common claim that merits consideration. It is that grievances are the main cause of collective political action because they are what inspire people to seek change. However, just because something is a necessary condition for collective action does not mean that it is sufficient, or that other conditions are not equally necessary. While one cannot imagine people taking to the streets without something bothering them, many studies have found that people often remain deeply aggrieved without ever acting collectively to change their shared predicament.<sup>24</sup> Egyptians have been angry for years about social inequalities, widespread corruption, political repression, continued emergency laws, and Mubarak's maneuvering to ensconce his son in power.<sup>25</sup> Likewise, events immediately prior to the revolution—most notably the fall of El-Abadine Ben-Ali—began to ratchet up enthusiasm for Mubarak's removal. Yet barriers to association—government policies

---

*al-Jazeera*, March 21, 2011; Evgeny Morozov, *Frontline* interview, February 22, 2011.

<sup>24</sup> Doug McAdam, *Political Process and the Development of Black Insurgency 1930–1970*, Chicago: University of Chicago Press, 1982; Olson, 1965; Charles Tilly, *From Mobilization to Revolution*, Reading, Mass.: Addison-Wesley, 1978.

<sup>25</sup> "Egypt: Seeds of Change," *al-Jazeera*, February 9, 2011.

and societal divisions—kept most Egyptians depoliticized and focused on their discrete concerns. The next section outlines how social media provide activists the tools to overcome these obstacles and channel collective grievances into large-scale action on the first day of the demonstrations—setting in motion a series of events that culminated in Mubarak’s fall.

Another argument against social media’s importance is that the majority of Egyptians do not use the Internet or social media. Cyber-skeptics find it damning that only around 20–25 percent of the population (depending on the source) had access to the Internet at the time of the revolution, the assumption being that since “the masses” (75–80 percent of the population) had no access to the Internet, cyberactivism could not be responsible for mobilizing the huge demonstrations that brought down the regime.<sup>26</sup> Penetration percentages, however, belie the magnitude of the Internet’s impact in a country as populous as Egypt: Even the lowest percentage figure of 20 percent equates to more than 16.7 million people—more than the entire population of the Netherlands.<sup>27</sup> Furthermore, experts assume that reported access percentages underrepresent the actual number of users because a large number (estimates vary) access the web through Internet cafes, libraries, and Internet clubs where a single connection serves multiple users.<sup>28</sup>

The more relevant issue, however, is not Internet use in the general population but rather Internet use by the organizers of the January 25 protest and their closest associates. If the masses, no matter how aggrieved, rarely take action on their own, then the key to why collective action took place lies with the motives and capabilities of the organizers. An entire subfield of political science, social movement theory, is based on this very assumption.<sup>29</sup> And when the lens is narrowed to examine the organizers of the Egyptian revolution, it is clear that they

---

<sup>26</sup> Rich, 2011.

<sup>27</sup> CIA, *CIA World Factbook—Country Comparisons, Population*, web page, statistics for 2012, undated.

<sup>28</sup> “Internet Filtering in Egypt,” *OpenNet Initiative*, August 6, 2009.

<sup>29</sup> Steven M. Buechler, *Social Movements in Advanced Capitalism*, Oxford, England: Oxford University Press, 2000.

relied heavily on the Internet and social media.<sup>30</sup> It has been well documented that the original call for the January 25 protest was posted on Facebook and that demonstration organizers (April 6 Youth Movement, “We Are All Khaled Said,” “My Name is Khaled Mohamed Said,” Revolutionary Socialists, National Association for Change), their closest associates (political bloggers, human rights advocates, labor organizers), and many of the front-line “shock troops” (Muslim Brotherhood youth and soccer Ultras<sup>31</sup>) all used social media to communicate with other like-minded, cyberconnected Egyptians. Cyber-skeptics point out that the young, urban, and largely secular organizers of the revolution were not reflective of the Egyptian masses, the implication being that they could not, therefore, connect with enough people to mobilize large numbers.<sup>32</sup> However, they shared characteristics with a much larger swath of the Egyptian public than they are typically credited for and they connected with what was the most important demographic for launching an uprising: Egyptian youth.

Young people have historically been on the front lines of urban revolts, due in large part to their “biographic availability,” namely “the absence of personal constraints that may increase the costs and risks of movement participation, such as full-time employment, marriage, and family responsibilities.”<sup>33</sup> Sixty percent of Egypt’s population is under 30,<sup>34</sup> and at the time of the revolution, a quarter of Egyptian youth were unemployed.<sup>35</sup> The unemployment rate does not include

---

<sup>30</sup> “Timeline: Egypt’s Revolution,” *al-Jazeera*, February 14, 2011.

<sup>31</sup> Wael Ghonim, *Revolution 2.0*, Boston, Mass.: Houghton Mifflin Harcourt, 2012, p. 145.

<sup>32</sup> See Barkawi, 2011; and Evan Conway, “How Wired Are Egyptians?” *PBS Newshour*, January 31, 2011.

<sup>33</sup> Lim, 2012, p. 234.

<sup>34</sup> Marga Peeters, *Demographic Pressure, Excess Labour Supply and Public-Private Sector Employment in Egypt: Modeling Labour Supply to Analyze the Response of Unemployment, Public Finances and Welfare*, MPRA Paper No. 31101, 2011, p. 7.

<sup>35</sup> Heba Handoussa, Ashraf el Araby, Hoda el Nemr, Zeinat Tobala, Ghada Barsoum, Mohamed Ramadan, Safaa el Kogali, et al., *Egypt Human Development Report 2010, Youth in Egypt: Building Our Future*, United Nations Development Program and the Institute of National Planning, 2010, p. 82.

the 58.5 percent of Egyptians between 18 and 29 years of age who are out of the labor force and not looking for work.<sup>36</sup> What also made Egyptian youth more susceptible to political mobilization than other demographic strata or earlier generations of youth was that they were less invested in the government than their parents' generation. Traditionally, Arab regimes have used government employment as a means to pacify the population and quell dissent. Because public sector jobs are respectable and secure, older generations of Egyptians have tenaciously held on to them, and over time this trend has blocked entrance by younger Egyptians. Today, even though 30–40 percent of all Egyptian employees work in the public sector,<sup>37</sup> only 18.5 percent of public-sector employees are between 20 and 35 years of age.<sup>38</sup> Another shared characteristic of Egyptian youth is their use of the Internet: Egyptians 35 years of age and under constitute 78 percent of all Internet users.<sup>39</sup> They are also the greatest users of social media. On the eve of the revolution, Egypt had 4.6 million Facebook users, 89 percent of whom were under 35.<sup>40</sup> Hence, while more Egyptians do not use the Internet than do, a large portion of Internet users are characterized as having time on their hands and less to lose by participating in a revolt, and as being less invested in the state.

Another argument made by cyber-skeptics is that other, more accessible, sources of information had a greater impact on Egyptian mobilization than social media.<sup>41</sup> Here we will deal with arguments pertaining to the significance of independent/satellite media, while

---

<sup>36</sup> Handoussa et al., 2010, p. 38.

<sup>37</sup> A rough estimate of the total number of public-sector employees is 6 million. Peeters, 2011, p. 12.

<sup>38</sup> Handoussa et al., 2010, p. 126.

<sup>39</sup> Arab Republic of Egypt, Ministry of Communications and Information Technologies, *The Future of Internet Economy in Egypt: A Statistical Profile*, May 2011, p. 10.

<sup>40</sup> Sarah Birke, "After the Revolution, Older Egyptians Take the Leap into Facebook," *National*, March 7, 2011. As of October 16, Facebook has 11,804,060 Egyptian users, 86.1 percent of whom were under 35 years of age.

<sup>41</sup> Rugh, 2004.



arguments concerning other forms of communication will be taken up later in the chapter.

Many Egyptians reported receiving information about the demonstrations from independent television channels. This is not surprising, considering that satellite TV penetration is estimated at 43 percent.<sup>42</sup> Further, like Internet use, it is probably underreported because many public venues (cafes, restaurants, clubs) have satellite hook-ups and some Egyptians watch online.<sup>43</sup> And yet, far from being a competing source of influence during the revolution, independent media channels amplified the influence of the Internet.<sup>44</sup> Well before the revolution, independent media outlets had increasingly relied upon social media as a source for news.<sup>45</sup> For some news organizations, such as al-Jazeera, this reliance quickly evolved into outright dependence when the Mubarak regime closed their Cairo offices and cracked down on their coverage of the uprising.<sup>46</sup> To circumvent government measures, the channel solicited video postings, blog posts, and tweets recounting events on the streets. Social media's enhanced influence was also a result of explicit strategies on the part of Internet activists, who targeted satellite and independent news organizations as a means of spreading their message and controlling the narrative of the revolution. As a result of satellite television's reliance on social media and activists' outreach strategies, it is impossible to untangle the independent impact of broadcast media from social media. It is also difficult to know the extent to which watching footage of the demonstrations diminished

---

<sup>42</sup> Jeffery Ghannam, *Special Media in the Arab World: Leading Up to the Uprisings of 2011*, Washington, D.C.: Center for International Media Assistance, February 3, 2011, p. 25.

<sup>43</sup> J. Hunter Price, "The New Media Revolution in Egypt: Understanding the Failures of the Past and Looking Toward the Possibilities of the Future," *Democracy and Society*, Vol. 7, No. 2, Spring 2010, p. 3.

<sup>44</sup> Mohamed Nanabhay and Roxane Farmanfarmaian, "From Spectacle to Spectacular: How Physical Space, Social Media and Mainstream Broadcast Amplified the Public Sphere in Egypt's 'Revolution,'" *Journal of North African Studies*, Vol. 16, No. 4, December 2011, p. 574.

<sup>45</sup> Miriyam Aouragh and Anne Alexander, "The Egyptian Experience: Sense and Nonsense of the Internet Revolution," *International Journal of Communication*, Vol. 5, 2011, p. 1,351.

<sup>46</sup> "Defiant al-Jazeera Asks Egyptian Audience for Help," *CBS News*, January 31, 2011.

Egyptians' fear thresholds and motivated them to take to the streets. It could have been the key to mobilization, or it could be that word of mouth—marchers calling onlookers down from their balconies, and the Muslim Brotherhood's joining the demonstrations on January 28—was largely responsible for the explosion in demonstration participants. As this chapter demonstrates, establishing the critical role of social media in the Egyptian uprising is not dependent upon measuring the relative impact of satellite media and various other mobilization tools.

## How Social Media Bridged Egypt's Mobilization Gaps

### Social Media Was the Opposition's Only Tool for Reaching and Mobilizing a Mass Base

Under Mubarak, the political system in Egypt was as authoritarian as the regime was censorious. Numerous regulations restricted the Freedom of Speech, and especially the Freedom of Assembly and Association. Under the Emergency Laws in place since Mubarak came to power in 1981, insulting the president, defaming Egypt, distributing leaflets or posters, and blocking traffic were all offenses punishable by jail time and fines.<sup>47</sup> The state had extraordinary powers to decide who could participate in politics, as well as their room for maneuver. When Egyptians stepped outside of these bounds, they faced harassment at minimum, and often arrest and torture. The formation of new parties was rare because all applicants had to be licensed by the Political Parties Committee, which was controlled by members of the ruling National Democratic Party (NDP).<sup>48</sup>

Parties and other political groups had difficulty building constituencies because opportunities for raising their profile were severely curtailed. Public demonstrations required a rarely granted license from the Ministry of Interior, and when they did occur, they were quickly cor-

<sup>47</sup> Freedom House, "Egypt: Freedom in the World 2010," undated.

<sup>48</sup> Carlyle Murphy, *Passion for Islam: Shaping the Modern Middle East, The Egyptian Experience*, New York: Scribner, 2002, p. 159.

doned off and dispersed by security forces before they could generate significant public attention. Most media outlets were state-controlled; even those in private hands were highly influenced by the regime. The result was little coverage for any group other than the NDP (an Islamist exception is described below).

Prospects for political reform improved slightly in 2005 due to U.S. pressure, but experienced sharp reversals soon afterward. That year, Mubarak held Egypt's first multicandidate election for president, yet soon after winning the election (always a foregone conclusion), he imprisoned his main challenger, *al-Ghad* (Tomorrow) Party leader Ayman Nour, for three years on politically motivated charges of forgery.<sup>49</sup> Also in 2005, the Muslim Brotherhood—an illegal, yet tolerated, Islamist party with deep roots in Egyptian society whose candidates run as independents—captured 20 percent of parliamentary seats in what was widely considered one of Egypt's fairest elections (a low bar, to be sure). To ensure that they would never achieve that level of success again, state security forces arrested 1,200 Brotherhood members, including eight of its candidates, prior to the 2010 parliamentary elections.<sup>50</sup> The elections were marred by violence and electoral fraud, a common occurrence that over the years had turned most Egyptians off of political participation.

Though all political groups faced repression by the state, the Muslim Brotherhood in many ways fared better than liberal/secular activists. Granted, the group was denied legal status due to its religious platform, and typically bore the brunt of state violence, but contrary to many accounts, they were not considered a severe threat to the regime. Rather, the Muslim Brotherhood was on the whole a tolerated opposition presence that served the interests of the state. Hoping to further its social agenda and one day secure legal status, the Brotherhood was often willing to work with Mubarak. During the 1980s and early '90s, the Muslim Brotherhood helped the state discredit radical Islamists and marginalize secularists, and in exchange was allowed access to the

---

<sup>49</sup> Freedom House, "Egypt Freedom in the World 2010," undated.

<sup>50</sup> "Muslim Brotherhood Withdraws from Egyptian Elections," *Telegraph*, December 10, 2010.

political arena.<sup>51</sup> The presence of an Islamist opposition also helped Mubarak dampen demands for political reform that would have constituted a direct threat to his hold on power. Many Coptic Christians, Egyptian secularists, and Western allies agreed with state claims that the Mubarak regime was Egypt's only hope for fending off an Islamist takeover.<sup>52</sup> Another reason the Muslim Brotherhood was not considered a direct threat to the regime is that much of what the organization wanted—greater influence over personal status laws, education, religious issues, artistic expression, etc.—could be accommodated within an NDP-controlled political system. Even when individual members of the Muslim Brotherhood joined with liberal/secular opposition forces in the 2004–2006 *Kefaya* (Enough) Movement—aimed at pressing for political reform and opposing the possible succession of Mubarak's son Gamal—democracy never replaced the organization's ultimate goal, the Islamization of Egyptian society.

The real existential threat to the Mubarak regime was the potential formation of a popular, liberal, political movement with democracy as its primary objective. Such a movement's *raison d'être* would require the removal of Mubarak. In addition, whereas the regime's allies were sometimes reluctant to openly question the use of state violence against Islamists, Western nations were less likely to stand by if brutal force were used against a democratic movement. Harsh U.S. criticism of the imprisonment and vilification of liberal activists, such as American University in Cairo professor Saad Eddin Ibrahim and *al-Ghad* Party leader Ayman Nour, demonstrated that blatant oppression of Egyptian democrats might ultimately put U.S. assistance to Egypt at risk.

On top of the restrictions that all political organizations faced, Egypt's liberal opposition had additional hurdles. To deter the rise of a serious liberal opposition movement, Mubarak tried to satisfy upper-class liberals by enacting liberal economic reforms, in the hope that

---

<sup>51</sup> Julie E. Taylor, "Prophet Sharing: Strategic Interaction Between Muslim Clerics and Middle Eastern Regimes," *Journal of Islamic Law and Culture*, Vol. 10, No. 1, April 2008, p. 51.

<sup>52</sup> Khairi Abaza, *Egyptian Legislative Elections: A Reading of the Results*, Policy #1061, Washington, D.C.: The Washington Institute, December 12, 2005.

greater economic opportunity would peel them off the growing, yet nascent, movement for political reform. Opportunities for liberals to recruit and organize supporters paled in comparison to those available to Islamists. Islamists were able to use state institutions for building their constituencies. Above all, the Brotherhood had the mosques, where they could deliver sermons, run schools, and distribute charity.<sup>53</sup> Though Egypt's mosques were ostensibly under the control of the Ministry of Religious Endowments, there were too many of them for the state to actively oversee even if it had wanted to, and cracking down on Brotherhood activities, especially their charity work inside the mosques, would be politically costly. Hence, mosques were a protected outreach venue for the Brotherhood.<sup>54</sup> Likewise, Muslim Brotherhood members or sympathizers were often featured in religious television programming on state-controlled networks. Though these programs avoided overtly political topics, they tended to "affirm the Islamist outlook that there must be an 'Islamic point of view' on all issues, or an 'Islamic solution' to them."<sup>55</sup> Liberal activists, in contrast, had no built-in base for raising their profile or connecting with a broader audience. Their entire reason for being was political change. There was no other significant characteristic or issue that bound them as a group, or that could naturally bring them together with larger segments of the Egyptian population and present nonobvious opportunities for recruitment. Everything that liberals did was inherently political and risked running afoul of state restrictions on freedom of expression and assembly. Opportunities for establishing officially recognized liberal or secular parties were extremely limited, in part because a requirement for party formation was the uniqueness of the political platform.<sup>56</sup> To prevent

---

<sup>53</sup> Salwa Ismail, *Rethinking Islamist Politics*, New York: I.B. Tauris, 2006, p. 30.

<sup>54</sup> Mona Eltahawy, *Frontline* interview, February 22, 2011.

<sup>55</sup> Jakob Skovgaard-Petersen, "Islamic Fundamentalism in Arab Television: Islamism and Salafism in Competition," in Ulrika Martensson, Jennifer Bailey, Priscilla Ringrose, and Asbjorn Dyrendal, eds., *Fundamentalism in the Modern World, Vol. 2*, New York: I.B. Tauris, 2011, p. 270.

<sup>56</sup> Shahram Akbarzadeh and Benjamin MacQueen, *Islam and Human Rights in Practice: Perspectives Across the Ummah*, New York: Routledge, 2008, p. 80.

formation of new parties that could build a following, the state instead continued to recognize several moribund leftist and nationalist parties that had lingered for decades, yet were little more than clubs where “graybeard” elites fought out their personal rivalries.<sup>57</sup> Party formation restrictions forced liberal reformers to retreat to the realm of advocacy NGOs. While the NGOs have been able to raise awareness of issues that liberals care about by advocating on behalf of specific groups, they were “ill equipped to mobilize a much broader set of constituencies around the larger goal of regime change.”<sup>58</sup> By abandoning the political realm, they undercut prospects for a viable democratic movement.

Despite these impediments, liberal activists had been openly protesting regime policies for more than a decade prior to the revolution. They began with protests on international issues (Palestine in 2000 and Iraq in 2003) that were coordinated with the Muslim Brotherhood. During the *Kefaya* Movement from 2004 to 2006, liberal opponents of the regime led a series of protests against Mubarak’s domestic policies. After that, judges and lawyers demanded judicial independence, and liberal activists began documenting and protesting electoral fraud. Labor strikes became a persistent part of Egypt’s political landscape.<sup>59</sup> But despite the mounting protests, none of these efforts flowered into a mass-based movement that could seriously challenge the regime.

Even early attempts to mobilize opposition using social media failed to generate widespread participation. The April 6 Movement, the group that spearheaded the January 25 demonstrations, took its name from the date in 2008 on which it supported a strike at the al-Mahalla textiles factory. The movement started a Facebook campaign encouraging Egyptians to strike in support of the workers. Though the page attracted 70,000 members, the results were disappointing, in part because the observable effects were limited—if Egyptians independently decided to stay home that day, no one would know that their

---

<sup>57</sup> Murphy, 2002, p. 160.

<sup>58</sup> Vickie Langohr, “Too Much Civil Society, Too Little Politics?” in Marsha Pripstein Posusney and Michele Penner Angrist, eds., *Authoritarianism in the Middle East*, Boulder, Colo.: Lynne Rienner, 2005, pp. 193–195.

<sup>59</sup> Marc Lynch, “Watching Egypt (But Not on al-Jazeera),” *Foreign Policy*, January 25, 2011.

decision was a political act of protest.<sup>60</sup> Another reason there was little lasting impact from the online action was that there were no shared connections between the groups that were targeted. The intent of this online campaign was to foster cooperation between the population on the Internet—young, educated, and urban Egyptians—and industrial laborers in the factories.<sup>61</sup> Yet, Egypt's deep social and economic divisions made it difficult for Egyptians to unite on issues and form cross-cutting cleavages (the one exception being the issue of religion, which the Muslim Brotherhood exploited to full advantage). The protest ended without establishing a strong, continuing, connection between the two groups. Even the labor activists shared little in common with the young online activists championing their cause and there was minimal coordination between them.<sup>62</sup>

The Facebook group “We Are All Khaled Said” succeeded in bridging this gap. It fostered a cross-cutting connection, uniting Egyptian youth from many segments of society over their disgust with regime repression and police brutality. Khaled Said was a 28-year-old entrepreneur who was dragged out of an Internet café by police and brutally beaten to death on June 6, 2010. The police claimed that Said was a drug dealer, but it emerged later that the package of drugs he supposedly swallowed had been forced into his mouth. Gruesome pictures of his battered corpse circulated widely on the web, juxtaposed with photos of Said when he was alive, appearing young, handsome, and full of potential. The news about Khaled Said's death spread rapidly in cyberspace (Figure 3.1).

Several days later, a Facebook page “We Are All Khaled Said” was created by Wael Ghonim, the Google executive who sought to create a forum that would first foster empathy with Khaled Said, followed by incremental measures aimed at defining the group and its common beliefs, identifying who was responsible (Mubarak and the police),

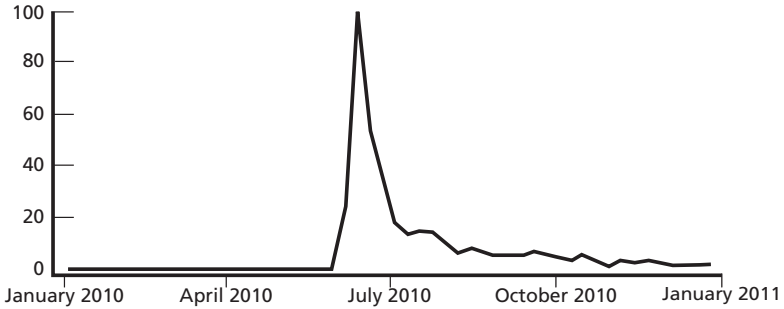
---

<sup>60</sup> Ghonim, 2012, pp. 35–36.

<sup>61</sup> Sonia Verma, “How a Brutal Beating and Facebook Led to Egyptian Protests,” *Globe and Mail*, January 28, 2011.

<sup>62</sup> “POMED Notes: Economics, Youth, and Technology in the ‘Arab Spring,’” *Project on Middle East Democracy*, March 23, 2012.

**Figure 3.1**  
**Frequency of Google Search Queries for Key Word “Khaled Said” in Egypt**



SOURCE: Google Trends.

NOTE: The y-axis indicates how many searches have been done for a particular term, relative to the total number of searches done on Google over time.

RAND RR295-3.1

and finally, presenting opportunities for users to channel their outrage through collective political action.<sup>63</sup> On the eve of the revolution, “We Are All Khaled Said” was said to have more than 500,000 members.<sup>64</sup> By starting off as simply a cathartic venue for expressing shock and disappointment, it was much more effective than the April 6 Movement or other liberal opposition forces at reaching a broad audience. Likewise, by starting off apolitical, encouraging participation through postings and survey responses, and slowly introducing an activist prism through which to view events in Egypt, “We Are All Khaled Said” had greater success in politicizing the members it reached. The group organized several silent protests in remembrance of Said during the summer of 2010 that drew large numbers and avoided being broken up by police. Energized after the Ben-Ali government in Tunisia was brought down by public demonstrations on January 14, 2011, “We Are All Khaled Said,” in conjunction with the April 6 Movement and other organizations, posted an online invitation for Egyptians to protest against regime and police brutality on January 25. More than 100,000 con-

<sup>63</sup> Lim, 2012, p. 242.

<sup>64</sup> Verma, 2011.



firmed their attendance.<sup>65</sup> Though the precise number is not known, tens of thousands participated in the marches with approximately 10,000 eventually collecting in Cairo's Tahrir Square.<sup>66</sup> The size of the protests shocked organizers and participants alike.

It is hard to know whether the joint success of "We Are All Khaled Said" and the April 6 Movement came from building a "shared identity,"<sup>67</sup> fostering "individual empowerment,"<sup>68</sup> or creating an "Internet public,"<sup>69</sup> though each of these arguments for how social media creates social capital makes intuitive sense. Regardless, we do know that, for the reasons outlined above, activist youth—and for that matter, Egypt's liberal opposition as a whole—failed to attract a broad cross-section of Egyptians to their cause up until that time, and that "We Are All Khaled Said" helped them overcome associational barriers and enhance the appeal of their message. The site presented a space where Egyptians angry with the regime could "congregate" and interact, while the case for collective action was slowly rolled out in a manner that was accessible and meaningful to a larger segment of Egyptian society. In other words, only through social media were organizers able to make and maintain contact with such a large group of people. Text messages, telephone conversations, and word of mouth all played roles in mobilizing individuals to join the demonstration, but these "tools" could not manage contact among a large group of people for a sustained period of time.

Social media also played a critical role in helping organizers outwit security forces long enough to make joining the revolution seem less risky. Facebook and Twitter were used to deceive state security

---

<sup>65</sup> Ghonim, 2012.

<sup>66</sup> Maggie Michael, "Three Dead as Egyptian Protesters Clash with Police," *Washington Times*, January 25, 2011.

<sup>67</sup> Hao Jiang and John M. Carroll, "Social Capital, Social Network and Identity Bonds: A Reconceptualization," in *Proceedings of the Fourth International Conference on Communities and Technologies*, University Park, Pa.: Penn State University, 2009, pp. 51–60.

<sup>68</sup> Eltahawy, 2011.

<sup>69</sup> Parry, 2011.

about meeting locations.<sup>70</sup> As the number of those accepting the invitation increased, the state security officials monitoring Facebook likely gained greater confidence in the information's accuracy and devised their suppression strategy accordingly. Organizers then used protected communication channels to contact key participants and arrange different gathering places.<sup>71</sup> While those gathered at the "secret" locations were a limited number of core activists, the ruse made it possible to circumvent state security and have groups enter Tahrir Square from unexpected directions, ultimately overwhelming security personnel. These diversion tactics significantly reduced the perceived risks of demonstrating. During past political protests, cordons of security personnel scared Egyptians off from supporting activists. On January 25, the absence of security forces at many of the starting points encouraged observers to set their fears aside and get caught up in the excitement. By the time they marched closer to Tahrir Square and encountered the police, they were already part of—and likely invested in—their group.

More tech-savvy activists also used circumvention technologies—downloadable from the web—to protect themselves from the prying eyes of state security. Though used by only a handful of activists, web journalists, and bloggers, software such as Tor helped Internet users remain anonymous and allowed them to navigate around state censorship efforts. Initially, this technology was not used at all in Egypt because the Mubarak regime did not filter the Internet. According to an Administrative Court's ruling, blocking websites was an unconstitutional infringement upon the freedom of expression. Even in cases of adult websites, there were disagreements within the Mubarak administration on whether blocking those sites was feasible. Although in 2009 the court ruled that these sites should be blocked, the Ministry of Communications and Information Technology, responsible for enforcing this decision, criticized it as impossible to enforce on technical grounds. Instead, the authorities controlled online content by selec-

---

<sup>70</sup> Pollock, 2011.

<sup>71</sup> Jon Jensen, "Behind Egypt's Revolution: Youth and the Internet," *Global Post*, February 13, 2011.

tively intimidating and prosecuting online journalists who crossed the “red line” and openly criticized the authorities.<sup>72</sup>

The fairly censorship-free environment explains the low demand for Tor software in the first half of 2010 even among activists. Demand began to pick up during summer 2010, about the time of Khaled Said’s murder, but did not exceed 500 users per day. The first spike in the number of computers directly connected to the Tor network was observed during the last two weeks of August 2010 when rumors spread that Mubarak was soon planning to hand power to his son, Gamal Mubarak.<sup>73</sup> This number ebbed during protests that took place in September and rose slightly during the November legislative elections, but the numbers on the whole remained low. They rose once the revolution started, reaching 2,400, but plummeted abruptly when the Internet was shut down by Mubarak on January 27, 2011, blocking access to Twitter and Facebook. The second spike occurred on May 29, 2011, four days after the court charged Hosni Mubarak with murder and imposed a \$90 million fine on him for shutting down mobile services and the Internet. Figure 3.2 indicates that even in a country like Egypt, with a relatively free Internet, a small segment of Internet users (about 0.012 percent) still use Tor, and the demand for it peaks at the time of sensational and controversial news. For Egyptian activists, it was one of the many ways that web-based technologies helped them outmatch security forces.

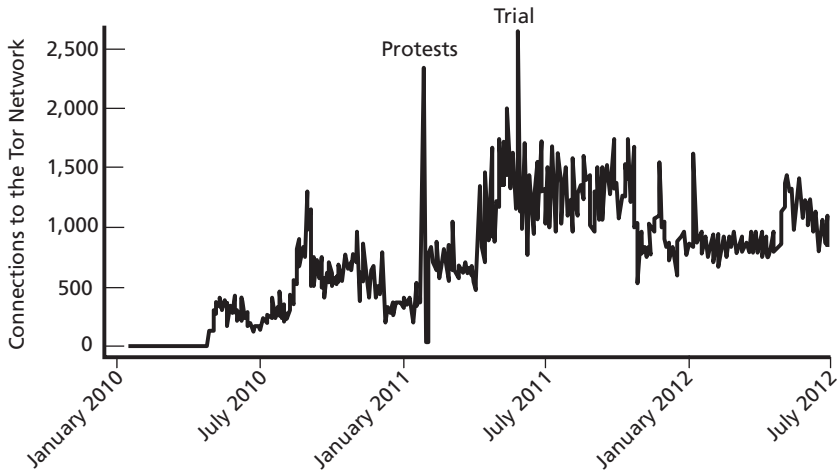
The argument that social media needed to reach all walks of Egyptian life to have been a significant factor in Mubarak’s downfall has no substantive support or theoretical merit. All the organizers needed was to get a large number of people onto the streets, for a prolonged period of time, without suffering a police crackdown. Those who discount social media’s impact and say that what brought people into the streets was watching events on al-Jazeera and being called down by demonstrators passing under their balconies, are putting the cart before the horse: Without social media there would have been no demonstrators

---

<sup>72</sup> Kelly and Cook, 2011.

<sup>73</sup> Avi Issacharoff, “Mubarak Signals Egypt Succession by Taking Son to Washington,” *Haaretz*, August 31, 2010.

**Figure 3.2**  
**Number of Connections from Egypt to the Tor Network**



SOURCE: Tor Project.

RAND RR295-3.2

passing by and no event for al-Jazeera to report. Social media brought a critical mass of people into the streets; once they were in place, then word of mouth, text messaging, telephones, and media coverage were able to exponentially grow the number of participants.

### **No Other Opposition Force Would Confront the State with Mass Action**

That liberal youth relied on social media to reach, and mobilize, a large number of protesters does not in and of itself demonstrate why social media was a necessary component of Mubarak's ultimate downfall. After all, other groups joined the protests, and participation by Egypt's largest political group, the Muslim Brotherhood, was critical for sustaining the demonstrations and expanding them to cities throughout Egypt. But while Brotherhood participation was a key factor in the revolution's success, it would not have happened without tens of thousands of Egyptians first taking to the streets without the Brotherhood. There was no indication that the Brotherhood had any intention of ever organizing a mass action targeting the legitimacy of the regime, thus

leaving Egypt's liberal youth groups as the only ones willing to fire the first volley.

Some of the reasons the Muslim Brotherhood was unlikely to act against the regime have already been mentioned: The group's desire to become a recognized party, plus their interest in Islamizing Egyptian society—with or without changes to the political system—made them hesitant to rile the regime and undermine these efforts. They also valued the gains from cooperation with the regime. Brotherhood attacks against regime opponents often coincided with greater Brotherhood participation in the political system and with Mubarak's periodic enthusiasm for promoting the Islamic character of Egypt.<sup>74</sup> While the Brotherhood's desire to further its interests caused its leaders to avoid direct confrontation, so too did their fear of regime reprisals. Members already suffered considerable hardships during the regime's periodic crackdowns, including the seizure of assets, harassment of family members, imprisonment, and torture.

Once the demonstrations were announced, the Muslim Brotherhood had additional reasons to avoid entering the fray. Though organizers tried to ensure that the protest was perceived as an "Egyptian" event, the main organizers were primarily liberal youth. Like much of Egyptian society, status within the Brotherhood is strongly based on seniority, and younger members are typically sidelined and silenced. Senior leadership was "dismissive" of the young organizers' ability to mobilize a large crowd, especially by using the Internet.<sup>75</sup> Also, the Muslim Brotherhood was not keen to further the interests of secular liberals, a group whose objectives—especially their social policies—are in many ways less desirable to the Brotherhood than Mubarak's. The Brotherhood's interest lies in creating a more Islamic society, and while political conditions made it advantageous for them to embrace democracy, inclusiveness, and a civil state—all of which are also trumpeted by liberals—they have not presented reasons for why these would be

---

<sup>74</sup> Eltahawy, 2011.

<sup>75</sup> Charles Sennott, "Inside the Muslim Brotherhood, Part 1," Special Report: The Muslim Brotherhood's Role in the Egyptian Revolution, *Frontline* and *Global Post*, February 21, 2011.

their goals, beyond political expediency. Hence, they had little interest in joining an action that could empower their rivals.

But once the January 25 demonstrations exceeded everyone's expectations, the costs of remaining on the sidelines quickly began to mount. Muslim Brotherhood youth who had become increasingly frustrated by the organization's passivity toward the regime independently joined with liberal groups to organize the demonstrations, and pressured the Brotherhood's leadership to support them. The undemocratic nature of the organization was an increasingly divisive issue and there were fears that if the Brotherhood was seen as supporting the regime, there would be a serious schism and members would peel off to join other groups.<sup>76</sup> Also, if the Muslim Brotherhood remained on the sidelines, especially once casualties began to mount, they risked losing their credibility as an opposition group and being labeled lackeys of the regime, undermining decades of meticulously cultivating their reputation as the pious opposition. And finally, at the end of the day on January 25, the Interior Ministry issued a statement blaming the Muslim Brotherhood for the demonstrations, signifying that sitting out the protests was no guarantee of avoiding government retaliation.<sup>77</sup> As a result, on January 28, three days after demonstrations began, the Brotherhood's leadership officially announced its participation.<sup>78</sup>

The entrance of the Muslim Brotherhood provided the critical mass, organizational skill, and logistical infrastructure needed to sustain the demonstration in Cairo and in cities throughout Egypt. Members established checkpoints to deter pro-government thugs from entering the square, and when security was breached, they were the

---

<sup>76</sup> These fears were in part borne out when a large number of youth and some veterans, such as Abdel Moneim Abul Futouh, left the Brotherhood to start their own organization after Mubarak's downfall. Some experts blame the Brotherhood's hesitation to join the January 25 demonstration for the split because the delay provoked "autonomous political activism" among its members, something the organization actively attempts to suppress. Serene Assir, "The Muslim Brotherhood's Youth: An Independent Course to Revolution?" *alakhbar english*, November 28, 2011.

<sup>77</sup> "Timeline: Egypt's Revolution," 2011.

<sup>78</sup> Karim Fahim, "Violent Clashes Mark Protests Against Mubarak Rule," *New York Times*, January 26, 2011, p. A1.

“muscle on the frontlines.”<sup>79</sup> They established emergency clinics to treat the wounded and provided food, water, microphones, and blankets. As the demonstrations grew and state security’s brutal tactics and Mubarak’s statements hardened protesters’ resolve, the Egyptian military was faced with a difficult decision: force Mubarak out or move against the people.

### **Military Considered Defection Only After Demonstrations Grew and It Was Forced to Either Shoot or Remove Mubarak**

Before the demonstrations became sustained and widespread, there were no indications that the removal of Mubarak was seriously considered by the Egyptian military, even though the military’s frustration with the Mubarak had been growing for years.<sup>80</sup> From the time of Nasser, the Egyptian military had been the preeminent institution in the country and the main pillar of regime support, but Mubarak had increasingly nurtured the ascension of the NDP, much to the chagrin of the generals. Crony capitalists and NDP insiders close to Gamal Mubarak, the president’s son (and presumed heir), were exercising greater influence over the direction of the country while at the same time lining their pockets through corrupt business deals. Hosni Mubarak appeared to be grooming Gamal to succeed him, which would have made him the first leader of the Egyptian Republic to not have a military background.<sup>81</sup> The possibility of hereditary succession was unpopular with the military and with most Egyptians, but the military was likely most concerned with the loss of influence sure to come with Gamal’s ascension.

Removing Mubarak presented more than just an opportunity for the military to gain lost ground; if officers could get out in front of the demonstrations and establish military control, they could secure many other benefits. They could extend the military’s control over national security issues and prevent civilian oversight of military affairs by the

---

<sup>79</sup> Sennott, 2011.

<sup>80</sup> Steven Cook, “Political Instability in Egypt,” contingency planning memorandum no. 4, Center for Preventative Action, Council on Foreign Relations, August 2009, p. 1.

<sup>81</sup> Azzam, 2012, p. 3.

next regime. They could also expand or consolidate their business holdings and personal perks. And, siding with the protesters could win the generals considerable public support by freeing them of their association with Mubarak, who had become a growing liability.

But while the benefits of defection may have sweetened the pot, the timing of the military's removal of Mubarak suggests that their decision was strongly influenced by the dynamics of the demonstrations, rather than a belief in the protesters' aims or a compelling interest in exploiting events to strengthen the military's position. Police and government thugs started beating protesters on January 26, and even though the violence escalated in the following days, the army never stepped in to protect the protesters. Even after uniformed police left the streets on January 30 and the only security forces available were the military, they sat on the sidelines, protecting key assets such as hotels, banks, and some government buildings (though, notably, not the NDP headquarters, which protesters torched on January 28). To scare Egyptians into abandoning the protests, the military brass spoke frequently about the danger of looters and other criminals, suggesting that Egyptians go home to distance themselves from the brutality of "thugs." On January 30, a fighter jet buzzed Tahrir Square—a gesture whose meaning was confusing, but by all accounts certainly was not friendly. The military later claimed that the jet was signaling enforcement of a curfew. On January 31, even with army tanks lining the Square, the military once again did not intervene as pro-government protesters—many of whom were paid thugs—entered Tahrir on camels and horses and began a pitched battle with protesters. After the protesters successfully repelled the attack, forcing Mubarak supporters to flee, it was clear that the protests could only be put down through brutal force, and that the military was the only force that could make that happen.

Indeed it was only after the so-called "Battle of the Camel"—the height of the protests—that the military began to take a more conciliatory tone with the protesters. Two reasons for the generals' change of heart were likely the growing consensus that that tide had turned irreversibly against the regime, and because they feared defections within the rank and file—and that soldiers might not follow orders if forced to



shoot.<sup>82</sup> Though more positive toward the protesters, the generals sent mixed messages that many believe indicated divisions within the officer corps. Finally, on February 12, 2012, the military forced Mubarak's resignation, but as the series of events indicates, it was a difficult decision reached only after the size and momentum of the protests eliminated many of their other, less radical options.

## **Conclusion: What This Means for the Study of Social Media**

Social media was pivotal to the success of the Egyptian uprising because it was the sole means that Mubarak's foes had that could bring thousands of Egyptians into the streets. The massive display of discontent on January 25 set in motion the regime's downfall, spurring the Muslim Brotherhood's entrance into the protests and the military's defection from the regime. Even if bringing Egyptians into the streets on January 25 was social media's only contribution to the uprising, that would make it key to the fall of Mubarak.

However, social media made a much broader contribution to events in Egypt than simply mobilizing demonstrators on the first day of the demonstrations. While cyberenthusiasts' broad claims about social media are difficult to affirm, this chapter points to a number of examples of social media's other notable contributions. As discussed throughout the chapter, there was a symbiotic relationship between social media and the independent media outlets covering the uprising. These media outlets reached a high percentage of the population, and a broad international audience, allowing them to present a competing narrative of what was occurring on the streets to the one presented by the Mubarak regime. By "informing" broadcast media, social media activists were able to influence the level of foreign pressure on the Mubarak regime despite having few direct connections to foreign

---

<sup>82</sup> Yasmine Fathi, "Egypt's 'Battle of the Camel': The Day the Tide Turned," *Abramonline*, February 2, 2012; Azzam, 2012, p. 3.

decisionmakers, and they were able to get their message across to a portion of Egyptian society unlikely to venture online.

In addition, while the Mubarak regime had a large and active internal security force, it was completely unprepared for the sophisticated Internet mobilization strategies of Egyptian activists. Once the uprising started, the regime was left with two unappealing choices: It could cut off the Internet and endure the economic consequences, or it could allow online activities to continue and use other (and often more violent) methods to crack down on protesters. Ultimately the regime tried both strategies; neither was very successful.

In drawing broader lessons from Egypt for Internet policy it is important to consider the rarity of the circumstances faced in Egypt. Though nondemocratic like most Middle Eastern regimes, Egyptian society had more open Internet access than most Middle Eastern states, making it more likely that a vibrant population of social media activists could emerge. In addition, after witnessing events in Egypt, other nondemocratic regimes are now well aware (if they were not before) of the potential danger that cyberactivism poses to their survival. They are developing a range of approaches to block and target Internet activities without completely disconnecting their societies from the web, something Mubarak likely regrets forgoing. The overall media environment varies widely in nondemocratic states. In Egypt, the impact of social media was magnified by the numerous independent, regional, and international media outlets with correspondents and operations in Cairo. These alternative media sources do not exist in many nondemocratic states, and in many cases the mass media is completely controlled by the regime. It is far more difficult in such circumstances to build a counternarrative against the government than it was in Egypt.

But, while the broader Egyptian political context played a critical role in facilitating the uprisings, that does not diminish the importance of the heroic acts of Egyptian youth who skillfully used social media to topple a longstanding authoritarian regime. Nor does the broader context adequately account for the harshness of the backlash against social media's significance. Perhaps this impulse to challenge social media's political import is due to the frivolity of most social media use, or to the concerns of anti-imperialists that the "Facebook Revolution"

label was concocted by Western countries to claim responsibility for the heroic acts of Arab youth. Whatever the reason, downplaying the role that social media played in Egypt is just as dangerous as overselling it. Social media, by its very nature, is only an extension of the social context in which it operates. By ignoring it and its potential ability to trigger social change, as it did in Egypt, we are deliberately overlooking a vital piece of today's political space.

## Internet Freedom and Political Change in Syria

---

In March 2011, the wave of unrest that toppled the leaders of Tunisia and Egypt reached Syria. At the outset, the demonstrations were confined to Daraa, a secondary city on the Jordanian border, but the unrest quickly spread to the central and western regions of Syria and soon a nationwide revolt was in swing. The initial uprising relied on demonstrations and strikes, although after increasingly violent responses from the Assad regime's notorious state security forces, street politics morphed into an armed uprising led by defectors from the Syrian military. This chapter focuses on one particular aspect of the Syrian uprising: how the Internet has been employed by both opposition and the regime to contest the political space. It covers the period from the spring of 2011 until the summer of 2012, when the uprising developed into a civil war.

The purpose of this chapter is twofold. First, it explores the role netizens often play in a sustained political crisis when the legitimacy of an authoritarian regime is being challenged. It analyzes these efforts and seeks to determine what impact this can have on the political space within the country. Second, it explores how deepening and broadening Internet freedom is likely to affect the political space in dictatorships immersed in a deep political crisis. Syria is interesting from this perspective because it has an active but relatively small population of netizens. However, these netizens have played an important role in the uprising, providing information to the outside world about what is occurring inside Syria and helping to organize protests and demonstrations. Broadening Internet freedom has also played a role in Syria

as the low level of Internet penetration has upon occasion been overcome through the use of mobile phone technology. Mobile phones have allowed people without direct Internet access a way to gather and spread information about the uprising.

Syria is a fully authoritarian state that ranks 157 out of 167 states in the *Economist* Democracy Index.<sup>1</sup> Only a handful of states—including Iran, Saudi Arabia, and North Korea—are less democratic. Syria has high levels of Internet censorship and a powerful internal security service, and is run by a regime extremely resistant to even modest reform that might dilute its power. It also has a very low rate of Internet penetration, although a somewhat higher level of mobile phone usage.

As such, Syria is a particularly interesting case study: It presents some of the toughest conditions in the Middle East region for activists seeking to use the Internet to mobilize political action. The role of the Internet in Syria's uprising has been limited by low levels of Internet penetration, poor connection speeds, and pervasive government censorship. That the uprising has morphed into an armed conflict has also reduced the relative importance of the Internet as a platform for mobilizing public dissent. On the other hand, Internet activism has played an important role in the Syrian uprising by enabling citizen journalists to keep Syrian nationals and the outside world abreast of developments inside the country. Citizen reporting on regime repression has helped to push fence-sitters into the opposition's camp and may yet galvanize the international community to increase the scope of its assistance to the opposition. The fact that the Internet has emerged as a tool of the Syrian opposition demonstrates that the Web is of some use in even the most challenging environments as a platform for political change.

## Internet Usage by the Numbers

Even by modest regional standards, Internet penetration in Syria is quite low. It is estimated that only 4.5 million Syrians—or about 20

---

<sup>1</sup> Economist Intelligence Unit, December 16, 2011.

percent of the population—have Internet access.<sup>2</sup> This is 15 percent below the regional average and represents one of the lowest Internet penetration rates in the Middle East. The transmission speeds are also quite poor; nine out of ten Internet connections in Syria operate via dial-up rather than ADSL (Asymmetric Digital Subscriber Line) or ISDN (Internet Services Digital Network), much less the cable and fiber connections prevalent in the United States.<sup>3</sup> In fact, the majority of Syria's Internet users are limited to connection speeds of 56 Kb. This means that even when Internet users are able to employ circumvention tools to access streaming video on YouTube, the download speeds are often too slow to reliably view the content. There is no granular data that breaks down Internet usage in Syria by demographic, but extrapolating from regional trends, it is safe to assume that usage is highest among younger, urban males of higher socioeconomic standing.

Low overall levels of Internet access and the presence of significant government filtering help explain why social media in Syria is restricted to a small portion of the country (see Figure 4.1). Just over a million Syrians have registered for a Facebook account—under 6 percent of the population—and only 6,000—roughly .03 percent of the population—can be classified as active Twitter users.<sup>4</sup> What these absolute numbers hide, however, is a significant upsurge in usage over the past year. Facebook was blocked in Syria until February 2011, so many of Syria's users are new subscribers. Moreover, while the profile of Syria's social media users is not broadly reflective of society, users have attributes that make them good candidates to be potential activists and youth leaders. As noted by one analyst, “we have to be careful not to get into the fallacy we had in Egypt when we thought, ‘Oh, it's only 12 percent Internet penetration.’ It's the key connectors, those opinion shapers among a certain educated class . . . These are the people that

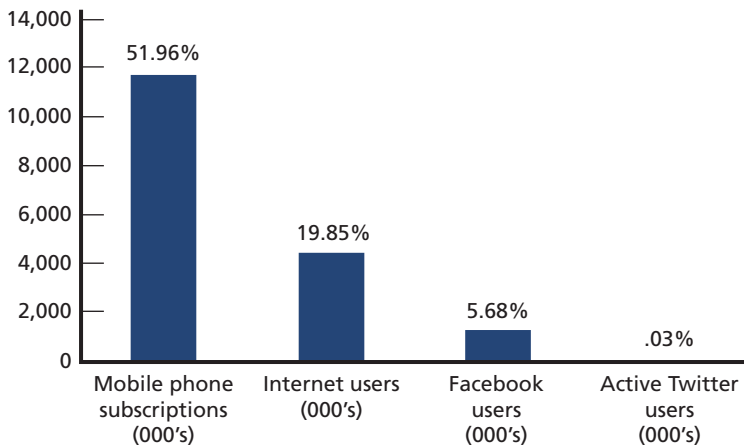
---

<sup>2</sup> Internet World Stats, *Usage and Population Statistics*, web page, 2012a.

<sup>3</sup> Dana Kassab and Edwin Lane, “The Digital Divide,” *Syria Today*, June 2011.

<sup>4</sup> Racha Mourtada, Fadi Salem, May Al-Dabbagh, and Ghalia Gargani, “The Role of Social Media in Arab Women's Empowerment,” *Arab Social Media Report*, Vol. 1, No. 3, Governance and Innovation Program, Dubai School of Government, November 2011.

**Figure 4.1**  
**Syria's Internet and Mobile Penetration**



SOURCE: Mourtada, Salem, al-Dabbagh, and Gargani, 2011.

RAND RR295-4.1

want to be playing a leadership role, and [the Internet] is helping them participate in the public sphere.”<sup>5</sup>

In contrast to Internet access, mobile phones in Syria are ubiquitous. There are nearly 12 million cellular subscribers in a country of 22 million people, or roughly one mobile phone account for every two Syrians.<sup>6</sup> Few of these subscribers have mobile Internet access through their phones, although text messaging is quite common. As it relates to the current uprising, mobile phones have also played a crucial role in enabling “citizen journalists” to capture events on the ground via mobile phone cameras. With local media firmly under state control and high levels of violence hindering the operations of international media, mobile phone videos have served as a crucial source of information on the uprising.

<sup>5</sup> As quoted in Jeffrey Ghannam, “Digital Media in the Arab World One Year After the Revolution,” *Center for International Media Assistance*, March 28, 2012, p. 11.

<sup>6</sup> Mourtada et al., 2011.

## Internet Censorship

Even prior to the current unrest, the Syrian regime engaged in significant censorship of the Internet. In fact, since Reporters without Borders inaugurated its list of “Internet Enemies” in 2005, Syria has been a consistent designee, sharing that distinction with the likes of Myanmar, North Korea, and China. The Syrian regime’s means of controlling access to Internet content are many, including state ownership and regulation of telecommunications, aggressive filtering of Web content, monitoring of Internet use, and repression of Internet-based activism. These methods create major barriers to any use of the Internet—particularly for political activism.

Like many industries and services in Syria, the telecommunications market is a government monopoly. Syrian Telecom manages all telecommunications infrastructure, and this state-owned enterprise is embedded within the Syrian Ministry of Telecommunications and Technology.<sup>7</sup> The state has licensed a number of smaller private providers, but all rely on government-managed infrastructure and are government regulated. This leaves ISPs effectively under regime control to include wired and the much more limited wireless service. The same holds for cellular service; one public enterprise, Syriatel, controls an estimated 55 percent of the country’s cellular phone market.<sup>8</sup>

A second lever of state control is intrusive filtering of Internet content. Ironically, the uprising in Syria has led to some lifting of restrictions on access, a point addressed more fully in the section dealing with regime responses to the unrest. But prior to the onset of the revolt, the Syrian regime regularly blocked email services including Hotmail and Yahoo, popular social media sites such as Facebook and Twitter, and forums hosting user-created content such as YouTube. In addition to email services, social media, and streaming video, the regime filters a wide array of websites that challenge regime legitimacy. Blocked content includes URLs for human rights organizations, Islamist opposi-

---

<sup>7</sup> “Internet Filtering in Syria,” *OpenNet Initiative*, 2009.

<sup>8</sup> U.S. Treasury Department, “Fact Sheet: New Executive Order Targeting Human Rights Abuses via Information Technology,” April 23, 2012.



tion groups, critical press, independent bloggers, and more. Estimates put the total number of blocked sites at 240.<sup>9</sup> The extent of the regime's capabilities in this area are not precisely known, but testing conducted by the OpenNet Initiative found that URL filtering in Syria is accomplished through use of a product called ThunderCache solution.<sup>10</sup> Importantly, the regime also uses its URL filters on anonymizers in an attempt to deny this tool to cyberdissidents.

Another layer of the government-imposed firewall is the monitoring of Internet use. At its most basic level, monitoring takes place through the requirement that users of Internet cafes sign in by providing their name and national identification number. The requirement is a deterrent for Syrians who do not wish to raise their profile with state security. In addition to overt monitoring, observation takes place surreptitiously through electronic surveillance. The cat-and-mouse game between cyberdissidents and regime security has evolved considerably, but the continued arrest and harassment of bloggers and journalists confirms that security services possess the capability to monitor online activity.

The final layer of Internet censorship in Syria is repression against those who employ the Internet to challenge the regime. Prior to the uprising, the application of state repression was relatively targeted. That is to say, individuals who posted content questioning the legitimacy of the Syrian regime were arrested and jailed under the authorities granted by Syria's Emergency Laws, or they were simply prosecuted under Syria's regular penal code, which criminalizes such offenses as the "weakening of national morale." Since the uprising, there are indications that repression has become even broader, with suspicion cast on anyone who uses the Web, particularly Facebook, as a regime opponent.<sup>11</sup> Although this blanket approach risks alienating fence-sitters, the Syrian regime appears to have made a judgment that the benefit of deterring Internet use outweighs the potential costs of doing so.

---

<sup>9</sup> "Internet Enemies: Syria," Reporters Without Borders website, March 12, 2012.

<sup>10</sup> "Internet Filtering in Syria," 2009.

<sup>11</sup> Jennifer Preston, "Seeking to Disrupt Protesters, Syria Cracks Down on Social Media," *New York Times*, May 22, 2011.

## Use of the Internet in the Syrian Uprising

The contribution of the Internet to political action is often erroneously collapsed into the organization and coordination of protests, whereas most online activity actually involves the more modest aims of following and publicizing unrest. Granted, Internet-based communication methods, particularly Skype, are employed by core activists to coordinate efforts.<sup>12</sup> In Syria this has taken place through aptly named Local Coordination Committees that have “responsibility for meeting, planning and organizing events on the ground within their own communities.”<sup>13</sup> But survey research conducted in Syria’s regional counterparts that have undergone mass unrest such as Egypt and Tunisia indicates that only 3 percent of men and 9 percent of women reported that their “primary use” of social media during the uprisings was organizing protest action or managing fellow activists.<sup>14</sup> The vast majority were using social media to follow developments and raise awareness inside and outside their country on the cause.

This dynamic in which social media is primarily used for dissemination of information and to provide ordinary citizens a channel for expressing solidarity with a popular movement—rather than to coordinate demonstration times and tactics—is particularly true in the Syria case. In fact, many of Syria’s largest demonstrations are launched from mosques after Friday prayers or grow out of funeral processions for protesters killed by regime security.<sup>15</sup> As an example, on one Friday in February 2012, more than 35 demonstrations were launched from differ-

---

<sup>12</sup> Radwan Ziadeh, “The Double Edged Sword of Social Media” *Mark*, July 21, 2011.

<sup>13</sup> The mission of the organization is as described on the Local Coordination Committees homepage, undated.

<sup>14</sup> Mourtada et al., 2011.

<sup>15</sup> “Suqūt al-Shuhadā’ mundhu Sabāh wa Janāza al-Shahīd al-Halabī Tahawwulat ila Muzhāhara Hāshida ghayr Masbūqa [Fallen Martyrs Since this Morning and the Funeral of a Martyr Morphs into a Unprecedented Mass Demonstration],” *Suriya Mustaqbal*, December 26, 2011; Michael Doran and Salman Shaikh, “The Syrian Crucible,” *American Interest*, January/February 2012.

ent mosques across the country.<sup>16</sup> In this respect, the current uprising actually exhibits a strong historical parallel to the anti-colonial movement, in which the mosque operated as a platform for political action.

As noted by a Syrian political activist commenting on the role of mosques in the current uprising, “In Syria’s modern history—and especially during the period of colonization—the mosque was the place from which the majority of demonstrations were launched . . . In Islamic history, the mosque has not just been a house of worship, but rather a site overflowing with different sociopolitical interactions . . .”<sup>17</sup> Put in terms of Western social science, mosques and funeral processions are natural “focal points” for dissent in Syria. For Syrians seeking to join demonstrations, the focal point is even more obvious—the mosque after Friday afternoon prayers. While some action is coordinated online, ordinary Syrians do not need Facebook to know how to join an uprising.

Where social media has made a big contribution is in disseminating information on events to those outside Syria, in addition to those within the country who seek alternatives to state-controlled media. It is citizen journalists who have exposed the international community and Syrians removed from the uprising’s hotspots to the brutality of the regime’s response. The defining images of the Syrian uprising have been recorded on mobile phones and uploaded to live streaming websites such as Bambuser<sup>18</sup>—a selection of which makes its way on to popular viewing sites like YouTube. And while the number of views is impressive—sometimes numbering in the hundreds of thousands—the most significant impact comes when the videos are picked up and broadcast by pan-Arab and international TV outlets that reach millions of viewers. The point is made forcefully by a bureau chief for al-Jazeera who notes, “The use of social media and reliance on pictures sent via social media to satellite television have become a fact of life . . .

---

<sup>16</sup> List of demonstrations on February 24, 2012, as compiled on syrianrevolution.org website (in Arabic), undated.

<sup>17</sup> Faras Qasas, “Bashar al-Asad wa Tawsīfihi lil Sirā’ al-Dā’ir fī Sūrīya [Bashar al-Asad and His Description of the Ongoing Conflict in Syria],” *Al-Arabiya.net*, November 30, 2011.

<sup>18</sup> Ghannam, 2012, p. 14.

You get these videos from an Arab country like Syria, where the international press cannot get . . . ”<sup>19</sup>

In an example of a particularly stirring video that was broadcast by satellite television, a Syrian youth was shot and killed while filming a protest with his mobile phone. Although the feed is cut off after the dying youth drops his phone, the follow-on scene of his companions trying to save him is captured by another mobile phone user who focuses his camera on the phone of the wounded youth lying in the street. The clip symbolizes the outsized role that phones have played in documenting the uprising, with one commentator noting, “A mobile phone films another mobile phone whose owner—a youth protester and activist that doesn’t have any weapon other than this symbolic weapon—is killed. The mobile phone has become the star of the popular revolutions . . . This small instrument has actually become stronger than the television cameras.”<sup>20</sup> Videos of protesters killed by regime snipers, dissidents tortured by state security, and conscripts declaring their allegiance to the Free Syrian Army provide a visceral counterpoint to the state media’s portrayal of the conflict.

In addition to contesting the regime’s narrative and delegitimizing it, social media provides ordinary Syrians with an avenue for participation in the uprising. At the lowest level of involvement, online forums are simply a means for users to keep up with events, express solidarity with the protesters, or feel part of a popular movement. For more committed activists, blogging or posting on Facebook may be one aspect of broader involvement that includes physical participation in demonstrations, boycotts, strikes, etc. The highest level of involvement encompasses the small cadre of core activists who use the Internet to organize, coordinate action, and manage volunteers.

For better and for worse, social media has been a means for Syria’s expatriate community to remain connected to the uprising and to each other. Many of Syria’s leading opposition figures left the country for Western Europe and the United States long before the uprising, so access to web videos and Internet postings were an important

---

<sup>19</sup> Ghannam, 2012, p. 20.

<sup>20</sup> “Mashhadiyāt Sūriya [Vignettes from Syria],” *al Hayat*, March 26, 2012.

source of information for this community and increased their sense of connectedness to events on the ground. On the other hand, it has also facilitated their heavy involvement in establishing a government in exile that can operate as the representative of the Syrian people vis-à-vis the international community. The downside has been that the long absence of these individuals from their home country has led many on-the-ground activists to question their relevance and credibility as representatives of the Syrian people. This dynamic played out most visibly in the November 2012 replacement of the exile-dominated Syrian National Council with the National Coalition for Syrian Revolutionary and Opposition Forces.

### **Circumvention Technologies During the Protests**

Syrian college students began using proxies and other tools to access Facebook, YouTube, Wikipedia, and other blocked sites well before the uprising. Internet cafes, most of which had high-speed access that was unavailable in private homes, constituted a primary venue for accessing those sites.<sup>21</sup> The opportunities for circumvention began to shrink starting in 2008, when the Syrian authorities upgraded filtering software, expanded the list of banned sites, and began requiring Internet café owners to take IDs from customers and/or to install software to spy on their customers. Technological improvements were further supplemented by the crackdown on self-expression that culminated in the imprisonment of two prominent bloggers, Habib Saleh and Tariq Biasi, for posting anti-government blogs.<sup>22</sup>

Thus, on the eve of the protests, the Syrian authorities closely monitored online activity and had sophisticated surveillance technology. Therefore, uprising on the streets quickly escalated into cyberwarfare during which the Syrian authorities deployed malware to access activists' computers.

---

<sup>21</sup> "Syrian Youth Breaks Through Internet Blocks," Institute for War and Peace Reporting, June 3, 2008.

<sup>22</sup> Phil Sands, "Syria Tightens Control over Internet," *National*, September 30, 2008; Open Net Initiative, *Syria*, web page, August 7, 2009.

### Regime Adaptation

The Syrian regime, while not particularly tech savvy, recognizes the challenge of cyberdissent and is responding to it in myriad ways. The regime's strategy is based on balancing two parallel approaches. The first approach is to shut down, slow, and filter Internet access so as to render it a less valuable tool for protesters. To achieve this, the regime is ratcheting up its traditional efforts at Internet censorship. In parallel, the regime has also tried to keep the tap open just enough to use online forums as a means of surveillance. For example, the state actually lifted its restrictions on Facebook in February 2011 to exploit it as tool for identifying dissidents and targeting state repression. In these efforts, the Syrian regime appears to be assimilating tactics employed by the Iranian regime in its response to unrest after the disputed 2009 presidential elections.

The Syrian regime's bluntest tools in disrupting the Internet are periodic shutdowns and the slowing of connection speeds. The former is rare—but the regime has regularly slowed Internet connection speeds since the onset of the uprising, and the targeted way they have done it shows some sophistication. Specifically, the regime typically slows connection speeds on Fridays, when the bulk of demonstrations occur just as the regime has focused its efforts on hotspots of unrest rather than subjecting the entire country to the slowdown.<sup>23</sup> When the regime wants to take the more extreme measure of shutting down a network, it is often accompanied by power and phone cuts, exacerbating a restive locality's isolation. In more targeted action, the regime has updated its URL filtering to capture sites that are central to the efforts of cyberdissidents. For example, in February 2012, the governments shut down access to Bambuser—the live-video streaming site that was a crucial node in activists' efforts to document regime violence and disseminate that information to the outside world.<sup>24</sup>

But rather than simply plugging holes in the dike, the Syrian regime has also sought to exploit the opportunity that online dissent

---

<sup>23</sup> "Internet Enemies: Syria," 2012.

<sup>24</sup> Ryan Devereaux, "Syrian Government Blocks Live Video Streaming Site Bambuser," *Guardian*, February 17, 2012.

provides to identify dissidents and preempt opposition activity. Specifically, Facebook and Twitter are monitored by government forces to build lists of dissidents, who are then targeted for arrest.<sup>25</sup> As noted by one Syria watcher, “Lifting the ban on Facebook helped the regime pinpoint where the [activists] were coming from . . . It was not about being magnanimous; it was a way to allow more surveillance, leading to thousands of arrests.”<sup>26</sup> Some activists have countered by switching to instant messaging services or accessing social media through Tor, but enough activists ignore the risk to feed a steady stream of detentions based on social media postings.<sup>27</sup> And even for those oppositionists who use encryption software, there are instances of regime security simply detaining laptop owners and literally beating the user’s password out of him.<sup>28</sup>

In addition to the repression of online activism, the Syrian regime and its supporters make use of the Internet as a platform for their own cyberoffensive. Such Trojans as Darkcomet and Xtreme that acted as remote action tools capable of capturing webcam activity, monitoring key strokes, and stealing passwords were embedded in fake revolutionary documents claiming to assist the opposition forces and spread through email and chat programs; they were also disguised as a Skype encryption tool.<sup>29</sup> The most visible and organized actor in this cyberbattle is a group of Assad supporters known as the Syrian Electronic

---

<sup>25</sup> “Social Media: A Double-Edged Sword in Syria,” *Reuters*, July 13, 2011.

<sup>26</sup> Joby Warrick, “Iran Reportedly Aiding Syrian Crackdown,” *Washington Post*, May 27, 2011.

<sup>27</sup> “Internet Enemies: Syria,” 2012.

<sup>28</sup> Preston, 2011.

<sup>29</sup> Eva Galperin and Morgan Marquis-Boire, “New Trojan Spread Over Skype as Cat and Mouse Game Between Syrian Activists and Pro-Syrian-Government Hackers Continues,” Electronic Frontier Foundation web page, June 19, 2012c; Eva Galperin and Morgan Marquis-Boire, “New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan,” Electronic Frontier Foundation web page, July 12, 2012d; Eva Galperin and Morgan Marquis-Boire, “Campaign Targeting Syrian Activists Escalates with New Surveillance Malware,” Electronic Frontier Foundation web page, April 4, 2012a; Eva Galperin and Morgan Marquis-Boire, “Fake Skype Encryption Tool Targeted at Syrian Activists Promises Security, Delivers Spyware,” Electronic Frontier Foundation web page, May 2, 2012b.

Army. It has not been definitively determined whether this group is simply given space to operate, or is actively recruited, financed, and managed by the regime. Whatever the level of state support, the Syrian Electronic Army engages in a variety of activities aimed at disrupting the online access of those the group views as opponents of the Assad regime.

Thus far, the Syrian Electronic Army has taken a kitchen-sink approach, engaging in everything from DDOS attacks and spamming to defacing the sites of regime critics and phishing for the personal information of oppositionists—the latter presumably to aid the regime in the targeting of its repression.<sup>30</sup> The group attempts to convey a pro-Assad message while also attacking opponents of the regime as foreign lackeys or apologists for an uprising launched by “thugs and terrorists.” Although the capabilities of the group are not particularly sophisticated, the Syrian Electronic Army is large in number and very active.<sup>31</sup> The group has had some success in disrupting the websites of international media through sheer persistence, overwhelming Twitter with pro-Assad messages, and hacking the Facebook pages of oppositionists. The Syrian Electronic Army also engages in a tit-for-tat campaign against opposition “hacktivists”—most prominently the collective known as Anonymous—who have employed similar tactics as the Syrian Electronic Army but directed against the Assad regime.

As the conflict unfolded, the demand for Tor software began to pick up and reached as many as 22,000 daily users (0.49 percent of Internet users) in the aftermath of the Houla massacre on May 25, 2012, which resulted in 108 civilian deaths, including 49 children (Figure 4.2). YouTube videos and photos uploaded by the survivors provided shocking evidence on the scope of this tragedy. The events prompted bitter debates about who was responsible for this massacre, with Syrian authorities blaming terrorists, and the United Nations and opposition forces accusing the *shabiha*, a militia dominated by mem-

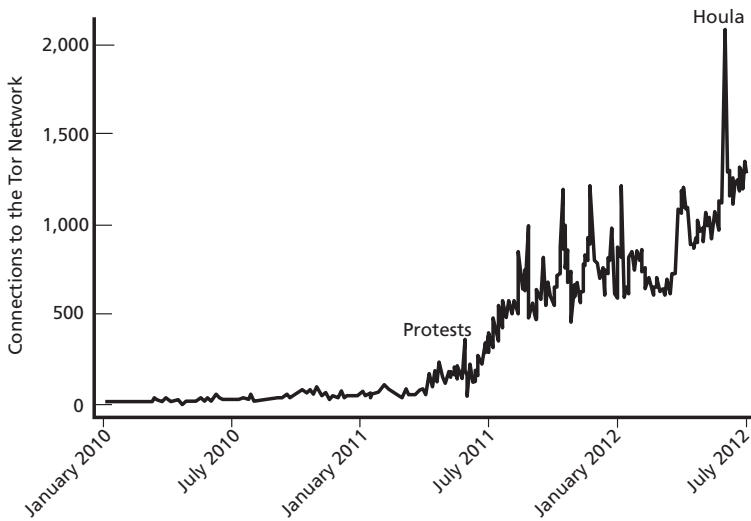
---

<sup>30</sup> Max Fisher and Jared Keller, “Syria’s Digital Counter-Revolutionaries,” *The Atlantic*, August 31, 2011.

<sup>31</sup> Deborah Amos, “Pro-Assad ‘Army’ Wages Cyberwar in Syria,” *National Public Radio*, September 25, 2011.



**Figure 4.2**  
**Number of Connections from Syria to the Tor Network**



SOURCE: Tor Project.  
 RAND RR295-4.2

bers of Assad's Alawite sect.<sup>32</sup> The growing demand for Tor may reflect netizens' desire to access coverage of the events provided by nongovernment sources.

Alkasir is another circumvention technology that became popular after the outbreak of the conflict. Developed by Yemeni blogger Walid Al-Saqaf, it is based on virtual private network (VPN) tunneling. In 2011, Syria accounted for the largest concentration of Alkasir users, who relied on it most frequently to access blocked political news sites and social media. Similar to Tor, Alkasir witnessed a tremendous rise in the number of users, from about 1,500 in January 2011 to 28,500 in January 2012.<sup>33</sup>

<sup>32</sup> "Houla: How a Massacre Unfolded," BBC News website, June 8, 2012.

<sup>33</sup> Walid al-Saqaf, "Circumventing Internet Censorship in the Arab World," in Larry Diamond and Marc F. Plattner, eds., *Liberation Technology: Social Media and the Struggle for Democracy*, Baltimore, Md.: The Johns Hopkins University Press, 2012, p. 134.

### External Dimensions

Many analysts see the adaptations of the Syrian regime as informed by the experience of its state ally, Iran, in countering the Green Movement that took to the streets in 2009. Not surprisingly, open-source reporting on the international dimensions of Syria's crackdown is thin. However, two Assistant Secretaries, the Secretary of State, and the U.S. President have all fingered Iran as providing material support to aid Syria in their crackdown.<sup>34</sup> In off-the-record interviews, U.S. officials have been more explicit in noting that Iranian assistance has specifically included technology and training in the repression of Internet freedom. On the record, they have suggested that Syria is receiving "a steady stream of aid from Tehran that includes not only weapons and riot gear but also sophisticated surveillance equipment that is helping Syrian authorities track down opponents through their Facebook and Twitter accounts."<sup>35</sup> This charge is further developed by the U.S. Treasury Department in a fact sheet that details coordination between the Iranian Ministry of Intelligence and Security and the Syrian General Intelligence Directorate in monitoring and repressing online dissent.

While the comments of U.S. officials are based on intelligence reporting, Syria-watchers outside of government have long made the same argument based on observation of the Assad regime's growing capabilities. Namely, analysts note that Syrian state security rapidly developed their capabilities to monitor social media after appearing fairly clueless at the outset of the revolt. Given that Tehran is a close ally of Damascus—and quite formidable in countering online dissent—they reason that Iran is a probable source of the equipment

---

<sup>34</sup> Michael H. Posner, Assistant Secretary, Bureau of Democracy, Human Rights, and Labor, and Jeffrey D. Feltman, Assistant Secretary, Bureau of Near Eastern Affairs, "U.S. Human Rights Policy Toward Iran and Syria," testimony before the House Foreign Affairs Subcommittee on the Middle East and South Asia, July 27, 2011; Hillary Rodham Clinton, Secretary of State, remarks with European Union High Representative for Foreign Affairs and Security Policy Catherine Ashton, Washington, D.C., July 11, 2011; White House, "Statement by the President on Syria," Washington, D.C., April 22, 2011.

<sup>35</sup> Warrick, 2011. Similar statements by U.S. officials are quoted in Adam Entous and Matthew Rosenberg, "U.S. Says Iran Helps Crackdown in Syria," *Wall Street Journal*, April 14, 2011.

and training that have enabled Syria to upgrade its own capabilities in this area. Syria has yet to assimilate Iran's entire tool kit, but analysts like Joshua Landis, associate professor and director of the Center for Middle East Studies at the University of Oklahoma, have noted that Iranian support has helped Syria address the initial gap in capability. "You've got to train up a cadre of young Syrians who can get on all these social media, and that's what they've tried to do."<sup>36</sup>

Of course, outside support has not only been to the benefit of the Syrian regime. Western groups—both government-supported outfits and independent "hacktivists"—are aiding Syrian oppositionists by providing them the knowhow to better protect themselves from state repression. A particular focus of efforts has been informing Syrian oppositionists on the availability of anonymizers and circumvention tools. The former mitigate the risk of Iranian surveillance of cyberdissidents while the latter allow activists to bypass government filtering. It should be noted that much of this outreach is not specifically targeted at the Syrian arena; rather, Syrians are just one recipient of a program that is regional (e.g., the Middle East and North Africa) or global in scope.

The U.S. government has also attempted to block the export of technologies to Syria (and Iran) that limit Internet freedom. In an executive order issued in April 2012, the President sanctioned individuals, government entities, and corporations that are responsible for or enable the Syrian and Iranian regimes' use of the Internet to stifle dissent. The order was based on a determination that serious human rights abuses in Syria and Iran are "facilitated by computer and network disruption, monitoring, and tracking by those governments, and abetted by entities in Iran and Syria that are complicit in those governments' malign use of technology for those purposes."<sup>37</sup> The order also affirmed the "vital importance of providing technology that enables the Iranian and Syrian people to freely communicate with each other and the outside world."

---

<sup>36</sup> Amos, 2011.

<sup>37</sup> White House, Executive Order, "Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology," Washington, D.C.: April 23, 2012.

However, the effectiveness of this action is hindered by the Syrian and Iranian regimes' limited vulnerability to additional sanctions. In the case of Syria, the only two entities named were the state-run telecommunications firm Syriatel and the head of the Syrian General Intelligence Directorate, Ali Mamluk. The U.S. charges that Syriatel has cut or slowed network connections as well as facilitated government eavesdropping on private phone conversations. As for Mamluk, he is accused of "oversee[ing] a communications program in Syria which was directed at opposition groups" that "included both technological and analytical support from Iran's [Ministry of Intelligence and Security]."<sup>38</sup> That said, both Syriatel and Mamluk are already designated under existing sanctions and it is unclear how the new order will actually curb the activities it condemns.

## How Internet Freedom Affected Political Change in Syria

The preceding review of the Syrian uprising cannot definitively answer the question as to the degree to which Internet freedom contributes to political change. One important analytical constraint is that the situation in Syria has rapidly evolved since the uprising first occurred. Initially the contest was similar to those in Arab states, a long-standing and entrenched regime facing off against a mobilized population willing to use demonstrations and street politics to challenge the state. This has now mutated into an armed conflict with strong ethnic divisions emerging between the two sides. Whether the current state of armed conflict will lead to the toppling of the Assad regime—as the uprisings/wars did to Ben-Ali in Tunisia, Mubarak in Egypt, and Muammar al-Qadhafi in Libya—remains an open question. In addition, as was the case in Egypt, it is very difficult, if not impossible, to isolate the impact the Internet is having on political activism in Syria vis-à-vis other variables contributing to the conflict.

What this chapter does reveal is the real limitations that Internet freedom confronts in a sustained and violent conflict. The role of the

---

<sup>38</sup> U.S. Treasury Department, 2012.

Internet in Syria's uprising has been limited by low levels of Internet penetration, poor connection speeds, and pervasive government censorship. Less than 20 percent of Syrians have Internet access, and even among users, it is not clear that political activism is a primary focus of their Web activity. Furthermore, social media such as Facebook and Twitter that are often viewed as having fanned or enabled the unrest elsewhere in the Arab world have small followings among Syrians.

That said, there is a risk of being too literal in interpreting what the data on Internet penetration mean for the role of the Internet in mobilizing and sustaining political action in Syria. This case study provides support for the notion that deepening Internet freedom can have an important impact on the political situation. Available information suggests that the profile of Internet users in Syria broadly matches the characteristics associated with emerging youth leaders. Moreover, even if the sheer volume of Internet traffic is low, the use of web-based platforms by citizen journalists to break the Syrian regime's stranglehold on coverage of events is a significant contribution.

This also points to an important difference between the impact the Internet had in Egypt and Syria. In Egypt, social media played an important role in coordinating demonstration times and tactics. It was the glue that allowed a diverse group to organize itself into enough of a coherent force to challenge the regime. This is not the case in Syria, where a very narrow core of committed activists are using web-based platforms to coordinate tactics, and even then, conventional "focal points" such as Friday prayers and funeral processions are far more important than Facebook as a point of entry for those wishing to participate in the unrest.

On the other hand, the Internet has allowed Syrian activists to challenge the regime's framing of the conflict for both internal and external audiences. This was less important in Egypt, where media coverage was extensive and multiple satellite channels with large audiences reported what was occurring. Inside Syria, independent reporting, citizen journalism, and social media postings are being used as resources by concerned citizens to formulate their personal positions on the issue at hand. Regardless of whether those individuals side with the regime or the opposition, once a position is formulated, those same

resources are available to mobilize fellow citizens and draw attention to a cause. The Internet is making information available about Syrian human rights violations and the progress of the conflict to audiences outside Syria. This shaped the international community's view of what is going on and affected possible outside responses to it.

Access to social media is a double-edged sword for the opposition. On the one hand, it provides a powerful tool for challenging the state's narrative of events. By removing the state from its role as the gatekeeper that filters all information, the opposition is in a stronger position to win over and mobilize fence-sitters. On the other hand, the opposition's use of social media provides state security with another means of surveillance, just as it increases the state's situational awareness—feeding it useful intelligence that can be used to contain or repress the uprising.

Finally, although the biggest stakeholders in this conflict are inside Syria, the potential for political change in that country is greatly affected by Syria's external environment. As is the case with other pieces of the Syria conflict, the Internet has become involved in the proxy conflict between Iran (with tacit support from China and Russia) and the West. Specifically, Syria has relied on Iranian support to develop its electronic surveillance capabilities while opposition forces rely on the West for tools to counter state repression.

Thus, although our case studies focus on the domestic situation inside countries, the battle for Internet freedom is often a global contest. Governments such as Iran, Russia, and China are seeking to limit Internet freedom, and their policies have an important impact on developments in other regions of the world. This is directly manifested in the Syria conflict, where the power of Internet freedom to spur political change assisted by the United States is being directly confronted with regime tactics seeking to curtail and control its influence.



## The Internet in China: Threatened Tool of Expression and Mobilization

---

On August 2011, BBC News pointed out that the Internet and microblogs “have not changed the fundamental nature of government in China, but they are forcing officials to change the way they operate.”<sup>1</sup> About a year later, BBC News noted that “the breadth and the nature of public debate in China has been drastically changed by the use of social media, but is it really just a poor replacement for real social change?”<sup>2</sup> Both statements capture the uncertainty regarding the profundity of changes brought about by the Internet. Has the Internet expanded the political space in China? If so, in what ways and channels? Were these political changes brought about via the transformation of the elite behavior or by making Chinese netizens more tech-savvy at circumventing Internet censorship?

In addressing these questions, we juxtapose authorities’ responses to popular mobilization in urban and rural areas and areas populated by ethnic minorities to assess relative importance of the new media in different contexts. This comparison underscores how structural constraints can alter the mechanism by which Internet freedom can expand political space. We begin by first examining how Chinese citizens and authorities interact in cyberspace and then trace how online activism manifests itself offline. The rapidly growing scholarly literature suggests that the Internet has affected political processes in China

---

<sup>1</sup> Michael Bristow, “Can Microblogs Change China’s Rulers?” BBC News website, August 7, 2011.

<sup>2</sup> Duncan Hewitt, “Weibo Brings Change to China,” BBC News website, July 31, 2012.



by expanding social space,<sup>3</sup> intensifying state-society conflict,<sup>4</sup> improving the transparency of the legal system,<sup>5</sup> changing political attitudes, and enhancing mobilization.<sup>6</sup> After discussing these mechanisms, we turn our attention to three types of online mobilization: (1) protests in urban areas in the aftermath of the Wenzhou train crash and popular demonstrations against reopening the Dalian chemical plant; (2) Wukan village protests against land confiscation and popular mobilization against pollution by the Luliang Chemical factory in Xinglong village, located in Yunnan; and (3) protests in Xinjiang province in July 2009 that culminated in a ten-month suspension of Internet services in the entire province. We show that in the first case, social media contributed to social mobilization by fostering the diffusion of information to all parts of the country and transforming the terms of debate from a regional matter to a national one. Online discussion of the events prompted the traditional media's response, and journalists began covering the events in spite of the authorities' ban. In rural areas, however, protesters were less effective at using the new technologies, partially due to lower rates of Internet penetration, and were less successful in persuading the authorities to change the status quo. In the case of the Xinjiang protests, the Internet enabled the diaspora to attract the attention of the international community to gross human rights violations during the protests and their aftermath. We conclude our discussion by examining how this case study of China contributes to our understanding of the relationship between Internet freedom and broadening and deepening of the political space.

---

<sup>3</sup> Guobin Yang, *The Power of the Internet in China: Citizen Activism Online*, New York: Columbia University Press, 2009.

<sup>4</sup> Zheng, 2008.

<sup>5</sup> Xuanyu Huang, "Re-Legalization or De-Legalization? Netizens' Participation in Criminal Justice Practices in China," *British Journal of Criminal Justice*, Vol. 52, 2012, pp. 724–743.

<sup>6</sup> Ya-Wen Lei, "The Political Consequences of the Rise of the Internet: Political Beliefs and Practices of Chinese Netizens," *Political Communication*, Vol. 28, No. 3, 2011, pp. 291–322.

## Netizens and Authorities in Cyberspace

As of January 2012, approximately 500 million Chinese citizens, almost 40 percent of the population, used the Internet. The typical Internet user is male (60 percent), young (60 percent are under 29), educated (55 percent have at least a high school diploma), and part of the urban middle class.<sup>7</sup> That said, the percentage of users who have yet to complete high school has risen from 3 percent in 2000 to 44.2 percent in 2012.<sup>8</sup> Increasing numbers of Internet users—more than a quarter—are from rural areas.<sup>9</sup> Additionally, the use of mobile devices and desktop computers to access the Internet is beginning to converge, and usage of Internet cafes has gone down while connecting from home has risen. Internet use, therefore, is becoming more widespread across all sectors of the population. The number of microblog users also expanded rapidly. In July 2012, the number of those using Weibo (the Chinese equivalent to Twitter) reached 300 million. As many as 35 million use Twitter and 65.2 million had Facebook accounts in spite of the fact that Chinese authorities block access to these two sites.<sup>10</sup>

Internet users in China proudly refer to themselves as “netizens.” Although this term has been widely used in U.S. literature to describe Internet users who are actively engaged in online discussion of public matters, the Chinese use this term to emphasize Internet users’ pursuit of freedom of expression and assembly in the virtual space because they cannot exercise these freedoms offline.<sup>11</sup> Global surveys show that Chinese Internet users are more likely to blog and share content than are Americans, and that they use cyberspace to have more fulfilling social lives by reaching out to like-minded individuals.<sup>12</sup> Microblogging has

---

<sup>7</sup> East-West-Connect.com, *Chinese Mobile Internet User Demographics 2012*, February 20, 2012.

<sup>8</sup> East-West-Connect.com, 2012.

<sup>9</sup> East-West-Connect.com, 2012.

<sup>10</sup> Stephanie Mlot, “Millions Bypass Chinese Firewall to Use Facebook, Twitter,” *PC Magazine*, September 28, 2012.

<sup>11</sup> Fung, 2012.

<sup>12</sup> “What Are You Allowed to Say on China’s Social Networks?” *IEEE Spectrum*, June 2011.

become an obsession in China: half of all Chinese Internet users are microbloggers and have accounts on Sina Weibo, the largest of China's Twitter equivalents.<sup>13</sup> Not all of this discussion is politically motivated. As Demm says, Chinese netizens "are for the most part concerned not with politics and subversion but with identity politics, in particular, lifestyle identities and regional identities."<sup>14</sup> Thus, for many users, the Internet is a getaway from the confines of the norms of conduct imposed by the regime.

### Censorship and Circumvention Methods

Though widespread, the Internet is also heavily censored at varying rates throughout the country. The outermost layer of Internet censorship in China is known as "The Great Firewall." This is the method by which the Chinese government prevents those within China from accessing foreign websites. This is relatively easy to accomplish because Chinese Internet connects to the global Internet through only eight gateways. Internet routers are posted at each gateway and are configured to filter and block certain websites and keywords.<sup>15</sup> These devices (called "tappers" or "network sniffers") mirror every packet of data entering or exiting the country back to a set of "Golden Shield" computers. Therefore, while other normal routers and servers are sending these packets to their destinations, Golden Shield computers are looking at the same packets and deciding whether they should be stopped en route.<sup>16</sup>

---

<sup>13</sup> East-West-Connect.com, 2012; David Bamman, Brendan O'Connor, and Noah A. Smith, "Censorship and Deletion Practices in Chinese Social Media," *First Monday*, Vol. 17, No. 3, March 5, 2012.

<sup>14</sup> Jens Demm, "The Internet and the Fragmentation of Chinese Society," *Critical Asian Studies*, Vol. 39, No. 2, 2007, pp. 273–294.

<sup>15</sup> Rebecca MacKinnon, "Inside China's Censorship Machine," *National Post*, January 29, 2012.

<sup>16</sup> James Fallows, "The Connection Has Been Reset," *The Atlantic*, March 2008.

More than 60 legal regulations govern Internet content in China. These regulations are enforced at the local, provincial, and national level by at least 12 overlapping government bodies.<sup>17</sup> As comprehensive as this sounds, it is not designed to be foolproof; rather, it is designed to compel Chinese netizens to self-censor. Says Kissel, “enforcement [of censorship] is designed to cause every user and every business in the country to believe that if an Internet law is violated, the violation will be caught and the punishment will be severe. This causes individuals, and ISPs to self-censor. This way, the government does not have to block as much offensive content or locate as many violators.”<sup>18</sup> The urge to self-censor is also rewarded. One American businessman told the *New York Times* of an award ceremony held by the Internet Society of China for Internet Firms: “I’m sitting there in the audience for this thing and they say, ‘And now it’s time to award our annual Self-Discipline Awards!’ And they give ten companies an award. They gave them a plaque. They shook hands. The minister was there; he took his picture with each guy. It was basically like Excellence in Self-Censorship—and everybody in the audience is, like, clapping.”<sup>19</sup>

Some Chinese citizens see the merit of censorship. Said one user in an email, “Trying to make over 50 ethnic groups into a cohesive whole is a problem unique to China and requires unique measures that may seem unpalatable to outsiders. But it works—China is the No. 2 economy now. Why risk potential chaos? So that people can watch YouTube? The government isn’t evil, it’s just practical.”<sup>20</sup> Others, however, fight back—sometimes literally. In May 2011, a college student snuck into a lecture hall at Wuhan University and threw eggs and shoes at Fang Binxing, credited as “the father of the Great Firewall.”<sup>21</sup> Three

---

<sup>17</sup> Trina K. Kissel, “License to Blog: Internet Regulation in The People’s Republic of China,” *Indiana International and Comparative Law Review*, Vol. 17, 2007, pp. 233–234.

<sup>18</sup> Kissel, 2007, p. 242.

<sup>19</sup> Clive Thompson, “Google’s China Problem (and China’s Google Problem),” *New York Times*, April 23, 2006.

<sup>20</sup> “China’s Web Users Debate Internet Freedom,” BBC News website, January 22, 2010.

<sup>21</sup> Andrew Jacobs, “Chinese Student Takes Aim, Literally, at Internet Regulator,” *New York Times*, May 19, 2011.

other students who had planned to take part changed their minds after seeing their professors and supervisors in the audience. Nevertheless, the lone student quickly gained approval on Internet microblog posts hailing him as a hero. Said one poster: “If you, the shoe thrower, get kicked out of school for this, my company will hire you in a minute.” Indeed, the public gloating over the incident is evidence of some level of widespread animosity toward Fang and the system of Internet control he created.<sup>22</sup>

Although the Chinese authorities have technological capabilities to block all politically incorrect content, the context analysis of blocked messages suggests that messages calling for popular mobilization are more likely to be blocked than the ones that simply express dissatisfaction with government policies.<sup>23</sup> Reilly further notes that selective censorship of some, but not all, anti-government content enables authorities to monitor public opinion for any drastic shifts in attitudes and to use it as early warning for political unrest.<sup>24</sup>

Netizens who do not wish to self-censor have two options: They can use circumvention technology like VPNs or programs like UltraSurf,<sup>25</sup> or they can employ code words and pictures to obscure the meaning behind the message so that it does not automatically raise a censor’s red flag. The Chinese authorities have used sophisticated means to curtail the diffusion of circumvention technologies, and consequently, a lifespan of each of them was about three years. A year after the inventions of Freenet and Triangleboy, which enabled connecting to blocked sites via proxy site, the Chinese authorities launched static Internet provider (IP) blocking software to neutralize that access.<sup>26</sup>

---

<sup>22</sup> Jacobs, 2011.

<sup>23</sup> Gary King, Jennifer Pan, and Margaret Roberts, “How Censorship in China Allows Government Criticism but Silences Collective Expression,” *American Political Science Review*, May, 2013.

<sup>24</sup> James Reilly, *Strong Society, Smart State: The Rise of Public Opinion in China’s Japan Policy*, New York: Columbia University Press, 2011, pp. 35–37.

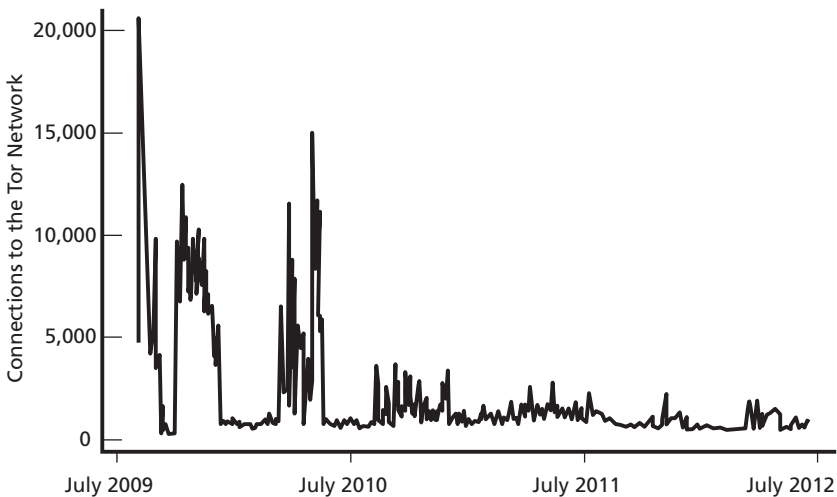
<sup>25</sup> “Digital Weapons Help Dissidents Punch Holes in China’s Great Firewall,” *Wired*, November 2010.

<sup>26</sup> Sara Rimensnyder, “Triangle Boy Howdy,” Reason.com website, March 2002.

When the next-generation circumvention tools such as UltraSurf, Tor, and Coral were developed to anonymize incoming and outgoing traffic, the Chinese authorities responded by blocking access to the Tor network. Tor responded by developing a system of bridges that connect China-based users to the Tor network.<sup>27</sup>

No reliable estimates exist on the number of netizens who use circumvention tools. Tor project is the only tool developer that provides statistics on the estimated daily number of Internet users directly connected to the Tor network (Figure 5.1). However, these data grossly underestimate the number of actual connections, especially for China, because authorities block direct access to Tor. When the Chinese authorities blocked more than 80 percent of Tor relays in September

**Figure 5.1**  
**Number of Connections from China to the Tor Network**



SOURCE: Tor Project.  
RAND RR295-5.1

<sup>27</sup> Christopher S. Leberknight, Mung Chiang, Harold Vincent Poor, and Felix Wong, "A Taxonomy of Internet Censorship and Anti-Censorship," working paper, December 2010.

2009, the number of Chinese netizens directly connected to Tor network dropped abruptly from 20,000 to 0, but picked up again several months later.<sup>28</sup> Studies conducted in 2006 suggest that Tor was less popular in China at that time than DynaWeb, Garden, and Ultra-Surf.<sup>29</sup> A report released by GlobalWebIndex in September 2012 suggests that the share of Internet users who circumvent the Great Firewall can be as high as 15 percent because this percentage corresponds to the percentage of Chinese Internet users who have Facebook accounts. Since Facebook is blocked in China, people have to use either VPN or proxies to access Facebook.<sup>30</sup>

Circumvention technology is not the only weapon to fight censorship. In fact, the vast majority of Internet users favor code words: “scaling the wall” (*fan qiang*, meaning to access blocked content), “buying soy sauce” (*da jiangyou*, meaning that something has nothing to do with the poster or that the poster is unable to change things), “May 35” (which refers to the June 4 Tiananmen incident), and other coded phrases all help netizens express themselves freely.<sup>31</sup> These codes are eventually detected by censors and added to the list of sensitive keywords; for example, “harmony” (*hexie*), Hu Jintao’s frequently cited rationale for government regulation, had been the code word for “repression.” Once Internet censors caught on, the near-homonym “river crab” (also *hexie*, though tonally different) became the new term. This highlights not only the desire to evade censorship, but the rapidity with which Chinese netizens can do so with their constantly evolving lexicon.

---

<sup>28</sup> Tor Project.org, “Tor Partially Blocked in China,” September 27, 2009.

<sup>29</sup> Xiao Tian, *Battle for Freedom in Chinese Cyberspace*, unpublished manuscript, May 2006.

<sup>30</sup> Mlot, 2012.

<sup>31</sup> Mark McDonald, “Watch Your Language! (In China, They Really Do),” *New York Times*, March 13, 2012.

## Online Activists and Authorities in Political Space

The rapidly expanding Chinese blogosphere ignited scholarly debate about possible channels through which new technologies may have affected political space, and several competing explanations emerged. Some argue that the Internet primarily contributed to the expansion of social rather than political space because empowerment has been largely symbolic and manifested itself in the promotion of counterculture and the rise of nationalist identities. For example, the aforementioned popular “river crab” and “harmony” homonyms trace their roots to the vulgar song of the Grass-Mud Horse posted on YouTube, which went viral and even stimulated production of a Grass-Mud Horse toy.<sup>32</sup> The toy became popular with adults because it provided a political means for expressing dissatisfaction with the regime. The Internet also facilitated the expression of nationalist identities among Chinese youth in social context, rather than political, by increasing their exposure to cross-cultural interactions.<sup>33</sup>

Some argue that the expansion of social space has had visible implications for civil rights and the due process of the law. According to Yang, the Internet has fostered interaction among people with similar backgrounds for nonpolitical purposes, and in so doing made it easier for individuals to seek injunction against the state when their civil rights were violated. The first instance when online activism has had a visible impact took place in 2003, when 25-year-old Zhang Xianzhu, who finished first out of 30 candidates competing for a civil job, was turned down because he was infected with hepatitis-B. Zhang shared his story with the members of a China-based hepatitis-B forum and immediately received both emotional support and legal advice, and subsequently filed a lawsuit. The forum members raised public awareness about health-based discrimination, collected donations, and recruited the best legal experts to represent Zhang. This online cam-

---

<sup>32</sup> Lijun Tang and Peidong Yang, “Symbolic Power and the Internet: The Power of a ‘Horse,’” *Media, Culture, and Society*, Vol. 33, No. 5, 2011.

<sup>33</sup> Fengshu Liu, “‘Politically Indifferent’ Nationalists? Chinese Youth Negotiating Political Identity in the Internet Age,” *European Journal of Culture and Studies*, Vol. 15, No. 1, 2012.



paign culminated in the landmark decision that outlawed discrimination against people infected with hepatitis-B.<sup>34</sup>

Yang further notes that the Internet improved civil rights protection in China by fostering online access to court decisions in most cases pertaining to civil offenses.<sup>35</sup> In December 2009, China's Supreme People's Court (SPC) stipulated that all lower-level courts publicize all their verdicts and judgments online and also broadcast trials over the Internet. In some provinces, higher courts took this requirement further. They began ranking lower courts' decisions posted online as the "best" and the "worst" decisions of the year. In 2010, the SPC launched a survey to evaluate each lower court on a 100-point scale on such dimensions as openness of trial and judgment, openness of hearing, and the extent of online dissemination of judgments.<sup>36</sup>

The open trial reform made lower civil court judges more sensitive to online discourse, especially when renowned legal experts engaged in online discussion of the specific case or ruling. Blogs, Weibo, and other social media networks made it easier for Chinese citizens to seek fair trial in civil litigation by soliciting experts' opinions and disseminating them online. As Huang notes, "online public opinion has the capacity to bring vertical influence (from the higher-level government or central government) and lateral influence (from lawyers, scholars, and other legal professionals)" on courts promptly and efficiently.<sup>37</sup>

These examples illustrate that the expansion of social space has had spillover effects on political space by empowering individuals in cases where their civil rights were violated and granting them access to fair trial in criminal procedures. This became possible because of the growth of rights consciousness among Chinese citizens and party officials' concerns about corruption.

A similar trend has been observed in other areas. Online activism led to visible policy changes only in those cases when activists' demands

---

<sup>34</sup> Yang, 2009.

<sup>35</sup> This provision does not seem to apply to criminal cases.

<sup>36</sup> Shumei Hou and Ronald C. Keith, "A New Prospect for Transparent Court Judgment in China?" *China Information*, Vol. 26, No. 1, March 2012, pp. 61–86.

<sup>37</sup> Huang, 2012, p. 736.

were consistent with party officials' objectives. Chinese authority is fragmented vertically and horizontally. The vertical fragmentation stems from the federal constitution that grants subnational officials the power to promote economic development as well as to regulate online content. The horizontal fragmentation is rooted in the intra-party factionalism and ideological divisions between conservative and progressive factions. Both vertical and horizontal fragmentation fosters internal policy conflicts. Contesting factions, therefore, capitalize on social discontent to achieve specific policy outcome or to strengthen their positions within the power hierarchy. This internal competition affected the success of online protests. Online mobilization brought about visible political changes when the progressive faction capitalized on social discontent to advance its reform agenda. Online mobilization was unsuccessful when it challenged the overall political system or called for democratization. In those cases, the conservative and progressive factions united to suppress it.<sup>38</sup> Thus, the success of online activists in shaping policy outcomes depended on strategic calculation of party elite who used social grievances to advance their agenda.

## Online Mobilization and Policy Outcomes

Although the literature on the Internet and politics in China provides interesting insights into the structural constraints on the democratizing potential of the Internet, the existing accounts are incomplete because they neglect the mechanisms that first enable online mobilization in a tightly censored environment and then lead to political action offline. As we pointed out in the theoretical section in Chapter Two, the menu of online activism is specific to the regime and is most limited in authoritarian societies like China. Since the Chinese Communist Party bans all organized political opposition, online mobilization is undertaken not by professional politicians or interest groups, but by individual activists interlinked by virtual ties.

---

<sup>38</sup> Zheng, 2008.

Unlike democratic regimes with a vibrant civil society, virtual ties among Chinese netizens are not complemented by strong social ties because the civil society is anemic and cannot foster offline social mobilization in the same manner as in democratic regimes. Despite vivid online discourse, Chinese civil society has not caught up with the rapidly expanding social space online, and most online interactions are not anchored in organizational structures that can facilitate collective action offline. Only a small share of netizens who comprise the rapidly growing social space online have ties to NGOs or civil society organizations. More nuanced analysis is needed to understand how online activism maps into offline actions.

We now look at two widely publicized accounts of online mobilization. We selected recent cases to make them relevant to rapidly changing censorship and circumvention methods. Both protests took place in 2011: protests after the train crash in Wenzhou and the protests against a local chemical plant in Dalian. In both cases, citizens were motivated by economic considerations triggered by lax regulation of economic activity. Citizens used the Internet to mobilize, spread facts that the government officials were trying to conceal, and question the government policies. These cases also highlight the growing power of the rising middle class, that segment of Chinese society that has been statistically more likely to be Internet users and Weibo account holders. We show that, in contrast, the Internet was less effective for citizens in rural areas, partly because only about a quarter of them use the Internet, but also because they are more easily marginalized and repressed. To put it plainly, the power of the Internet in China is a function of the power of the person using it.

### **Wenzhou Train Crash**

Online activity after the high-speed train crash in Wenzhou in the summer of 2011 is an example of the Chinese government's attempt to censor and repress the facts surrounding a catastrophe along with any and all reporting of those facts. It is also a striking case of the Chinese print media, bolstered by an enraged online citizenry, refusing to be censored.

At 8:27 p.m. on July 23, train D301 from Beijing crashed at full speed into the back of train D3115 from Zhejiang. The official explanation was that train D3115 had stopped on the tracks after a power outage, but passenger accounts and video clips uploaded by witnesses showed that train D3115 was still moving.<sup>39</sup> The impact caused six cars to derail; four fell from the elevated bridge on which the crash occurred. The accident killed more than 40 people and injured approximately 200.<sup>40</sup>

None of the major state-run newspapers ran any story of the crash on the front page of their Sunday editions. Rather, a user of Sina Weibo first broke the story; this was the medium that continued to spread the news during the aftermath of the crash. By the railway minister's first press conference 24 hours later, millions of Chinese had already seen images of the wreckage, read reports about what had caused the crash and expressed outrage over photos of bulldozers crushing the crumpled cars on the ground and burying them.<sup>41</sup> In response, the Chinese government backtracked quickly; Wang Yongping, China's railway spokesman, said a colleague had told him the reasons for burying the wreckage was to fill a ditch and make the rescue effort easier. The media was ordered not to send reporters to the crash site, not to report on the crash too frequently, and, specifically, not to link the crash to any other story about how China had developed its high-speed rail capability.<sup>42</sup> "There must be no seeking after the causes [of the accident;] rather, statements from authoritative departments must be followed," said one directive. Another specifically prohibited "dissemination [of crash information] on personal microblogs!"<sup>43</sup> Instead, the media was to focus on "stories that are extremely moving. . . . From now on, the

---

<sup>39</sup> Anna Zhang, "Public Outrage Mounts Over Train Wreck's Botched Rescue," *Forbes*, July 27, 2011.

<sup>40</sup> Steven Jiang, "Chinese Netizens Outraged over Response to Fatal Bullet Train Crash," *CNN World*, July 25, 2011.

<sup>41</sup> Jiang, 2011.

<sup>42</sup> Tania Branigan, "Chinese Anger over Alleged Cover-Up of High-Speed Rail Crash," *Guardian*, July 25, 2011.

<sup>43</sup> Branigan, 2011.

Wenzhou train accident should be reported along the terms of ‘major love in the face of major disaster.’”<sup>44</sup>

Chinese newspapers did not comply with the government directives. The *Economic Observer*, China’s equivalent of the *Financial Times*, ran an eight-page special on the crash, the cover of which showed a picture of the wreckage with the blood-red logo of the railway ministry superimposed. The *Beijing News*, the most popular news daily in the capital, reported the story in code, describing in detail how an item of pottery in a Beijing museum broke into six pieces (mirroring the six derailed train carriages); the story ran below a photograph entitled “China’s Speed,” showing Chinese swimmer Sun Yuan but also alluding to the criticism that the Chinese government has modernized the country too recklessly.<sup>45</sup>

These reports followed a week of furious online activity on China’s microblogs, particularly Sina Weibo. The theme of some of the comments centered on the idea that the government has a duty to report accurate and timely information. “We have the right to know the truth! That’s our basic right!” wrote one microblogger. Others criticized the speed with which the government was pursuing progress.<sup>46</sup>

Most of China received news reports and information online, with Sina Weibo also becoming an information exchange to help people find missing relatives.<sup>47</sup> One of the most damning pieces of evidence that the Chinese government mishandled the situation was that rescue efforts were called off only eight hours after the crash. One rescue worker, Shao Yerong, a police captain from Wenzhou, refused to follow orders and found a 2-year-old girl named Xiang Weiyi 21 hours after the accident. This caused Internet users to speculate who

---

<sup>44</sup> Zoe Murphy, “China Struggles to Censor Train Crash Coverage,” *BBC News*, July 28, 2011.

<sup>45</sup> “Chinese Newspapers Defy Ban to Report on Train Tragedy,” *Guardian*, August 2, 2011.

<sup>46</sup> Branigan, 2011.

<sup>47</sup> Zhang, 2011.

else might have been found had the government allowed rescue work to continue.<sup>48</sup>

The 2011 train crash illustrates that the speed with which information can be circulated defies the keyword-based filtering that Chinese authorities use to censor the Internet. Throughout the aftermath of the crash, the public's desire for knowledge moved faster than the government's ability to censor information. This served as a warning to China's government leaders that censorship is a weak weapon against the speed with which the Internet moves.<sup>49</sup> As Xie Yue, a political scientist at Tongji University in Shanghai, said after the crash, "There has been progress in more quickly disclosing information, but the Internet is forcing that change, because with the Internet and microblogging, witnesses and the public can spread news nationwide instantly, so that the government can't control information like it did."<sup>50</sup>

This case suggests that the authorities responded to online mobilization because bloggers generated nationwide publicity. High volumes of information posted online prompted the traditional media to break the silence despite the ban. Microblogging also changed the point of reference from a natural disaster to a tragedy caused by a systemic corruption and poorly considered modernization of the country. Such framing of the event resonated with a much wider audience than victims' families and friends. After the train crash became an issue of national importance, inaction became too costly for the party officials. They had to respond by dismissing high-ranking officials at the Railway Ministry.

### **Dalian Chemical Plant**

The protest that closed the Dalian chemical plant in Liaoning Province in 2011 is another example of the power of the Internet to effect change, and another unintended consequence of China's enthusiastic adoption of wireless communication. During the summer of 2011,

---

<sup>48</sup> Zhang, 2011.

<sup>49</sup> Chris Buckley and Ben Blanchard, "China High-Speed Crash Shows Leaders' Struggle to Keep Up," Reuters website, July 29, 2011.

<sup>50</sup> Buckley and Blanchard, 2011.

waves created by a tropical storm broke the sea wall around the Fujia chemical plant and sparked protests to move the plant farther away from the city center. Fujia produces paraxylene (PX), a toxic chemical used in plastics that can cause eye and skin irritation in small doses and genetic defects and death after prolonged exposure.<sup>51</sup> Much like the Wenzhou train crash that summer, the protests against Dalian were enabled by the speed of the Internet and the number of people using it. Said one citizen of Dalian, “Once [the protest] was happening, I could follow everything through the pictures.”<sup>52</sup>

The idea for the protest began on Sina Weibo after a post on Saturday called for people to “stroll” on Sunday morning starting from 10 a.m. on the People’s Square, near which the Dalian government is located,” according to a resident of Dalian.<sup>53</sup> Though it only began a day before, protesters created large banners, T-shirts, professionally printed placards, and other items.<sup>54</sup> More than 12,000 demonstrators marched in Dalian, one of the largest protests reported since 2008; in a dramatic moment, the Communist Party Secretary of Dalian stood on top of a car and pleaded with the demonstrators to go home.<sup>55</sup> The protesters of Dalian saw results very quickly: Chinese authorities ordered the factory to close the same day as the protest.

Censors were unable to delete posts quickly enough to contain news of the protests on Sunday, but they did try to hide the fact that the protest happened at all. The Monday after the protest, all mention of Dalian and the protests began to disappear from search results and microblogs. The China Media Project tracked which words had specifi-

---

<sup>51</sup> Jamil Anderlini, “Mass Protest Forces Chinese Factory to Close,” *Financial Times*, August 14, 2011.

<sup>52</sup> Sharon LaFraniar and Michael Wines, “Protest Over Chemical Plant Shows Growing Pressure on China from Citizens,” *New York Times*, August 15, 2011.

<sup>53</sup> Sui-Lee Wee, “China Says It Will Shut Plant as Thousands Protest,” Reuters website, August 14, 2011. “Stroll” is a code word for protest.

<sup>54</sup> LaFraniar and Wines, 2011.

<sup>55</sup> LaFraniar and Wines, 2011.

cally been blocked—words like “stroll,” “Dalian,” and “PX.”<sup>56</sup> Authorities also canceled a news show about dangerous projects in Dalian just before it was about to be aired. When the host, Bai Yansong, complained on his Weibo page, his account froze. Undeterred, he logged into another account and wrote, “This is the public information sphere! I really don’t know what you are afraid of.”<sup>57</sup>

A characteristic common to the Wenzhou outcry and the Dalian protest is that both were led by China’s increasingly powerful—and increasingly vocal—middle class, whom Chinese leaders fear alienating. The average Dalian citizen is relatively well off, well educated, and well connected via the Internet, social media, and text messages. Some residents of Dalian are also well connected politically. Yang Yang, a political scientist at China University of Political Science and Law, says that “Dalian has a lot of wealthy, upper-class people, and their influence over the government is far greater than ordinary people. It’s no surprise that the project was canceled amid the public anger.”<sup>58</sup> Similarly, the victims of the train crash were members of “China’s new wealthy elites, given the much-criticized high price of tickets.” It was difficult to contain the story because the people it affected regularly use the microblogs that spread the story. Estimates of the number of posts about the train crash range in the tens of millions.<sup>59</sup>

Middle-class discontent expressed publicly is most threatening to Chinese leadership because it contradicts the Chinese truism—the so-called Beijing Consensus—that as long as people enjoy economic progress, other issues like democracy and freedom of expression will not be a major concern. What the response to the train crash and the chemical plant protest prove is that China’s middle class not only wants a government that does not place economic progress above the safety

---

<sup>56</sup> David Bandurski, “Dalian Protests Erased from Social Media,” blog post at China Media Project, August 14, 2011.

<sup>57</sup> LaFranier and Wines, 2011,

<sup>58</sup> “China Closes Chemical Plant Targeted by Protesters,” *USA Today*, August 15, 2011.

<sup>59</sup> Michael Wines, “China Expands Program Requiring Real-Name Registration Online,” *New York Times*, January 18, 2012.



of its citizens, but also believes it has a right to say so publicly.<sup>60</sup> Being so connected, China's middle class is who notices the "conspicuous silence" of China's Internet censorship the most.<sup>61</sup>

### **Internet and Popular Mobilization in Rural Areas**

The level of Internet penetration is significantly lower in rural areas. In 2011, 50 percent of urban residents had access to the Internet, compared with only 18 percent in rural areas (Figure 5.2).<sup>62</sup> The rate of Internet diffusion in rural areas is affected by the type of economic activity in a village and the socioeconomic status of villagers. Traditional villages in which residents are engaged in subsistence farming lag far behind industrialized or commercialized ones.<sup>63</sup>

The lower level of Internet penetration in rural areas makes it more difficult to find evidence that it facilitated popular mobilization and that it was successful. For example, residents of Xinglong village located in Yunnan, one of China's poorest provinces, have been battling for years to remove the Luliang Chemical factory. Its byproducts, such as chromium, are carcinogenic, and after having dumped more than 5,000 tons of wastewater into nearby Nanpan River, cases of cancer and sickened cattle rose. Unlike the protesters in Dalian, Yunnan protesters have been ignored and arrested at worst, and given small amounts of compensation at best.<sup>64</sup> Local authorities have been ineffective.

Similarly, officials in Beijing responded to a land confiscation dispute in Wukan village in Guangdong province only after it escalated into a violent confrontation between villagers and local police. Wukan village benefited by the Internet indirectly because it attracted national

---

<sup>60</sup> David Pilling, "China Crashes into a Middle Class Revolt," *Financial Times*, August 3, 2011.

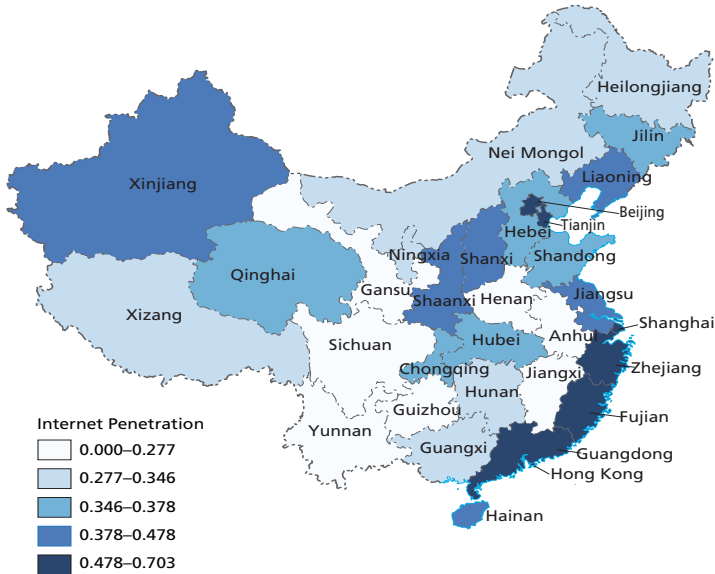
<sup>61</sup> Peter Foster, "Beijing Fears Nimbyism of Angry Middle Classes," *Telegraph*, August 19, 2011.

<sup>62</sup> East-West-Connect.org, *Rural Internet Usage in China*, web page, October 28, 2011.

<sup>63</sup> Yuhua Guo and Peng Chen, "Digital Divide and Social Cleavage: Case Studies of ICT Usage Among Peasants in Contemporary China," *China Quarterly*, Vol. 207, September 2011, pp. 580–599.

<sup>64</sup> "Chemical Plant Protest Highlights China's Class Divide," *Guardian*, August 18, 2011.

**Figure 5.2**  
**China Internet Penetration Rate**



SOURCES: Technasia.com, “China Internet Penetration Map,” January 17, 2012; tealeafnation.com, “A Map of Two Chinas — Internet Penetration and Economic Development,” January, 22, 2013.

RAND RR295-5.2

attention to the widespread problem of land embezzlement by corrupt local officials. However, Chinese authorities made it more difficult to obtain information about the conflict by filtering out searches containing “Wukan.” Wukan practically vanished from the web, because when users queried this keyword, they received a message saying, “According to relevant law, regulations, and policies, search results for Wukan cannot be displayed.”<sup>65</sup>

A low level of Internet penetration, combined with low population density and remote geographic location, made it easier for Beijing to ignore protesters in Yunnan. Less than a quarter of the 41 million people of Yunnan province, spread over a territory about the size of

<sup>65</sup> “China Protest in Guangdong’s Wukan ‘Vanishes from Web,” *BBC News*, December 15, 2011.

Spain,<sup>66</sup> use the Internet.<sup>67</sup> By contrast, Liaoning province has roughly the same population (42 million),<sup>68</sup> half of whom use the Internet in an area two-fifths the size.<sup>69</sup> Fewer people with restricted Internet access makes it easier for censors to stay a step ahead of any unrest, and to buy people off in the meantime.

The second factor is that, because home computers are expensive, rural residents are more likely to access the Internet in cybercafes, where it is easier to monitor and censor activity because the computers use the same Internet connection. By contrast, wealthier Chinese citizens can connect to the Internet individually at home or on their mobile phones.

These combined factors reduce the likelihood that a rural resident, however motivated, can transmit a message to the general public. Thus, the rural populations of China are least likely to be able to effect change.

## Ethnic Riots and the Internet

Unlike the middle class, ethnic minorities only marginally benefited by the advent of the Internet because of the heavy-handed measures that Chinese authorities took to suppress protests that challenged the existing order. Content deletion rates (by censors or authors) have been the highest in Tibetan Autonomous Region and Qinghai province, which has a large Tibetan and Hui Muslim population (Figure 5.3). Posts originating from the Ningxia Hui Autonomous Region also have high removal rates. The second highest rates of content deletion have been for the Xinjiang Uyghur Autonomous Region, which has large number of Uyghur Muslims, and the Inner Mongolia Autonomous Region, with large population of ethnic Mongolians.

---

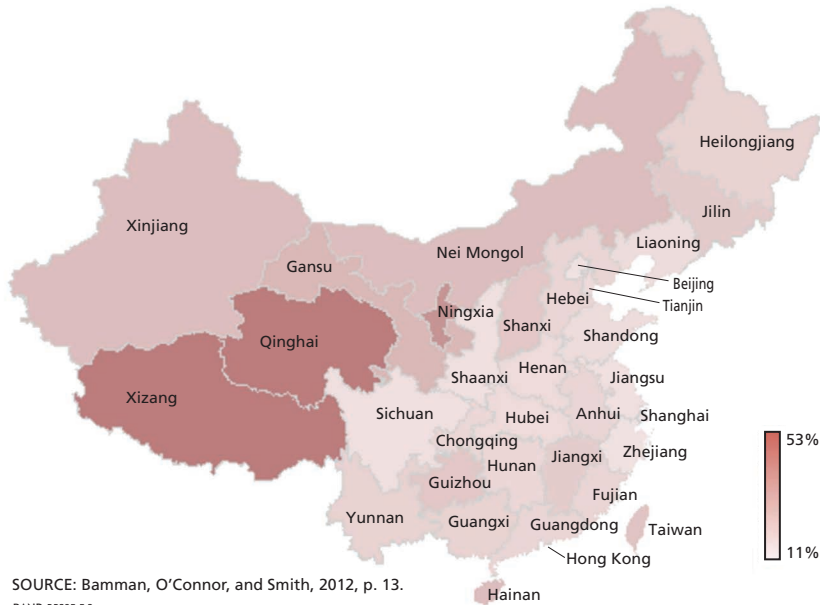
<sup>66</sup> China Internet Information Center, *Yunnan: Illuminating China's Provinces, Municipalities and Autonomous Regions*, web page, undated.

<sup>67</sup> Techinasia.com, 2012.

<sup>68</sup> Consulate General of the United States, *Overview of Liaoning Province*, web page, undated.

<sup>69</sup> Techinasia.com, 2012.

**Figure 5.3**  
**Deletion Rates by Province**



This section examines in greater depth the impact the Internet had on the nature of the Uyghur struggle for greater autonomy, religious freedom, and better economic opportunities. Although Xinjiang territory has been under the Chinese rule since at least 1759, Uyghur managed to preserve a distinct identity, religion, and language. The Uyghur resistance to the Chinese rule manifested itself in occasional mass protests and violent attacks against party and law enforcement officials appointed by Beijing, and in private resistance to the official propaganda. Popular culture, poems, and novels transmitted coded subversive messages that defied official propaganda. Mosques further reinforced Uyghurs' distinct identities and cultural heritages.

Seeking to curtail private resistance, the Chinese authorities imposed tighter censorship in the region than in the rest of the country and frequently imprisoned Uyghur writers, singers, and intellectuals. In the pre-Internet era, the Chinese authorities were able to delegitimize any popular protest in Xinjiang region as a challenge to the territorial

integrity and in so doing could justify using heavy-handed measures against “separatists.” Frequent human right abuses against Uyghurs went unnoticed by the international community due to Xinjiang’s geographic isolation from the rest of the world and its minimal interactions with the diaspora. Fearing the Soviet Union’s fate, the Chinese authorities responded to most of Uyghurs’ demands with silence, repression, and policies that directly contradicted those advocated by protesters.<sup>70</sup>

With the advent of the Internet, Han-Uyghur tension migrated online. The Uyghur organizations located abroad waged campaigns to construct pan-Uyghur identity and to challenge the Chinese interpretation of the history.<sup>71</sup> The Uyghurs’ growing online presence triggered more aggressive blocking and hacking of Uyghur sites by the Chinese authorities. Central Asian states followed suit and also began blocking the Uyghur sites. As a result, Uyghur diaspora organizations that gained international online visibility were not well integrated with actors in Xinjiang. For example, the Uyghur American Association has served as an information hub for the Western media and international NGOs but has been unable to establish strong ties with the China-based Uyghur population because the Chinese authorities shut down forums that sought to bridge the two communities.<sup>72</sup>

These online international networks, although porous, proved to be capable of attracting international attention to ethnic protest in Xinjiang in July 2009. The protests in Xinjiang’s capital, Urumchi, began in response to a violent attack of Uyghur workers in the Guangdong province located 2,000 miles away. The news quickly spread throughout China and reached Xinjiang. Ten days later, thousands took to the streets of Urumchi to express their dissatisfaction with how the authorities in Beijing handled the episode. After the authorities shut

---

<sup>70</sup> Gardner Bovington, *The Uyghurs: Strangers in Their Own Land*, New York: Columbia University Press, 2010.

<sup>71</sup> Kristian Petersen, “Usurping the Nation: Cyber-Leadership in the Uighur Nationalist Movement,” *Journal of Muslim Minority Affairs*, Vol. 26, No. 1, April 2006.

<sup>72</sup> Yu-Wen Chen, *Who Made Uyghurs Visible in the International Arena: Hyperlink Analysis*, Global Migration and Transnational Politics, Working Paper No. 12, June 2010; John Kennedy, “China: Ethnically Diverse Forum Shut Down,” *Global Voices Advocacy*, May 20, 2008.

down Internet access in the entire province and brutally suppressed the demonstration, protests were staged in front of the Chinese embassies in Turkey, the Netherlands, Norway, Kazakhstan, and other countries with a significant presence of the Uyghur diaspora. The Chinese authorities responded to the growing concerns of the international community by letting international journalists be present to cover the riots. This was an unprecedented measure; only government-controlled media were allowed to cover previous riots. The journalists could access the Internet at the hotels where they were staying. Among images that emerged from the scene were those that documented how well-armed police suppressed female demonstration.<sup>73</sup>

Xinjiang was without Internet access for ten months, and this blackout paralyzed as much as 85 percent of all Uyghur sites.<sup>74</sup> The government also cracked down on many Uyghur civil rights activists. As many as a dozen were sentenced to death and others received lesser sentences. Three men were sentenced to prison terms of three to ten years for posting improper content on their websites, which were subsequently blocked by the authorities. Among these three activists was the founder of the most popular Uyghur website, Diyarim, who was prosecuted for failing to delete in a timely manner posts about an upcoming rally and other posts criticizing the government.<sup>75</sup> Ilham Tohti, the founder of another popular website called Uighur Online, was detained after protests but released several months later, after Reporters Without Borders staged an online campaign emphasizing the important work he was doing to promote Han-Uyghur dialogue.<sup>76</sup>

---

<sup>73</sup> "China Riots: Uighurs Stage Fresh Protest in Urumqi," *Telegraph*, undated.

<sup>74</sup> "Survey of Blocked Uyghur Websites Shows Xinjiang Still Cut Off from the World," Reporters Without Borders website, October 29, 2009.

<sup>75</sup> Andrew Jacobs, "China Imprisons Three Men Who Maintained Uighur Web Sites," *New York Times*, July 30, 2010.

<sup>76</sup> "Campaign for Jailed Uyghur Blogger," Reporters Without Borders website, July 16, 2009.

## Internet Freedom Technologies: Tools for the Motivated Elites or Mass-Use Technologies?

Online mobilization in China during the 1990s consisted primarily of mass emails from the leaders of Falungong, Tibetan activists, and the China Democratic Party to their followers. In those emails, the dissenters circulated materials about movement goals and other literature outlawed by the authorities. Very few of these emails were encrypted so as not to raise suspicion among the Chinese authorities and were sent out to movement followers and to Communist Party officials. Bulletin board sites and websites provided additional venues for one-way flows of information.<sup>77</sup> Such a top-down communication left little opportunity for grassroots input into the movement's goals and its development of strategies.

The advent of Web 2.0 technologies, such as microblogging platforms and social media, changed the nature of online activism by increasing netizens' involvement in coordinating bottom-up online mobilization. Since around 2010, microblogs have been the primary tool by which Chinese dissidents have spread news and mobilized. As of 2012, two new regulations directly threaten this ability. First, all bloggers must now register with their real names to get accounts, whereas before they could remain anonymous. Second, Sina Weibo must review the posts of bloggers who have more than 100,000 followers and must delete any "harmful" post within five minutes.<sup>78</sup> Registering with one's real name will encourage self-censorship; code words and phrases will not be enough anymore. Says Peter Guo, a Xiamen-based blogger and online activist, "Most people are more daring about what they say if they can stay anonymous. [The authorities] have created an atmosphere of fear, so those who aren't so willing to take risks

---

<sup>77</sup> Michael Chase and James Mulvenon, *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies*, Santa Monica, Calif.: RAND Corporation, MR-1543, 2002.

<sup>78</sup> McDonald, 2012.

. . . will just censor themselves the whole time now. That will be the biggest effect of real-name registration: self-censorship.”<sup>79</sup>

The second regulation will give censors a head start in preventing the dissemination of dissentious posts, because rather than having to maintain an ever-evolving list of terms that might catch a censor’s eye, now they only need to focus on the most popular bloggers as potential sources of unrest. As one member of the online rights advocacy group HR China said, “If one person has a few million followers, it doesn’t matter if a sensitive post is deleted after a few minutes or a few hours—a few *million* people will see it anyway.”<sup>80</sup> This new regulation will go far toward preventing that from happening.

Chinese authorities’ attempts to further curtail Internet freedom gives rise to the following policy dilemma: Should Internet freedom efforts focus on broadening of the political space by expanding average netizens’ access to circumvention technologies? Or should the efforts be concentrated on deepening political space by reaching out primarily to civil society activists? Our discussion suggests that the most visible political gains emerged as a spillover effect of nonpolitical uses of the Internet. Promoting mass use of circumvention technologies may have a greater impact on the political space than would programs that target a handful of activists. Therefore, the most effective efforts may be focused on enhancing online privacy for all Internet users, be it through building public awareness of already existing circumvention technologies, facilitating their access to non-China based microblogging platforms that protect users’ anonymity, or both.

---

<sup>79</sup> “China Clamps Down on Microblogs,” Radio Free Asia website, December 22, 2011.

<sup>80</sup> Interview with HR China member, February 17, 2012.





## Fighting Electoral Fraud in the 2011 Russian Election with Internet and Social Media

---

Chapters Three through Five discussed when and how the Internet can transform state-society relations by expanding opportunities to post, browse, and share information online for netizens, i.e., those Internet users who actively use this medium for self-expression and networking. This chapter introduces new actors, cyberactivists, and examines their role in expanding political space. Cyberactivists are high-profile individuals or organizations who turn to the Internet to advance a specific cause, and their numbers are extremely small. To understand how they can expand political space, it is important to examine the factors enabling them to reach out to those citizens whose support allows virtual mobilization to grow into visible offline political action. This chapter examines how this link emerged in the context of the 2011 Russian election that culminated in postelection protests in major cities. Since the scale of the protests was unprecedented by Russian standards, both foreign and domestic media quickly drew parallels between these protests and the Arab Spring and credited social media with igniting them.<sup>1</sup> Rather than looking at the protests themselves, in this chapter we step back and examine the events that took place online shortly before protests broke out. The key protagonist of this chapter is elec-

---

<sup>1</sup> Alissa de Carbonnel, "Insight: Social Media Makes Anti-Putin Protests 'Snowball,'" Reuters website, December 7, 2011; Nataliya Dzhanpoladova, "Sotsial'nye Seti v Bor'be za Chestnye Vybery" ["Social Technologies Network's Fight for Fair Election"], Radio Liberty website, December 8, 2011; "RuNet Organizuyet Massovye Protesty v Moskve y za Eye Predelami" ["RuNet Organizing Mass Protests in Moscow and Beyond"], CyberSecurity.ru, Russian website, December 8, 2011; Frida Ghitis, *World Citizen: Facebook, Twitter and the Protests of 2011*, World Politics Review website, December 15, 2011.

tion watchdog Golos, which was among a handful of cyberactivists in Russia taking advantage of the rapid expansion of Internet access. Golos launched a crowdsourcing platform that enabled voters to upload information about electoral violations.

Our analysis begins with a theoretical section that explains why information about fraudulent elections can trigger massive protests even in the most nondemocratic regimes. We then provide a background on the Internet use in Russia, and Golos' activities. A large-N analysis follows, which examines the link between nonpolitical uses of the Internet and political activism and shows that the Internet facilitated whistle-blowing of electoral abuses only in those regions where voters are accustomed to using the Internet at their workplace. Finally, we discuss how social media and the Internet subsequently facilitated popular mobilization in Moscow, St. Petersburg, and several other major cities in the aftermath of the 2011 election.

This chapter contributes to the ongoing debate about the relationship between the Internet and democratization by bringing to the foreground those actors who are the key link between cyberactivists and rank-and-file voters. By launching an election violations map, Golos expanded the opportunities for all Russian voters to post information about electoral abuses; however, those who were accustomed to using the Internet for nonpolitical activities were most likely to take advantage of this whistle-blowing opportunity. Thus, Russian employers became an unintentional yet critical link between political and nonpolitical uses of the Internet. In examining how Internet freedom can affect political space, careful attention should be paid to the context in which the expansion of Internet freedom occurs.

## **Critical Information and Postelection Protests**

During the past decade, a wave of postelection protests—color revolutions—rocked the post-Communist countries. They started in 2000 in Serbia and had a domino effect in Georgia in 2003, Ukraine in 2004, and Kyrgyzstan in 2005, eventually reaching Russia in December 2011, when thousands of angry voters took to the Moscow streets to protest

the results of the legislative election in which United Russia, led by Prime Minister Putin, won 52 percent of the seats in the lower chamber (hereafter, Duma). As with Russia, color revolutions in other countries were sparked by massive ballot-stuffing and electoral violations that undermined the role of elections as instruments of democracy.

Anecdotal evidence suggests that new information and communication technologies (i.e., the Internet) facilitated voter mobilization. The first Internet-enabled protest broke out in Serbia in the 1996 aftermath of President Slobodan Milosevic's decision to annul the results of the municipal elections at which the opposition coalition, *Together*, won majorities in 14 major cities. These protests came to be known in Serbia as the Internet Revolution because a handful of politically active and tech-savvy students at Belgrade University spread the word about anticipated protests via email and helped B92, the only independent radio station in Serbia at that time, to circumvent the authorities' ban on its broadcast. Four years later, on the eve of the so-called Bulldozer Revolution, the Serbian civic youth movement *Otpor* (Resistance) turned to the Internet again to recruit its members.<sup>2</sup> Similarly, the Orange Revolution in Ukraine was facilitated by mobile phones. Victor Yushchenko's supporters rapidly circulated information about the place and time of protests by texting the message "Go to *Maydan*, wear orange" to thousands of friends and acquaintances.<sup>3</sup> The 2009 postelection protests in Moldova, frequently referred to as the Twitter Revolution, disputed the outcomes of the parliamentary elections in which the Communist Party won the majority of seats—another example of technology-facilitated postelection protests.<sup>4</sup>

The rapidly growing theoretical literature on the color revolutions emphasizes that they were sparked by critical information that

---

<sup>2</sup> David S. Bennahum, "The Internet Revolution," *Wired*, Vol. 5, No. 4, April 1997; James Aulich, "The Democratic Delusion: New Media, Resistance and Revolution in Serbia, 1995–2000," *Studies in Russian, European and Central European New Media*, Vol. 5, 2011, pp. 1–21.

<sup>3</sup> Josh Goldstein, *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution*, Berkman Center Publication, No. 2007-14, December 2007.

<sup>4</sup> "Moldova's 'Twitter Revolution,'" Radio Free Europe press release, April 8, 2009.

altered individuals' decision to participate. In nondemocratic regimes, the extent of political opposition is unknown because most individuals who oppose the regime falsify their preferences to avoid retribution by authorities. As Kuran notes, individuals in nondemocratic regimes hold two sets of preferences: private preferences that they share only with a small circle of close friends, and public ones they exhibit to everybody else.<sup>5</sup> This observation is consistent with studies of public opinion and behavior in the Soviet Union. As Zimmerman shows, while many *nomenklatura* members voted for the Communist Party (the only party printed on the ballot), they also regularly listened to the BBC and read *samizdat*.<sup>6</sup> In Kuran's terminology, this situation constitutes preference falsification in which public behavior and private beliefs diverge. Undoubtedly, there were many others in the Soviet Union who sincerely supported the Communist Party and voted for it because they subscribed to the Marxist-Leninist ideals. However, neither the Soviet authorities nor the general public could differentiate the former from the latter. Kuran further argues that individuals' decisions to reveal their true preferences depend on the actions of others. Some are willing to expose their anti-regime attitudes with only a handful of others challenging the regime; others would participate in a demonstration only if the size of a protesting crowd surpasses thousands.

Unofficial election results make private preferences public. Individuals who voted against the incumbent realize that the majority of others did the same. This information lowers the costs of protests because the authorities are less likely to use coercion against thousands of protesters. As Tucker notes, collective knowledge about electoral fraud becomes a "focal point" that facilitates demonstrations by reducing the cost of collective action.<sup>7</sup> The information affected not only rank-and-file voters

---

<sup>5</sup> Kuran, 1991, pp. 7–48.

<sup>6</sup> William Zimmerman, "Mobilized Participation and the Nature of the Soviet Dictatorship," in James R. Millar, ed., *Politics, Work, and Daily Life in the USSR: A Survey of Former Soviet Citizens*, New York: Cambridge University Press, 1987.

<sup>7</sup> Joshua Tucker, "Enough! Electoral Fraud, Collective Action Problems, and Post-Communist Color Revolutions," *Perspectives on Politics*, Vol. 53, No. 5, September 2007, pp. 537–553.

but also security forces and the army. As Kuntz and Thompson show, unofficial election results in Serbia and Ukraine prompted the military's defection from the incumbents.<sup>8</sup>

The above studies suggest that although the information about electoral abuses posted online in the aftermath of the 2011 failed to provide accurate assessment of electoral fraud, it nevertheless may have served as a focal point that brought together opposition groups from across the ideological spectrum, including liberals, nationalists, anti-corruption activists, celebrities, and other reformers. We will examine whether and how the expansion of Internet access and social media may have created conditions for voters to take advantage of whistleblowing opportunities provided by Golos.

Before proceeding, it is worthwhile to define a set of cases to which the argument of this chapter applies. Postelection protests share several distinct features that set them apart from other forms of civil unrest. In most cases, unofficial election results unambiguously indicate which of the candidates or parties would have won if elections were fair. This creates an "endowment effect." Behavior economists discovered this effect when analyzing people's willingness to give up goods they possessed and determining that individuals demand higher compensation for giving them up compared to what they initially paid.<sup>9</sup> Unofficial election results produce a similar endowment effect by creating an illusion of victory among those voters who supported the opposition candidates, thereby contributing further to voters' frustration with electoral fraud. Presidential systems further exacerbated voters' frustration with unmet expectations. With the exception of Moldova, color

---

<sup>8</sup> Philipp Kuntz and Mark R. Thompson, "More than Just the Final Straw: Stolen Elections as Revolutionary Triggers," *Comparative Politics*, Vol. 41, No. 3, April 2009, pp. 253–272.

<sup>9</sup> Daniel Kahneman, Jack L. Knetsch, and Richard H. Thaler, "Experimental Tests of the Endowment Effect and the Coase Theorem," *Journal of Political Economy*, Vol. 98, No. 60, 1990, pp. 1325–1348; W. Michael Hanemann, "Willingness to Pay and Willingness to Accept: How Much Can They Differ?" *American Economic Review*, Vol. 81, No. 3, June 1991, pp. 635–647; C. Morewedge et al., "Bad Riddance or Good Rubbish? Ownership and Not Loss Aversion Causes the Endowment Effect," *Journal of Experimental Social Psychology*, Vol. 45, 2009, pp. 947–951; David W. Harless, "More Laboratory Evidence on the Disparity Between Willingness to Pay and Compensation Demanded," *Journal of Economic Behavior and Organization*, Vol. 11, 1989, pp. 359–379.

revolutions erupted in presidential or semi-presidential systems in the aftermath of presidential elections. This is not surprising: Elections in presidential systems leave no opportunities for the defeated candidate to participate in policymaking. In parliamentary systems, even when elections are rigged, the opposition may still win enough seats to influence the composition of government and policies.<sup>10</sup> Finally, the timing of the color revolutions in Eastern Europe coincided with the influx of voters who had no recollection of the life under the Soviet system and who became eligible to vote for the first time after 2000. These young voters were also tech-savvy and the primary consumers of online news. When generalizing from this study to other situations, it is important to bear in mind these three peculiar features of the context in which this analysis is situated.

## **RuNet: Russian Internet**

A rapid expansion of Internet access fostered the rise of political activism online. Between 2000 and 2012, the rate of Internet penetration in Russia increased from about 2 percent to 43.5 percent (or 60 million people). Of that number, 72 percent use the Internet on a daily basis.<sup>11</sup> Although Internet usage has remained higher among people under the age of 24 (81 percent), the expansion of Internet usage grew more rapidly among middle-aged Russians and reached 69 percent for Russians

---

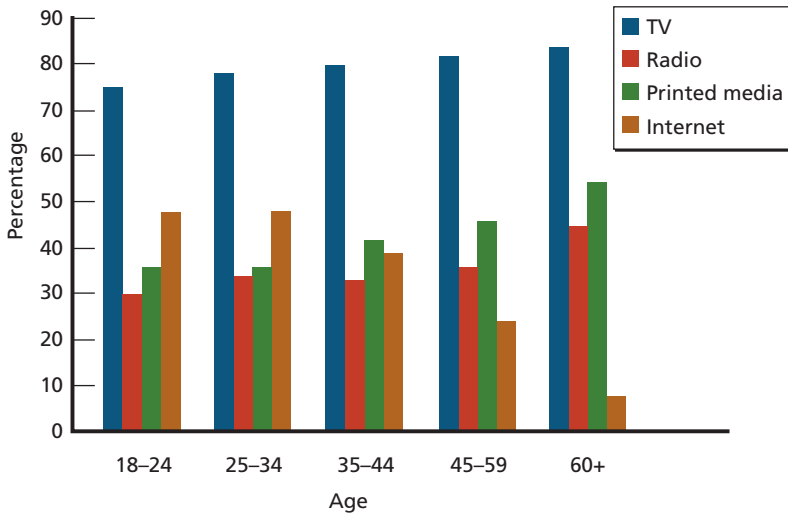
<sup>10</sup> Although protests began after the parliamentary election in Russia, parliamentary elections are considered a rehearsal for the presidential one that always takes place three months later.

<sup>11</sup> World Bank, World Development Indicators, ComScore, "Russia Has Fastest Growing Internet Population in Europe," press release, August 27, 2008. Several factors propelled this growth: (1) the expansion of the telecommunication infrastructure and mobile phones that made Internet services more affordable outside of Moscow and St. Petersburg; (2) the modernization of the workplace that promoted Internet usage among adults in their mid-thirties and mid-forties; and (3) the federal programs that improved Internet access at public schools and universities.

between the ages of 25 and 34, and 55 percent for those 35–44, who tend to be more politically engaged than those in their 20s.<sup>12</sup>

The Internet has been catching up rapidly with other media as the source of political information, especially for Russians younger than 35. In 2011, almost 50 percent of Russians under 35 said the Internet constituted an important source of political information, compared with only 35 percent for radio and newspapers (Figure 6.1). A similar conclusion emerges from another survey that asked more specific ques-

**Figure 6.1**  
**Important Source of Political Information, March 2011**



SOURCE: Compiled from VTsIOM, 2011.

NOTE: A national representative sample of 1,600 respondents was asked: “Does the television (radio, newspapers, Internet) constitute an important source of political information for you?” The answer options were “important,” “not very important,” “do not use this medium,” and “decline to answer.” The percentages are for the “important” category.

RAND RR295-6.1

<sup>12</sup> Federal’noye Agenstvo po Pechati i Massovym Kommunikatsiyam (Federal Agency for Press and Mass Communications), *Internet v Rossii: Sostoyaniye, Perspektivy, iTendentsii Rasvitiya* [Internet in Russia: Status, Prospects, and Trends of Development], 2011, pp. 8–11.



tions about media preferences. The Russian search engine Yandex and the Russian version of Facebook, vKontakte, emerged as the most frequently mentioned sources of daily news consumption for respondents under 35. The national television channel, the First Channel, ranked third as the most frequently mentioned news source.<sup>13</sup>

Several features of RuNet should be noted because they may have affected how protests unfolded. First, in spite of the rapid growth of Internet penetration, the level of access has remained much lower in regions outside Moscow and St. Petersburg, which prompted some Russian observers to conclude that the Internet is still a tool of the urban elite.<sup>14</sup> This digital divide may have contributed to the fact that protests were confined to Moscow, St. Petersburg, and several other major cities with sufficiently high levels of Internet penetration.

Second, the Russian blogosphere has not fully evolved into a place where active discussion of public matters takes place. Although there is lots of political discussion, Russian blogger Eugene Gorny says most of it is informal chats among friends, rather than public discourse.<sup>15</sup> Thus, it is possible that Russian Internet users were more influenced by firsthand accounts of electoral fraud than by media coverage of any other political events.

Third, although online anonymization is still a novelty for the vast majority of Russian Internet users, Tor usage was correlated with the timing of elections: The number of Russians connected to the Tor network reached its maximum in December, shortly before the election (Figure 6.2).

Fourth, the level of discussion across different ideological camps is very high. Unlike the United States, where bloggers cluster with like-minded others, there is no evidence of “echo chamber” formation. Most Russian blogs are linked to a wide variety of news sources and to blog-

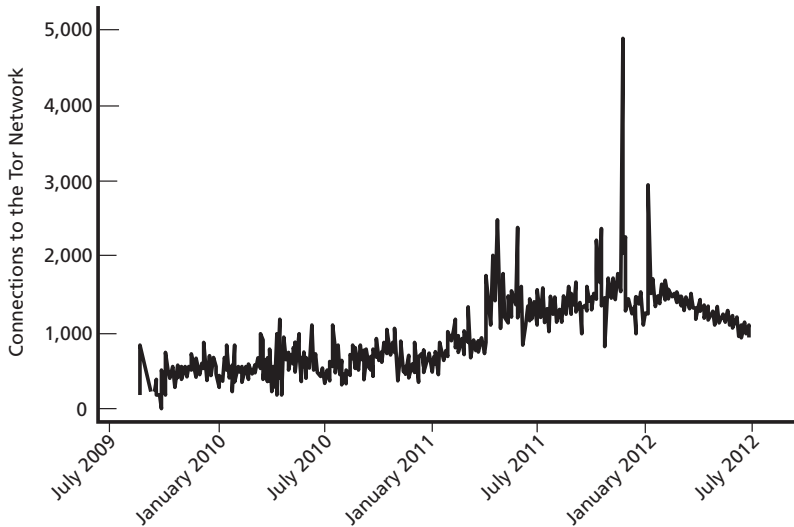
---

<sup>13</sup> Federal'noye Agenstvo po Pechati i Massovym Kommunikatsiyam, 2011, p. 17.

<sup>14</sup> Karina Alexanyan, “The RuNet—Lost in Translation,” *Russian Analytical Digest*, Vol. 69, December 2009, pp. 3–6.

<sup>15</sup> Eugene Gorny, “Understanding the Real Impact of Russian Blogs,” *Russian Analytical Digest*, Vol. 69, December 2009, pp. 7–11.

**Figure 6.2**  
**Number of Connections from Russia to the Tor Network**



SOURCE: Tor Project.  
 RAND RR295-6.2

gers with different ideological orientations.<sup>16</sup> Lower levels of ideological fragmentation may have made it easier for the diffusion of information about the electoral fraud across different ideological camps.

### **Russian Authorities and Cyberactivists**

Unlike Chinese authorities, whose filtering of online content targets the masses, Russian authorities developed sets of tools to target cyberactivists. Prior to summer 2012, these measures included coercion against selected bloggers, DDOS attacks, and eavesdropping. In the summer of 2012, censorship of online content was added to the menu of options.

#### ***Eavesdropping***

The legal grounds for selective policing of online traffic stem from the law on System for Operative Investigative Activities (SORM) II and

<sup>16</sup> Etiling et al., 2010.

III that defines the information space as a vital resource and authorizes the government to use all available means to protect it. This legal framework allows authorities to request information about website owners from ISPs and de-register any website or remove content from it. For example, the website Kompromat.ru that reports the information about abuses of public office by high-ranking officials has been de-registered several times. In 2008, Russia amended the SORM III that mandated ISPs to purchase and install eavesdropping equipment that also permit local Federal Security Service (FSB) offices to monitor online traffic of any user.<sup>17</sup> In the aftermath of the 2011 elections, the Russian authorities used the SORM technology to tap phone conversations and email traffic of opposition leaders and subsequently posted them on pro-government site lifenews.ru to discredit the opposition.<sup>18</sup>

### **DDOS**

DDOS has constituted an alternative method of dealing with cyber-activists.<sup>19</sup> The first wave of politically motivated DDOS was documented in March and April of 2011, at the time of regional elections.<sup>20</sup> These attacks were resumed in December 2011 on Election Day and took down more than a dozen opposition sites.<sup>21</sup> All attacked sites were

---

<sup>17</sup> Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in Ronald Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, Mass.: MIT Press, 2010.

<sup>18</sup> Andrei Soldatov, "In Ex-Soviet States, Russian Spy Tech Still Watches You," *Wired*, December 21, 2012.

<sup>19</sup> Soldatov, 2012.

<sup>20</sup> Soldatov, 2012.

<sup>21</sup> See Hal Roberts and Bruce Etling, "Coordinated DDOS Attack During Russian Duma Elections, Internet Democracy Blog, December 8, 2011. The sites attacked were the New Times, an oppositional news site; the Echo of Moscow, a leading independent radio station; Novaya Gazeta, a major oppositional newspaper, often critical of the Kremlin; Novaya St. Petersburg; Kommersant, a major Russian news daily; Public Post, an online news site that had published stories about maps of violations and Golos; Slon, an online news site that partnered with Golos to publish a "map of violations" after Gazeta backed out; Bolshoi Gorod, a St. Petersburg news site; Golos, an independent election monitor; Ikso, an outlier, the election commission of Sverdlovsk region; Ridus, an online news/citizen journalism site; Zaks, a popular political website in St. Petersburg; Pryaniki, a popular portal in Tula; Map

more likely than any others to report electoral violations. The DDOS attacks continued after the election and targeted those websites that covered postelection protests.<sup>22</sup>

As protests unfolded, the Russian authorities even attempted to take down one of the most popular Russian social media sites, vKontakte, after its chief executive officer refused to block the page with the information about upcoming protests. The company spokesman noted that they had been closely monitoring the activity on the protest page and blocked those users who called for violence and disorders.<sup>23</sup> Several days later, vKontakte was subjected to a massive spam attack and subsequently had to terminate open registration, which slowed new member enrollment.<sup>24</sup>

### ***Violence Against Cyberactivists***

There have been also a handful of cases when coercion was used against online activists, including a murder of an online journalist, ten physical attacks, and 38 prosecutions of independent newspapers for extremist content.<sup>25</sup> Although this number pales in comparison to repression of online activists in China or other authoritarian regimes, these cases nevertheless generated enough publicity that may have deterred others from engaging in activism online.

---

of Violations, a Golos crowdsourced election violations map web page; files.kartanarusheniy.ru, a subdomain of the “map of violations” page; LiveJournal, a major Russian blog platform; Kotlin Forum, a forum related to the Kronshdat region; Kotlin, a site with news and info related to the Kronshdat region; GosZakupki, another apparent outlier in the group, a portal for Russian federal and local government tenders; The Other Tver, an oppositional Tver news and analysis site; and RosAgit, a website connected to activist and blogger Alexey Navalny.

<sup>22</sup> For example, Agentura.ru and Facebook pages with information on dates and places of upcoming protest rallies were attacked. See Andrei Soldatov, “Vladimir Putin’s Cyber Warriors,” *Foreign Affairs*, December 9, 2011.

<sup>23</sup> “Russian Social Network Rebuffs FSB Request to Close ‘Opposition’ Accounts—Spokesman,” RIA News, December 8, 2011.

<sup>24</sup> “Chislo Novykh Pol’zovateley vKontakte Posle Otmeny Registratsii Socratilos’ Pochti v Dvoye” [“Number of New vkontakte Members Drops by Nearly Half After Abolition of Open Enrollment”], Korresponnet.net, February 17, 2012.

<sup>25</sup> “Nepравitelstvennyy Doklad: ‘Nesvobodniy Internet’” [“Non-Governmental Report, ‘The Lack of Internet Freedom’”], *Novaya Gazeta*, January 28, 2012.

### **Censorship**

The enactment of the Internet law (*Federal'niy Zakon 139-F3*) in July 2012 marked the beginning of a new era in the regulation of RuNet.<sup>26</sup> The new law gives the government the right to shut down any website without a court order if it fails to comply with its request to remove content deemed harmful for minors. Under this law, the government can compile a list of sites that must be blocked by ISPs and can order search engines to filter searches. Blocked websites have only three months to appeal the decision in court. Although the law is intended to protect minors from pornography, drugs, and other harmful information, it gives the federal government enough authority to impose Chinese-style censorship on RuNet.<sup>27</sup>

In September 2012, YouTube became the first target of this law when authorities in several Russian regions blocked access to it because of the controversial video “Innocence of Muslims.” In November, YouTube was included in a national register of banned sites that was created to enforce the Internet regulation law. Several hours later, however, the Russian authorities issued a statement that this blacklisting was erroneous and removed YouTube from the list. This new Internet regulation law underscores the precarious state of Internet freedom in Russia. Under the pretense of protecting minors from harmful online content, opponents of Internet freedom erected legal and technological apparatuses to impose full-scope censorship of the Internet.

### **Golos and Online Election Fraud Reporting**

The analysis that follows will focus on the online activism of Golos, the only independent election watchdog in Russia, which sought to expand whistle-blowing opportunities for Russian citizens. Golos, which means “voice” in Russian, was established on the eve of the 2000 presiden-

---

<sup>26</sup> Duma RF, *Federal'niy Zakon [Federal Law] 139-F3*, June 30, 2012.

<sup>27</sup> Yaroslav Garbonevskiy, “Anton Nosik Comments on the Internet Law: Lawmakers Deserve ‘D’ for this Law,” RFI, Russian website, July 12, 2012; Vladimiar Kar-Murza, “On the Introduction of Control of the Russian Internet,” (in Russian) RFE/RL, July 11, 2012.

tial election to monitor ballot counting. By mid-2012, it had opened branches in 48 of 83 regions to train volunteers on how to detect and report any violations of electoral law either during the registration of candidates and political campaigning or on Election Day. During the 2003 Duma election, Golos worked with the two opposition parties, Yabloko and the Union of Right Forces, in conducting the first parallel ballot-counting in Russian history, verifying more than 12,000 election protocols. In 2005, Golos created a hotline that could be used by any voter in Russia to report electoral violations either by calling, texting, or sending an email.<sup>28</sup> During the 2008 presidential election, Golos received 1,166 reports about electoral violations, most of which involved regional authorities exerting undue pressure to vote in a certain way, inaccuracies in the lists of registered voters, and ballot stuffing.<sup>29</sup>

As the number of Internet users grew in Russia, Golos began using the Internet to facilitate citizen monitoring. In October 2011, Golos supplemented the hotline with a web-based application that enabled voters to report violations during regional elections by filling out a form on Golos's website. These reports were immediately posted on the "Map of Violations."<sup>30</sup> In May 2011, Golos put together a comprehensive data set with election results at the precinct level for all elections that had taken place in Russia since 2003 as a way to facilitate statistical analysis of election results. Although these results are also available at the Central Election Commission, downloading them for the entire country required sophisticated programming skills. Golos provides these results in an easily accessible, comma-separated values file, along with links to articles that discuss alternative statistical meth-

---

<sup>28</sup> "10 Let na Zashchite Izbiratelnykh Prav" ["10 Years on the Protection of Electoral Rights"], Golos, April 28, 2010.

<sup>29</sup> "Na Goryachuyu Liniyu 'Prozrachniye Vybory' Prishlo 1166 Zhalob" ["Transparent Elections' Hotline Received 1,166 Complaints"], novayagazeta.ru website, March 2, 2008.

<sup>30</sup> "Karta Narusheniy Popolnyayetsa Narusheniyami" ["A Collection of Election Violations"], Golos, October 11, 2011.

odologies for detecting irregularities.<sup>31</sup> Golos also provided an interactive online training manual.

Golos has had uneasy relations with the Russian authorities. In some regions, authorities attempted to shut down local branches on procedural grounds; in others, authorities impeded access to polling stations.<sup>32</sup> As the 2011 Duma election approached, Russian authorities charged Golos with violating election laws by posting the results of public opinion polls five days prior to the election.<sup>33</sup> A day before the election, when Golos's president was returning from a trip abroad, Russian customs officials detained her for 12 hours, then confiscated her laptop. The next morning, a DDOS attack followed. The Golos site was attacked along with sites of 14 other independent newspapers. Golos, however, was able to relaunch its site on Google Docs and post the map with electoral violations on Google Maps. By the end of Election Day, the site contained 7,800 messages about violations.<sup>34</sup> Golos put up a similar map for the 2012 presidential elections, and 5,144 violations were reported.<sup>35</sup>

Golos's map should not be interpreted as the measure of overall electoral fraud. It is voter-reported instances of electoral violations that happened during the registration process, ballot casting, and ballot counting. Thus, the frequencies reported on the map depend on the magnitude of violations, as well as voters' abilities to both detect those violations and report them. Cross-regional comparisons about the mag-

---

<sup>31</sup> "Organizatsiya Golos Otkryla Sayt so Statistikooy po Vyboram" ["Golos to Open Election Statistics Website"], Golos, May 11, 2011.

<sup>32</sup> "Pravozashchitniki Obespokoyeny Sud'boy Samarskogo Golosa" ["Human Rights Activists Concerned About Fate of Samara Voices"], Golos, June 23, 2008; "Golos-Povolzhye Vozobnovlyayet Rabotu" ["Golos-Volga Resumes Work"], Golos, May 14, 2008; Raido Svoboda, "U Assotziatziy Golos Izyali Dokumenty dlya Nablyudeniya za Vyborami v Orle" ["Golos Observes Document Seizures in Election"], Golos, February 14, 2010; "Nenuzhniy Svidetel" ["Needless Witness"], Golos, April 2, 2011.

<sup>33</sup> Grakon.org homepage, undated; "Prosecutors Accused the 'Voice' of Violating the Election Law," BBC Russian website, December 1, 2011; patdollard.com, *Head of Russian Political Watchdog Group Arrested Ahead of Elections*, web page, December 3, 2011.

<sup>34</sup> "Karta Narusheniy Na Vyborakh 2011," undated.

<sup>35</sup> "Karta Narusheniy Na Vyborakh 2011," undated.

nitude of electoral fraud can be misleading based on this map, because reporting rates can be lower for regions with higher levels of electoral violations. This map is still useful for comparing cross-regional differences in whistle-blowing by voters if we find a proxy measure for the amount of electoral fraud in the region. Other limitations of the map are that it does not discriminate between minor and major violations, or whether reports refer to the same or different violations. In spite of these limitations, this map is very useful for examining the factors that contributed to cross-regional differences in reporting rates.

### **Golos and Citizens' Whistle-Blowing**

By launching the election violation maps, Golos created a new venue for voters to express their dissatisfaction with the election process. But it is far from clear who took advantage of this opportunity. Voters may have ignored Golos because they were not aware of this opportunity, were afraid to use it, or simply did not have the IT skills necessary to transmit information. This section examines the conditions under which voters were more likely to take advantage of the available technology. In particular, we juxtapose three alternative mechanisms that could have strengthened the links between Golos and voters and thus encouraged whistle-blowing.

The first mechanism is the informational environment of the traditional media, which affects the cost of learning about Golos activities and politics in general. Access to political news enhances citizens' political knowledge, which can in turn promote civic engagement by (1) enhancing citizens' understanding of the link between their own and group interests, (2) making citizens' views more consistent across issues and across time, and (3) providing a framework for interpreting political events, thus increasing political participation.<sup>36</sup> The second mechanism is the diffusion of IT skills that make it less costly to use the Internet for political purposes. The third mechanism involves the

---

<sup>36</sup> For review of the literature, see William A. Galston, "Political Knowledge, Political Engagement, and Civic Education," *Annual Review of Political Science*, Vol. 4, 2001, pp. 217–234.



level of economic development needed to increase citizens' whistleblowing by strengthening their attachment to democratic values.<sup>37</sup>

An original data set was collected to evaluate relative importance of these mechanisms. Informational environment is measured by a set of variables that capture the rate of traditional media penetration:

- the number of newspapers per capita published in the region
- the percentage of local stations that receive and transmit two major radio stations (*Mayak* and *Radio Russia*)
- the percentage of local telecommunication companies that can receive and transmit NTV Channel in the analog mode. (Although there is more than one major channel, we included only NTV in this analysis because it was the only channel in the 1990s that was independent of the government and provided national coverage.)

We measure the rate of IT skills by the rate of Internet penetration at the workplace because for many Russians residing outside of major cities, their workplace constitutes the primary place of Internet access. Modernization of the workplace occurred between 2005 and 2010, when the number of computers per 100 employees increased from 23 to 36 on average. The number of computers connected to the Internet at the workplace grew from 7 in 2005 to 18 in 2010. Mobile phones constitute another new technology that could enable citizen monitoring. Therefore, the number of phone subscriptions per capita was included in the model specification.

The percentage of urban population and gross domestic product (GDP) per capita serve as measures of regional modernization. A dummy variable was included to account for possible differences between the two major cities of Moscow and St. Petersburg and the rest of the country.

Finally, we needed to account for the extent of electoral fraud in the region because the number of reported violations depends on both the

---

<sup>37</sup> Seymour Martin Lipset, "Some Social Requisites of Democracy: Economic Development and Political Legitimacy," *American Political Science Review*, Vol. 53, No. 1, March 1959, pp. 69–105.

amount of fraud and on citizens' willingness to report violations. Since the amount of fraud is not directly observed, a complicated statistical procedure (described in the appendix) was used to construct a proxy variable. Higher values of this variable correspond to more fraud. (Summary statistics are reported in the appendix.)

Using these data, a negative binomial model was estimated and coefficients are reported in Table 6.1. These results should be interpreted as correlation, not causation. Although the variables were measured before the elections, there might still be some unobserved regional characteristics correlated with the number of reported violations and Internet penetration. Since the model is nonlinear, marginal effects are reported in column 2 to facilitate substantive interpretation. They capture the percentage change in the dependent variable as a result of a unit change in the independent variable, while holding all other factors constant.<sup>38</sup>

Although the access to traditional media should increase citizens' political awareness and should contribute to civil activism, we find little empirical evidence that Russian traditional media fostered political activism. Access to traditional media either has a negative effect or no effect at all on the number of posted violations. This might be due to the tight control by the government that makes the traditional media reluctant to publish any information on electoral irregularities. Out of all variables, the coefficients on newspapers are the only ones that are statistically significant.

### **Access to Technology**

The positive coefficient on the number of computers connected to the Internet at work suggests that the average number of reported violations increases by almost 8 percent for each additional computer connected to the Internet per 100 employees. If we compare an *oblast*, or region, with the average value of computers connected to the Internet (about 15 computers per 100 employees)—e.g, Ivanovskaya *oblast*—and a region that has 16 computers connected to the Internet per 100

---

<sup>38</sup> Jeffrey Wooldridge, *Cross-Sectional and Panel Data Analysis*, Cambridge, Mass.: MIT Press, 2002, p. 648.

**Table 6.1**  
**Correlates of Whistle-Blowing in the 2011 Election in Russia**

Variable	Negative Binomial Coefficients	Marginal Effects	Negative Binomial Coefficients
<b>Access to traditional media</b>			
Newspapers per capita	-0.24* (0.06)	-15.57* (5.30)	-0.23* (0.08)
Access to NTV	0.01 (0.01)	0.23 (0.37)	0.01 (0.01)
Access to Radio <i>Mayak</i>	-0.01 (0.01)	-0.64 (0.54)	-0.01 (0.01)
Access to Radio Russia	-0.01 (0.01)	-0.18 (0.89)	-0.01 (0.12)
<b>Access to technology</b>			
Computers at work connected to Internet	0.12** (0.06)	7.93** (3.72)	0.12** (0.06)
Computers at work	-0.12** (0.05)	-7.71** (3.09)	-0.11** (0.05)
Mobile phones per capita	0.86 (0.53)	56.60 (35.21)	0.89*** (0.53)
<b>Modernization</b>			
Urban population	0.01 (0.01)	0.89 (0.86)	0.02 (0.01)
GDP per capita	0.00 (0.00)	-0.01 (0.00)	0.00** (0.00)
Moscow and St. Petersburg	1.64*** (0.93)	262.82 (297.13)	1.41 (0.92)
Proxy for electoral fraud	-0.99 0.64	-65.08 (42.48)	
Constant	5.33* (1.78)		5.04* (1.79)
Ln-alpha	-0.33** (0.16)		-0.31** (0.15)
Pseudo-R <sup>2</sup>	0.07		0.07
Log-Likelihood constant only	-428.56		-428.56

Table 6.1 (Continued)

Variable	Negative Binomial Coefficients	Marginal Effects	Negative Binomial Coefficients
Log-Likelihood full model	-398.53		-399.66
LR-statistic	60.08		57.81
p-value	0.00		0.00
Observations	77	77	77

NOTES: The dependent variable equals the number of electoral violations; standard errors are in parentheses.

\* indicates significant at 1 percent; \*\* at 5 percent, \*\*\* at 10 percent; marginal effects were evaluated at the mean values.

employees—e.g., Kaluzhskaya *oblast*—there will be 7.5 more violations reported in the latter region. When we compare an average region with Moscow, which has 42 computers connected to the Internet per 100 employees, the expected number of reported violations should be 202 higher for Moscow than for an average region.

The positive coefficient on the Internet variable suggests that when two regions have identical levels of technological development, citizens are more likely to report electoral violations when they have access to the Internet at work. These spillovers into the political realm are not surprising. Surfing the web for job-related purposes makes people more skillful at identifying relevant and timely information and increases their familiarity with major online newspapers, blogging sites, and other online resources. Those who use computers and the Internet at work are more likely to use them at home and are more likely to have email accounts and social media profiles. All these factors increase the probability that citizens will become aware of Golos's activities and will report electoral violations when they encounter them.

Similar to the Internet variable, the coefficient on the rate of mobile phone penetration is positive—but it is not statistically distinguishable from zero. The coefficient may not be statistically significant because the rate of mobile phone penetration is highly correlated with the Internet variable. To account for this possibility, one needs to test if both the Internet and mobile phones jointly contribute to whistle-blowing. The

log-likelihood test result (LR – test(2) = 7.89, p-value = 0.019) suggests that these two variables both contribute to citizens' political activism.

Unlike the variable that measures the number of computers connected to the Internet, the coefficient for the number of computers at work is negative. This finding could be due to the fact that technologically advanced regions, concentrated in the northwest, have higher levels of political pluralism and electoral fraud is less prevalent. Less-advanced regions tend to be located in the northeast and the southeast and to have natural resource endowments. These regions, however, have never fully democratized and even after the collapse of the Soviet Union continued to be governed by the former *nomenklatura*. The level of political pluralism has been extremely low there because regional governors have relied on coercive means to mobilize electoral support.<sup>39</sup>

### **Modernization**

The correlation between the rate of urbanization and reporting of electoral fraud is small and is not distinguishable from zero. Similarly, the GDP per capita does not have any effect on the number of violations. Moscow and St. Petersburg together had 164 percent more reported violations than the average region in the rest of the country.

The proxy for electoral fraud has a negative sign, but is not statistically significant. This proxy measures the distance between the actual distribution of turnout and a hypothetical distribution if elections were fair. Since this is not the actual measure of fraud, the correlation is not strong enough to be either statistically significant or to have a correct sign. Therefore, the model was re-estimated excluding this variable. The results are reported in Table 6.1, column 3. The signs of the coefficients remain the same for all variables.

This empirical analysis illustrates that the Internet has a distinct effect on political behavior in Russia that is different from other media. Regions where citizens had access to the Internet at work had higher levels of whistle-blowing than regions with lower Internet penetration.

---

<sup>39</sup> See, for example, Henry Hale, "Correlates of Clientelism: Political Economy, Politicized Ethnicity, and Post-Communist Transition," in Herbert Kitschelt and Steven I. Wilkinson, eds., *Patrons, Clients, and Policies: Patterns of Democratic Accountability and Political Competition*, New York: Cambridge University Press, 2006.

The Internet has a statistically significant effect, even when access to traditional media is accounted for.

## **Electoral Fraud, Social Media, and Post-Election Protests**

The Golos map of violations was not the only source of information about electoral violations. YouTube videos documenting various violations at polling stations began flooding the Internet on Election Day. The exact number of those videos is unknown, but a simple keyword search for “Elections 2011: Violations” returned 155 unique YouTube entries, and these videos attracted slightly less than 2.5 million views (15,000 views on average). Links to some of these videos were posted on the sites of independent newspapers.

The Central Election Commission’s (CEC) announcement of official election results on December 7 that confirmed 49 percent of the popular vote for United Russia prompted another spike of online activity, especially on the blogging platform LiveJournal.ru, the e-journal Slon.ru, and other popular newspapers. Those sites compared election results obtained by independent observers at polling stations with official results reported by the CEC on its site. In many cases, the commission overstated the number of pro–United Russia votes. To facilitate the exchange of this information, several websites were created on which people could upload documentation showing discrepancies.<sup>40</sup>

Articles with different statistical methodologies for documenting electoral fraud began flooding RuNet. An analysis by Aleksey Zakharov, a professor at the Higher School of Economics, compared the results for Moscow electoral precincts at which violations were detected with the ones without violations. On average, United Russia won 26.7 percent of the popular vote in districts without violations and 42.6 percent where violations were reported. The turnout was 10 percent higher

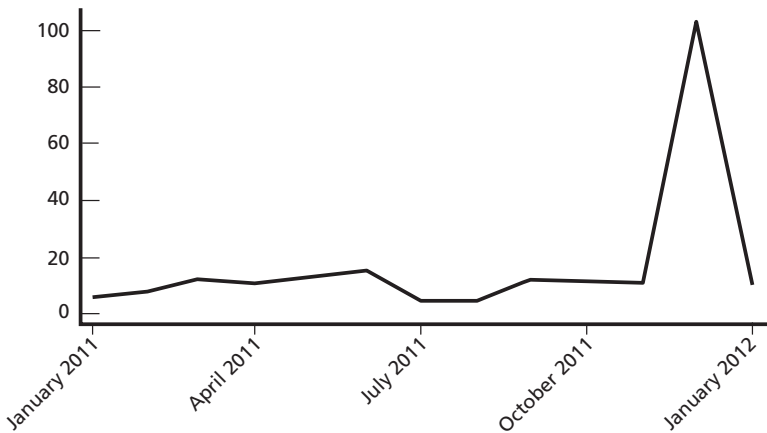
---

<sup>40</sup> “Collection Protocols: Elections to the State Duma,” *komiunity.ru* website, December 4, 2011; “Results of the Election in Russia,” *elections.grakon.org* website, undated.

at the precincts where violations were reported.<sup>41</sup> Another methodology for identifying electoral fraud consists of comparing the distribution of turnout in Russia with turnout in other countries that have clean elections. The number of Russian precincts in which turnout exceeded 90 percent is disproportionately high. Furthermore, this high turnout is strongly correlated with votes for United Russia.<sup>42</sup>

Evidence that the Internet facilitated the diffusion of information about electoral violations emerges from the analysis of Google search trends. The frequency of searches in Russian for such terms as “falsifications” (*falsificatsii*) rose drastically in December 2011 (Figure 6.3).

**Figure 6.3**  
Frequency of Searches for “Falsifications,” 2011



SOURCE: Google Trends.

NOTE: The y-axis reflects how many searches have been done for a particular term, relative to the total number of searches done on Google over time.

RAND RR295-6.3

<sup>41</sup> Alexey Zakharov, “How Many Votes Observers Saved in the Parliamentary Election,” Slon.ru, December 7, 2011.

<sup>42</sup> Sergei Shpilkin, “Election Statistics Examined,” Herald, Russian website, December 10, 2011; “Dubious Vote in Russia,” InoPressa, Russian website, December 28, 2011; Sergei Shpilkin, “No Choice,” *Esquire*, Russian website, December 1, 2011; Alexander Kireev, *Politics, Elections and Beyond* blog, undated.

Online allegations of electoral fraud, however, failed to produce agreement on which parties suffered the most. Some suggested that *Yabloko* was hurt the most because it failed to overcome the 7 percent vote threshold required for getting Duma seats. Others pointed out that ballot padding only marginally benefited United Russia because the true share of its vote hovered around 42 percent. Still others asserted that the Communist Party would have emerged as the largest party in the Duma if the election were fair.

Such uncertainty about the extent of fraud was partially due to the lack of reliable exit poll results. Two polling organizations in Russia, Russian Public Opinion Research Center (VTsIOM) and Public Opinion Fund (FOM), published exit poll results that attributed, respectively, 48.5 percent and 45.5 percent to United Russia. However, the nonresponse rate for the VTsIOM poll was as high 23.7 percent.<sup>43</sup> FOM reported neither the nonresponse rate nor the margin of error. Thus, the violations reported on YouTube and on Golos's site constituted the only available evidence of electoral fraud. They were insufficient, however, to estimate the extent to which the official results overstated the actual vote.

### **Social Media and Voter Mobilization**

While the information about electoral fraud circulated on the RuNet, the opposition turned to Facebook and vKontakte to mobilize Internet users. Four Facebook members—Kirill Mezhtentsev, a high school student; Grigory Efimov, a postdoctoral fellow at Engelhardt Institute of Molecular Biology; his wife, Sasha Primakova, who used to work at the market research company; and Ilya Klishin, a journalist and blogger—put up pages with the information about upcoming protests. These pages served as focal points for the supporters of fair elections by providing information about the place, date, and time of the protests. Activists could also solicit technical help with broadcasting those protests.

---

<sup>43</sup> “United Russia Wins 48.5 Percent; KPRF, LDPR, and Just Russia Also Win Duma Seats: Exit Poll” (in Russian), RIA News website, December 4, 2011; “Exit Poll: V Den’ Vyborov v Gosdumy RF,” FOM website, December 4, 2011.



These pages also created a peer pressure by posting the names of Facebook members who were invited to participate in the demonstration with their corresponding replies. About 90,000 invitations were sent out for the December 9 event, and almost 39,000 (43 percent) recipients responded that they would attend. Almost 11,000 (12 percent) said “maybe.” About 50,000 (45 percent) did not reply. In preparation for the December 24 meeting, 87,000 invitations were sent out, and about 61 percent agreed to participate. Only 27 percent did not respond. More than 51,000 invitations were sent out for the February 4 meeting, and about 53 percent of those recipients confirmed their participation (Table 6.2). A similar mobilization took place at vKontakte.ru, albeit on a more modest scale. For example, the page with the February 4 event attracted only 9,024 registered users and 7,055 of them responded with “may attend.”

Facebook also facilitated communication between rank-and-file voters and the opposition leaders. Visitors to the event pages could indicate which of the opposition leaders they would like to join them. The persons in most demand were journalist Leonid Parfenov, online activist Aleksei Navalny, *Yabloko* party founder and leader Grygoriy Yavlinskiy, and rock celebrity Yuriy Shevchuk, most of whom subsequently joined the protesters.<sup>44</sup>

**Table 6.2**  
**Facebook and Demonstrations for Clean Elections**

Details	December 9, 2011	December 24, 2011	February 4, 2012
Invited	90,913	87,187	51,851
Going	38,999 (42.90%)	53,616 (61.50%)	27,652 (53.33%)
Maybe	10,924 (12.10%)	9,820 (11.30%)	6,382 (12.03%)
Place	<i>Bolotnaya Square</i>	<i>Sakharov Prospect</i>	<i>Bol'shaya Yakimanka</i>

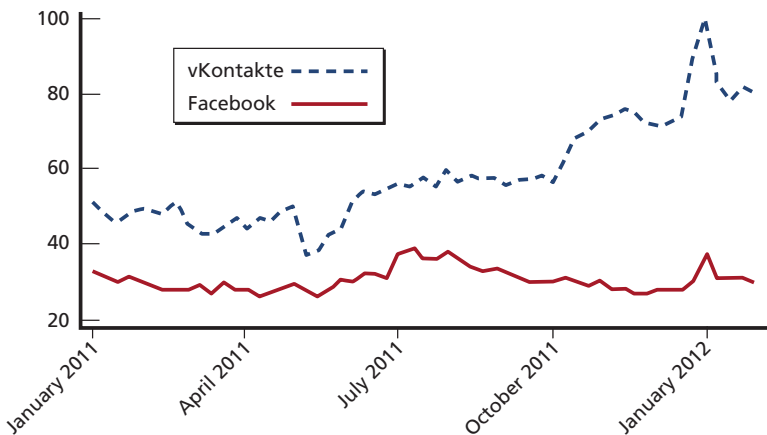
SOURCES: Compiled from Facebook events pages (in Russian): *Saturday at Bolotnaya Square, Meeting on Dec. 24*, and *A Peaceful March for Fair Elections, February 4*.

<sup>44</sup> St. Petersburg for Fair Elections, “Who Would You Like to See Speak at the Rally on February 4 in St. Petersburg?” Facebook, January 10, 2012; “League of Voters Decided on the List of Speakers at the Rally on February 4,” Kasparov.ru, Russian website, February 1, 2012.

The importance of social media during the postelection protests is indirectly documented in the frequency of Google keyword searches for Facebook and vKontakte that rose right after the December election (Figure 6.4). In addition to more intense traffic, Facebook added 1.5 million new members within six months.<sup>45</sup>

A survey of those who participated in the February 4 demonstration provides additional evidence for the Internet-enabled mobilization. On the day of protest, VTsIOM surveyed 800 participants. The majority of them were males (71 percent) younger than 45 (71 percent) who had graduated from college (56 percent). About 60 percent of them used the Internet daily; 70 percent said they found out about the event from online news sources, 22 percent from social media sites. Only 35 percent of participants found out about the event from television.<sup>46</sup>

**Figure 6.4**  
Frequency of Searches for “Facebook” and “vKontakte,” 2011



SOURCE: Google Trends.

NOTE: The y-axis reflects how many searches have been done for a particular term, relative to the total number of searches done on Google over time.

RAND RR295-6.4

<sup>45</sup> Socialbakers.com, *Russia Facebook Statistics*, undated.

<sup>46</sup> VTsIOM, “Miting 4 Fevralya na Bolotnoy Plochadi: Rezulaty Oprosa Uchastnikov” [“The February 4 Rally: Member Survey Results”], Russian web page, February 15, 2012.

### ***Aftermath of the Duma Election***

Postelection protests had several important implications for the electoral process. Seeking to restore legitimacy to the institution of elections and to his assured victory in the upcoming presidential election, Putin mandated that regional officials install web cameras at all polling stations. These cameras could be used by any eligible voter to monitor any polling station in the country. In spite of the short notice, web cameras were installed at about 90,000 of the 94,000 stations, which made Russia the first country in the world to introduce online monitoring of elections nationwide.<sup>47</sup> On the day of the presidential election, 11 percent of Russian voters monitored the election online. The supporters of the opposition candidates were more likely to take advantage of this opportunity. About 20 percent of those who voted for Vladimir Zhirinovskiy or for Mikhail Prokhorov followed the election online, whereas only 10 percent of those who voted for Putin did the same.<sup>48</sup>

The second important development was the emergence of online election watchdog Grakon, which took the idea of grassroots monitoring a step further by facilitating coordination among observers. This site was created a month before the presidential election by a handful of Russian students at Western universities. They introduced the same mobilization techniques that U.S. President Barack Obama employed in his 2008 campaign. The site facilitated networking among voters, journalists, and lawyers who lived in the same precincts. Three days before the presidential elections, 5,000 voters, 2,092 observers, 965 election commission members, 232 journalists, and 42 lawyers signed up to monitor the election either online or in person. About 3,533 violations were reported on Election Day, and ten days after the election (by March 14), 1,592 protocols with the results from election precincts were uploaded. Those protocols revealed that, on average, the official

---

<sup>47</sup> Web cameras were also used in Azerbaijan in 2009, but only at 500 polling stations.

<sup>48</sup> Russian Public Opinion Research Center, Russian survey web page. On March 11, 2012, a representative sample of 1,600 respondents was asked: "Did you personally participate in any of the activities [followed elections on the Internet or watched the webcast from the polling station]?" and "If elections were held this coming Sunday, which candidate would you vote for?"

vote count for Putin was 5 percent higher than the results reported in protocols uploaded by voters.

These positive developments, however, were overshadowed by the introduction of the Internet regulation law that granted Russian authorities legal and administrative means for censoring online content and filtering search results. The authorities also began intimidating online activists, especially those who created Facebook protest pages.<sup>49</sup>

## Conclusion

Internet use for nonpolitical purposes facilitated online activism among Russian voters in the aftermath of fraudulent elections. As in China, where nonpolitical uses of the Internet had spillover effects on the political space, online mobilization in Russia was more prevalent in those regions where voters had access to the Internet at their workplace. Online activism first manifested as a higher probability that voters reported electoral violations to the independent election watchdog Golos, which posted this information on its website. This information was supplemented by YouTube videos that provided additional information about abuses committed by polling station officials. Both Golos statistics and YouTube videos stimulated online discussion about the extent of violations. As popular discontent intensified, social media provided the means for coordinating protests by circulating information about locations, numbers, and identities of participants.

This case study suggests that the Internet contributed to the expansion of all three spheres of the political space—voice, vote, and assembly spheres—albeit to uneven degrees. The Internet amplified citizens' voices by providing them with opportunities for whistle-blowing and subsequently facilitated mobilization. This became possible partially because the digital revolution occurred concurrently with underlying changes in popular attitudes. Overall apathy of the early 2000s gave way to the growing popular discontent with the stagnant economy and shrink-

---

<sup>49</sup> Novaya Gazeta, Russian website, January 28, 2012; Marc Bennetts, "Russian Bloggers Fear Crackdown," *RIA News*, February 4, 2012.

ing career opportunities for white-collar professionals, who became extremely disenchanted with rampant corruption, suppression of media, and the unchecked expansion of the state power.<sup>50</sup> The digital revolution coincided with gradual shifts in popular preferences, especially among urban residents employed in white-collar occupations, and they became the nucleus of postelection protests. As many as 56 percent of protesters in Moscow had a university degree and came from the middle class, and as many as 60 percent were active Internet users.<sup>51</sup>

The Internet also contributed to the “assembly” aspect of political space by facilitating interactions among civil society organizations and citizens. In the literature on social protests in democratic regimes, civil society organizations provide resources to political activists for grassroots mobilization. This case study reveals, however, that in the regimes where a vast majority of civil society organizations depend on the state for their budgets, the Internet can level the playing fields for a handful of independent NGOs. Golos effectively supplemented its scattered offline outreach activities with web resources that made it possible to reach out to voters in those regions where Golos lacked organizational presence. The DDOS attack, however, underscored the NGOs’ vulnerability in cyberspace.

Social mobilization in Russia also contributed to the expansion of the “vote” aspect of political space by increasing the transparency of the voting process. All polling stations were equipped with web cameras that enabled voters to monitor any polling station. The long-term effects of the introduction of these cameras remain to be seen. In the short run, this measure has already triggered a similar initiative in Ukraine and might be adopted by other countries.<sup>52</sup>

This case study suggests that Internet Freedom programs can contribute to the expansion of political space in regimes such as Russia,

---

<sup>50</sup> Andrey Pertsev, “Social Media Brings People on the Streets,” Itar-Tass, Russian website, July 12, 2011.

<sup>51</sup> VTsIOM, “VTsIOM Puts Together a Collective Portrait of the Participants of the Russian Opposition Meeting,” Russian web page, February 16, 2012.

<sup>52</sup> “All Polling Stations to Be Equipped with Web Cams by Mid-October, Says Azarov,” Interfax News website, October 1, 2012.

primarily by enhancing online anonymity for all netizens and providing cybersecurity assistance to NGOs. Unlike the capitalist powerhouse of China or the tyrannical charnel house of Syria, the expansion of Internet access in Russia prior to summer 2012 was not accompanied by the imposition of tight online censorship. Most Russian netizens could post, browse, and share practically any information online. Although there have been instances of selective targeting of online journalists and bloggers by the regime, the Internet remained much less censored than the traditional media. When the protests unfolded, the protection of online anonymity became the most important issue for thousands of social media users who declared on Facebook and vKontakte their intentions to participate in mass protests. Although the two companies refused authorities access to the account, they were not able to protect all online activists from state repression, especially those who voluntarily identified their names as hosts of Facebook protest pages. Therefore, programs that protect anonymity of social media users could reduce the cost of online mobilization for many activists. Technical assistance provided by Google to Golos during the DDOS proved to be indispensable for overall anti-electoral fraud campaign. Other steps also could have been taken to make Golos less vulnerable to state measures: Apparently the Golos president's computer was not encrypted, so when customs officials confiscated it, all her email contacts were compromised and a spam attack was launched against all listings in the address book. This could have been avoided by providing cybersecurity training to the Golos team.



## Information Freedom During the Cold War: The Impact of Western Radio Broadcasts

---

Although the Internet is relatively new, the challenge explored in our contemporary case studies of expanding the political space of countries ruled by authoritarian governments is not. Many of the subchallenges facing Internet freedom programs are also historic: For instance, is it better for outside influences to concentrate on committed individuals, in the hopes that the conversation will resonate in the closed country, or to take a broader approach, at the risk of diluting the effect? Thus, it is extremely useful to investigate and draw lessons from previous U.S. information efforts that focused on expanding political space within authoritarian countries. Exploring historical cases can also provide insights into the potential long-term impact of U.S. Internet freedom programs.

This final case study seeks to provide this historical perspective through an exploration of U.S. information efforts during the Cold War to expand political space within the Communist bloc. It focuses on the efforts of Radio Free Europe and Radio Liberty (RFE/RL), which were U.S.-sponsored short-wave radio stations that sought to break through the information monopoly imposed by communist regimes, and it explores the long-term influence RFE/RL had on political opinion and civil society development within the Soviet Union and Eastern Europe.

We begin with a review of the short- and long-term objectives that policymakers had for the stations, and examine why senior policymakers established the stations and how the objectives for the station were linked to broader foreign policy goals. We then consider how



policymakers sought to measure the effectiveness of their efforts. How could they determine whether the stations were meeting their objectives? Finally, as with Syria today, Cold War policymakers had to grapple with the role the stations should play in the periodic uprisings that occurred within the Communist bloc.

We conclude the chapter by discussing some of the particular issues and challenges associated with promoting Internet freedom. From a long-term historical perspective, we explore the impact that accurate outside information can have on the political space inside authoritarian societies, and consider the pluses and minus of deepening vs. broadening strategies in promoting political change. For the radio station, this centered on the size and type of audience they were trying to reach and the most effective ways for assisting opposition figures. We then discuss the jamming of radio broadcasts (the 20th-century version of Internet censorship), what Communist authorities were trying to achieve, and how the United States sought to counter them. This final section also offers some conclusions about whether the stations achieved the objectives that policymakers established for them.

### **Short-Term and Long-Term Objectives of RFE/RL**

An important element of RFE/RL success was their linkage to the broader U.S. Cold War strategy. In 1948, U.S. diplomat George Kennan laid out a vision for a grand U.S. strategy of containment and “counterforce,” which meant placing pressure on the Soviet Union in a variety of ways as a means of curtailing Soviet expansive tendencies.<sup>1</sup> This strategy had two pieces: strengthening Western Europe—and later, other regions—to discourage Soviet attempts at expansionism, and placing pressure on Soviet control over Eastern Europe. Kennan believed this grand strategy should be implemented through all spheres of national power, including economic (the Marshall Plan), military

---

<sup>1</sup> “Organized Political Warfare,” Policy Planning Staff memorandum to National Security Council, May 4, 1948.

(NATO and other military alliances), diplomatic, and information activities.

Kennan, in his role as director of the State Department's policy planning staff, set up a variety of organizations to place pressure on communist regimes in Eastern Europe and the Soviet Union. The main political warfare organizations devoted to this cause were the National Committee for a Free Europe, later called the Free Europe Committee (FEC), and the American Committee for Liberation from Bolshevism (Amcomlib).

The FEC was set in motion by Frank Wisner, head of Office of Policy Coordination (which eventually was folded into the CIA), who provided the initial funding for the project and assembled an amazing array of public figures to support the venture. It is important to note, however, that leading public figures of the time, such as John Foster Dulles and Charles Douglas Jackson, were already seeking ways to organize the community of refugees from Eastern Europe.<sup>2</sup> The FEC board of directors included Allen Dulles, future head of the CIA; publisher Henry Luce; General Lucius Clay; Joseph Grew, former ambassador to Japan; and future President Dwight D. Eisenhower.<sup>3</sup>

The FEC's best-known and most important activity was RFE, which began in 1950. RL, sponsored by Amcomlib (an organization very similar to FEC for the Soviet Union), was broadcast in Russian and other languages of the Soviet Union while RFE broadcast to the people of Eastern Europe. These short-wave radio stations provided an alternative news source for Communist bloc citizens. RFE and RL presented themselves as what a national radio station would sound like if

---

<sup>2</sup> American officials during the early years of the Cold War used a variety of terms, including propaganda, psychological warfare, psychological operations, political warfare, and publicity policy, to describe government activities to influence and shape public opinion abroad. Dr. Edward P. Lilly wrote in an early history of American Psychological Operations for the Psychological Strategy Board in 1951 that this "broad politico-military area of national policy had been variously identified as propaganda, psychological warfare, or psychological operations." See Edward P. Lilly, *The Development of American Psychological Operations 1945-1951*, December 19, 1951.

<sup>3</sup> Arch Puddington, *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty*, Lexington, Ky.: University Press of Kentucky, 2000, p. 12.

it came from a free country. In addition to the news, they presented a full slate of programming, including entertainment, cultural, and commentary shows. A mixed staff of Americans and émigrés housed in New York and Munich developed the content of the broadcasts.

During the initial years of the Cold War, there were vigorous debates over the strategy and programming of RFE/RL. As was the case for the overall U.S. strategy toward the Soviet Union, policy divisions over the role of RFE/RL clustered in two camps: revolutionary and evolutionary.

The revolutionary camp included a group of national security experts who promoted a policy of liberation, such as President Eisenhower's Secretary of State John Foster Dulles. This group embraced a policy of freeing the "captive peoples" of Eastern Europe from Communist "enslavement."<sup>4</sup> Eisenhower also embraced this policy, at least declaratively. In a campaign speech before the American Legion convention in August 1952, he advocated that the United States use its "influence and power to help" the satellite nations throw off the "yoke of Russian tyranny." Eisenhower also said American aid to the "enslaved" peoples of Eastern Europe would not stop until their countries were free.<sup>5</sup>

Jackson, an expert on psychological warfare who served in the Office of Strategic Services during World War II and then as special assistant to the president during the Eisenhower administration, believed psychological warfare was the key to undermine Communist rule in Eastern Europe and that it could be done without provoking war between the superpowers. Before Eisenhower became President, Jackson organized a meeting in Princeton with government and private officials to discuss the potential for waging psychological warfare against Communist rule.<sup>6</sup> All of the semiprivate liberation organiza-

---

<sup>4</sup> John Foster Dulles, "A Policy of Boldness," *Life*, Vol. 33, May 19, 1952.

<sup>5</sup> Stephen E. Ambrose, *Eisenhower: Soldier and President*, New York: Simon and Schuster, 1990, p. 275.

<sup>6</sup> "I give full endorsement to your efforts," Eisenhower told Jackson. Dwight D. Eisenhower, personal letter to Charles Douglas Jackson, May 8, 1952

tions were also present, including members of the FEC and the Committee for Free Asia.<sup>7</sup>

At the meeting, Jackson expressed his desire to use RFE to encourage revolts behind the Iron Curtain. He believed RFE efforts were making progress—especially in Czechoslovakia, and that with an additional push, the country might be ready to revolt.<sup>8</sup> Many of the other RFE representatives supported this policy, believing that a public statement by the U.S. government, broadcast over RFE, that articulated its desire to liberate Eastern Europe through nonmilitary means, coupled with the launching of an overt psychological warfare offensive inside Eastern Europe, would be enough to begin the process.<sup>9</sup>

RFE/RL's early programming reflected this strategy. The first RFE policy manual describes the purpose of stations as “contributing to the liberation of the nations imprisoned behind the Iron Curtain by sustaining their morale and stimulating in them a spirit of noncooperation with the Soviet-dominated regimes by which they are, for the time being, ruled.”<sup>10</sup> The radio stations also sponsored hot air balloon operations into Communist Eastern Europe from 1951 to 1956, dropping leaflets, newspapers, stickers, and political souvenirs that supported the themes featured in RFE broadcasts. Along with their broadcasts, RFE saw the balloon drops as one of the only ways to break the total information control of Communist regimes.

Those who supported using RFE/RL to promote liberation within the Communist bloc took a broad view of the audience they were trying to reach and influence. They believed that RFE/RL should strive to reach not only the elites of these nations, but also the masses. In the initial phases, RFE/RL targeted its political message toward workers and peasants, the classes celebrated as the backbone of Communist regimes. In addition, RFE/RL directly targeted ethnic divi-

---

<sup>7</sup> Scott Lucas, *Freedom's War: The American Crusade Against the Soviet Union*, New York: New York University Press, 1999, p. 152.

<sup>8</sup> Dwight D. Eisenhower, Princeton meeting with Charles Douglas Jackson and others, transcript, May 10–11, 1952.

<sup>9</sup> Dwight D. Eisenhower, Princeton meeting, 1952.

<sup>10</sup> Puddington, 2000, p. 43.

sions, particularly within the Soviet Union. By the late 1950s, RL was broadcasting in 17 languages—including Ukrainian, Armenian, Azerbaijani, Georgian, and Belorussian.<sup>11</sup> These broadcasts were used to keep alive the history and cultural identities of the peoples of the Soviet Union, many of which were being systematically destroyed by the Soviet government.<sup>12</sup>

The second, or evolutionary, camp took a different view of the role RFE/RL should play in confronting the Soviet Union, promoting slower, more gradual action. John Ferguson, a State Department official, was one example of this group. In a reaction to the Princeton meeting, he wrote his colleagues about the dangers of overselling the ability of the United States to influence events behind the Iron Curtain. Ferguson noted the substantial gap between the rhetoric of those such as Jackson, who advocated liberation, and the reality of actually achieving this policy. Ferguson warned that it would be unwise to state that American policy was to restore political independence to Eastern Europe unless it was prepared to undertake the expansion of U.S. and allied military capabilities required to back up this policy.<sup>13</sup>

By the mid-1950s, U.S. national security policy was moving toward the evolutionary camp. A key national security document written in 1955 stated the new U.S. new policy as:

Continue its basic opposition to the Soviet system and continue to state its evils; but stress evolutionary rather than revolutionary changes. At the same time, make clear that while the U.S. is determined to protect its vital security interests by force if necessary, it does not seek to impose its ideas of government on the USSR by force.<sup>14</sup>

---

<sup>11</sup> “Radio Liberty Profile 1964,” Box 32, RFE-RL/CA, HIA 1964; Gene Sosin, *Sparks of Liberty: An Insider’s Memoir of Radio Liberty*, University Park, Pa.: Pennsylvania State University Press, 1999, p. 24.

<sup>12</sup> Interview with Gene Sosin, Westchester, N.Y., April 2005.

<sup>13</sup> John Ferguson, “Eastern Europe: 1949–1953,” memorandum to David Bruce, July 1, 1952.

<sup>14</sup> National Security Council, “Exploitation of Soviet and Eastern European Vulnerabilities,” NSC 5505/1, January 31, 1955.

This statement was a major shift in policy as the United States acknowledged it could not win the Cold War rapidly or through military force. Eisenhower fully recognized these changes, noting the United States was “not in a position to state that it would promote revolution in the Soviet Union” and therefore the United States had to “win these guys over.”<sup>15</sup> The long-term objectives of the policy were twofold: first, to develop the “kind of Soviet collective leadership which will permit the U.S. the greatest opportunity for promoting peaceful change within the Soviet system,” and second, “to impress on Soviet officials that the hostility of the peoples of Eastern Europe to their imposed government diminishes Soviet security.”<sup>16</sup>

The informational and cultural sphere was regarded as one of the critical ways to achieve this policy. U.S. officials held the view that the governments of the Soviet Union and Eastern Europe were ideologically vulnerable and that their vulnerabilities could be exploited, starting with the desire of the intelligentsia inside the Communist bloc to be part of a world cultural community, and the alienation of Eastern European and Soviet youth from Communist ideology. The United States sought to use RFE/RL and other mechanisms both to break down the isolation of the Communist peoples and to correct the distorted image of the West presented in Communist propaganda. It was hoped that contact with the outside world would introduce modern concepts and reform ideas to key social groups, spurring an open discussion of liberal ideas inside the Communist world. The hope was that these discussions would shift Soviet policies in a direction favorable to the United States.

According to the evolutionary camp, the key target audience for RL/RFE was intellectuals. The U.S. government and its allies held that public opinion, such as it existed in Eastern Europe and the Soviet Union, was informed by “educated people,” including students, intellectuals, technicians, and executives. U.S. influence operations such

---

<sup>15</sup> Gregory Mitrovich, *Undermining the Kremlin: America's Strategy to Subvert the Soviet Bloc 1947–1956*, Ithaca, N.Y.: Cornell University Press, 2000, quoting the minutes of the 234th National Security Council meeting, January 27, 1955.

<sup>16</sup> National Security Council, NSC 5505/1, 1955.

as RFE/RL were principally shaped to appeal to the audience that the government believed could be influenced. The hope was that over the long term, these efforts would undermine ideas and tendencies hostile to U.S. interests and correct the Communist media's distortions of U.S. policies and society.

George Kennan shared this opinion.<sup>17</sup> He dismissed the utility of information operations directed at key government officials and the Communist party, writing that “the fate of these groups is both morally and materially so irrevocably tied to that of their masters that repudiation of the Cause is well near impossible.” Kennan also discounted the laboring and peasant classes, which he doubted could exert much pressure on the regime or would pay attention to material from foreign sources. The intelligentsia struck him as a far better target for U.S. propaganda.

According to Kennan, the intelligentsia were somewhat removed from the power structure, but their ideas had an overall effect on the direction of society and therefore they might subtly impose restrictions on Soviet and Eastern European policies. Their professions taught them to think independently, Kennan wrote, and their economic status made it possible for them to buy books and radios capable of receiving foreign broadcasts. Kennan further posited that due to their isolation, they were curious about the outside world both in terms of the latest fashions and the view of foreigners on world events; further, they had a built-up skepticism regarding the accuracy of statements of the party and therefore might be susceptible to outside influence.

For the most part, the evolutionary strategy was the dominant one adopted by RFE/RL throughout the Cold War. In the short and medium term, it would pursue the long-term goal of ending communism by fostering evolutionary developments resulting in the weakening of Soviet controls and the progressive attainment of national independence in Eastern Europe. However, some elements of the liberation strategy remained—particularly the focus on broadcasting to non-Russian republics within the Soviet Union. RL staff were among the

---

<sup>17</sup> George Kennan, “Russian Language Broadcasts: Their Purpose, Potentialities, and Policies,” undated.

few Kremlinologists who saw the multinational nature of the Soviet empire as one of its chief weaknesses and an area the United States could exploit.<sup>18</sup>

## Measuring the Size of RFE/RL Audiences and Determining Its Effectiveness

One major challenge RFE/RL faced was determining the size of its audience. In 1957, Dr. Wilbur Schramm, a specialist in communication research from Stanford University, compared RL's attempts to determine the size of its audience to "a fisherman who drops his line through a hole in the ice and tries without any bait to identify the fish that brushes against the line."<sup>19</sup> But determining the size of its audience was only the beginning of the challenges RFE/RL faced, as its goal was not only to attract listeners, but also to change their attitudes toward the society they lived in.

The opposition RFE/RL faced in this endeavor was formidable, as the Communist system was designed around instilling total loyalty in its citizens and blocking any piece of information that might arouse criticism or dissent. One of the more effective methods Communist authorities had in limiting the impact of RFE/RL was extensive jamming of their broadcasts. Jamming inside the Soviet Union was done both through long-range sky-wave jammers that operated like the RL's radio transmissions, bouncing into the atmosphere on the same frequency, and by local ground-wave jammers that broadcast within cities. By 1950, the Soviet Union was employing 100 long-range jammers and 500 local ones.<sup>20</sup> And jamming was far from the only mechanism Communist authorities had to isolate their citizens. In the harshest periods of the Cold War, almost all forms of contact with the

---

<sup>18</sup> Lowell Schwartz, *Political Warfare Against the Kremlin: U.S. and British Propaganda Policy at the Beginning of the Cold War*, New York: Palgrave Macmillan, 2009.

<sup>19</sup> Sosin, 1999, p. 74

<sup>20</sup> Michael Nelson, *War of the Black Heavens: The Battles of Western Broadcasting in the Cold War*, Syracuse, N.Y.: Syracuse University Press, 1997, p. 22.



West were cut off. This made it very difficult to ascertain how large an audience RL had, if any, and what effect the broadcasts were having on its limited number of listeners.

Despite these challenges, both RFE and RL developed extremely sophisticated systems for determining the size of their audiences. This brief overview will focus exclusively on RL, which has the greatest available data set.<sup>21</sup>

For the first three or four years, there was only limited evidence that RL was reaching its target audience. In the first three years, there were only 53 pieces of evidence (letters from listeners, conversations with listeners inside and outside the Soviet Union) that indicated that RL was being heard.<sup>22</sup> For RL President Howland Sargeant, who was constantly being asked by RL funders whether their efforts were producing any listeners,<sup>23</sup> this seeming lack of results was a serious problem. To fix it, he hired Max Ralis, a sociologist who was the first of a number of talented communications specialists who worked for RL.<sup>24</sup>

Ralis applied general social science techniques to determine the answer. He reasoned that, in order to understand how large an audience is, one must interview a representative sample of listeners. The problem, of course, was that people inside the tightly restricted Soviet Union could not be contacted or interviewed. So Ralis employed a Russian speaking staff who contacted Soviet citizens traveling abroad, clandestinely interviewing them about their listening habits. The opening up of Soviet society in the mid- and late 1950s allowed numerous Soviet citizens to travel abroad, either for tourism or international festivals, and Ralis sought these people out wherever they were.

---

<sup>21</sup> For a taste of the data available, see R. Eugene Parta, *Discovering the Hidden Listener: An Empirical Assessment of Radio Liberty and Western Broadcasting to the USSR During the Cold War*, Stanford, Calif.: Hoover Institute Press, 2007.

<sup>22</sup> Maxis Ralis, Manager of Audience Research and Evaluation Department, *Three Years of RadLib Audience Research, Part 1*, October 1, 1959.

<sup>23</sup> James Critchlow, *Radio-Hole-in-the-Head: Radio Liberty; An Insider's Story of Cold War Broadcasting*, Washington, D.C.: American University Press, 1995, p. 101.

<sup>24</sup> Critchlow, 1995, p. 101.

By the 1970s and 1980s, data collection had been systematized to the point that preliminary generalized estimates could begin to be made about audience size and composition. During the period 1972–1990, more than 50,000 interviews with Soviet travelers were conducted and analyzed, using a sophisticated mass media communications computer simulation model developed at the Massachusetts Institute of Technology (MIT). The Soviet population allowed to travel to the West was demographically and ideologically skewed. Travelers tended to be more male, more urban, more educated, more middle-aged, and more likely to be members of the Communist party than the population at large, whereas the elderly and the less educated rarely traveled abroad.<sup>25</sup> To correct this problem, the MIT team normalized RL survey data through the use of Soviet census information. In 1980, it was estimated that 7.5 percent of the Russian population listened to RL broadcasts on a weekly basis.<sup>26</sup>

By the mid-1980s, RL was able to determine the size of its listening audience with a reasonable amount of precision, as well as its characteristics (demographic information, geographical spread, fit in the political spectrum, etc.).<sup>27</sup> The weekly reach—defined as the percentage of the population who listened at least once a week to any Western broadcast (BBC, Voice of America [VOA], and RL)—was around 25 percent of the population; RL had a weekly audience around 10 percent. RL's audience tended to be older, less urban, and slightly better educated than those listening to other stations. VOA offered a heavier emphasis on entertainment, particularly popular U.S. music, and had a younger and more urban audience.

RL research noted that jamming had a significant impact on the size of the listening audience. Listeners reported they tuned in less frequently and for shorter periods of time when jamming was in place. When jamming was lifted, as it was occasionally during periods of *détente*, the number of listeners increased. When jamming finally

---

<sup>25</sup> Critchlow, 1995, p. 108.

<sup>26</sup> Parta, 2007, p. 7.

<sup>27</sup> Audience statistics are from Parta, 2007.

ended for good in 1989, RL became the leading Western broadcaster in terms of audience size.<sup>28</sup>

During the earliest period of RL audience research, Ralis and his team sought to apply mass communication techniques developed in the 1940s and 1950s to RL programming. As part of the process, Ralis invited Schramm, a prominent communications specialist, to examine RL operations in Munich and offer recommendations. Schramm completed his report, entitled “A Communication Research Man Looks at Radio Liberation,” for RL management in August 1957.<sup>29</sup>

In the report, Schramm pointed out that RL had to “jump several hurdles to accomplish anything.” First it needed to attract the attention of a listener—a difficult feat by itself. Schramm noted that RL listeners had to believe the reward for listening was greater than the amount of effort required to listen. According to Schramm, jamming by the Soviet regime helped in this regard, as “forbidden fruit has been attractive since the beginning of man’s history.” The basic message, however, was that RL programming had to be worthwhile and interesting to Soviet listeners if it wanted to attract an audience.<sup>30</sup>

The second hurdle RL had to overcome, Schramm went on to say, was meaning; that is, the Soviet listener had to be able to decode what was being said. This process could only occur on the Soviet listener’s terms—he or she could only understand things that fit into their frame of reference, which had been stored away from their personal experiences of life inside the Soviet Union. This was particularly important for RL: Soviet listeners, because of their education and the information environment they lived in, had a very different frame of reference than people in the West. Third, listeners had to accept what was being broadcast to them as truthful. In his report, Schramm explained that this acceptance would be based on the amount of conflict between

---

<sup>28</sup> RL’s large audience lasted until the end of the Communist period in 1991, becoming much smaller in the mid-1990s, when a more diverse and somewhat freer media environment developed in the former Soviet Union.

<sup>29</sup> Wilbur Schramm, *A Communication Research Man Looks at Radio Liberation*, Radio Liberty, August 1957.

<sup>30</sup> Schramm, 1957.

what the listener was hearing and what he or she “has been led to know or believe.” The more that broadcasts conflicted with experiences or beliefs, the more likely it was that Soviet listeners would reject them. According to Schramm, this points to the “importance of accuracy in all matters relating to events within the Soviet Union,” as Soviet citizens could easily check the validity of such broadcasts.

Finally, Schramm pondered what impact RL might have on its audience. He wrote that RL should not expect to have any effect on real Communists because “there is no evidence either in scientific experiment or in practice that international radio can convert people who held strong positions on the other side.” Schramm was more hopeful about RL’s effect on those already disaffected with the regime, as RL messages could reinforce and strengthen their beliefs. For those in the middle who did not actively support or oppose the regime, RL could hope to “plant some ideas and facts that could make a significant change in the general picture.” This could be done by slowly adding political information to their frame of reference that, in time, might form new attitudes and values favorable to a “free system.”<sup>31</sup> However, Schramm also wrote that the people in the middle were extremely difficult to reach, as they were least likely to be interested enough in RL to fight the effects of jamming.

When listener data became more reliable in the 1970s and 1980s, RL was able to confirm some of its initial findings.<sup>32</sup> In a 1984 study, the Soviet population was broken into five groups based on a series of questions that measured their attitude toward civil liberties in the Soviet Union. These attitudinal types included liberal, moderate, indifferent, conservative, and hardline. Perhaps not surprisingly, liberals were the most likely to listen to Western radio, with around 80 percent of this group listening to broadcasts. A fair number of moderates, 40 percent, were also listening. Liberals also reported they used word of mouth as an information source, suggesting an amplifier impact for information broadcast over RL and other Western radio stations.

---

<sup>31</sup> Schramm, 1957.

<sup>32</sup> Parta, 2007.

Listeners were also asked about their motivation for tuning in to Western radio broadcasts. The most frequently cited reason was a desire to hear uncensored news, followed by the need to obtain information not readily available from sources within the Soviet Union. A third major reason was to learn about the outside world from non-Soviet sources of information. A less-cited but still important reason for listening was verifying or disproving information that had been heard from the Soviet media.

### **The Role of RFE/RL in Social Unrest**

One of the critical questions policymakers faced during the Cold War was the stations' role in social protests that occasionally occurred inside the Communist bloc. Should they be directly involved in fostering revolts and revolutions? For example, should they advocate the overthrow of Communist governments? Broadcast protesters' demands? Assist efforts to organize protests? Or should they adopt the more neutral stance of a traditional news organization, providing a credible and truthful account of the protests and authorities' reaction to it?

The first test of the U.S. broadcasting policies occurred between 1953 and 1956, when a series of riots and revolts shook Eastern Europe and the Soviet Union. This posed a big problem for the Soviet Union leadership after Joseph Stalin. Many historical accounts of this period give Western radio broadcasts, particularly those of RFE, far too much credit for inspiring this unrest.<sup>33</sup> A more accurate description is the underlying social, economic, and political conditions of Eastern Europe caused the unrest, with the Western radio stations playing the normal role of a media organization; i.e., they provided immediate news and coverage of breaking news stories. However, in a Communist society where news is carefully censored, the mere reporting of unrest could cause instability to spread throughout a country or a region.

The social and economic problems in Eastern Europe between 1947 and 1953 are well documented. In Hungary, for example, a

---

<sup>33</sup> Lucas, 1999, pp. 160–163.

Stalinist policy of forced industrialization raised production targets while lowering wages.<sup>34</sup> Living standards fell dramatically, with real wages falling 16.6 percent between 1949 and 1953.<sup>35</sup> In East Germany, the policies of collectivization, forced industrialization, and a harsh anti-religious campaign caused a half-million people to flee westward in 1952 and 1953.<sup>36</sup>

The information environment in Eastern Europe was also conducive for foreign broadcasts. In Hungary, the Communist regime in the late 1940s took over official Hungarian radio, which had been fairly free and democratic between 1945 and 1947, forcing it to become propaganda instruments of the regime.<sup>37</sup> The Hungarian government also tried to block foreign broadcasts, which had been extremely popular and an important information source about the outside world for Hungarians since the Second World War. This censorship of information only served to increase the credibility of foreign radio stations, particularly RFE, as these stations were often the first place people heard about important news events. For example, most people in Eastern Europe first heard about Stalin's death on RFE, which broadcast the news before the official pronouncement by the Soviet news agency.<sup>38</sup> All of these factors contributed to the popularity and influence of foreign broadcasts, with the multiple language broadcasts of RFE being especially popular.<sup>39</sup>

The first major incident of unrest in Eastern Europe occurred on June 16, 1953, in East Berlin. According to CIA accounts at the time, the unrest began when 5,000 workers began protesting a decreed increase of 10 percent in work norms. This spread into a more general

---

<sup>34</sup> Mark Pittaway, "The Education of Dissent: The Reception of the Voice of Free Hungary, 1951–1956," *Cold War History*, Vol. 4, No. 1, October 2003, pp. 97–116.

<sup>35</sup> Pittaway, 2003.

<sup>36</sup> William Taubman, *Khrushchev: The Man and His Era*, New York: W.W. Norton and Company, 2003, p. 247.

<sup>37</sup> Pittaway, 2003, p. 102.

<sup>38</sup> Pittaway, 2003, p. 108.

<sup>39</sup> By 1953, RFE was broadcasting to five main countries: Bulgaria, Czechoslovakia, Hungary, Poland, and Romania. See Puddington, 2000, p. 2.

attack on the regime, and by 4:30 p.m., a full-fledged riot was taking place.<sup>40</sup> A group of workers from East Berlin then approached Radio in the American Sector (RIAS), a popular American station in Berlin, asking permission to broadcast an appeal for a general strike the next morning.<sup>41</sup> The political director of the station refused to allow the strikers on the air, but did provide a news account of both the riot and the strikers' visit to the station.<sup>42</sup> The next day, an even larger demonstration gathered in Potsdamer Platz, ranging from 50,000 into the hundreds of thousands. This demonstration turned into a riot, with the crowd attacking the police station and tearing down the Soviet flag from the Brandenburg Gate.<sup>43</sup> Order was restored only after three armored divisions of Soviet troops moved into East Berlin to disperse the crowd.

In response to the riots, the U.S. government outlined a media strategy for broadcasting stations. They were to report factually on the demonstrations, but emphasize "that the demonstrations are spontaneous in nature" and that the Soviet reaction "demonstrates the true relationship between Soviet Communists and the workers and population of East Germany."<sup>44</sup> This strategy worked extremely well, as RIAS broadcasts of the events unfolding in Berlin caused anger and uprising across East Germany the next day. RIAS reporting provided eyewitness accounts of the demonstrations that were rebroadcast by all West German radio stations. RIAS broadcasts were widely praised inside the U.S. government and by the leaders of major political parties in West Germany. Frank Wisner of the CIA commented that RIAS carefully walked the line between "inciting violence" and giving "moral sup-

---

<sup>40</sup> CIA, Office of Current Intelligence, "CIA Comment on East Berlin Uprising," June 17, 1953.

<sup>41</sup> Stewart Alsop, "Courage in Berlin and Its Reward," *Washington Post*, June 20, 1953.

<sup>42</sup> Alsop, 1953.

<sup>43</sup> CIA, Office of Current Intelligence, 1953.

<sup>44</sup> Richard Status, "East Berlin Demonstrations," briefing of the Under Secretary for Psychological Strategy Board luncheon, June 17, 1953.

port and highly complimentary treatment to actions of the East Zone populace.”<sup>45</sup>

As is often the case today with online media, reports about unrest spread rapidly, with sometimes surprising results. By 1953, RL and BBC broadcasts were being heard inside Soviet forced-labor camps located in remote portions of Siberia. Prisoners in Vorkuta, a coal-mining complex, heard about East Berlin riots and decided if the Berliners could go on strike, so could they.<sup>46</sup> This sparked a strike that quickly spread throughout the coal-producing region. By July 29, 1953, more than 15,000 people were on strike. The strike was so widespread that local camp bosses were intimidated; they granted strikers their demand that they be allowed to meet with Communist party officials from Moscow.<sup>47</sup>

A Moscow commission actually presented the prisoners with a new list of privileges, including a nine-hour workday, visits with relatives, and permission to receive letters and money if they returned to work. The prisoners refused, demanding amnesty. The Communist Party decided enough was enough, and the military was brought in to smash the strike at the cost of hundreds of lives.<sup>48</sup> While the strike was put down, it did end up having an important effect: The Soviet government dismantled the “Gulag” prison system set up under Stalin, at first slowly, then more quickly after 1956. The government decided, partly due to the unrest, that the camps were unprofitable and the time had come to re-examine the whole Stalinist justice system on which the camps were based.<sup>49</sup>

The largest and most significant period of unrest in Eastern Europe occurred in 1956, launched by Nikita Khrushchev’s astounding attack on Stalin at a secret session of the 20th Congress of the

---

<sup>45</sup> Frank Wisner, “White House Inquiry Concerning the Performance of RIAS,” memorandum to Charles Douglas Jackson, July 20, 1953.

<sup>46</sup> Anne Applebaum, *Gulag: A History*, New York: Anchor Books, 2003, p. 488.

<sup>47</sup> Applebaum, 2003, p. 491.

<sup>48</sup> Taubman, 2003, p. 242.

<sup>49</sup> Applebaum, 2003, p. 507.



Soviet Communist party, held February 25, 1956.<sup>50</sup> In the speech, Khrushchev denounced Stalin as gravely abusing power and personally causing the Soviet Union to become a police state in the 1930s. He also assailed Stalin for his wartime leadership, calling him incompetent for failing to prepare the Soviet Union for Hitler's invasion. Khrushchev did not try to keep the speech secret for long; he purposely spread the content throughout the Soviet Union and the Eastern bloc,<sup>51</sup> intent on breaking with the Stalinist past and moving the Soviet Union forward. This could only be done if the speech received wide attention within the Soviet Union and Eastern Europe.<sup>52</sup>

Whatever Khrushchev's motives, the speech and the gradual opening up of political control caused extreme tension throughout Eastern Europe, as the already limited political legitimacy of Communist party rule was further undermined. By mid-1956, a crisis had broken out, with Hungary at the center of it.

On October 22, 1956, Hungarian students and intelligentsia held a mass rally in front of the Parliament building demanding the reinstatement of Prime Minister Imre Nagy, who had been deposed by the Soviet Union in 1955. Shots were fired by the secret police, and protests spread throughout the country. On October 23, the Hungarian government brought Nagy back to power and he promised "democratization and improved living standards," but this did not stop the rioting. With Hungarian forces putting up little resistance, Moscow moved in the next day, sending thousands of troops and tanks into the heart of Budapest. President Eisenhower issued a statement condemning the intervention, but refused to allow the CIA to air-drop arms and supplies to Budapest.<sup>53</sup> Unlike in East Germany three years before, Soviet troops did not calm the situation—their presence deepened the crisis. The Hungarian army began deserting in large numbers.

---

<sup>50</sup> Taubman, 2003, p. 271.

<sup>51</sup> Taubman, 2003, pp. 283–284.

<sup>52</sup> Taubman, 2003, p. 283.

<sup>53</sup> Ambrose, 1990, p. 423.

For those inside the U.S. government devoted to the active liberation of Eastern Europe, this was the moment they had been waiting for. The entire Soviet empire seeming to be cracking, RFE supported this policy, moving from attacking the Hungarian government to openly supporting the revolution. RFE's scripts from an October 27, 1956, broadcast provide detailed instructions on how partisans and Hungarian forces should fight the Soviets, including suggestions to sabotage railroad and telephone lines and advising local authorities to secure stores of arms for Freedom Fighters.<sup>54</sup>

On October 30, with hundreds of Hungarian and Soviet soldiers already dead, the Kremlin seemed to accept the Hungarian government's demands. The Soviet government declared it would withdraw its troops, pledging "to observe the full sovereignty of each socialist state."<sup>55</sup> In a meeting with Eisenhower, CIA head Allen Dulles called the statement "one of the most significant to come out of the Soviet Union since the end of World War II." Eisenhower wasn't so sure, replying, "yes, if it is honest."<sup>56</sup> Nagy, in an attempt to control the revolution, called for Hungary to leave the Warsaw Pact, as well as for open talks about a withdrawal of all Soviet troops.<sup>57</sup> Nagy's demand that Hungary leave the Warsaw Pact proved to be too much; the entire Soviet bloc seemed to be crumbling, causing panic in the Kremlin. After much wavering, Khrushchev decided he had to take a stand, declaring, "If we leave Hungary, that will encourage the American, English, and French, the imperialists."<sup>58</sup> On November 4, 200,000 Soviet troops and 4,000 tanks moved into Budapest.

The Hungarians refused to retreat and intense fighting ensued. The Hungarian government asked for help from the United States,

---

<sup>54</sup> Puddington, 2000, p. 105.

<sup>55</sup> Taubman, 2003, p. 296.

<sup>56</sup> Ambrose, 1990, p. 426.

<sup>57</sup> Partly in reaction to the integration of West Germany into NATO, the Warsaw Pact was signed May 14, 1955, as a mutual defense treaty among eight Communist states of Central and Eastern Europe: Albania, Bulgaria, Czechoslovakia, East Germany, Hungary, Poland, Romania, and the Soviet Union.

<sup>58</sup> Taubman, 2003, p. 297.

which they thought they had been promised, per the numerous statements by key figures such as Dulles and Eisenhower supporting liberation. In the midst of the fighting, RFE indicated that if the Hungarians kept fighting, the U.S. government would be forced to send military help due to public pressure.<sup>59</sup> However, no help was forthcoming. Eisenhower once again refused CIA requests to air-drop arms and supplies to the Hungarians.

RL broadcast the details of the trial, then established a special program during which *samizdat* was read. During the 1970s, RL *samizdat* broadcasts became the central mechanism for democratic and human rights movements in the Soviet Union, and later Poland, to convey their message to the world. Initially, these essays were typed into transcripts that circulated within the narrow confines of Soviet and Polish intellectual groups. They might reach an audience of a few hundred; perhaps several thousand, at best. Once RL started broadcasting these works, however, there was the potential to reach millions of listeners.

By mid-November, the Soviet government and its Communist allies in Hungary were back in charge of the country. More than 20,000 Hungarians and 1,500 Russian troops were killed during the conflict. The Eisenhower administration was left to pick up the pieces of its policies toward Eastern Europe, which were now completely discredited. This result should hardly have been surprising: State Department officials such as Charles Bohlen had been warning that overt statements by officials supporting liberation and broadcast over RFE would put the United States in position of assuming responsibility for Eastern European resistance. Unless the United States was willing to back these statements up through military support for Eastern European revolutions, which risked general war, these statements were damaging and dangerous for American national security.<sup>60</sup>

RFE/RL played a very different role during the social unrest that occurred during the late 1960s and 1970s inside the Communist bloc.

---

<sup>59</sup> Puddington, 2000, p. 106.

<sup>60</sup> The shift in RFE and U.S. policy toward a less inflammatory stance is apparent from the very different coverage RFE provided of the revolt and subsequent invasion of Czechoslovakia in 1968. See Puddington, 2000, pp. 142–152.

The repression of dissent and the official refusal to permit the publication of literary works that failed to receive government approval helped lead to the *samizdat* phenomenon in both the Soviet Union and Poland. *Samizdat* means, literally, “self-published materials,” and these essays and reports were the work of dissidents who wanted to express their views to the Soviet intellectual community and the outside world. They became part of the Soviet intellectual scene in 1966, when the transcript of the trial of Andrei Sinyavsky and Yuri Daniel was leaked to RL. Sinyavsky and Daniel were the first dissidents tried and sentenced to prison for anti-state activities.<sup>61</sup>

When RL set up regular programming for *samizdat* material, they were inundated with documents from inside the Soviet Union. In fact, it became a major objective of *samizdat* authors to have their documents smuggled to the West so RL could broadcast them. This presented a problem for RL, as it had to verify the authenticity of the documents and attempt to weed out any attempts by the KGB to plant a report; such a broadcast might discredit the dissent movement. At its height in the early 1970s, RL was devoting one-sixth of its Russian-language programming (58 hours a week) to *samizdat* documents.<sup>62</sup>

Research by RL indicated that slightly less than half of the population of the Soviet Union was aware of the *samizdat* phenomenon.<sup>63</sup> About three in ten knew about the *samizdat* movement from Western radio broadcasts, while a slightly higher percentage knew about it from official sources attempting to discredit the dissenters’ message. It appears that approval of the *samizdat* movement was closely linked to listening to RL broadcasts. Not surprisingly, RL research indicated that the most liberal members of Soviet society approved of *samizdat*, and this group was also the most likely to be regular listeners to RL.

By the late 1980s, RFE/RL had become a trusted news source for Eastern bloc citizens. As the revolutionary movements swept across Eastern Europe, RFE reported on events throughout the region. During the Polish elections of 1989, RFE sought to ensure Polish citizens were

---

<sup>61</sup> Puddington, 2000, p. 171.

<sup>62</sup> Sosin, 1999, p. 152.

<sup>63</sup> Parta, 2007, p. 52.

aware of all of the non-Communist candidates. The election was conducted on a nonparty basis and the RFE broadcast information to Polish citizens about which candidates were and were not representing the Communist party. RFE broadcasts caused some concern within the State Department, which feared that a landslide for the opposition would erode Soviet President Mikhail Gorbachev's standing in the Soviet Union. After the opposition victory, RFE rapidly began establishing bureaus inside Poland to take advantage of the newly established press freedoms.

RL played an even more central role during the 1991 coup inside the Soviet Union. In August 1991, hardline forces within the Communist party made a last-ditch attempt to roll back Gorbachev's reforms. This became known as the *Putsch*. As in previous times, the leadership of the *Putsch* tried to stanch the flow of information inside the country by putting folk dancing and concert music on the television and the radio. Russian President Boris Yeltsin resisted the coup from inside the 11th floor of the White House (the Russian Parliament), which was under siege.

Two RL reporters were holed up with Yeltsin and they provided continuing coverage of the crisis for Russian citizens. They telephoned a steady stream of information back to RL headquarters, which was then broadcast back into the Soviet Union. RL reports helped spread the word that Yeltsin was resisting the coup and that thousands of Moscow citizens had gathered to block the tanks surrounding the building. Yeltsin's call for a general strike against the coup was immediately broadcast by RL, which helped to organize and increase resistance. Gorbachev relied upon Western broadcasts for information during the coup, while he was imprisoned in the Crimea.

After the coup Yeltsin thanked RL:

During the three or four days of this coup, Radio Liberty was one of the very few channels through which it was possible to send information to the whole world—and most importantly, to the whole of Russia, because now virtually every family in Russia listens to Radio Liberty.<sup>64</sup>

---

<sup>64</sup> Boris Yeltsin, *In Country and the World*, RL program, August 24, 1991.

## **Learning from the Cold War Experience: Lessons and Analysis from Communist Archives for Promoting Internet Freedom**

As discussed in the introduction, U.S. efforts to promote Internet freedom face a number of challenges. Many of these challenges mirror those faced by policymakers and broadcasters throughout the Cold War. In this section, we briefly analyze how Cold War policymakers dealt with some of these questions. We will also offer some conclusions about the degree of success Western broadcasters had in achieving the objectives that policymakers established for them. To do this, we will utilize new information that has become available since the end of communism that sheds additional light on the challenges Western broadcasters faced in reaching and influencing audiences behind the Iron Curtain. Particularly pertinent in judging Western broadcasters' degree of success are files released from Eastern European and Soviet archives that provide a window into how Communist authorities viewed Western broadcasts, their attempts to measure the impact Western broadcasts were having on Communist societies, and the sustained efforts they made to limit their effectiveness.

### **What Impact Did U.S. Policymakers Hope to Achieve Through Their Efforts to Improve Communist Citizens' Access to Outside Information?**

One question often raised about Internet freedom programs is what would occur if they succeeded in allowing unfiltered access to objective and truthful information. Could authoritarian regimes survive under these circumstances? And if they did survive, what impact would access to outside information have upon their societies?

Although Western policymakers were optimistic at first, they grew to understand that providing objective and truthful information—even if it was not intercepted by government authorities—was unlikely to end Communist regimes or even change many loyal citizens' minds about the morality or effectiveness of the Communist system. The ideological attachment of many citizens to the regime and the power of the security services were too great for opposition forces

to overcome. Instead, by the mid-1950s, policymakers began focusing on a series of other positive impacts that RFE/RL could have as an alternative news source.

First, policymakers and Cold War radio broadcasters noted that providing outside information made it more difficult for Communist authorities to repress and cover up information about embarrassing events. Perhaps the famous example of this was the Chernobyl nuclear accident, which the official Soviet media did not report on until two days after it occurred. Even after it began reporting on the accident, the official Soviet media continued to distort and minimize the extent of the tragedy. In this information vacuum, many Soviet citizens turned to RL for information about what was happening. RL provided initial public health information and medical instruction for those in the affected areas. Without RL broadcasts, the Russian media might well have completely avoided reporting on the accident, as they had done in the past.

Second, policymakers realized that outside information could correct inaccurate information put out by official media. Large amounts of disinformation on U.S. society and U.S. domestic and foreign policies were put out by government-controlled media sources. Generally, RFE/RL did not seek to openly rebut Communist media reports but instead objectively and accurately reported world events. As the official voices of U.S. and British governments, VOA and the BBC presented alternative viewpoints of Western society that sought to correct distortions the Soviet media made about the United States and Britain.

Third, broadcasts about life outside the Communist bloc had the ability to draw out the fundamental differences between the Communist and Western systems. One theme that was consistently stressed throughout the Cold War was freedom in the West. Broadcasts on this topic explained to audiences the everyday freedoms that all Western citizens enjoyed, including freedom of thought and conscience, legal rights of citizens as individuals, and the absence of restrictions on personal freedom such as identity papers, police passes, and the right to travel at home and abroad. Another area where comparisons were drawn was social justice. This was done by analysis and criticism of Communist practice in areas such as workers' rights and the distribu-

tion of privileges among the population. Communist practices were compared explicitly and implicitly to demonstrate the greater degree of social justice underlying Western society.

In the long run, Cold War policymakers believed that providing access to outside information would correct the distorted image of the West presented in Soviet propaganda. Policymakers also believed that information from the outside world had the potential to introduce modern concepts and reform ideas to key social groups, spurring an open discussion of liberal ideas inside the Communist bloc. Evolutionally, the hope was that these discussions would shift some of the more extreme Soviet policies in a direction more favorable to the United States.

### **How Could RFE/RL Safely Assist Opposition Figures and Parties to the Communist Regime? How Did this Assistance Affect the Political Space?**

One of the major U.S. Internet freedom programs is Internet training for journalists and civil society actors living in repressive environments. This training includes effective use of online media technology to improve communication and avoid surveillance and monitoring by security forces. These efforts have been criticized in two opposite directions. Some critics worry that local in-country Internet freedom efforts will be delegitimized in the eyes of local populations through even loose linkages with U.S. government efforts. They want the United States to avoid any contact with these organizations. Other critics take the opposite tack: They say U.S. Internet freedom programs are not aggressive enough in confronting authoritarian regimes. They want U.S. Internet policies and efforts to be more explicitly directed toward empowering movements that seek to overthrow authoritarian governments. Policymakers during the Cold War faced similar pressure from outside critics.

As discussed previously, after the failure of U.S. efforts in the late 1940s and early 1950s, policymakers concluded that their capability to affect the internal dynamics of Communist societies was extremely limited. They grew to realize that only the governments and people of Communist countries, not an outside power, could eradicate Com-



munist control of Eastern Europe and the Soviet Union. Any active association between groups inside the Communist bloc openly calling for political change and the West would result in the violent repression of these groups.

Instead, policymakers decided that bolstering democratic networks in Western Europe both stabilized these societies and established channels to reverse the flow of ideas. Instead of Communist ideas flowing into Western Europe via the Soviet Union and its front organizations, democratic ideas could infiltrate behind the Iron Curtain via the newly established networks.<sup>65</sup>

RFE/RL played a critical role in this endeavor. Broadcasting from the West, these stations were able to highlight the views of leading opposition figures living abroad as well as dissenting views of citizens still living inside Communist countries. While this was not true for everyone, many individuals who lived in Communist states were happy to have their dissident views broadcast by RFE/RL. They fully understood the political and personal danger that came from being associated with Western radio stations, but they believed in their cause and wanted to exploit every available advantage.

One of the strategies RFE/RL employed to affect the political space were broadcasts about aspects of society that were being actively suppressed, including moral and religious issues, celebrating historical and culture events that contradicted the narrative of Communist societies, and providing a platform for repressed artistic/cultural works. In this way, RFE/RL believed they were supporting an emerging civil society that would flower once Communist rule ended.

Although a slower process than today, RFE/RL did assist in a two-way information flow between authoritarian countries and the outside world. As noted, once the stations had established themselves as credible news sources, opposition figures and ordinary people began providing information to the stations. This information could be about

---

<sup>65</sup> For more on how the West bolstered non-Communist networks in Western and Eastern Europe, see Chapters Two and Three in Angel Rabasa, Cheryl Benard, Lowell H. Schwartz, and Peter Sickel, *Building Moderate Muslim Networks*, Santa Monica, Calif.: RAND Corporation, MG-574-SRF, 2007.

corrupt officials, unaddressed problems in society, events that authorities were trying to cover up, or—in the case of *samizdat*—long essays critiquing communist society. After the stations received the information, they verified it as best they could and broadcasted the information back into the country.

This process improved the ability of RFE/RL to provide an alternative frame for its listeners in a number of ways. First, the broadcasts more accurately reflected the situation inside the country, making its programs more credible to listeners. Second, the alternative viewpoint of the station was bolstered by concrete evidence that people within communist societies shared these views. Third, alternative views from inside the country were given a platform to reach a sizable internal audience. For listeners who shared these dissenting views, hearing voices that mirrored their viewpoint but that normally were suppressed would reinforce their attitudes and let them know they were not alone in their concerns.

One of the most interesting findings in the Communist archives is how RFE/RL acted almost as an opposition party to the regimes. This was particularly pronounced in Poland, where top leaders and Party and media elites were well aware of RFE broadcast content, even if they did not discuss it openly. Polish leaders received daily transcripts of RFE broadcasts and circulated them to high Party officials. According to archive material, Polish leaders viewed RFE at various times as one of the chief elements undermining Poles' support for the government, a weapon of internal elite politics, an organizer for the opposition in Poland, and a source of information on what was actually happening in Poland and the rest of the bloc.<sup>66</sup>

Polish leaders occasionally asked government officials to correct problems that had been raised by RFE and reacted negatively to officials criticized by RFE.<sup>67</sup> One example of the relationship between

---

<sup>66</sup> Jane Curry, "Poland" from Session Four: Impact of the Broadcasts in Eastern Europe: Evidence from Archives, in the *Report on the Impact of Cold War Broadcasting*, a conference organized by the Hoover Institution and the Cold War International History Project of the Woodrow Wilson International Center for Scholars at Stanford University, October 13–16, 2004, p. 21.

<sup>67</sup> Curry, 2004.

Polish authorities and RFE was on economic policies. After shifts in economic policy were announced, Polish officials listened closely to RFE views on the subject and reacted to their criticisms by making changes. In many ways, RFE served as a check upon the power of the Polish government and improved the effectiveness of its policies. RFE provided Poland's leaders a way to gauge public opinion on critical issues, a method for holding incompetent and corrupt officials accountable, and an informed critic of its policies.

### **What Did Communist Authorities Hope to Achieve Through Jamming Western Radio Broadcasts? How Did Western Broadcasters Attempt to Overcome Jamming? Did Jamming Alter the Impact of Western Radio Broadcasts?**

Authoritarian regimes today employ a wide range of methods to block user access to sites and to censor information available on the Internet. They also attempt to disable sites they view as hostile through DDOS and other forms of cyberattack. Regimes undertake these sometimes-costly measures to prevent their citizens from accessing information from sources outside the country and to suppress debate within the country that they find threatening. Although not an exact parallel, communist regimes during the Cold War did employ technical measures such as jamming to block the signal of foreign radio stations.

Immediately after World War II, when the West started short-wave broadcasts to the Soviet Union, this did not appear to be a problem. For several years, the Soviet Union appeared willing to allow its citizens to listen to short-wave stations such as VOA and the BBC, unlike Nazi Germany. As the Cold War heated up, however, the leadership of the Soviet Union decided that all contact between Communist states and the West—social, economic, or political—had to be carefully controlled. VOA, BBC, and, later, RFE/RL broadcasts represented a stream of information that Soviet authorities could not control but nevertheless felt threatened their hold on power. These broadcasts provided information contrary to the illusory portrayals of life inside the Soviet Union and in the West that the Soviet government was trying to create in the minds of its citizens.

This discrepancy was emphasized by an incident on August 12, 1948. A Russian schoolteacher, Anna Kasenkina, jumped to her death from the USSR Consulate in New York. The Soviet press did not report this news, but it was covered extensively by VOA and the BBC. Within hours of the incident, employees of the U.S. and other embassies reported it was the talk of Moscow. This forced the Soviet press to respond to the incident the next day.<sup>68</sup> To answer this challenge, the Soviet government unleashed a massive jamming effort on April 24, 1949, against all frequencies of VOA and BBC, attempting to reimpose control over the information its citizens were receiving. This began a policy of jamming that lasted more than 40 years and constituted one of the Communist authorities' principal defenses against Western broadcasting.

One oddity of the Soviet policy was that despite jamming Western broadcasts, they continued to produce a large number of short-wave radios capable of receiving Western stations. A 1958 Soviet memorandum uncovered by Michael Nelson revealed that before the Second World War, there were only 200,000 short-wave receivers in the Soviet Union. In 1949, this number had grown to 500,000, and by 1958 there were more than 20 million receivers capable of picking up Western stations. In 1953, the Council of Ministers proposed that all production of receivers capable of "picking up hostile broadcasts" should be stopped. Yet, in 1954, the Ministry of Communications allowed the production of more than 4 million units. The memorandum concluded that, "Our technical measures directed against hostile radio broadcasts were brought to nothing by the mass production of short-wave receivers."<sup>69</sup> This was one case where security concerns were overridden by the demands of the Soviet consumers—who, according to defector reports, were willing to deprive themselves of necessities to purchase a radio set capable of receiving foreign stations.

As is the case today, Western governments and broadcasters adopted a number of strategies for overcoming jamming. The first was technical. Western broadcasters sought to overpower jamming

---

<sup>68</sup> Edward W. Barrett, *Truth Is Our Weapon*, New York: Funk and Wagnalls, 1953, p. 116.

<sup>69</sup> Nelson, 1997, pp. 91–92.

by increasing the number of transmitters while strategically placing them to cover as wide a broadcast area as possible. In addition, they broadcasted on multiple frequencies to force the jammers to cover a number of targets. This started a veritable electromagnetic arms race with the regimes responding to Western efforts by further increasing the number of jamming stations. Eventually, they would build some 3,000 transmitters to block the approximately 150 Western transmitter stations.<sup>70</sup>

Another strategy was to change the programming of the stations. For example, when jamming was not in effect, a popular program was *English by Radio*, which taught conversational English. This had to be dropped when jamming occurred because it could not be understood through the loud, irritating noises that jamming transmitters created. Instead, jammed broadcasts had to be read at a slower tempo than usual and elaborate forms of presentation had to be avoided. Broadcasts sought to stress a style of maximum clarity so listeners had the best chance of understanding what was being said. Programming focused more on the news and political commentary, which were more straightforward and easier to understand.

A final strategy was diplomatic. According to international law, it is illegal to intentionally interfere with radio, television, or other electronic communications for peaceful purposes. In diplomatic broadcasts, the United States addressed the jamming of Western broadcasts, highlighting a key difference between free democratic societies and Communist ones: Communist societies were afraid of allowing their citizens access to open information. On a number of occasions, the United States also proposed removal of all barriers to normal exchange in information media, culture, education, books and publications, science, sports, and tourism between the United States and the Soviet Union. These overtures were always rejected, with the long-standing Soviet Foreign Minister Vyacheslav Molotov once saying he had no

---

<sup>70</sup> George Woodard, "Poland," from Session Three: Impact of the Broadcasts: Jamming and Audiences, in the *Report on the Impact of Cold War Broadcasting*, a conference organized by the Hoover Institution and the Cold War International History Project of the Woodrow Wilson International Center for Scholars at Stanford University, October 13–16, 2004, p. 16.

interest in allowing “freedom in the exchange of ideas” that simply gave the West an opportunity to press its “war propaganda.”<sup>71</sup>

As noted earlier, jamming did have a negative impact on Western radio broadcasts. Listeners reported they tuned in less frequently and for shorter periods of time when jamming was in place. Soviet studies conducted in the 1960s concluded that jamming and other efforts to discourage listening were working. Their studies showed that Western radio stations did not offer serious information competition to Soviet media and was not gaining a significant audience share.<sup>72</sup> This conclusion had changed by the 1970s and 1980s, however, when Soviet studies found more listeners were regularly tuning in to Western broadcasting stations. Of more concern for the Soviet authorities was the fact that a high level of Soviet listeners considered Western radio trustworthy: 37 percent admitted that they somewhat trusted Western programming, compared with 32 percent who did not trust it and 31 percent who could not form an opinion.<sup>73</sup>

### **Who Was the Target Audience for Western Short-Wave Broadcasts? How Confrontational Toward Communist Authorities Should the Broadcasts Be?**

The U.S. government’s Internet freedom programs face two challenges in balancing between the various types of activities they support. One challenge, which has been discussed throughout this report, is how to balance efforts between deepening and broadening Internet freedom. A second challenge is balancing between programs that focus on developing and distributing circumvention technology and programs directly targeted at training activists operating in repressive environments. Technology programs in general are more global in nature and in many ways less directly confrontational to nondemocratic govern-

---

<sup>71</sup> J.D. Parks, *Culture, Conflict, and Coexistence: American Soviet Cultural Relations 1917–1958*, Jefferson, N.C.: McFarland, 1983, p. 271.

<sup>72</sup> Elena Bashkirova, “Soviet Union,” Session Three: Impact of the Broadcasts: Jamming and Audiences in the *Report on the Impact of Cold War Broadcasting*, a conference organized by the Hoover Institution and the Cold War International History Project of the Woodrow Wilson International Center for Scholars at Stanford University, October 13–16, 2004.

<sup>73</sup> Bashkirova, 2004.

ments. On the other hand, training activists is more confrontational, making it clear the United States is choosing to empower certain portions of particular societies that, from the regimes' perspectives, are hostile. These types of training programs have the potential to make targeted nondemocratic regimes less willing to work with the United States in other areas.

Western policymakers and broadcasters in the Cold War faced similar, but not identical, challenges. Both of these challenges related to the size and type of audience they were trying to reach. If Western broadcasts wanted to reach the largest possible audience, they could focus their efforts on two areas: broadcasting material that attracted the widest and most diverse audience, such as the news and music, and avoiding topics or methods of presentation that might offend loyal Communist listeners and/or anger Communist authorities. Of particular concern to those authorities were hard-hitting political commentaries and broadcasts that highlighted serious problems inside Communist societies. By avoiding these topics, Western stations could benefit when authorities, during more relaxed periods of the Cold War, halted the jamming, allowing these stations to reach a much larger audience. The risk of this strategy was that watered-down programs might not be very effective in shaping the viewpoint of their audience.

The BBC Russia service faced this dilemma early on as it attempted to attract a Soviet audience while providing an articulate portrayal of Western views and interests, which at their core were hostile to the Soviet system. This problem was compounded by jamming, which BBC broadcasters feared was making it impossible for Soviet listeners to hear their broadcasts. The first cessation of jamming, which occurred in 1956, led to an intense debate about how BBC Russia service should deal with these new circumstances.

The view inside the BBC was that the cessation of jamming provided a tremendous opportunity to widen the scope of their audience. To do this, they sought to tone down strident political criticism of the regime, instead focusing on lighter cultural programming. This would ensure a larger audience of the news, which had the greatest potential to shift Russian views in a direction more favorable to Britain. Other officials in the British Foreign Office strongly disagreed with

this point of view and wanted to use this opportunity to present the British point of view with maximum force. They advocated using well-known leaders of British society whom Russians would recognize to present a tougher tone toward Soviet policies. They believed the BBC too often “went out of its way to avoid treading on Russian toes” and that its “anxiety to appeal to the Soviet intelligentsia . . . tended to blur its presentation of the British case by trying to be too conciliatory.”<sup>74</sup>

RL embraced a different approach to its broadcasts, partly because they were targeting a different audience than the BBC. RL aspired to be a full-service national broadcasting station, and like a national station, it had news coverage along with a comprehensive slate of programs including entertainment, culture, and commentary. RL as an exile station attracted people already hostile to the regime, but it also sought to attract “loyal Soviet citizens” who would be interested in its diverse set of programs that could not be found on official Soviet stations. Thus, it was willing to spend time broadcasting on topics that would attract a smaller, more niche, audience.

RL’s tone and strategy were far more confrontational than the BBC, with an overall objective of causing doubt and uneasiness about the regime in the mind of educated Russians. RL was very creative in finding a variety of ways to go about this, using humor, religion, and culture to attack the Soviet regime. RL sought to identify and exploit key vulnerabilities in the Soviet system, among them the repression of the history and cultural identities of the peoples of the Soviet Union, the deliberate distortions of historical events by the Soviet regime, the general untruthfulness of Soviet news reports, and the censorship of cultural works.

Not surprisingly, the Soviet regime was extremely hostile to RL. From the beginning of its broadcasts, RL was heavily jammed and this jamming continued without interruption until 1988. In some ways, this limited the audience of the station. American officials, particularly those who had diplomatic dealings with the Soviet Union, often did not

---

<sup>74</sup> P.C. Storey, “Publicity and Propaganda Policy Towards the Soviet Union and the Satellites,” August 22, 1956; P.C. Storey, “BBC Russia Service May–September 1956,” September 12, 1956.



have a positive view of RL. They believed RL was excessively polemic in its approach, which offended its Soviet audience. They viewed RL as a waste of time and money with very little indication that this style of political warfare would be successful. Furthermore, they believed the station was a hindrance to the establishment of better relations with the Soviet Union. Instead, these officials advocated an approach more like that of the VOA and the BBC, with more objective and news-oriented programming.<sup>75</sup>

### **How Did U.S. Policymakers Measure Success in the Medium and Long Term of Western Radio Broadcasts?**

One difficulty officials face today is measuring the effectiveness of Internet freedom programs and determining what constitutes success for those activities. U.S. policymakers during the Cold War era had a similar challenge, with constant concerns being expressed by Congress about whether the money being spent on Western radio broadcasts was worthwhile. In addition, lawmakers wanted a better understanding of how the State Department and other pieces of the executive branch evaluated the stations' success or failure.

In the short and medium term, U.S. Cold War policymakers sought to portray short-wave radio broadcasts as part of the broader U.S. strategy of constraining Soviet power without triggering a global conflict. One method for doing this, according to these officials, was forcing the Soviet Union and its allies to spend resources defending themselves. The theory was that the more time and effort the Soviet Union had to spend defending itself, the less resources it had for foreign adventurism. This worked, for the most part, as Western broadcasts triggered a powerful response. Communist regimes devoted massive resources to counter Western broadcasts, including jamming, counterpropaganda efforts, and placing spies inside the radio stations in an attempt to undermine broadcasts' effectiveness.

Another desired impact was to show solidarity and support for democratic forces inside communist countries. Policymakers in the

---

<sup>75</sup> Charles E. Bohlen, Edmund A. Gullion, and Col. Joseph Coffey, Special Assistant to the Secretary, memorandum of conversation, Department of State, March 30, 1960.

United States grew to recognize that the correlation of forces in the short and medium term did not favor democratic revolution. However, the United States was able to show through RFE/RL that the West had not given up on the potential for a free and democratic Eastern Europe and Soviet Union. RFE/RL was designed to keep hope alive in these states for a better future and to assure reform-minded forces that they still had friends in the West.

A third desired impact was broadening the boundaries of internal debate inside communist societies. RFE/RL sought to achieve this in several ways. One method was to broadcast and highlight reform-oriented viewpoints. Communist media sources only presented the official point of view; dissenting voices were never allowed to be heard. RFE/RL broadcasts were able to break through the official media's information monopoly, providing a platform for alternative and dissenting figures.

Another method for broadening debate was providing information about ongoing global intellectual trends. Western broadcasters grew to realize that the Eastern European public did not need arguments against communism—they were well aware of its deficiencies. They needed to fill the spiritual void left by communist society. Providing information about intellectual debates and cultural trends in the West was a way to provide food for thought for educated citizens trapped inside isolated societies, and helped to introduce modern and reform-minded ideas into communist countries.

A final goal was to limit the tyranny of Communist rule, albeit in small ways: Bringing to light the corruption of officials, the brutality of the secret police, and events that the official press refused to cover did provide some checks upon the system. Although there was no direct outlet for public opinion, government officials, especially in Eastern Europe, had to be concerned about how general society viewed communist rule. Maintaining public order and economic activity were more difficult for regimes during periods of social conflict. RFE/RL broadcasts also provided evidence that the West knew about human rights abuse and was concerned. Again, the knowledge that outsiders had some knowledge of Communist authorities' actions likely had a small deterrent effect.

In the long term, U.S. broadcasts had a powerful impact upon elite and public opinion of Eastern Europe and the Soviet Union during the Cold War. Evidence documented by external and internal audience surveys, elite testimony from people like former President Vaclav Havel, and the magnitude of communist regime countermeasures against the broadcasts all indicate the significant impact that radio broadcasts had. Many historians regard U.S. information and cultural policies as one of the key reasons for the West's victory in the Cold War.<sup>76</sup> Western information programs achieved a remarkable degree of success during the Cold War, which was achieved at a very low cost, in national security terms.

---

<sup>76</sup> Since the collapse of the Soviet Union, numerous theories have been put forth to explain why the Cold War ended. One emphasizes the long-term economic crisis inside the Soviet Union that was exacerbated by high military spending. According to this school, the Soviet Union could not maintain its economic and military position without collapsing under its own weight. Another group of historians cites the role of ideas that caused a transformation of the outlook of Soviet leaders, particular Gorbachev. This group believes the Cold War ended because the Soviet government and people lost faith in the social and economic system of the Soviet Union and wanted to embrace a more Western/modern outlook.

## Internet Freedom: Measure and Countermeasure

---

Politics is the struggle over power, and the expansion of political space is therefore about altering the rules for that struggle.<sup>1</sup> Regimes that have power, want to keep power, and do not respect the norms of a liberal democracy tend to limit the political space of its citizens. They also want the freedom to carry out policies they deem worthwhile without having to work under the constraints that an aroused citizenry would place on freedom of action.

Accordingly, we started thinking about measure and countermeasure—not with the desire for greater political space on the part of the population, but with the regime’s goal of maintaining and maximizing its power. The regime, for its part, has many challenges to its continued power. Many of them have nothing obvious to do with political space (among the general polity). Some are external; others arise from the threat of military coup, violence by criminal groups, and the corrosive effect of (unsanctioned) corruption. But core challenges to the regime are possible if an expansion of political space leads to such civic actions as individual protests (e.g., self-immolations), mass demonstrations, labor strikes, or urban riots. In some cases, the effect of expanding political space is to open up the menu of political options to include more violent approaches such as forming an insurgency.

Regimes therefore can be expected to cast a wary eye on many of the following activities:

---

<sup>1</sup> For a tongue-in-cheek but completely serious sketch of this contest, see Laurier Rochon, “The Dictator’s Practical Internet Guide to Power Retention,” Present Working Directory website, 2012.

- **Circulation of Bad News from the Inside:** Events in China demonstrate that social media can rapidly spread all sorts of information, from what would be news (if it took place in the United States) to what would otherwise be a human-interest story. News of a high-speed train crash, coupled with indicators that evidence was being literally covered up, got combined with associated rumors and raged through China's microblogosphere. Such stories placed unwelcome attention on government incompetence, corruption, and misplaced values (trophy-system development over human safety), all of which was thought to call the legitimacy of the regime into question. More recently, a woman's forced abortion in the Shaanxi province threw an uncomfortable light on the human cost of China's one-child policy and the brutality with which it was "enforced."<sup>2</sup> Much of what is circulated as news, however, is rumor (e.g., military coups associated with the ouster of Bo Xilai from leading Chongqing's provincial government). This has given the regime an excuse to crack down.
- **Circulation of Good News from the Outside:** The danger of showing how well citizens of other countries lived was a potent theme of Communist communications policy during the Cold War; countering this was one rationale for supporting RFE. Yet the desire to show how well others live has not entirely disappeared today; note the attempts in North Korean media to portray South Korea as suffering under capitalism's lash.
- **Delegitimization of Fraudulent Elections:** Many hybrid states run fraudulent elections, and, as the chapter on Russia's election monitoring indicates, the winning regimes would just as soon not have people closely examine how the results were generated. The primary defense against cheating is to keep inquiring minds away from the mechanisms by which the cheating has taken place. An important secondary defense is to suppress circulation of direct reports (e.g., thugs keeping people away from the polling booth), or analyses of anomalies in the results.

---

<sup>2</sup> "The Brutal Truth," *The Economist*, June 23, 2012, p. 49.

- **Spreading Dangerous Memes:** Dangerous ideas include those suggesting that current governance structures in the regime are neither optimal nor inevitable. Alternatives exist that better conform to human nature or desire and deserve to be given a good airing. Similar memes could include intellectual constructs (e.g., Marxism) that explain the world and against which current practices may be found wanting.

How far nondemocratic regimes are willing to go and what methods they use to combat these concerns largely depend upon the type of the regime holding power. In authoritarian regimes such as China, a great deal of effort is spent curtailing or redirecting attention from bad internal news. When an earthquake occurs, media coverage is directed toward the heroic efforts to save people trapped in rubble or to rebuilding efforts, instead of the potential corruption that caused inferior structures to be built in the first place. Dangerous memes are removed as rapidly as possible from circulation or are carefully rebutted. In hybrid states such as Russia, there is a greater willingness to tolerate these challenges as long as they cause no more than grumbling or passive resistance.

Nondemocratic regimes also fear situations where citizens mobilize and organize themselves into a potentially threatening opposition movement. Individuals rarely overthrow governments spontaneously, but with a little mobilization and organization, they just might—hence, nondemocratic regimes have an interest in preventing communications that would foster such activities. Such communications can foster:

- **Mobilization of Opposition:** Mobilization is the process of converting an individual grievance into the possibility of mass action to pressure a regime, or possibly replace it. The type and process of mobilization follows the technology of the age, from the pamphlets used in the American Revolution to various Internet-based social media of today. The age of modern communications-driven revolutions began in the 1970s, when cassettes were used in Iran; in the 1980s, mobile phones were employed in the Philippines. In the more recent color revolutions and the Arab Spring, Web

2.0 technologies epitomized by Facebook and Twitter—or Sina Weibo in China—were particularly useful for near-spontaneous generation of activity.<sup>3</sup> The mesh-like networks they foster make them difficult to break one node at a time, which leaves suppression of the entire medium or repression of certain uses as the next best alternative. The most repressive states are upset with any mobilization of civil society, even if those being mobilized are not (or at least did not start as) opponents of the government.

- **Organization of Opposition:** Organization is the process of channeling protest through more structured outlets. By way of illustration, the rapidly generated Tahrir Square protests illustrate mobilization; the slower, less dramatic but ultimately successful work of the Muslim Brotherhood illustrates organization. As the example also suggests, one-to-many-to-more social media communications are less important for organization, since operating a more hierarchical organization means that messaging can largely be handled one-to-one (e.g., telephony) in the case of small-unit coordination or via broadcast for mass action. That noted, the more that social media becomes the dominant form of messaging for the upcoming generation, the more likely it is that such communications will fit the instruments available.

Perhaps it should go without saying, but an Internet with certain characteristics is required before individuals or organizations utilizing the medium can mount the many challenges noted above to the regime.

First, it must exist, and with the kind of economics that allows sufficiently wide participation. One way repressive states handle the risks associated with the Internet is to ban widespread public use of it (at least for anyone outside the governing elites). North Korea has done so. Cuba restricted Internet use as well, although restrictions are loosening there for those with money. Restriction is quite costly for any country that wishes to enjoy the benefits of international trade (and

---

<sup>3</sup> Clay Shirky, “The Political Power of Social Media: Technology, the Public Sphere, and Political Change,” *Foreign Affairs*, January–February 2011.

access to education materials). Not only are communications essential for trade itself, but opening up a country to international businessmen requires allowing them an environment that they are used to operating in. In short, they expect to see the Internet when they arrive in-country. This is why only the most isolated and repressive regimes have chosen banning as a course of action.

Second, the Internet should have international connections. Such connections are important not only to enable news from outside to filter into the country but also to permit citizens to interact with sites that are not beholden to the repressive government and thereby are free not to be a proxy for their repressive habits. Iran, for its part, is attempting to block all external Internet use for everyday consumers by creating a Halal Internet, although businesses get more leeway to connect internationally. China has international connections, but has banned Facebook and Twitter in favor of homegrown alternatives (e.g., Renren, Sina Weibo)—but these alternatives are more restrictive and acquiescent to government influence than are U.S. counterparts.<sup>4</sup>

Third, the Internet must be available for all uses (that conform to universal moral standards). Site and content blocking contravenes this principle. So do threats, whether explicit or implicit, against accessing certain sites and content—and, similarly, threats against those who post certain content. There should also be a warranted expectation that those who form private spaces will not be intruded upon by others whose primary purpose is to keep these spaces from functioning.

---

<sup>4</sup> No country, at least no country as large as China, needs to ban these sites forever—just long enough for the homegrown alternatives to exploit network effects to keep the market share of Western firms low. Each user may prefer the unrestricted access of Facebook to the restricted access of Renren, but if everyone already has friends on the homegrown system, then the small annoyances of restriction would pale for most users before the large advantage of using a site also used by one's friends.



## The Struggle for Internet Freedom: A Multiplayer Strategic Competition

A useful analogy for understanding the struggle for Internet freedom is to think of it as a multiplayer strategic competition between authorities, the civil society, and the international Internet freedom community.

As described in the previous section, the existence of the Internet exacerbates many of the challenges that nondemocratic regimes face in maintaining and maximizing their power. In responding to the challenge the Internet poses, these regimes face a series of choices about what strategies to adopt to meet it. Many governments resort to repressing free speech through a wide variety of methods: some extreme (e.g., refusing to be wired at all), some broad (e.g., a Halal Internet),<sup>5</sup> and many of them finely targeted (e.g., site blocking, pwning dissident computers). Many, but not all, of the measures have countermeasures—some of these countermeasures, in turn, can be countered.

The second actor in this competition is civil society. On the low end, individuals may simply desire the ability to receive information from sources blocked or banned by the government. The desire to seek banned information might come simply from curiosity, or from citizens' suspicion that their government is hiding information that could be relevant. On the high end are attempts to organize and mobilize opposition to the regime. Mobilization is sometimes triggered by individuals or organizations seeking to hold the government accountable for its actions, such as corruption or environmental pollution. Mobilization can also occur because of deep alienation from the current power structure and a strong desire to replace the regime.

These civil society activists will decide what strategies to adopt both in the virtual and nonvirtual world to counter limits upon their freedom. Part of this decision will revolve around the technical dimensions they embrace to circumvent government Internet control. Social movements will also need to decide how to organize themselves and what tactics they want to adopt to confront regime forces. These orga-

---

<sup>5</sup> The term "Halal Internet" was first used publicly by an Iranian official, Ali Agha-Mohammadi, in April 2011; see Neal Ungerleider, "Iran Cracking Down Online with 'Halal Internet,'" *Fast Company*, April 17, 2011.

nization patterns and tactics will be reflected on the web as well as outside of it. Part of these strategic decisions will involve how much risk activists are willing to run—with the potential for arrest and physical violence always looming as a possibility.

The third actor is the Internet freedom community that seeks to counter a wide range of measures that regimes use to repress Internet freedom. Through technological innovations and training, this community provides tools that improve citizens' abilities in nondemocratic countries to browse, share, and post information.

Two factors further complicate the struggle for Internet freedom. As is the case in all strategic contests, the struggle is dynamic, with each side seeking to counter the moves of the other. Regime measures to curtail Internet freedom trigger an online response by advocates; subsequent countermeasures enacted by the regime trigger another response from the online community, and so on. U.S. Internet freedom programs are part of this reaction cycle. Internet programs assess the regime's Internet repression measures and provide online communities with technology and tools to help counter them. Regimes then respond with new measures, triggering a reassessment and online distribution of new tools.

Another complication in the struggle is the flow of information between the actors. Repressive regimes generally do not announce the introduction of new measures to curtail Internet freedom; these measures are launched in secret—and only slowly do civil society actors realize what has occurred. The same is also true in the other direction. It takes a certain period of time for regimes to realize that their citizens have adopted new strategies and tactics to circumvent the Internet control measures they have put in place. Thus the measure-countermeasure cycle may vary depending upon how quickly each side adjusts to the other's tactics.

The United States faces a two-sided information problem. To devise effective Internet freedom tools, one needs to understand both the regime's Internet control mechanisms and the civil society's strategy to countering them. Further complicating the situation is the diversity of social movements within a state and the difficulty of effectively communicating with them. This makes it extremely challenging

to make advance determinations of the impact that a new Internet freedom technology will have upon the struggle. For a sustained period of time, it may not be possible to measure the degree of citizens' awareness about new technology and whether it is meeting their strategic needs.

## Countermeasures and Counter-Countermeasures

We will now indicate and assess the various countermeasures that governments can take against Internet freedom, and how the forces fighting for Internet freedom respond. In some cases, we extend the cycle, noting the state's counters to these counter-countermeasures and, correspondingly, counters against them.

### No or Expensive Internet

As noted previously, several states restrict all or most Internet usage regardless of content, or otherwise make it very expensive. They do so in the face of evidence that such restrictions are costly. If such regimes understand as much, they must believe the costs to be a necessary price to pay for their survival and may even believe their own propaganda that emphasizes the virtues of self-sufficiency (e.g., *juche* for North Korea).

There are two classes of countermeasures for this style of repression. The first assumes that the Internet exists but is unaffordable for any number or reasons (e.g., a monopoly provider). The counter to unaffordability is, essentially, Moore's Law. To wit, the Internet gets cheaper and there are more things it can do. The pace and force of these counters are largely outside the control of any one government, much less the U.S. Department of State's Internet Freedom program.

The second assumes that the Internet does not exist (or a publicly accessible one does not exist). The task, therefore, is for outside forces to create one.

One tack toward this goal is to develop software that converts commonly owned instruments—notably mobile phones—into Internet nodes. The hope is that local Internet networks could be created by meshing together mutually available nodes. This would enable indi-

viduals in a small geographic space to communicate via the Internet. A broader hope would be to engineer access to the international component of the Internet if the available nodes span international borders. Current technologies for doing so, however, are not particularly promising. In general, today's technologies handle low-bandwidth communications better than high-bandwidth ones, making it difficult to generate enough bandwidth for effective web browsing. Another difficulty is that repressive states are likely to carefully monitor border areas in ways that make the international Internet hops difficult. Geography also could be a concern, as the distance between the repressive state and the closest available international Internet portal (e.g., Cuba to Miami) could present technical challenges.

A second possibility is to establish one or more high-power antennas that would communicate into and out of the country; two possibilities include satellite and high-powered microwave (e.g., Wi-Max). Clearly, this is an expensive proposition, and the cost per bit is also relatively high. Finally, any system accessible to private individuals is also accessible to, and can be jammed by, the repressive state. Conversely, one way to avoid jamming is to use electronic countermeasures, but such measures require a trusted relationship between someone inside the country and whoever operates the high-powered antenna (think of encryption as an analog). This option may work when nothing else does, but it comes with costs.

### **Halal Internet**

Iran's move to sever most connections between its own Internet and the rest of the world's cybersphere raises several issues related to Internet freedom, as does Russia's governmental support of the development of Cyrillic domains. Such moves, if successful, could restrict local knowledge of global events, including global commentary on local events. Furthermore, because websites would all be internal, such providers can be pressured to censor local users in ways that international companies would have been more reluctant to do.<sup>6</sup> The permeability of such a

---

<sup>6</sup> This brings up the separate issue of the steps that regimes ask international companies to take (and companies' willingness to do so) to maintain their access to local markets.

system would be a function of its construct. In Iran's case, critical business interests would have access to international communications but private individuals and noncritical interests would not. International access may depend on arrangements that can be made through the former's circuits; they may be voluntary or involuntary (e.g., via hacking or open Wi-Fi nodes). Even if Internet access were completely locked down, if other networks were internationalized (notably the phone system), there would be way to shift content across borders.

The counters to a Halal Internet would include the measures described above to serve areas with no Internet. An international link is not necessary to permit the Internet to allow social and political spaces—except for the likelihood that Web 2.0 vendors would listen to the government and squash dangerous associations (or keep thorough tabs on users and report them to the police). Hence, another counter is to encourage individuals and groups to offer their own unrestricted spaces, using available (or open source) software. Such sites are no panacea; since their establishment would be personally risky, they may well be here today and gone tomorrow. Nonetheless, in spite of these limitations, they are still technologically feasible.

### **Site and Content Blocking**

Most suppression is more selective. Some repressive tools operate against web owners. One such measure is to use legislation to make it easy to remove certain content. The Russian Duma passed a law in July 2012 that allowed state officials to compile a black list of illicit websites and request that ISP take sites down if someone posted a link to them. This makes it relatively easy for someone to poison someone else's site (or force them to edit every submission by hand). Broad decency provisions can also be used as a justification to block significant platforms, as happened in China with Facebook.<sup>7</sup>

Other repressive tools target users. China blocks access to certain sites all the time, and to a broader selection of sites and messages based on the content of the communications (e.g., references to jasmine tea during the Jasmine Revolution, the first manifestation of the

---

<sup>7</sup> These types are drawn from Deibert and Rohozinski, 2010.

Arab Spring). China's regulations put the legal onus on China's ISPs to enforce these restrictions, often leading to more aggressive blocking and filtering than prior State efforts were.

Some of the counters to such measures are homegrown. For instance, systems that are optimized to spot and stop certain words are less efficient when handling audio and video material. Chinese dissidents, as noted earlier, have come up with a robust set of euphemisms that permit talking about sensitive topics without triggering word-catchers.

As noted, circumvention tools such as Tor, Ultrasurf, and Psiphon permit users to access forbidden content and maintain their anonymity in the process. Such tools have several problems, however. One is that the user must trust the tool. There are suspicions that certain tools reportedly developed by dissidents were actually created by repressive regimes and were created with back doors into them. If true, users are compromised; if false, users may still be misleadingly scared off from using such tools.

A second problem is that some of these tools (notably Tor, the most secure of the lot) are difficult to properly install and provide a less-than-ideal web surfing environment. Improper installation of these tools can compromise the security of the connection and they carry latency and throughput penalties—particularly for audio and video.

A final problem is that repressive regimes can duplicate the process the user utilized to circumvent blocked access. If random users can find routers and bridges that carry circumvention traffic, so can repressive regimes. If regimes manage to map these pathways, they can block access to them, depriving citizens of the circumvention technologies. Because of these factors, the percentage of circumvention users in repressive countries is quite low.

Two of the three problems are being addressed by projects to improve the Tor network's performance in routing packets smoothly. One method to frustrate this regime strategy is to multiply the number of addresses that have to be blocked. Another method makes it impossible to block access to routers without blocking access to third-party sites that are of value to the repressive state (e.g., the educational material of a top-flight university). Such projects are also looking at ways to

make Tor sessions look indistinguishable from everyday e-commerce. Until such projects reach deployment, it will be hard to know how well they solve the problem or whether they, in turn, can be defeated by further countermeasures from the repressive state.

### **Green Dam**

In 2009, the Chinese government floated a proposal to require that new computers in China be equipped with software that could block pornographic content. Alert netizens quickly realized that such a capability could also block politically sensitive content as well. Computers, so equipped, would not be able to profit from circumvention technologies because, presumably, state-sponsored software would sit between the receipt and decryption of the material, on the one hand, and its display, on the other. This proposal went nowhere, but the concept may attract renewed interest one day.

Countermeasures would depend on the details of implementation and are thus impossible to predict. However, history suggests that such software will contain vulnerabilities that can be exploited to turn it off. Since such vulnerabilities help the user, they are less likely to be reported than harmful vulnerabilities, and there may be ways for individual users to evade or mask fixes to such vulnerabilities.

### **Pwning Dissident Computers**

The Syrian government has started to introduce malware to the computers of dissidents by creating software with capabilities that dissidents might find appealing (e.g., Skype encryption) but which is, instead, infected with a Trojan horse.<sup>8</sup> This is only the latest phase of a broader campaign to spy on dissidents using malware. Successful implantation of such malware allows repressive states to determine who its most dangerous dissidents are, and may also provide information on who they are communicating with or what their plans are (e.g., by viewing dissidents through their own computer-mounted webcams). Pwning (taking control of) dissident computers is a very handy tool in a world in which as many as half of all computers host malware and a

---

<sup>8</sup> See Galperin and Marquis-Boire, 2012b.

large percentage of them are bots. Indeed, it is a wonder that this tool has not been used more often.

Should this technique spread, countermeasures would be challenging to devise. By way of illustration, if it were simple to keep computers clean of malware, such solutions would have been snapped up by corporations that are under a constant barrage of advanced persistent threats.<sup>9</sup> Teaching users good computer hygiene can help, but will not eliminate the possibility of compromise, and some platforms have proven to be much more resilient to malware than others. Technology to determine whether a computer is infected may help (particularly if it looks for certain capabilities, such as turning on webcams when not otherwise ordered to), but it would take work.

## **Finding and Targeting Dissidents Through Their Internet Use**

Circumvention technologies, notably Tor, facilitate anonymity. But gathering information on everyone's surfing habits is not terribly difficult in countries that can freely monitor Internet traffic because they own (or can pressure) ISPs. Someone who uses circumvention, and thus encryption, for every Web session may be suspect. Conversely, someone who uses circumvention some of the time may inadvertently reveal their politics through the websites they visit in the clear. Such profiling is common in advanced countries, but it is usually employed by commercial companies that are willing to accept a high rate of false positives in finding subjects for targeted advertisements and discounts. So far, it is only a notional threat in repressive states. Counters to such measures would include normalization technologies that would overlay a user's interactions in ways that make them appear unexceptional in total.

---

<sup>9</sup> In some ways, it is a little easier to safeguard personal computers whose only connection is to an ISP. Organizational computers can infect one another and generate certain types of network traffic that individual computers do not.



It may be a mistake to assume dissidents seek the anonymity provided by circumvention technologies. Clearly, some dissidents want to announce themselves to generate publicity and support for their cause, as well as ensure their credibility among the like-minded. Others may already be too familiar to hide, and thus assume authorities are already monitoring their communications. Repressive states that wish to harass such individuals do not need to monitor their Internet use to find them, although such monitoring may help provide evidence for future legal actions. However, citizens in the initial phases of political activism may not want to announce this fact to repressive governments. Wael Ghonim, the Google engineer who became the public face of Egyptian dissidence, started his “We Are All Khaled Said” Facebook page anonymously.

### **DDOS Attacks**

Sites that cannot be legally blocked can be pushed off the Internet through DDOS attacks, particularly if such attacks are well timed. Of particular importance to regimes would be hobbling websites at sensitive moments, such as before a planned protest or in the middle of an election. Such attacks could limit the ability of independent organizations that monitor and report on voting irregularities. For example, as discussed in the case study on Russia, the website of Golos was attacked and shut down during Russia’s 2011 parliament elections. In contrast to most forms of repression, a DDOS attack can target and silence sites and individuals outside the country of repression. This allows non-democratic regimes to attack exile groups in the West that are critical of their governments. Also, unlike most forms of repression, DDOS attacks are generally anonymous, making it difficult to link the act of repression to a specific state.

Countermeasures to DDOS attacks exist. Their use depends on what kind of DDOS attack is at issue. Those that exploit vulnerabilities of the particular server can be weakened by fixing the vulnerabilities.<sup>10</sup> Attacks that work through sheer numbers (e.g., from a botnet) can be

---

<sup>10</sup> For example, see Dan Goodin, “New DoS Tool Lets a Single PC Bring Down an Apache Server,” *ars technica* website, June 8, 2012.

alleviated by rehosting the affected site on a large content distribution network, such as Akamai. Google rehosted some affected sites for Georgia when they came under DDOS attack from Russia in 2008.<sup>11</sup>

### 50-Cent Party

The so-called 50-Cent Party consists of shills paid for by China's government to post comments favorable toward Community Party policies to sway public opinion on various Internet message boards.<sup>12</sup> There are counterparts in Russia as well. Such efforts do not forbid the free exchange of ideas, but they do corrupt it. There is no good countermeasure against such efforts, and it would be almost hypocritical to try.<sup>13</sup> However, if people are paid to promote government opinions, at what point will others assume that anyone who promotes government positions did so only for the money?

### Exceptional Violence

Not all countermeasures are restricted to the cyberdomain. Old-fashioned coercion strategies could be as effective for silencing bloggers and online journalists as the traditional media. For instance, both Iranian security forces and the Syrian army made haphazard efforts to physically attack protesters using mobile phones to document abuses. The lists of bloggers imprisoned for disseminating damaging information have been steadily growing, and in 2011, more bloggers and online journalists were in prison than journalists working in any other medium.<sup>14</sup>

Coercion is one of those measures against which there are few good countermeasures except to publicize the violence and make an

---

<sup>11</sup> Larry Dignan, "Georgia Turns to Google's Blogger to Counter Alleged Cyberattack," Seeking Alpha website, August 11, 2008.

<sup>12</sup> Michael Bristow, "China's Internet 'Spin Doctors,'" BBC News website, December 16, 2008. The term "50-cent party" came from early (and somewhat inaccurate) reporting that each comment garnered the contributor 50 Chinese cents (worth roughly 8 cents in U.S. currency).

<sup>13</sup> Particularly in light of articles such as Spencer Ackerman, "Newest U.S. Counterterrorism Strategy: Trolling," *Wired*, July 18, 2012.

<sup>14</sup> Committee to Protect Journalists, *2011 Prison Census: 179 Journalists Jailed Worldwide*, web page, December 1, 2011.

issue over the lack of justice in particular cases. Repressive states, one would hope, may ultimately conclude that they lose more than they gain that way.

### **Greater Surveillance of Mobile Communication**

Tightening of other forms of communication occurs concurrently with the restrictions on Internet freedom. This year, the Ethiopian government outlawed the use of voice-over IP services, such as Skype, making it punishable by up to 15 years in prison, and concurrently blocked access to the Tor website. Iran acquired \$130 million worth of equipment from China to locate and intercept voice and text messaging and other incoming and outgoing traffic from mobile phones.<sup>15</sup> The Syrian authorities used satellite phone metadata to locate and attack journalists.<sup>16</sup>

Developing countermeasures to surveillance of mobile communication is more challenging than anonymizing online traffic because of built-in global positioning system features, without which communication between a phone and the transmitting tower is not possible. Partial anonymization is still feasible through the use of phone calling cards and other similar technologies, which do not completely eliminate the possibility of identifying a receiver's number but do make it harder because of the rerouted dial-up process. Building awareness about mobile phone vulnerabilities both among the activists and foreign reporters that interact with them would be another strategy. A recently published Freedom House report, *Safety on the Line*, is a useful step in this direction.<sup>17</sup>

---

<sup>15</sup> Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," Reuters website, March 22, 2012.

<sup>16</sup> Jillian C. York and Trevor Timm, "Satphones, Syria, and Surveillance," Electronic Frontier Foundation website, February 23, 2012.

<sup>17</sup> Freedom House, *Safety on the Line: Exposing the Myth of Mobile Communication Security*, Washington, D.C., July 2012a.

## The Future Architecture of the Internet

The contest between measure and countermeasure may arise from basic human nature, but it is played on a terrain that reflects the architecture of the Internet and its component information systems. This architecture reified in computer code, to echo the logic of Lawrence Lessig,<sup>18</sup> has a great influence on whether this measure or that countermeasure succeeds. The issue is, what kind of architecture should the world's communications infrastructure adopt—or at least build toward?

Certain aspects of the Internet's architecture complicate the struggle of dissidents against repressive governments. For instance, circumvention technologies could have been built into browsers but are add-ons today. Encryption could become the default mode for communications, with interfaces only occurring when the proper technological handshake takes place. This would prevent users from risking the loss of control of their machines by accidentally wandering into the wrong website or opening up the wrong document. Anonymity on the web may be good enough to prevent companies and governments from tracking your movements.

This very different Internet would have its advantages. It would handicap repressive governments' attempts to curtail Internet freedom and likely would expand the world's political space. Dissidents would be freer to voice their opinions without fear of being identified and their browsing habits would be difficult to track. But there are advantages for the U.S. government in the fact that cyberspace is as it is. Perfect anonymity and opacity would complicate law enforcement, make it difficult to pay for free Web services (because the returns on advertising would be lower), could facilitate violations of intellectual property rights, and might even enable more WikiLeaks.

The basic architecture and protocols of the web are also increasingly being contested in international forums by powerful nondemocratic states such as China and Russia. These states object to the underlying design and purpose of the Internet as it evolved within the U.S. democratic context, which value openness, speed, and compatibility.

---

<sup>18</sup> Lawrence Lessig, *Code, and Other Laws of Cyberspace*, New York: Basic Books, 1999.

In place of this vision, Chinese and Russian authorities would base Internet governance on state sovereignty and security. China has stated that it wants to replace the current model of Internet governance, based upon transnational and private-sector-based organizations, with one that promotes sovereignty and intergovernmental institutions. From a technical perspective, this would provide China and other nondemocratic states the opportunity to build a different style of web within their territories; a web that would limit where you could navigate to, with much greater monitoring and control once you got there.

From a technical and operational standpoint, it would be very difficult to alter the basic architecture of the web. Openness and compatibility are built into the system, and reversing these priorities would not be easy. However, the increasing economic and political power of nondemocratic states such as China provides an increasing opportunity to steer the evolution of the web in a direction more in line with their values and interests.

All of this leads to the complex question surrounding the type of Internet the United States truly wants. This will require a thorough and honest evaluation of the values underlying U.S. Internet policies, including how willing it is to sacrifice other interests to promote Internet freedom.

## Key Findings and Policy Implications for Internet Freedom Programs' Design

---

The rapid expansion of Internet use in nondemocratic states provides a wealth of new opportunities for expanding political space. The basic technology of the web is friendly toward democratic values. The Internet is built around the concepts of openness, speed, and universal compatibility, which are antithetical to regimes that seek to manage and control political discourse. When authoritarian regimes attempt to control Internet access and the uses to which netizens put it, they must struggle against the underlying nature of the Internet itself. For Internet freedom programs, the opposite is true. They are merely trying to reinforce the basic characteristics of the Internet, a much easier job.

Before the case studies, this report identified channels through which online mobilization can expand political space. The case studies then described mechanisms by which new technologies can bring about visible outcomes. The penultimate chapter examined the choices involved in maintaining this mechanism through the struggle between measure and countermeasure. In this concluding chapter, we draw on the existing literature in the field and the empirical evidence in the case studies to draw some initial conclusions about the relationship between Internet freedom and political space, and tease out some implications for the design and implementation of Internet freedom programs. We identify areas where U.S. Internet programs are likely to have the greatest impact and leverage, as well as some inherent limitations of such programs.

## Summary of Case Studies: The Relationship Between Internet Freedom and Political Space

The conceptual framework for this study was based on the literature on framing and social movements. Framing, as discussed in Chapter Two, involves a set of prior notions that individuals rely on to understand and respond to facts or events they are presented with. The Internet can expand the set of actors involved in frame creation, reduce social activists' dependence on the traditional media for that task, and restructure the framing process so it is less hierarchical. This happens because in the virtual community, weak links serve as key conduits of information, connecting social media users who do not interact with each other on a daily basis. Although these networks are too superficial to create peer pressure for social mobilization on their own, they are very effective for creating "a buzz" around certain events because they facilitate rapid diffusion of information among netizens who rarely interact with each other offline and who may belong to different social strata. Offline communities are structured around strong social ties, which facilitate social mobilization in political space. Strong offline ties are highly correlated with having similar socioeconomic, religious, ethnic, or cultural backgrounds; they thus make cross-stratum mobilization unlikely. The Internet broadens the coalitions of actors by enabling actors with different backgrounds to engage in joint construction of frames.

Our case study analysis built on this process by capturing the different links between online and offline mobilization. In Egypt, social media facilitated both frame-building and coordination among protest leaders. The protests began with a circulation of photos documenting a mid-2010 incident of police brutality against Khaled Said among Facebook users and rapidly grew into a "We Are All Khaled Said" frame—that violence against one is repression against all—cutting across social and economic strata. Social media introduced new voices into Egypt's political space that were not affiliated with either of the existing opposition parties. This was possible because social media enabled them to compensate for their lack of formal organization or access to religious institutions. The number of protesters who came out on the streets on

January 25, 2011, caught the regime off guard and triggered a domino effect that led key supporters to defect from Mubarak.

In Syria, a far more repressive autocracy, the mobilizing potential of the Internet was severely curtailed by the regime's tight censorship of online content, the ban on Facebook, and repressive measures against civil rights activists. In the Syrian case, we found little evidence to support the claim that social media was necessary for protests. However, the Internet was indispensable for attracting international attention to the protests by getting information out of the country. The evidence of the atrocities committed by the regime increased the political costs of supporting Bashar al-Assad to Russia and other states, although that has not led them to abandon the regime to date. We also found that as the civil conflict unfolded, more netizens turned to anonymizing tools, such as Tor, to conceal their behavior from officials and to access censored information.

Our third case study was China, for which we presented two instances of online mobilization that took place in 2011. This case study indicated how—even in an authoritarian state that severely limits freedom of assembly—the Internet can spur social mobilization that authorities find difficult to stop. The first incident was the Wenzhou train collision in July 2011 that killed 40 and injured approximately 200. Chinese officials tried to cover up this crash by prematurely concluding rescue operations and burying damaged train cars using bulldozers. Chinese party officials also ordered the mainstream media not to cover the event. However, the entire world found out about this tragedy within several hours from blog posts on the Sina Weibo micro-blogging platform.

This case illustrated how the Internet could be used to contest the accuracy of frames that Chinese authorities used to describe the event. According to Chinese officials, the accident was caused by a lightning strike that led to malfunctioning of a signaling system—supporting the narrative that accidents are unavoidable. Bloggers, on the contrary, argued that corruption and poor enforcement of safety regulations was the primary cause. The most frequently forwarded comment on Sina Weibo was: “When a country is so corrupt that one lightning strike can cause a train crash . . . none of us are exempt. China today is a train



rushing through a lightning storm . . . we are all passengers.”<sup>1</sup> This post questioned the legitimacy of the entire high-speed train program, which cost the country billions of dollars and exposed the vulnerability of railway infrastructure nationwide. The broader frame was that the rush to growth was being undertaken at the cost of lives. The extent of popular distrust is captured well in a note posted on Sina Weibo: “I’m going to take a high-speed train back to Beijing. My friends all say I’m heading for death. Please bless me.”<sup>2</sup> A change of frame alone sufficed to trigger Chinese authorities’ response and the dismissal of high-ranking officials at the Railway Ministry.

The second incident involved protests in the city of Dalian against reopening a chemical plant in the aftermath of a sea storm that damaged the protective dike around the plant, sparking fears that PX, an extremely toxic chemical, spilled into the water. Calls for demonstrations to have the plan closed circulated rapidly on Sina Weibo; subsequently, 12,000 people gathered in downtown Dalian to protest. Social media was extremely helpful for coordinating spontaneous protests and then for disseminating photos documenting the protests all around the country. Local officials had to yield to popular demand and ordered the relocation of the plant.

Both incidents provided important insights into how new technologies can foster consensus building and mobilization. The first showed how Web 2.0 technologies helped citizens frame issues in contrast to state authorities. No protests took place because the backing of the mainstream media was sufficient to prompt the authorities to respond to popular sentiment. The second incident illustrated how mobilization could take place because people shared strong consensus on the environmental threat and health hazard the plant posed. These two social movements lacked any organizational support and were devoid of any clearly identified leaders or any hierarchical structure. Instead, the unique organizational nature of the Internet enabled civil society to compensate for the lack of institutions for preference articulation and mobilization.

---

<sup>1</sup> Branigan, 2011.

<sup>2</sup> Bristow, 2011.

However, the China case study also provided evidence for the limitations of this form of mobilization. The empowerment provided by the Internet was not uniform across different segments of Chinese society, and authorities were more likely to respond to social pressures from better-educated and more-affluent citizens while ignoring similar demands from less-affluent and rural citizens. Unlike the incident in Dalian, citizens of Yunnan, a poorer, less-developed province, have been unable to close a chemical plant despite raising similar environmental concerns. Perhaps Internet freedom may lead to uneven expansion of voice, vote, and assembly across different segments of society because more-influential groups will also be more likely to have connection to the Internet.

Turning to Russia, protests in the aftermath of the 2011 elections to the national assembly (Duma) illustrated how online mobilization manifested in political space in the country with a relatively high level of Internet penetration and a relatively open political space. In an environment with tight government control over traditional media, NGOs can use the Internet to reach out to voters and to collect evidence challenging the validity of the frame put forward by authorities. The Internet was the only channel through which voters in Russia could expose electoral violations that took place on Election Day and during ballot counting. By documenting irregularities at polling stations and distributing them via YouTube, and by analyzing statistical data and posting the results, netizens were able to persuade many voters that election results were rigged. Social media subsequently facilitated the coordination of protests throughout the country by providing information about the day, place, names of opposition leaders who would head the demonstrations, and the expected number of social media users who would show up.

Unlike China, Russia already had an active civil society that can help organize protests. Opposition parties, NGOs, and online activities before the elections had established positive reputations, making them more effective in contesting the frame put forward by the government. The role of the Internet in Russia was to strengthen the links between the civil society, NGOs, and the opposition parties—whereas

personal networks helped with offline mobilization, especially among white-collar, college-educated, middle-class, urban residents.

The historical case study of RFE/RL in the Soviet Union and Eastern Europe draws parallels between the goals and constraints faced by U.S. policymakers during the Cold War and the challenges entailed in implementing Internet freedom programs. RFE/RL broadcast alternative information to people living behind the Iron Curtain in the hope that it would bring about political change either in a piecemeal or revolutionary fashion. The program exploited ideological vulnerabilities of the Soviet regime by appealing to the intelligentsia and youth who aspired to be part of a world cultural community. The goal of the program was to provide alternative frames for understanding the Western culture and policies that would compete with those propagated by the Soviet officials in the mainstream media and educational institutions. These programs played an important role in disseminating information about social protests, major environmental disasters, and *samizdat* literature. Although these programs did not directly alter the internal dynamics of the Soviet system, they did contribute to the rise of an alternative culture based on values inconsistent with the Soviet ideology.

The RFE/RL program, like today's Internet freedom programs, aimed to facilitate the flow of information from countries in which the United States had virtually no presence, enabled Western sources to create a frame about those events consistent with democratic ideals, and then feed this frame back to the country in which the event took place. This process is taking place today in Syria, with citizens inside Syria documenting atrocities being committed by the Assad regime and uploading the information. Once such evidence is on the web, international media sources, which faced difficulties reporting on the story, can inform international and internal Syrian audiences about what is taking place.

Our analysis yields several important results. First, the expansion of social space online may lead to the expansion of political space, even when netizens do not at first intend to use the Internet for political purposes. In Egypt, China, and Russia, political online mobilization grew out of nonpolitical uses of the Internet. In Egypt, active online

civil society evolved because the government restricted offline political activity without simultaneously censoring the Internet, and those vibrant online communities rapidly became politicized after the news about Khaled Said's death. In China, rapid economic changes brought about social transformation that contributed to the rise of new social identities. The Internet facilitated the interaction among these new social groups and enabled them to challenge the state. For example, Xianzhu was denied a civil service job because he was infected with hepatitis-B, but was able to challenge this decision in court because online discussion of his case attracted the attention of legal experts who agreed to represent him. Online publicity also contributed to a fairer trial by increasing the probability that a higher court would scrutinize the lower court's decision. In Russia, modernization of the workplace by using the Internet to conduct businesses introduced more Russians to Internet skills, which they subsequently used to document electoral violations in the aftermath of the legislative elections. A similar conclusion emerges from the historical case study of the RFE/RL programs in the Soviet Union. They explicitly tried to remind groups of their ethnic identities—which subsequently became the primary source of the nationalist movements that challenged Soviet rule in the late 1980s and brought about the collapse of the Soviet Union.

Second, online information can undermine the authoritarian power of nondemocratic regimes by underscoring the extent of opposition and triggering an information cascade. The cost of protests is frequently proportional to the number of protesters who appear on the streets. Nondemocratic rulers do not know the degree of actual popular support for the regimes because citizens hide their true attitudes out of fear of retribution. The Internet can facilitate social protests by enabling the anonymous expression of opinions and coordination of collective action that subsequently leads to a domino effect. In Egypt and Russia, online mobilization triggered a wave of protests that had long-term consequences. Although social media did not cause the popular uprising in Egypt, it substantially increased the number of participants in the first demonstration. The size of the crowd caught the authorities by surprise and triggered the defection of high-ranking army officials. In Russia, information about electoral fraud triggered a

wave of online mobilization that manifested itself in the series of mass demonstrations. Syria's activists used the Internet to publicize elite defection from the regime, albeit with limited success.

Third, the Internet can potentially make political coalitions more inclusive by opening possibilities for deliberation that generate frames that cut across socioeconomic cleavages. This conclusion emerges primarily from the review of theoretical literature on the diffusion of information online and the literature on social movements. While weak ties facilitate the diffusion of information online, strong ties create peer pressure that contributes to offline social mobilization. The Internet fosters the diffusion of information to people who do not interact on a daily basis; in so doing, it cuts across socioeconomic or cultural cleavages.

Fourth, online mobilization is more likely to manifest itself offline when it is targeted against specific policy outcome than against the regime. This conclusion is supported by the case study of China, where online activists benefited from intraparty competition between the progressive and old-guard factions, coupled with the vertical competition between the national and regional officials. Seeking to advance their policy agenda, progressive factions with the China's Communist party joined netizens when online mobilization was provoked by a specific policy outcome. The progressive faction then used popular discontent to advance its own policy agenda. When the mobilization targeted the regime per se, both the progressive and old-guard factions sided together trying to suppress online movements.

Fifth, technological empowerment has not been uniform and has benefited the middle class more than it has poorer individuals. In Russia, the majority of protesters were white-collar professionals who were also active users of the Internet. In China, the authorities were more responsive to the middle-class online and offline mobilization than to similar demands expressed by rural and less-affluent residents. In Egypt, secular students and recent college graduates in urban areas formed the core of the protesters who participated in the first demonstration.

## Impact of Opportunity Structures on the Outcomes of Online Mobilization

Although it has reduced the cost of collective action and information sharing, the Internet has expanded surveillance opportunities available to state actors. Case studies also show that the expansion of Internet freedom may not produce the same outcome across countries because such opportunity structures as elite fragmentation, state repressive capacity, and availability of allies affect how online mobilization manifests itself in the political space.

Elite fragmentation was especially visible in China and Russia because federal institutions in these countries fragment power both vertically (by dividing policy authority between the national and lower-tier governments) and horizontally (by increasing the number of channels through which citizens can affect policy outcomes). In both countries, subnational governments' competition for mobile resources and economic development policies indirectly contributed to political protests. In China, regional leaders' lackluster enforcement of environmental and safety standards, coupled with aggressive investment in the telecommunication infrastructure that facilitated online access, contributed to the rise of environmental movements. In Russia, regional government's investment in the telecommunication infrastructure made the Internet more affordable for businesses. Subsequently, whistleblowing about electoral violations was more frequent in regions with a higher share of enterprises connected to the Internet.

Federal institutions also affected governmental responsiveness to societal demands in both China and Russia. The relationship between the national and subnational governments is characterized by informational asymmetries about the true state of the world. In both China and Russia, national governments formulate national policies based on the information provided by subnational governments. Regional leaders, however, have a strong incentive to underreport information that may hinder their future promotion. For this reason, national officials (as noted in the Chinese case study) sometimes see online movements as a helpful check upon corruption and abuses conducted at the subnational level. National leaders can utilize problems highlighted by

online movements to show their responsiveness to problems raised by ordinary citizens and to deflect responsibility for governing inadequacies to lower-level officials.

International allies constitute the second important factor that affects the outcomes of online mobilization. Syrian and Russian cases demonstrated that some outsiders can help the regime and others can help the opposition. Iran shared Internet filtering technology with the Syrian authorities, whereas Google provided rehosting assistance to the Russian election watchdog after it was subjected to a DDOS attack. In addition to providing direct aid, international allies can raise the international community's awareness about ongoing events. The stronger a regime's economic and political linkages to the West, the more likely it is that cyberactivists will attract sufficient resources from abroad. Thus, online mobilization is most likely to have an impact on political space in countries with stronger ties to the West. Some scholars even argue that international linkages affect overall political development of non-democratic regimes because they increase the political and economic costs of repression.<sup>3</sup>

Repressive capacity is the third factor that affects the outcomes of online mobilization. As we showed in the Egypt case study, although the Internet was not the sole factor that contributed to the collapse of the Mubarak regime, online mobilization significantly increased the turnout on the first day of protests and subsequently undermined military support because it became too politically costly for the military to support the regime that lost legitimacy. Similar outcomes were observed in Serbia during anti-Milosevic protests and in Ukraine during the Orange Revolution. Therefore, the outcomes of online mobilization will depend on the extent to which the regime has control over its coercive apparatus.

These opportunity structures affect the extent to which online freedom can transform the political space. The expansion of political space along the three dimensions is the most likely in countries with strong links to the West—and in which elites are fragmented and repressive capacity is weak. When any of these three aspects—voice, vote,

---

<sup>3</sup> Levitsky and Way, 2010.

and assembly—are constrained, the expansion of political space will be uneven, and most likely to take place through voice rather than voting.

## **Implications for the Design and Implementation of Internet Freedom Programs**

Internet freedom programs can expand political space either by maximizing the number of rank-and-file netizens who can circumvent censorship, or by training a handful of agenda setters—bloggers, online journalists, and the opposition leaders—to become more sophisticated users of anonymization, circumvention, and communication technologies. The former strategy primarily focuses on broadening Internet freedom for all users, regardless of whether they will use their access for political purposes. The latter strategy deepens online mobilization and communication opportunities for a handful of motivated individuals who advocate political change. Which of these two options may have the most visible outcome in the political space?

As discussed in Chapter Two, there is a great deal of debate about the path from the few exercising their Internet freedom to the many doing so. Is the expectation warranted that empowering (largely self-selected) political activists, members of the media, and technical elites will lead to events that yield an expanded political space for all? History suggests that, under propitious circumstances, the actions of a small group (e.g., pioneers, a revolutionary vanguard, or apostles) will attract others, create positive feedback, and thereby build momentum for change. More recent history—notably, the self-immolation of a hitherto anonymous Tunisian street vendor—shows how a crystal dropped into a supersaturated media environment can precipitate a broad state change. That noted, the vast majority of such crystals simply dissolve into the media itself.

The influence of opinion leaders belies their small numbers, and has the potential for magnifying the effect of tools to evade restrictions on their Internet freedom. In 1986, detailed news of the Chernobyl nuclear accident did not reach Soviet citizens directly. Eyewitness accounts that were sent to Western sources and then bounced



back to Soviet citizens via Western short-wave radio stations kept such citizens informed about the magnitude and particulars of the disaster.<sup>4</sup> More recently, the ability of Chinese activists to access outside sources has allowed them to develop and refine the primary circumvention method: the use of circumlocutions to discuss topics that would otherwise be censored.

The existence of circumvention tools and citizens' knowledge that they are available may also affect regime behavior. In a crisis sparked by a particular event, such as an election, more individuals than usual will seek information and want to discuss its impact. Thus, even though few users normally employ circumvention technology, this number can quickly expand at critical junctures, as statistics repeatedly indicate. This makes it difficult for regimes to cover up major news stories and forces them to acknowledge and account for information their citizens have received from media sources outside their control.

Even in a crisis, the total number of users is likely to be limited by the technological sophistication necessary to use circumvention technologies. Users must understand, in general terms, what circumvention is and why it is important as well as how to install software. Some circumvention technologies will not work as advertised unless certain browser features are disabled, and the installation techniques can change with each new version of the browser software (which means users have to stay current with some fairly technical literature). Opinion elites, who shape debates, may be more technologically savvy than the average population, but to assume they are all savvy is a stretch. It is also a stretch to assume that those who are politically active are particularly tech-savvy. There are exceptions, of course—such as Egypt's Wael Ghonim, a Google engineer who became inspired to use his technological skills to assist the Egyptian movement—but they remain exceptions.

Another potential objective would be to broaden the political space by enabling the dissemination of Internet freedom technologies (including digital mobile telephony) to a much wider group of citizens. A broader space will allow more people to have access to infor-

---

<sup>4</sup> Parta, 2007.

mation about political issues and would enable them to participate in discussions about them. These efforts could also be targeted toward empowering individuals outside the historic mainstream (e.g., women, minority ethnic or religious groups, or the young). If successful, this approach would enlarge the politically active portion of the population and make it more difficult in general for nondemocratic regimes to repress citizens' freedom. Because these efforts are targeted at people who up until now have chosen to remain on the political sidelines, it may be hard to convince such individuals that they should engage in the political space online. Efforts will be needed to make potential users aware of U.S. Internet freedom programs and to convince them that they are worth using. Such individuals are more likely to worry about regime countermeasures and to be easily deterred by the difficulties of using Internet freedom technologies.

Another distinction worth noting is between expanding social spaces as a foundation for political freedom and expanding public spaces as an alternative foundation. Social spaces have an expectation of privacy; public spaces do not. But expanding political space solely through private spaces would seem to be a contradiction; the public arena is where such ideas ultimately must contend. The two are not necessarily antithetical: Individuals wanting to test and play with unauthorized political opinions may find growing room in social spaces, while finding that surfacing immature ideas in the public domain can result in their premature destruction.

Conversely, authoritarian governments, who so often embrace secrecy for their own maneuvers, demonstrate paranoia about secret plots against them. Hence, as demonstrated in totalitarian states, private social spaces (above a certain size) are anathema. The easier it is to form private social spaces, therefore, the greater the prospects for political space. This logic suggests a close relationship between privacy and freedom. Effective privacy, in many circumstances, is prerequisite for effective freedom; if the (repressive) state is unaware of what one is doing, the activities cannot be prohibited and the state has a much

harder time inhibiting it.<sup>5</sup> Then, as noted, ideas strengthened in private social spaces can be introduced into public spaces. The importance of this linkage is underlined by the finding that many people adopt circumvention technologies to construct social spaces. Thus, a strategy to enhance the ease or attractiveness of forming social spaces should therefore enhance political space.

Finally, it is worth noting that in no country is the Internet entirely free of some political repression and in no country is the Internet entirely repressed. Similarly, in no country has the political space expanded to its maximum extent and in no country is it completely absent (nor is it obvious that political space *should* be expanded past the point where it crowds out all other human activity). Correspondingly, the *value* of opening up political space in a particular country will vary depending on how open such political space already is. Although a more open political space is a value in and of itself (i.e., speech *should* be free), the instrumental value of greater political space—e.g., greater accountability, a broader menu of policy choices, faster innovations in solving problems, putatively greater equality—mean that the ultimate value of Internet freedom can be measured with respect to downstream, results-based criteria, not just process-based criteria.

## **Leveraging Internet Freedom Programs: Maximizing Their Impact and Understanding Their Limitations**

Internet freedom programs, perhaps uniquely across the U.S. governments' human rights activities, target a wide range of activities and geographic locations. Some programs, such as the technical development ones, are global in nature. Software released into the Internet is available for download or use by anyone who can access it. Other programs are more specific; for example, training programs for civil society groups are designed to allow them to better operate in repres-

---

<sup>5</sup> Inhibition is possible even with perfect privacy (i.e., zero chance of being detected either directly or indirectly, say, via friends) unless individuals actually believe they have perfect privacy.

sive environments. Certain programs are designed to respond rapidly to emerging situations when Internet access for civil society groups is threatened. Others are designed to assist civil society organizations conduct their business against the general state of repression they face every day in nondemocratic countries. Given these circumstances, it is not surprising that Internet freedom programs' impact upon the political space vary widely.

Our analysis began with consideration of how regime types may affect the effectiveness of various Internet freedom programs. As discussed throughout this report, hybrid states and authoritarian ones utilize very different means for controlling the Internet. The Russian case study provides strong evidence for the utility of attempting to deepen Internet freedom in hybrid states, which already have an active civil society that Internet freedom tools can further empower. Civil society groups can be trained to respond quickly to circumstances when Internet access is blocked. These groups can also be assisted when their websites come under DDOS attack by rehosting them on servers that are harder to overload and block.

Hybrid regimes do have other means at their disposal to shut down or curtail the Internet impact of civil society groups. They will undoubtedly use legal instruments to harass and punish opponents and will threaten them, sometimes physically. However, the greater degree of visibility and the higher level of repression required to control civil society groups comes at a serious cost for hybrid regimes. For domestic and international audiences, the repressive nature of the regime will not be hidden in the shadows of the Internet but exposed to the light of day—something the regimes seek to avoid.

Internet freedom programs can also have an impact upon elections. As in Iran in 2009 and Russia in 2011, the Internet (and programs that enhance its effectiveness) make voter harassment and outright fraud more difficult to carry out and hide from domestic and international audiences. Indications on the Internet that authorities are undertaking efforts to “steal the election” may undermine the overall legitimacy of the regime and have sparked protest movements in the past. The presence of these Internet tools may steer authorities away

from outright fraudulent activities for fear they could be uncovered. This gives the opposition a somewhat better chance at achieving victory.

The most recent developments in Russia demonstrate the precarious nature of Internet freedom in hybrid regimes, however. With Putin's ascendance to the presidency, the Duma enacted measures that gave the government legal grounds for shutting down entire sites if they fail to comply with the newly enacted amendment to the information law that justifies government censorship of online content as a way to reduce children's exposure to harmful information. Within less than two months of the enactment, YouTube found itself the first major government target when the Russian authorities demanded that it remove the trailer to the widely reviled movie "Innocence of Muslims," produced by an anti-Muslim provocateur. The authorities gave YouTube until November 1, 2012, to comply; according to legal experts, the entire YouTube service can be blocked in Russia under the new provision. Regional authorities in the predominantly Muslim Chechen Republic ordered all ISPs located in the republic to block access to YouTube. Some complied and blocked YouTube immediately.<sup>6</sup>

Since authorities in hybrid regimes can quickly change the regulatory environment from free Internet to a highly censored one, programs that raise rank-and-file netizens' awareness about Internet censorship, as well as where to find and how to install anonymization and circumvention technologies, can be valuable preemptive measures.

For authoritarian regimes, broadening the use of circumvention technologies for the largest number of netizens is the most critical for the expansion of political space. China, Iran, and similar regimes have undertaken vast efforts to filter the information their citizens can access and to prevent them from creating and posting information the authorities find threatening. These regimes do this to maintain the frame that authorities want their citizens to have about the society they live in and to eliminate their citizens' contact with any information that might allow them to start forming alternative views. Circumvention tools reverse this process by providing people with access to out-

---

<sup>6</sup> "Internet Providers in Chechnya Instructed to Block YouTube over Anti-Islam Film," RFE/RL website, September 28, 2012.

side information that is central to rebutting the frame of authoritarian regimes. Circumvention tools also help the more politically active stay abreast of developments outside their country.

An additional benefit of circumvention tools in authoritarian regimes is that they provide an opportunity to communicate without fear of being monitored and thus contribute to the development of social space. While the formation of any civil society group is difficult inside an authoritarian state, circumvention tools that provide anonymity allow for at least the rudiments of it. With circumvention technology, individuals inside the country have the ability to learn about and safely connect with each other even for nonpolitical purposes. Ideas can be exchanged between people within the country, and actions can be coordinated, at least for a time, between like-minded individuals.

Maximizing the effectiveness of Internet tools requires balancing between programs that assist day-to-day activities and those that might be useful in a crisis. While our case studies point out the important role the Internet can play during a revolution, in no case was its presence the sole or even the predominant causal factor. Many factors will determine whether an organized attempt to replace a regime will occur and its chances of surviving the crisis. What Internet freedom programs can do is help improve the organization and cohesion of civil society. However, many nondemocratic regimes are quite robust and are unlikely to fall easily even in the face of extreme violence against them, as the Syrian case shows.

On the other hand, Internet freedom tools can play an important role in improving the lives of citizens who live in nondemocratic states. They allow people to highlight unaddressed issues in society, such as environmental dangers or shoddy infrastructure. Corrupt local officials can be exposed anonymously with less fear of retribution. As a general principle, Internet freedom tools make it easier for citizens to hold their leaders accountable for their actions and provide those who wish an opportunity to learn about and explore the world unencumbered by the regime's ideological restrictions.

It is also important to keep in mind some of the challenges inherent in implementing Internet freedom programs. As identified in the previous chapter on measures and countermeasures, there is a high

degree of “strategic uncertainty” about the impact of Internet freedom programs, stemming from the fact that the programs’ impact on political space depends on coordination between those who use these tools (i.e., actors inside nondemocratic states) and those who develop them (i.e., most Western computer programmers). These actors do not communicate with each other very much, although both seek to preempt regime countermeasures.

Tool developers, although they have a good grasp on technology used by the regime, may not know netizens’ demand for specific technology and may not understand distributional channels by which these technologies are disseminated. The returns on developing new technologies depend on netizens’ awareness and willingness to use them. Therefore, even when new technologies become available, it will take netizens some time to adopt them. The longer the time lag between the release and the adoption of new technologies, the more chances there are for the regime to find a countermeasure, thereby attenuating the value of a new tool.

Another concern is whether U.S. Internet freedom activities are endangering local digital activism. There is some danger that foreign support, even if it is at arm’s length, may delegitimize in-country movements in the eyes of local populations. This support also may provide targets and justification for persecution by repressive regimes and divert NGO attention from grassroots activism in favor of initiatives funded by the U.S. government.

This poses something of a dilemma for U.S. Internet freedom efforts. On the one hand, it could avoid programs that specifically help activists inside countries, thereby avoiding direct criticism from foreign governments for assisting opposition movements. Under this strategy, the United States would focus on the global aspects of the “Freedom to Connect” agenda without directly engaging with groups under government-led cyberpressure. On the other hand, the United States could embrace a more aggressive strategy, attempting to use Internet freedom programs as a way to directly confront hostile authoritarian governments. Under this strategy, the United States would focus its efforts on using Internet freedom programs to empower opposition movements, viewing the concerns expressed and the backlash from

authoritarian regimes as a necessary price to support Internet freedom. At the moment, U.S. Internet policies are politically neutral and lack explicit political agendas or specific countries. They seek to expand the “Freedom to Connect” worldwide to all Internet users regardless of political leaning.

The Internet has become a new front in the struggle between freedom and autocracy. While this struggle occurred in print and over the airwaves in the past, it now will occur on the Internet, as parts of the rest of our lives do. On balance, the spread of the Internet and Web 2.0 technologies into nondemocratic states should be good for the United States. It raises the possibility for more-transparent and responsive government and that people in previously unreachable corners of the world will become aware of democratic ideals. Yet, it is also likely that nondemocratic regimes will continue to find new ways to use the Internet to entrench their own hold on power.





## Electoral Fraud Variable and Summary Statistics for the Russia Case Study

---

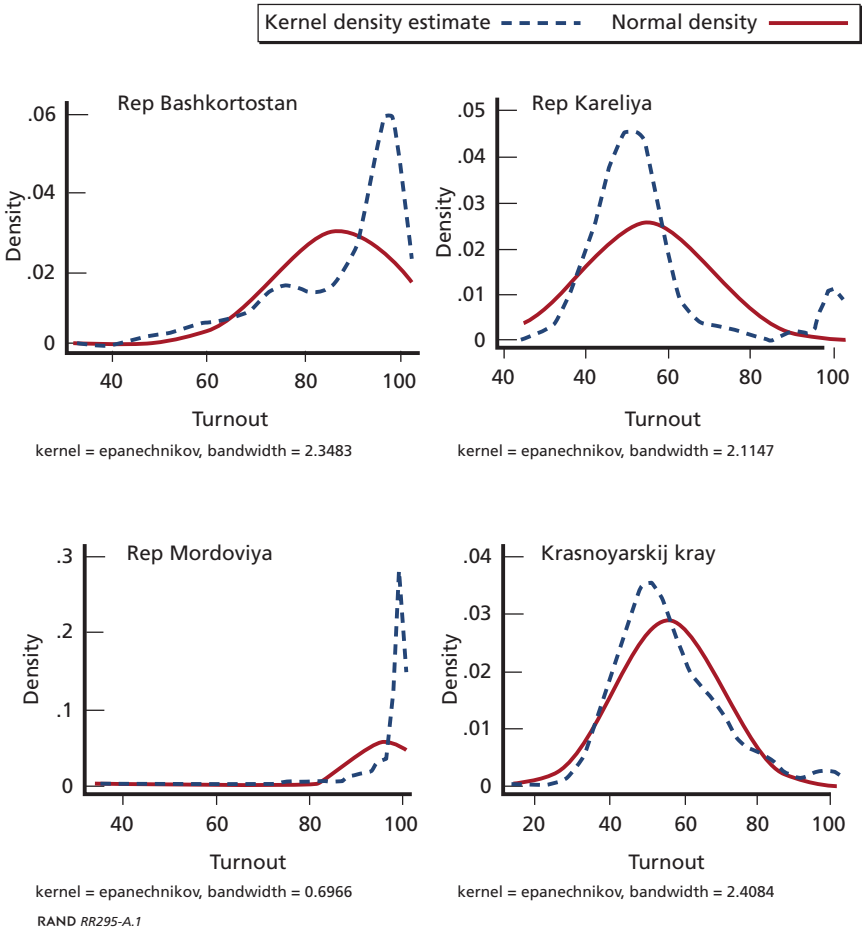
Political scientists have not reached consensus on the best methodology for detecting electoral fraud.<sup>1</sup> The approach adopted here is based on the assumption that in fair elections the distribution of voter turnout should follow a normal distribution because both 0 percent and 100 percent voter turnout are low-probability events. In many Russian regions, however, there are spikes around the 90-percent turnout (Figure A.1).

The Kolmogorov-Smirnov test is a standard statistical procedure for comparing any two distributions. This test computes the distance between the two distributions, and higher values indicate that the two distributions are less alike. Table A.1 reports the values for the Kolmogorov-Smirnov statistics and p-value for the null hypothesis that the data are generated from the normal distribution. The null hypothesis that the turnout data is normally distributed is rejected for 69 out of 83 regions. The Kolmogorov-Smirnov summary statistics reported in Table A.2 were used as a proxy measure of electoral fraud.

---

<sup>1</sup> The author is thankful to Kirill Kalinin for sharing the precinct level data. See Walter R. Mebane Jr. and Kirill Kalinin, *Electoral Fraud in Russia: Vote Counts Analysis Using Second Digit Mean Tests*, paper presented at the Midwest Political Science Association meeting, April 22–25, 2000; and Mikhail Myagkov, Peter C. Ordeshook, and Dimitri Shakin, *The Forensics of Election Fraud: Russia and Ukraine*, Cambridge, Mass.: Cambridge University Press, 2009.

**Figure A.1**  
**Distribution of Voter Turnout in Selected Russian Regions**



**Table A.1**  
**Kolmogorov-Smirnov Statistics**

Region	K-S Test	p-value
<b>Republics</b>		
Adygeya	0.201	0.000
Altay	0.253	0.000
Bashkortostan	0.539	0.000
Buryatiya	0.103	0.000
Chechnya	0.931	0.000
Chuvashiya	0.214	0.000
Dagestan	0.659	0.000
Ingushetiya	0.683	0.000
Kabardino-Balkariya	0.875	0.000
Kalmykiya	0.209	0.000
Karachaevo-Cherkessiya	0.748	0.000
Kareliya	0.002	0.500
Khakasiya	0.059	3.640E-286
Komi	0.306	0.000
Mariy-El	0.402	0.000
Mordoviya	0.760	0.000
North Osetiya—Alaniya	0.489	0.000
Sakha (Yakutiya)	0.176	0.000
Tatarstan	0.545	0.000
Tyva	0.588	0.000
Udmurtiya	0.064	0.000
<b>Krays</b>		
Altay	0.000	0.996
Kamchatka	0.201	0.000
Khabarovskiy	0.006	0.000

Table A.1 (Continued)

Region	K-S Test	p-value
<b>Krays (cont.)</b>		
Krasnodarskiy	0.360	0.000
Krasnoyarskiy	0.001	0.909
Permskiy	0.000	0.999
Primorskiy	0.018	9.56E-27
Stavropolskiy	0.001	0.833
Zabajkalskiy	0.005	0.015
<b>Oblasts</b>		
Amurskaya	0.014	1.60E-16
Arhangelskaya	0.001	0.681
Astrakhanskaya	0.001	0.920
Belgorodskaya	0.453	0.000
Bryanskaya	0.134	0.000
Chelyabinskaya	0.041	1.09E-141
Irkutskaya	0.001	0.695
Ivanovskaya	0.001	0.923
Kaliningradskaya	0.001	0.775
Kaluzhskaya	0.145	0.000
Kemerovskaya	0.272	0.000
Kirovskaya	0.004	0.041
Kostromskaya	0.112	0.000
Kurganskaya	0.106	0.000
Kurskaya	0.053	5.04E-232
Leningradskaya	0.000	0.999
Lipetskaya	0.082	0.000
Magadanskaya	0.036	5.62E-108

Table A.1 (Continued)

Region	K-S Test	p-value
<b>Oblasts (cont.)</b>		
Moskovskaya	0.000	1.000
Murmanskaya	0.052	2.20E-225
Nizhegorodskaya	0.067	0.000
Novgorodskaya	0.074	0.000
Novosibirskaya	0.092	0.000
Omskaya	0.147	0.000
Orlovskaya	0.000	0.966
Penzenskaya	0.261	0.000
Pskovskaya	0.000	0.994
Rostovskaya	0.076	0.000
Ryazanskaya	0.001	0.951
Samarskaya	0.001	0.804
Saratovskaya	0.234	0.000
Sakhalinskaya	0.081	0.000
Smolenskaya	0.001	0.726
Sverdlovskaya	0.000	0.998
Tambovskaya	0.288	0.000
Tverskaya	0.002	0.325
Tomskaya	0.000	0.998
Tulskaya	0.294	0.000
Tyumenskaya	0.463	0.000
Ulyanovskaya	0.197	0.000
Vladimirskaya	0.000	0.993
Volgogradskaya	0.000	0.993
Vologodskaya	0.036	3.70E-108

**Table A.1 (Continued)**

<b>Region</b>	<b>K-S Test</b>	<b>p-value</b>
<b>Oblasts (cont.)</b>		
Voronezhskaya	0.233	0.000
Yaroslavskaia	0.016	2.36E-21
<b>Autonomous Okrugs</b>		
Chukotskiy	0.593	0.000
Khanty-Mansiyskiy	0.003	0.244
Nenetskiy	0.000	0.997
Yamalo-Nenetskiy	0.529	0.000
<b>Federal Cities</b>		
Moscow	0.072	0.000
Saint-Petersburg	0.001	0.711
Autonomous Oblast:		
Yevreyskaya	0.001	0.801

**Table A.2**  
**Summary Statistics**

Variable Description	N	Mean	Standard Deviation	Source
Number of electoral violations reported on Golos site	83	93.70	148.53	Golos
Number of computers at workplace connected to the Internet, per 100 employees	83	15.18	4.66	Goskomstat, Regiony Rossii <sup>a</sup>
Number of computers at workplace per 100 employees	83	34.40	5.70	Goskomstat, Regiony Rossii
Mobile phones per capita	82	1.58	0.27	Goskomstat, Regiony Rossii
GDP per capita, in 2010 rubles	83	69.49	13.39	Goskomstat, Regiony Rossii
Percentage of urban population	80	412.26	2,027.65	Goskomstat, Regiony Rossii
Newspapers published, per capita	83	0.95	1.41	Goskomstat, Regiony Rossii
Percentage of population that receives NTV	81	62.68	22.51	Goskomstat, Regiony Rossii
Percentage of population that receives <i>Mayak</i>	80	84.39	16.97	Goskomstat, Regiony Rossii
Percentage of population that receives Radio Russia	82	92.31	9.12	Goskomstat, Regiony Rossii
Dummy for Moscow and St. Petersburg	87	0.02	0.15	Goskomstat, Regiony Rossii
Extent of electoral fraud	83	0.17	0.24	Constructed by the author

<sup>a</sup> Goskomstat, *Regiony Rossii* web page, Moscow, 2012.





## Bibliography

---

“10 Let na Zashchite Izbiratelykh Prav” [“10 Years on the Protection of Electoral Rights”], *Golos*, April 28, 2010 (file no longer available). As of March 12, 2012: <http://golos.org/news/3421>

Abaza, Khairi, *Egyptian Legislative Elections: A Reading of the Results*, Policy #1061, Washington, D.C.: The Washington Institute, December 12, 2005.

Ackerman, Spencer, “Newest U.S. Counterterrorism Strategy: Trolling,” *Wired*, July 18, 2012. As of June 1, 2012: <http://www.wired.com/dangerroom/2012/07/counterterrorism-trolls/all/>

Akbarzadeh, Shahram, and Benjamin MacQueen, *Islam and Human Rights in Practice: Perspectives Across the Ummah*, New York: Routledge, 2008, p. 80.

Al-Saqaf, Walid, “Circumventing Internet Censorship in the Arab World,” in Larry Diamond and Marc F. Plattner, eds., *Liberation Technology: Social Media and the Struggle for Democracy*, Baltimore, Md.: The Johns Hopkins University Press, 2012.

Alexanyan, Karina, “The RuNet—Lost in Translation,” *Russian Analytical Digest*, No. 69, December 2009: pp. 3–6. As of May 28, 2012: <http://www.css.ethz.ch/publications/pdfs/RAD-69.pdf>

“All Polling Stations to Be Equipped with Web Cams by Mid-October, Says Azarov,” Interfax News website, October 1, 2012. As of October 4, 2012: <http://www.interfax.com.ua/eng/main/119595/>

Alsop, Stewart, “Courage in Berlin and Its Reward,” *Washington Post*, June 20, 1953.

Ambrose, Stephen E., *Eisenhower: Soldier and President*, New York: Simon and Schuster, 1990.

Amos, Deborah, “Pro-Assad ‘Army’ Wages Cyberwar in Syria,” *National Public Radio*, September 25, 2011.

Anderlini, Jamil, "Mass Protest Forces Chinese Factory to Close," *Financial Times*, August 14, 2011. As of October 1, 2012:

<http://www.ft.com/cms/s/0/92a73bf0-c682-11e0-bb50-00144feabdc0.html#axzz284CZEW5F>

Aouragh, Miriyam, and Anne Alexander, "The Egyptian Experience: Sense and Nonsense of the Egyptian Revolution," *International Journal of Communication*, Vol. 5, 2011.

Applebaum, Anne, *Gulag: A History*, New York: Anchor Books, 2003.

Arab Republic of Egypt, Ministry of Communications and Information Technologies, *The Future of Internet Economy in Egypt: A Statistical Profile*, May 2011.

"Arab Spring: An Interactive Timeline of Middle East Protests," *Guardian*, January 5, 2012. As of April 4, 2012.

<http://www.guardian.co.uk/world/interactive/2011/mar/22/middle-east-protest-interactive-timeline>

Arendt, Hannah, *The Origins of Totalitarianism*, Orlando, Fla.: Houghton Mifflin, 1976.

Assir, Serene, "The Muslim Brotherhood's Youth: An Independent Course to Revolution?" *alakhbar english*, November 28, 2011.

Aulich, James, "The Democratic Delusion: New Media, Resistance and Revolution in Serbia, 1995–2000," *Studies in Russian, European and Central European New Media*, Vol. 5, 2011.

Azzam, Maha, "Egypt's Military Council and the Transition to Democracy," *Middle East and North Africa Programme Briefing Paper 2012/02*, London: Chatham House, May 2012.

Baamdadnews.blogspot.com, Arabic website, undated. As of May 14, 2012: <http://baamdadnews.blogspot.com/>

Bakshy, Eytan, "Rethinking Information Diversity in Networks," Facebook web page, January 17, 2012. As of May 4, 2012:

<http://www.facebook.com/notes/facebook-data-team/rethinking-information-diversity-in-networks/10150503499618859>

Bamman, David, Brendan O'Connor, and Noah A. Smith, "Censorship and Deletion Practices in Chinese Social Media," *First Monday*, Vol. 17, No. 3, March 5, 2012.

Bandurski, David, "Dalian Protests Erased from Social Media," blog post at China Media Project, August 14, 2011. As of October 1, 2012:

<http://cmp.hku.hk/2011/08/14/14785/>

Barkawi, Tarak, "The Globalisation of Revolution," *al-Jazeera*, March 21, 2011.

Barrett, Edward W., *Truth Is Our Weapon*, New York: Funk and Wagnalls, 1953.

Barry, Ellen, and Andrew E. Kramer, "In Biting Cold, Protesters Pack the Center of Moscow," *New York Times*, February 4, 2012. As of June 24, 2012.

[http://www.nytimes.com/2011/12/11/world/europe/thousands-protest-in-moscow-russia-in-defiance-of-putin.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2011/12/11/world/europe/thousands-protest-in-moscow-russia-in-defiance-of-putin.html?pagewanted=all&_r=0)

Bashkirova, Elena, "Soviet Union," Session Three: Impact of the Broadcasts: Jamming and Audiences in the *Report on the Impact of Cold War Broadcasting*, a conference organized by the Hoover Institution and the Cold War International History Project of the Woodrow Wilson International Center for Scholars at Stanford University, October 13–16, 2004.

Benford, Robert D., and David A. Snow, "Framing Process and Social Movements: An Overview and Assessment," *Annual Review of Sociology*, Vol. 26, August 2000.

Bennahum, David S., "The Internet Revolution," *Wired*, Vol. 5, No. 4, April 1997. As of May 9, 2012.

[http://www.wired.com/wired/archive/5.04/ff\\_belgrad.html](http://www.wired.com/wired/archive/5.04/ff_belgrad.html)

Bennetts, Marc, "Russian Bloggers Fear Crackdown," *RIA News*, February 4, 2012. As of October 4, 2012:

<http://en.rian.ru/analysis/20120321/172308792.html>

Best, Michael L., and Keegan W. Wade, "The Internet and Democracy: Global Catalyst or Democratic Dud?" *Bulletin of Science, Technology and Society*, Vol. 29, No. 4, September 30, 2005. As of January 11, 2012:

<http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/12-InternetDemocracy.pdf>

Birke, Sarah, "After the Revolution, Older Egyptians Take the Leap Into Facebook," *National*, March 7, 2011.

Bohlen, Charles E., Edmund A. Gullion, and Col. Joseph Coffey, Special Assistant to the Secretary, memorandum of conversation, Department of State, March 30, 1960.

Bolshoi Gorod, Russian website, undated. As of March 20, 2012:

<http://bg.ru/>

Boulianne, Shelley, "Does Internet Use Affect Engagement? A Meta-Analysis of Research," *Political Communication*, Vol. 26, No. 2, May 2009.

Bovingdon, Gardner, *The Uyghurs: Strangers in Their Own Land*, New York: Columbia University Press, 2010.

Brady, Henry E., Kay Lehman Schlozman, and Sidney Verba, "Prospects for Participants: Rational Expectations and the Recruitment of Political Activists," *American Political Science Review*, Vol. 93, No. 1, March 1999.

Branigan, Tania, "Chinese Anger over Alleged Cover-Up of High-Speed Rail Crash," *Guardian*, July 25, 2011. As of August 3, 2012:

<http://www.guardian.co.uk/world/2011/jul/25/chinese-rail-crash-cover-up-claims>

Bristow, Michael, "China's Internet 'Spin Doctors,'" BBC News website, December 16, 2008. As of August 13, 2012:  
<http://news.bbc.co.uk/2/hi/asia-pacific/7783640.stm>

———, "Can Microblogs Change China's Rulers?" BBC News website, August 7, 2011. As of August 9, 2012:  
<http://www.bbc.co.uk/news/world-asia-pacific-14422581>

"The Brutal Truth," *Economist*, June 23, 2012. As of March 4, 2012:  
<http://www.economist.com/node/21557369>

Buckley, Chris, "China Domestic Security Spending Rises to \$111 Billion," Reuters website, March 5, 2012. As of February 12, 2013:  
<http://www.reuters.com/article/2012/03/05/us-china-parliament-security-idUSTRE82403J20120305>

Buckley, Chris, and Ben Blanchard, "China High-Speed Crash Shows Leaders' Struggle to Keep Up," Reuters website, July 29, 2011. As of October 1, 2012:  
<http://www.reuters.com/article/2011/07/29/uk-china-train-idUSLNE76S04T20110729>

Buechler, Steven M., *Social Movements in Advanced Capitalism*, New York: Oxford University Press, 2000.

"Campaign for Jailed Uyghur Blogger," Reporters Without Borders website, July 16, 2009. As of February 24, 2013:  
<http://en.rsf.org/china-campaign-for-jailed-uyghur-blogger-16-07-2009,33859>

Carothers, Thomas, "The End of the Transition Paradigm," *Journal of Democracy*, Vol. 13, No. 1, 2002.

Chase, Michael, and James Mulvenon, *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies*, Santa Monica, Calif.: RAND Corporation, MR-1543, 2002. As of May 8, 2013:  
[http://www.rand.org/pubs/monograph\\_reports/MR1543.html](http://www.rand.org/pubs/monograph_reports/MR1543.html)

"Chemical Plant Protest Highlights China's Class Divide," *Guardian*, August 18, 2011. As of October 1, 2012:  
<http://www.guardian.co.uk/environment/blog/2011/aug/18/chemical-plant-protest-china-middle-class>

Chen, Yu-Wen, *Who Made Uyghurs Visible in the International Arena: Hyperlink Analysis*, Global Migration and Transnational Politics, Working Paper No. 12, June 2010. As of July 6, 2011:  
[http://cgs.gmu.edu/publications/gmtpwp/gmtp\\_wp\\_12.pdf](http://cgs.gmu.edu/publications/gmtpwp/gmtp_wp_12.pdf)

"China Clamps Down on Microblogs," Radio Free Asia website, December 22, 2011. As of October 1, 2012:  
<http://www.rfa.org/english/news/china/web-12222011143535.html>

“China Closes Chemical Plant Targeted by Protesters,” *USA Today*, August 15, 2011. As of October 1, 2011:

[http://usatoday30.usatoday.com/money/world/2011-08-15-china-shuts-down-chemical-plant\\_n.htm](http://usatoday30.usatoday.com/money/world/2011-08-15-china-shuts-down-chemical-plant_n.htm)

China Internet Information Center, *Yunnan: Illuminating China's Provinces*, web page, undated. As of October 1, 2012:

<http://www.china.org.cn/english/features/43609.htm>

“China Protest in Guangdong’s Wukan ‘Vanishes from Web,’” BBC News website, December 15, 2011. As of February 22, 2013:

<http://www.bbc.co.uk/news/world-asia-china-16192541>

“China Riots: Uighurs Stage Fresh Protest in Urumqi,” *Telegraph*, undated. As of February 10, 2013:

<http://www.telegraph.co.uk/news/picturegalleries/worldnews/5767926/China-riots-Uighurs-stage-fresh-protest-in-Urumqi.html?image=2>

“China’s Web Users Debate Internet Freedom,” BBC News website, January 22, 2010. As of August 1, 2012:

<http://news.bbc.co.uk/2/hi/asia-pacific/8475519.stm>

“Chinese Newspapers Defy Ban to Report on Train Tragedy,” *Guardian*, August 2, 2011.

“Chislo Novykh Pol’zovateley vKontakte Posle Otmeny Registrtsii Socratilos’ Pochti v Dvoye” [“Number of New vkontakte Members Drops by Nearly Half After Abolition of Open Enrollment”], Korrespondent.net, February 17, 2012. As of August 14, 2011:

<http://korrespondent.net/business/web/1187281-chislo-novykh-polzovatelej-vkontakte-posle-otmeny-otkrytoj-registracii-sokratilos-pochti-vdvoe>

Chong, Dennis, and James N. Druckman, “Framing Theory,” *Annual Review of Political Science*, Vol. 10, June 2007.

CIA—See U.S. Central Intelligence Agency.

*Civil Resistance 2.0*, Google document, undated. As of February 22, 2012:

<https://docs.google.com/spreadsheets/ccc?key=0AjKkO3odnjoedG5SckUtU1AtYnFVdm40T21nRDJGS2c#gid=2>

Clinton, Hillary Rodham, Secretary of State, “Remarks on Internet Freedom,” speech at Newseum, Washington, D.C., January 21, 2010. As of December 4, 2011:

<http://www.state.gov/secretary/rm/2010/01/135519.htm>

———, “Internet Rights and Wrongs: Choices and Challenges in a Networked World,” speech at George Washington University, Washington, D.C., February 15, 2011. As of March 7, 2012:

<http://www.state.gov/secretary/rm/2011/02/156619.htm>

———, remarks with European Union High Representative for Foreign Affairs and Security Policy Catherine Ashton, Washington, D.C., July 11, 2011. As of December 12, 2012:

<http://iipdigital.usembassy.gov/st/english/texttrans/2011/07/20110712102113su0.7593457.html#axzz277UJ7CWU>

“Collection Protocols: Elections to the State Duma,” *komiunity.ru* website, December 4, 2011. As of July 12, 2012:

<http://komiunity.ru/sutvremeni/sbor-protokolov-vybory-v-gd-04-12-2011>

Committee to Protect Journalists, *2011 Prison Census: 179 Journalists Jailed Worldwide*, web page, December 1, 2011. As of August 3, 2012:

<http://www.cpj.org/imprisoned/2011.php>

Consulate General of the United States, *Overview of Liaoning Province*, web page, undated. As of March 30, 2012:

<http://shenyang.usembassy-china.org.cn/ln.html>

Conway, Evan, “How Wired are Egyptians?” *PBS Newshour*, January 31, 2011.

Cook, Steven, “Political Instability in Egypt,” contingency planning memorandum No. 4, Center for Preventative Action, Council on Foreign Relations, August 2009.

Critchlow, James, *Radio-Hole-in-the-Head: Radio Liberty: An Insider’s Story of Cold War Broadcasting*, Washington D.C.: American University Press, 1995.

Curry, Jane, “Poland” from Session Four: Impact of the Broadcasts in Eastern Europe: Evidence from Archives, in the *Report on the Impact of Cold War Broadcasting*, a conference organized by the Hoover Institution and the Cold War International History Project of the Woodrow Wilson International Center for Scholars at Stanford University, October 13–16, 2004.

CyberSecurity.ru, “RuNet Organizes Mass Protests in Moscow and Other Places,” (Russian web page), December 8, 2011. As of November 1, 2011:

[http://www.cybersecurity.ru/news/139444.html?seccode=news&ID=139444&clast=;](http://www.cybersecurity.ru/news/139444.html?seccode=news&ID=139444&clast=)

Czernich, Nina, “Broadband Internet and Political Participation: Evidence for Germany,” *Kuklos*, Vol. 65, No. 1, February 2012.

Davis, Richard, and Diana Owen, *New Media and American Politics*, Oxford, England: Oxford University Press, 1998.

De Carbonnel, Alissa, “Insight: Social Media Makes Anti-Putin Protests ‘Snowball,’” Reuters website, December 7, 2011. As of November 4, 2012:

<http://www.reuters.com/article/2011/12/07/us-russia-protests-socialmedia-idUSTRE7B60R720111207>

“Defiant al-Jazeera Asks Egyptian Audience for Help,” *CBS News*, January 31, 2011.

Deibert, Ronald, and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in Ronald Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, Mass.: MIT Press, 2010.

Della Porta, Donatella, "Recruitment Process in Clandestine Political Organizations: Italian Left-Wing Terrorism," in Bert Klandermans, ed., *International Social Movement Research*, Vol. 1, Greenwich, Conn.: JAI Press, 1999.

Demm, Jens, "The Internet and the Fragmentation of Chinese Society," *Critical Asian Studies*, Vol. 39, No. 2, 2007, pp. 273–294.

Devereaux, Ryan, "Syrian Government Blocks Live Video Streaming Site Bambuser," *Guardian*, February 17, 2012.

Diamond, Larry, "Democracy's Third Wave Today," *Current History*, Vol. 110, No. 739, November 2011.

———, "Liberation Technology," *Journal of Democracy*, Vol. 21, No. 3, July 2010, pp. 69–83.

———, "Thinking About Hybrid Regimes," *Journal of Democracy*, Vol. 13, No. 2, 2002.

"Digital Weapons Help Dissidents Punch Holes in China's Great Firewall," *Wired*, November 2010. As of October 1, 2012:

[http://www.wired.com/magazine/2010/11/ff\\_firewallfighters/](http://www.wired.com/magazine/2010/11/ff_firewallfighters/)

Dignan, Larry, "Georgia Turns to Google's Blogger to Counter Alleged Cyberattack," Seeking Alpha website, August 11, 2008. As of January 12, 2012:

<http://seekingalpha.com/>

[article/90392-georgia-turns-to-google-s-blogger-to-counter-alleged-cyber-attack](http://seekingalpha.com/article/90392-georgia-turns-to-google-s-blogger-to-counter-alleged-cyber-attack)

Dobriansky, Paula, Under Secretary of State for Democracy and Global Affairs, "Global Internet Freedom Task Force," presentation, Washington, D.C., December 20, 2006. As of February 3, 2012:

<http://2001-2009.state.gov/g/rls/rm/78142.htm>

Doran, Michael, and Salman Shaikh, "The Syrian Crucible," *American Interest*, January/February 2012.

"Dubious Vote in Russia," InoPressa, Russian website, December 28, 2011. As of August 7, 2012:

<http://www.inopressa.ru/article/28Dec2011/wsj/russia1.html>

Dulles, John Foster, "A Policy of Boldness," *Life*, Vol. 33, May 19, 1952.

Duma R. F., *Federal'niy Zakon [Federal Law] 139-F3*, June 30, 2012. As of June 28, 2013:

<http://www.rg.ru/2012/07/30/zakon-dok.html>

Dzhanpoladova, Nataliya, "Sotsial'nye Seti v Bor'be za Chestnyye Vybory," Radio Liberty website, December 8, 2011. As of March 4, 2012:

<http://www.svoboda.org/articleprintview/24415132.html>



East-West-Connect.com, *Rural Internet Usage in China*, web page, October 28, 2011. As of March 4, 2012:

[http://www.east-west-connect.com/rural-chinese-internet-usage-2011\\_10\\_27](http://www.east-west-connect.com/rural-chinese-internet-usage-2011_10_27)

———, *Chinese Mobile Internet User Demographics 2012*, web page, February 20, 2012. As of May 13, 2012:

<http://www.east-west-connect.com/china-mobile/chinese-mobile-internet-user-demographics-2012>

———, *Chinese Internet User Age Distribution*, web page, undated. As of May 12, 2012:

<http://www.east-west-connect.com/china-mobile/chinese-mobile-internet-user-demographics-2012>

———, *Education Levels of Chinese Internet Users*, web page, undated. As of May 12, 2012:

<http://www.east-west-connect.com/china-mobile/chinese-mobile-internet-user-demographics-2012>

Echo of Moscow, Russian website, undated. As of January 23, 2012:

<http://www.echo.msk.ru/>

Economist Intelligence Unit, *Democracy Index 2011: Democracy Under Stress*, London, December 16, 2011. As of March 4, 2012:

[http://www.sida.se/Global/About%20Sida/Sa%20arbetar%20vi/EIU\\_Democracy\\_Index\\_Dec2011.pdf](http://www.sida.se/Global/About%20Sida/Sa%20arbetar%20vi/EIU_Democracy_Index_Dec2011.pdf)

“Egypt: Seeds of Change,” *al-Jazeera*, February 9, 2011.

“Egypt News: Revolution and Aftermath,” *New York Times*, July 19, 2012.

Eisenhower, Dwight D., personal letter to Charles Douglas Jackson, May 8, 1952.

———, Princeton meeting with Charles Douglas Jackson and others, transcript, May 10–11, 1952.

Elder, Miriam, “Russians Protest Against Vladimir Putin by Forming Human Chain in Moscow,” *Guardian*, February, 26, 2012. As of June 4, 2012:

<http://www.guardian.co.uk/world/2012/feb/26/russians-protest-putin-moscow>

“Electoral Statistics,” Golos, Russian web page, undated. As of March 2012:

<http://stat.golos.org/>

Eltahawy, Mona, *Frontline* interview, February 22, 2011.

Emrooznews.blogspot.com, Arabic website, undated. As of July 14, 2012:

<http://emrooznews.blogspot.com>

Entman, Robert M., *Projections of Power: Framing News, Public Opinion, and U.S. Foreign Policy*, Chicago: University of Chicago Press, 2004.

Entous, Adam, and Matthew Rosenberg, “U.S. Says Iran Helps Crackdown in Syria,” *Wall Street Journal*, April 14, 2011.

Etling, Bruce, et al., *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization*, Cambridge Mass.: Harvard University's Berkman Center for the Study of Internet and Society, October 2010. As of June 23, 2012:

[http://cyber.law.harvard.edu/publications/2010/Public\\_Discourse\\_Russian\\_Blogosphere/](http://cyber.law.harvard.edu/publications/2010/Public_Discourse_Russian_Blogosphere/)

"Exit Poll: V Den' Vyborov v Gosdumy RF," FOM website, December 4, 2011. As of June 15, 2012:

<http://fom.ru/partii/10270>

Facebook.com, *Saturday at Bolotnaya Square* (in Russian), undated. As of August 24, 2012:

<https://www.facebook.com/events/198328520252594>

———, *Meeting on Dec. 24* (in Russian), undated. As of October 2, 2012:

<http://www.facebook.com/events/231653370237319>

———, *A Peaceful March for Fair Elections, February 4* (in Russian), undated. As of March 3, 2012:

<https://www.facebook.com/events/212286018856867/>

Fahim, Karim, "Violent Clashes Mark Protests Against Mubarak," *New York Times*, January 25, 2011.

Fallows, James, "The Connection Has Been Reset," *The Atlantic*, March 2008. As of October 1, 2012:

<http://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/>

Faris, David M., and Patrick Meier, "Digital Activism in Authoritarian Countries," in Aaron Delwiche and Jennifer Jacobs Henderson, eds. *The Participatory Cultures Handbook*, Oxford, England: Routledge: Taylor and Francis, Inc., 2012.

Faris, Robert, and Bruce Etling, "Madison and the Smart Mob: The Promise and Limitations of the Internet for Democracy," *Fletcher Forum of World Affairs*, Vol. 32, No. 2, 2008.

Farrell, Henry, "The Consequences of the Internet for Politics," *Annual Review of Political Science*, Vol. 15, June 2012.

Farrell, Henry, and Daniel W. Drezner, "The Power and Politics of Blogs," *Public Choice*, Vol. 134, Nos. 1–2, 2008.

Fathi, Yasmine, "Egypt's 'Battle of the Camel': The Day the Tide Turned," *Ahramonline*, February 2, 2012.

Federal'noye Agenstvo po Pechati i Massovym Kommunikatsiyam (Federal Agency for Press and Mass Communications), *Internet v Rossii: Sostoyaniye, Perspektivy, iTendentsii Rasvitiya [Internet in Russia: Status, Prospects, and Trends of Development]*, 2011. As of July 22, 2012:

<http://www.fapmc.ru/magnoliaPublic/rospechat/activities/reports/2011/item6.html>

Ferguson, John, "Eastern Europe: 1949–1953," memorandum to David Bruce, July 1, 1952.

Fisher, Max, and Jared Keller, "Syria's Digital Counter-Revolutionaries," *The Atlantic*, August 31, 2011.

Ford, Peter, "China Sentences Quake Activist Tan Zuoren," *Christian Science Monitor*, February 9, 2010. As of October 1, 2012:  
<http://www.csmonitor.com/World/Asia-Pacific/2010/0209/China-sentences-quake-activist-Tan-Zuoren>

Fossato, Floriana, and John Lloyd with Alexander Verkhovsky, *The Web that Failed: How Opposition Politics and Independent Initiatives are Failing on the Internet in Russia*, Oxford: Oxford University Press, Reuters Institute for the Study of Journalism, 2008.

Foster, Peter, "Beijing Fears Nimbyism of Angry Middle Classes," *Telegraph*, August 19, 2011. As of October 1, 2012:  
<http://blogs.telegraph.co.uk/news/peterfoster/100101546/beijing-fears-nimbyism-of-angry-middle-classes/>

Freedom House, "Egypt: Freedom in the World 2010," undated.

———, *Freedom in the World 2012: The Arab Uprisings and Their Global Repercussions*, Washington, D.C., undated. As of January 19, 2012:  
<http://www.freedomhouse.org/report/freedom-world/freedom-world-2012>

———, *Freedom in the World: China*, web page, 2011a. As of July 2, 2013:  
<http://www.freedomhouse.org/report/freedom-world/2011/china>

———, *Freedom in the World: Syria*, web page, 2011b. As of July 3, 2013:  
<http://www.freedomhouse.org/report/freedom-world/2011/syria>

———, *Safety on the Line: Exposing the Myth of Mobile Communication Security*, Washington, D.C., July 2012a. As of August 13, 2012:  
<http://www.freedomhouse.org/report/special-reports/safety-line-exposing-myth-mobile-communication-security>

———, *Freedom on the Net 2012*, September 4, 2012b. As of July 3, 2013:  
<http://www.freedomhouse.org/report/freedom-net/freedom-net-2012>

Friedman, Thomas, commencement speech delivered at Tulane University, New Orleans, May 12, 2011.

Friedrich, Carl J., and Zbigniew K. Brzezinski, *Totalitarian Dictatorship and Autocracy*, Cambridge, Mass.: Harvard University Press, 1956.

Froomkin, A. Michael, "Habermas@Discourse.Net: Toward a Critical Theory of Cyberspace," *Harvard Law Review*, Vol. 116, No. 3, January 2003. As of July 12, 2012:  
<http://www.law.miami.edu/~froomkin/discourse/ils.pdf>

Fung, Brian, "Netizen: Why Is This Goofy-Sounding Word So Important in China?" *The Atlantic*, October 11, 2012. As of January 10, 2013: <http://www.theatlantic.com/international/archive/2012/10/netizen-why-is-this-goofy-sounding-word-so-important-in-china/263245/>

Galperin, Eva, and Morgan Marquis-Boire, "Campaign Targeting Syrian Activists Escalates with New Surveillance Malware," Electronic Frontier Foundation web page, April 4, 2012a. As of August 22, 2012: <https://www.eff.org/deeplinks/2012/04/campaign-targeting-syrian-activists-escalates-with-new-surveillance-malware>

———, "Fake Skype Encryption Tool Targeted at Syrian Activists Promises Security, Delivers Spyware," Electronic Frontier Foundation web page, May 2, 2012b. As of August 22, 2012: <https://www.eff.org/deeplinks/2012/05/fake-skype-encryption-tool-targeted-syrian-activists-promises-security-delivers>

———, "New Trojan Spread Over Skype as Cat and Mouse Game Between Syrian Activists and Pro-Syrian-Government Hackers Continues," Electronic Frontier Foundation web page, June 19, 2012c. As of August 22, 2012: <https://www.eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware>

———, "New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan," Electronic Frontier Foundation web page, July 12, 2012d. As of August 22, 2012: <https://www.eff.org/deeplinks/2012/07/new-blackshades-malware>

Galston, William A., "Political Knowledge, Political Engagement, and Civic Education," *Annual Review of Political Science*, Vol. 4, 2001.

Garbonevskiy, Yaroslav, "Anton Nosik Comments on the Internet Law: Lawmakers Deserve 'D' for this Law" (in Russian), *Times Online*, July 12, 2012. As of January 22, 2013: <http://inosmi.ru/politic/20120712/194836392.html>

Garrett, R. Kelly, "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs," *Information, Communication and Society*, Vol. 9, No. 2, April 2006.

Geddes, Barbara, and John Zaller, "Sources of Popular Support for Authoritarian Regimes," *American Journal of Political Science*, Vol. 33, No. 2, May 1989.

Gentzkow, Matthew, and Jesse M. Shapiro, *Ideological Segregation Online and Offline*, Cambridge, Mass.: National Bureau of Economic Research, NBER Working Paper No. 15916, 2010.

Gerber, Alan S., Donald P. Green, and Christopher W. Larimer, "Social Pressure and Voter Turnout: Evidence from a Large-Scale Field Experiment," *American Political Science Review*, Vol. 102, February 2008.

Ghannam, Jeffrey, *Special Media in the Arab World: Leading Up to the Uprisings of 2011*, Washington, D.C.: Center for International Media Assistance, February 3, 2011.

———, “Digital Media in the Arab World One Year After the Revolution,” *Center for International Media Assistance*, March 28, 2012. As of April 11, 2012:  
<http://cima.ned.org/publications/digital-media-arab-world-one-year-after-revolutions>

Ghitis, Frida, *World Citizen: Facebook, Twitter and the Protests of 2011*, World Politics Review website, December 15, 2011. As of August 10, 2012:  
<http://www.worldpoliticsreview.com/articles/10946/world-citizen-facebook-twitter-and-the-protests-of-2011>

Ghonim, Wael, *Revolution 2.0*, Boston, Mass.: Houghton Mifflin Harcourt, 2012.

Goldstein, Josh, *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution*, Berkman Center for the Study of Internet and Society, No. 2007-14, December 2007. As of March 4, 2012:  
[http://cyber.law.harvard.edu/publications/2007/The\\_Role\\_of\\_Digital\\_Networked\\_Technologies\\_in\\_the\\_Ukrainian\\_Orange\\_Revolution](http://cyber.law.harvard.edu/publications/2007/The_Role_of_Digital_Networked_Technologies_in_the_Ukrainian_Orange_Revolution)

Golkar, Saeld, “Liberation or Suppression Technology? The Internet, the Green Movement, and the Regime in Iran,” *International Journal of Emerging Technologies and Society*, Vol. 9, No. 1, 2011.

Golos, Russian website, undated. As of January 14, 2012:  
<http://www.golos.org/>

“Golos-Povolzhye Vozobnovlyayet Rabotu” [“Golos-Volga Resumes Work”], Golos, May 14, 2008 (file no longer available). As of March 15, 2012:  
<http://golos.org/news/1904>

Goskomstat, *Regiony Rossii* web page, Moscow, 2012. As of May 20, 2013:  
[http://www.gks.ru/bgd/regl/b12\\_14p/Main.htm](http://www.gks.ru/bgd/regl/b12_14p/Main.htm)

Goodin, Dan, “New DoS Tool Lets a Single PC Bring Down an Apache Server,” *ars technica* website, June 8, 2012. As of August 11, 2012:  
<http://arstechnica.com/security/2012/06/apache-killer-dos-tool/>

Google Trends, Frequency of Google Search Queries for Key Word “Khaled Said” in Egypt, undated.

———, Frequency of Searches for “Falsifications”, 2011, undated.

———, Frequency of Searches for “Facebook” and “vKontakte”, 2011, undated. As of June 28, 2013:

<http://www.google.com/trends/explore#q=vkontakte%2C%20Facebook&geo=RU&date=1%2F2011%2013m&ccmpt=q>

- Gorny, Eugene, "Understanding the Real Impact of Russian Blogs," *Russian Analytical Digest*, Vol. 69, December 2009. As of August 16, 2012:  
<http://www.css.ethz.ch/publications/pdfs/RAD-69.pdf>
- GosZakupki, Russian website, undated. As of February 4, 2012:  
<http://www.etp-micex.ru/>
- Grakon.org homepage, undated. As of March 14, 2012:  
<http://grakon.org>
- Greenberg, Andy, "Mubarak's Digital Dilemma: Why Egypt's Internet Controls Failed," *Forbes*, February 2, 2011.
- Groshek, Jacob, "The Democratic Effects of the Internet, 1994–2003," *International Communication Gazette*, Vol. 71, No. 3, April 2009.
- Grossman, Lawrence K., *Electronic Republic: Reshaping American Democracy for the Information Age*, New York: Penguin Books USA Inc., 1995.
- Guo, Yuhua, and Peng Chen, "Digital Divide and Social Cleavages: Case Studies of ICT Usage Among Peasants in Contemporary China," *China Quarterly*, Vol. 207, September 2011.
- Hale, Henry, "Correlates of Clientelism: Political Economy, Politicized Ethnicity, and Post-Communist Transition," in Herbert Kitschelt and Steven I. Wilkinson, eds., *Patrons, Clients, and Policies: Patterns of Democratic Accountability and Political Competition*, New York: Cambridge University Press, 2006.
- Handoussa, Heba, Ashraf el Araby, Hoda el Nemr, Zeinat Tobala, Ghada Barsoum, Mohamed Ramadan, Safaa el Kogali, et al., *Egypt Human Development Report 2010, Youth in Egypt: Building Our Future*, United Nations Development Program and the Institute of National Planning, 2010.
- Hanemann, W. Michael, "Willingness to Pay and Willingness to Accept: How Much Can They Differ?" *The American Economic Review*, Vol. 81, No. 3, June 1991.
- Hanson, Fergus, "Internet Freedom: The Role of the U.S. State Department," in *Baked in and Wired: eDiplomacy @ State*, Brookings, October 25, 2012. As of February 22, 2013:  
<http://www.brookings.edu/research/reports/2012/10/25-ediplomacy-hanson-internet-freedom>
- Harding, Luke, "Syria's Video Activists Give Revolution the Upper Hand in Media War," *Guardian*, August 1, 2012. As of June 4, 2012:  
<http://www.guardian.co.uk/world/2012/aug/01/syria-video-activists-media-war>
- Harless, David W., "More Laboratory Evidence on the Disparity Between Willingness to Pay and Compensation Demanded," *Journal of Economic Behavior and Organization*, Vol. 11, 1989.

Hassanpour, Navid, "Media Disruption Exacerbates Revolutionary Unrest: Evidence from Mubarak's Natural Experiment," paper presented to the American Political Science Association Conference, August 7, 2011.

Hauben, Michael, Ronda Hauben, and Thomas Truscott, *Netizens: On the History and the Impact of Usenet and Internet*, Los Alamos, Calif.: IEEC Computer Society Press, 1997.

Herlandmag.net, blog, undated. As of July 25, 2012:  
<http://www.herlandmag.net>

Hewitt, Duncan, "Weibo Brings Change to China," BBC News website, July 31, 2012. As of August 14, 2012:  
<http://www.bbc.co.uk/news/magazine-18887804>

Hou, Shumei, and Ronald C. Keith, "A New Prospect for Transparent Court Judgment in China?" *China Information*, Vol. 26, No. 1, March 2012.

"Houla: How a Massacre Unfolded," BBC News website, June 8, 2012. As of August 16, 2012:  
<http://www.bbc.co.uk/news/world-middle-east-18233934>

Houslohner, Abigail, "Is Egypt About to Have a Facebook Revolution?" *Time*, January 24, 2011. As of August 20, 2012:  
<http://www.time.com/time/world/article/0,8599,2044142,00.html>

Howard, Philip, *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*, Oxford, England: Oxford University Press, 2010.

Howard, Philip N., and Muzammil M. Hussain, *Democracy's Fourth Wave? Digital Media and the Arab Spring*, Cambridge, Mass.: Cambridge University Press, 2013.

Huang, Xuanyu, "Re-Legalization or De-Legalization? Netizens' Participation in Criminal Justice Practices in China," *British Journal of Criminal Justice*, Vol. 52, 2012.

Hufbauer, Gary Clyde, et al., *Economic Sanctions Reconsidered: History and Current Policy*, Washington, D.C.: Institute for International Economics, 1991.

Hume, David, *A Treatise of Human Nature*, London, 1740. As of July 14, 2012:  
<http://www.gutenberg.org/files/4705/4705-h/4705-h.htm>

Huntington, Samuel, *The Third Wave: Democratization in the Late 20th Century*, Norman, Okla.: University of Oklahoma Press, 2011.

Ikso, Russian website, undated. No longer available. As of July 23, 2012:  
<http://www.ikso.ru/>

International Telecommunications Union, *Reports* web page, undated.

"Internet Enemies: Syria," Reporters Without Borders website, March 12, 2012. As of February 24, 2012:  
<http://en.rsf.org/syria-syria-12-03-2012,42053.html>

“Internet Filtering in Egypt,” *OpenNet Initiative*, August 6, 2009. As of June 5, 2012:

[http://opennet.net/sites/opennet.net/files/ONI\\_Egypt\\_2009.pdf](http://opennet.net/sites/opennet.net/files/ONI_Egypt_2009.pdf)

“Internet Filtering in Syria,” *OpenNet Initiative*, August 6, 2009. As of July 14, 2012:

[http://opennet.net/sites/opennet.net/files/ONI\\_Syria\\_2009.pdf](http://opennet.net/sites/opennet.net/files/ONI_Syria_2009.pdf)

“Internet Providers in Chechnya Instructed to Block YouTube over Anti-Islam Film,” RFE/RL website, September 28, 2012. As of October 9, 2012 (link no longer works):

<http://www.rferl.org/content/Internet-providers-in-chechnya-instructed-to-block-youtube-anti-islam-film/24718583.html>

Internet World Stats, *Usage and Population Statistics*, web page, 2012a. As of March 26, 2012:

<http://www.Internetworldstats.com/stats5.htm>

———, *Internet Users in Europe*, web page, June 30, 2012b. As of July 4, 2013:

<http://www.internetworldstats.com/stats4.htm>

———, *Internet Users in the Middle East and the World*, web page, June 30, 2012c. As of July 4, 2013:

<http://www.internetworldstats.com/stats5.htm#me>

Ishani, Maryam, “Foreign Policy: Scramble to Silence Cairo Protests,” *NPR*, January 28, 2011. As of August 20, 2012:

<http://www.npr.org/2011/01/28/133306415/>

foreign-policy-scramble-to-silence-cairo-protests

Ismail, Salwa, *Rethinking Islamist Politics*, New York: I.B. Tauris, 2006.

Issacharoff, Avi, “Mubarak Signals Egypt Succession by Taking Son to Washington,” *Haaretz*, August 31, 2010. As of April 4, 2012:

<http://www.haaretz.com/news/diplomacy-defense/>

mubarak-signals-egypt-succession-by-taking-son-to-washington-1.311264

Jacobs, Andrew, “China Imprisons 3 Men Who Maintained Uighur Web Sites,” *New York Times*, July 30, 2010. As of February 24, 2013:

<http://www.nytimes.com/2010/07/31/world/asia/31china.html>

———, “Chinese Student Takes Aim, Literally, at Internet Regulator,” *New York Times*, May 19, 2011. As of October 1, 2012:

[http://www.nytimes.com/2011/05/20/world/asia/20china.html?\\_r=0](http://www.nytimes.com/2011/05/20/world/asia/20china.html?_r=0)

Jeffbullas.com, *20 Stunning Social Media Statistics Plus Infographic*, web page, undated. As of November 22, 2011:

<http://www.jeffbullas.com/2011/09/02/20-stunning-social-media-statistics/>

Jensen, Jon, “Behind Egypt’s Revolution: Youth and the Internet,” *Global Post*, February 13, 2011.



Jiang, Hao, and John M. Carroll, "Social Capital, Social Network and Identity Bonds: A Reconceptualization," in *Proceedings of the Fourth International Conference on Communities and Technologies*, University Park, Pa.: Penn State University, 2009, pp. 51–60.

Jiang, Steven, "Chinese Netizens Outraged over Response to Fatal Bullet Train Crash," *CNN World*, July 25, 2012. As of October 1, 2012:  
[http://articles.cnn.com/2011-07-25/world/china.train.accident.outrage\\_1\\_bullet-train-wang-yongping-railway-ministry?\\_s=PM:WORLD](http://articles.cnn.com/2011-07-25/world/china.train.accident.outrage_1_bullet-train-wang-yongping-railway-ministry?_s=PM:WORLD)

Kahneman, Daniel, Jack L. Knetsch, and Richard H. Thaler, "Experimental Tests of the Endowment Effect and the Coase Theorem," *Journal of Political Economy*, Vol. 98, No. 60, 1990.

Kar-Murza, Vladimiar, "On the Introduction of Control of the Russian Internet" (in Russian), RFE/RL, July 11, 2012. As of January 4, 2013:  
<http://inosmi.ru/social/20120711/194779362.html>

"Karta Narusheniy Na Vyborakh 2011" ["The 2011 Election Violation Map"], kartanarusheniy.org website, undated. As of June 28, 2013:  
<http://www.kartanarusheniy.org/2011-12-04>

"Karta Narusheniy Popolnyayetsa Narusheniyamy" ["A Collection of Election Violations"], Golos, October 11, 2011 (file no longer available).  
 As of March 14, 2012:  
<http://golos.org/news/4010>

Kassab, Dana, and Edwin Lane, "The Digital Divide," *Syria Today*, June 2011. As of June 4, 2012:  
<http://www.syria-today.com/index.php/June-2011/815-focus/15215-the-digital-divide>

Kelly, John, et. al, *Mapping Russian Twitter*, Berkman Center for the Study of Internet and Society, Publication No. 2012–3, March 2012. As of June 22, 2012:  
[http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Mapping\\_Russian\\_Twitter\\_2012.pdf](http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Mapping_Russian_Twitter_2012.pdf)

Kelly, Sanja, and Sarah Cook, eds., *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*, Freedom House, 2011.

Kennan, George, "Russian Language Broadcasts: Their Purpose, Potentialities, and Policies," undated.

Kennedy, John, "China: Ethnically Diverse Forum Shut Down," *Global Voices Advocacy*, May 20, 2008.

King, Gary, Jennifer Pan, and Margaret Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review*, May 2013. As of September 25, 2012:  
<http://gking.harvard.edu/files/censored.pdf>

- Kireev, Alexander, *Politics, Elections and Beyond* blog, undated. As of July 1, 2012: <http://kireev.livejournal.com/tag/>
- Kissel, Trina K., "License to Blog: Internet Regulation in the People's Republic of China," *Indiana International and Comparative Law Review*, Vol. 17, 2007.
- Kennan, George, "Russian Language Broadcasts; Their Purpose, Potentialities, and Policies" undated. Charles Thayer Papers, Box 5, Folder Voice of America. Harry S. Truman Presidential Library.
- Kommersant, Russian website, undated. As of January 21, 2012: <http://www.kommersant.ru/>
- Kotlin, Russian website, undated. As of March 4, 2012: <http://www.kotlin.ru/>
- Kotlin Forum, Russian website, undated. As of April 14, 2012: <http://www.forum.kotlin.ru/>
- Kuran, Timur, "Now Out of Never: The Element of Surprise in the East European Revolution 1989," *World Politics*, Vol. 44, No. 1, 1991.
- Kuntz, Philipp, and Mark R. Thompson, "More than Just the Final Straw: Stolen Elections as Revolutionary Triggers," *Comparative Politics*, Vol. 41, No. 3, April 2009.
- LaFraniere, Sharon, and Michael Wines, "Protest over Chemical Plant Shows Growing Pressure on China from Citizens," *New York Times*, August 15, 2011. As of October 1, 2012: <http://www.nytimes.com/2011/08/16/world/asia/16dalian.html>
- Langohr, Vickie, "Too Much Civil Society, Too Little Politics?" in Marsha Pripstein Posusney and Michele Penner Angrist, eds., *Authoritarianism in the Middle East*, Boulder, Colo.: Lynne Rienner, 2005.
- "League of Voters Decided on the List of Speakers at the Rally on February 4," Kasparov.ru, Russian website, February 1, 2012. As of May 4, 2012: <http://www.kasparov.ru/material.php?id=4F291881D0417>
- Leberknight, Christopher S., Mung Chiang, Harold Vincent Poor, and Felix Wong, "A Taxonomy of Internet Censorship and Anti-Censorship," working paper, December 2010. As of August 21, 2012: <http://www.princeton.edu/~chiangm/anticensorship.pdf>
- Lei, Ya-Wen, "The Political Consequences of the Rise of the Internet: Political Beliefs and Practices of Chinese Netizens," *Political Communication*, Vol. 28, No. 3, 2011.
- Lessig, Lawrence, *Code, and Other Laws of Cyberspace*, New York: Basic Books, 1999.
- Levitsky, Steven, and Lucan A. Way, *Competitive Authoritarianism: Hybrid Regimes After the Cold War*, New York: Cambridge University Press, 2010.

Lilly, Edward P., *The Development of American Psychological Operations 1945–1951*, December 19, 1951.

Lim, Chaeyoon, “Social Networks and Political Participation: How Do Networks Matter,” *Social Forces*, Vol. 82, No. 2, December 2008. As of July 25, 2012: <http://sf.oxfordjournals.org/content/87/2/961.full.pdf>

———, “Mobilizing on the Margin: How Does Interpersonal Recruitment Affect Citizen Participation in Politics?” *Social Science Research*, Vol. 39, No. 2, March 2010.

Lim, Merlyna, “Clicks, Cabs, and Coffee Houses: Social Media and Oppositional Movements in Egypt, 2004–2011,” *Journal of Communication*, Vol. 62, 2012.

Linz, Juan, *Totalitarian and Authoritarian Regimes*, Boulder, Colo.: Lynne Rienner, 2000.

Lipset, Seymour Martin, “Some Social Requisites of Democracy: Economic Development and Political Legitimacy,” *American Political Science Review*, Vol. 53, No. 1, March 1959.

Liu, Fengshu, “‘Politically Indifferent’ Nationalists? Chinese Youth Negotiating Political Identity in the Internet Age,” *European Journal of Culture and Studies*, Vol. 15, No. 1, 2012.

Liu, Yangyue, “Crafting a Democratic Enclave on the Cyberspace: Case Studies of Malaysia, Indonesia, and Singapore,” *Journal of Current Southeast Asian Affairs*, Vol. 30, No. 4, 2011.

LiveJournal, blog platform, undated. As of January 4, 2012: <http://www.livejournal.ru/>

Local Coordination Committees, *About the LCCS*, undated. As of March 30, 2102: <http://www.lccsyria.org/about>

Locke, John, *Second Treatise of Government*, London, 1690. As of June 4, 2012: <http://www.constitution.org/jl/2ndtreat.htm>

Lucas, Scott, *Freedom’s War: The American Crusade Against the Soviet Union*, New York: New York University Press, 1999.

Lum, Thomas, *China, Internet Freedom, and U.S. Policy*, Washington, D.C.: Congressional Research Service, Report R42601, July 13, 2012.

Lynch, Marc, “Watching Egypt (But Not on al-Jazeera),” *Foreign Policy*, January 25, 2011.

MacKinnon, Rebecca, “Inside China’s Censorship Machine,” *National Post*, January 29, 2012. As of October 1, 2012: <http://fullcomment.nationalpost.com/2012/01/29/rebecca-mackinnon-inside-chinas-censorship-machine/>

- Map of Violations, Russian website, undated. As of March 23, 2012:  
<http://www.kartanarusheniy.org>
- “Mashhadiyāt Sūrīya” [“Vignettes from Syria”], *al Hayat*, March 26, 2012.
- Masoud, Tarek, “The Road to (and from) Liberation Square,” *Journal of Democracy*, Vol. 22, No. 3, July 2011.
- McAdam, Doug, *Political Process and the Development of Black Insurgency, 1930–1970*, Chicago: University of Chicago Press, 1982.
- McAdam, Doug, John D. McCarthy, and Mayer N. Zald, *Comparative Perspectives and Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings*, Cambridge, England: Cambridge University Press, 1996.
- McDonald, Mark, “Watch Your Language! (In China. They Really Do),” *New York Times*, March 13, 2012. As of October 1, 2012:  
<http://rendezvous.blogs.nytimes.com/2012/03/13/watch-your-language-and-in-china-they-do/>
- McKenna, Laura, and Antoinette Pole, “What Do Bloggers Do? An Average Day on an Average Political Blog,” *Public Choice*, Vol. 134, Nos. 1–2, January 2008.
- McPherson, Miller, Lynn Smith-Lovin, and James M. Cook, “Birds of a Feather: Homophily in Social Networks,” *Annual Review of Sociology*, Vol. 27, August 2001. As of August 3, 2012:  
<http://www.annualreviews.org/doi/pdf/10.1146/annurev.soc.27.1.415>
- Mebane, Walter R., Jr., and Kirill Kalinin, *Electoral Fraud in Russia: Vote Counts Analysis Using Second Digit Mean Tests*, paper presented at the Midwest Political Science Association Meeting, April 22–25, 2000. As of March 23, 2012:  
<http://www-personal.umich.edu/~wmebane/mw10B.pdf>
- Meier, Patrick, *Do “Liberation Technologies” Change the Balance of Power Between Repressive States and Civil Society?* Ph.D. thesis, Fletcher School of Law and Diplomacy, 2011. As of January 14, 2012:  
<http://irevolution.files.wordpress.com/2011/11/meier-dissertation-final.pdf>
- , “The Role of Ushahidi as a Liberation Technology in Egypt and Beyond,” in Larry Diamond and Marc Plattner, eds. *Liberation Technology: Social Media and the Struggle for Democracy*, Baltimore, Md.: Johns Hopkins University Press, 2012.
- Michael, Maggie, “Three Dead as Egyptian Protesters Clash with Police,” *Washington Times*, January 25, 2011.
- Mikhaylov, Oleg, “Protesty Oppositiiv v Rossii: Internet Kipit, TV Molchit” [“Opposition Protests in Russia: Internet Boils, TV Is Silent”], BBC News website, December 7, 2011. As of February 11, 2013:  
<http://www.bbc.co.uk/russian/russia/2011/12/>

Mislove, Alan, et al., "Measurement and Analysis of Online Social Networks," IMC 2007, San Diego, Calif., October 24–26, 2007. As of March 4, 2012: <http://conferences.sigcomm.org/imc/2007/papers/imc170.pdf>

Mitrovich, Gregory, *Undermining the Kremlin: America's Strategy to Subvert the Soviet Bloc 1947–1956*, Ithaca, N.Y.: Cornell University Press, 2000.

Mlot, Stephanie, "Millions Bypass Chinese Firewall to Use Facebook, Twitter," *PC Magazine*, September 28, 2012. As of September 28, 2012: <http://www.pcmag.com/article2/0,2817,2410334,00.asp>

"Moldova's 'Twitter Revolution,'" RFE press release, April 8, 2009. As of May 3, 2012: [http://www.rferl.org/content/Moldovas\\_Twitter\\_Revolution/1605005.html](http://www.rferl.org/content/Moldovas_Twitter_Revolution/1605005.html)

Morewedge, C., et al., "Bad Riddance or Good Rubbish? Ownership and Not Loss Aversion Causes the Endowment Effect," *Journal of Experimental Social Psychology*, Vol. 45, 2009.

Morozov, Evgeny, *The Dark Side of Internet Freedom: The Net Delusion*, New York: Perseus Books Group, 2011.

———, *Frontline* interview, February 22, 2011.

Mourtada, Racha, and Fadi Salem, "Civil Movements: The Impact of Facebook and Twitter," *Arab Social Media Report*, Dubai School of Government, Vol. 1, No. 2, 2011, p. 16.

Mourtada, Racha, Fadi Salem, May Al-Dabbagh, and Ghalia Gargani, "The Role of Social Media in Arab Women's Empowerment," *Arab Social Media Report*, Vol: 1, No: 3, Governance and Innovation Program, Dubai School of Government, November 2011. As of April 4, 2012: <http://www.arabsocialmediareport.com/UserManagement/PDF/ASMR%20Report%203.pdf>

Murphy, Carlyle, *Passion for Islam: Shaping the Modern Middle East, The Egyptian Experience*, New York: Scribner, 2002.

Murphy, Zoe, "China Struggles to Censor Train Crash Coverage," *BBC News*, July 28, 2011. As of October 1, 2012: <http://www.bbc.co.uk/news/world-asia-pacific-14321787>

"Muslim Brotherhood Withdraws from Egyptian Elections," *Telegraph*, December 10, 2010.

Myagkov, Mikhail, Peter C. Ordeshook, and Dimitri Shakin, *The Forensics of Election Fraud: Russia and Ukraine*, Cambridge, Mass.: Cambridge University Press, 2009.

“Na Goryachuyu Liniyu ‘Prozrachniye Vybery’ Prishlo 1166 Zhalob” [“‘Transparent Elections’ Hotline Received 1,166 Complaints”], *novayagazeta.ru* website, March 2, 2008. As of March 12, 2012:  
<http://golos.org/news/1792>

Nanabhay, Mohamed, and Roxane Farmanfarmaian, “From Spectacle to Spectacular: How Physical Space, Social Media and Mainstream Broadcast Amplified the Public Sphere in Egypt’s ‘Revolution,’” *Journal of North African Studies*, Vol. 16, No. 4, December 2011.

National Security Council, “Exploitation of Soviet and Eastern European Vulnerabilities,” NSC 5505/1, January 31, 1955.

Nelson, Michael, *War of the Black Heavens: The Battles of Western Broadcasting in the Cold War*, Syracuse, N.Y.: Syracuse University Press, 1997.

“Nenuzhniy Svidetel” [“Needless Witness”], *Golos*, April 2, 2011 (file no longer available). As of March 13, 2012:  
<http://golos.org/news/284>

“Nepравителstvenniy Doklad: ‘Nesvobodniy Internet’” [“Non-Governmental Report, ‘The Lack of Internet Freedom’”], *Novaya Gazeta*, January 28, 2012. As of November 23, 2012:  
<http://www.novayagazeta.ru/politics/50694.html>

New Times, Russian website, undated. As of May 23, 2012:  
<http://newtimes.ru/>

Newman, Nic, “The Rise of Social Media and Its Impact on Mainstream Journalism: A Study of How Newspapers and Broadcasters in the UK and U.S. Are Responding to a Wave of Participatory Social Media, and a Historic Shift in Control Towards Individual Consumers,” Reuters Institute for the Study of Journalism Working Paper, September 2009. As of June 3, 2013:  
[https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/The\\_rise\\_of\\_social\\_media\\_and\\_its\\_impact\\_on\\_mainstream\\_journalism.pdf](https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/The_rise_of_social_media_and_its_impact_on_mainstream_journalism.pdf)

Nie, Norman H., Darwin W. Miller III, Saar Golde, Daniel M. Butler, and Kenneth Winneg, “The World Wide Web and the U.S. Political News Market,” *American Journal of Political Science*, Vol. 54, No. 2, April 2010.

Nir, Lilach, and James N. Druckman, “Campaign Mixed-Message Flows and Timing of Vote Decision,” *International Journal of Public Opinion Research*, Vol. 20, No. 3, August 2008.

Nisbet, Erik C., et al., “Internet Use and Democratic Demands: A Multinational, Multilevel Model of Internet Use and Citizen Attitudes About Democracy,” *Journal of Communication*, Vol. 62, April 2012.

Novaya Gazeta, Russian website, undated. As of July 22, 2012:  
<http://www.novayagazeta.spb.ru/>

Olson, Mancur, *The Logic of Collective Action*, Cambridge, Mass.: Harvard University Press, 1965.

Open Net Initiative, *Syria*, web page, August 7, 2009. As of July 2012:  
<https://opennet.net/research/profiles/syria>

“Organizatsiya Golos Otkryla Sayt so Statistikoym po Vyboram Organizatsiya Golos Otkryla Sayt so Statistikoym po Vyboram” [“Golos to Open Election Statistics Website”], *Golos*, May 11, 2011 (file no longer available). As of March 12, 2012:  
<http://golos.org/news/188>

“Organized Political Warfare,” Policy Planning Staff memorandum to National Security Council, May 4, 1948.

Ostrow, Adam, “What the Egyptian Revolution Taught al-Jazeera About Digital,” *Mashable Social Media*, March 5, 2011.

The Other Tver, Russian website, undated. As of March 21, 2012:  
<http://www.theothertver.com/>

Owen, Diana, “The Internet and Youth Civic Engagement in the United States,” in Sarah Oates, Diana Owen, and Rachel Kay Gibson, eds., *The Internet and Politics: Citizens, Voters and Activists*, New York: Routledge, 2006.

Pariser, Eli, *The Filter Bubble: What Is the Internet Hiding from You?* New York: Penguin Press, 2011.

Parks, J.D., *Culture, Conflict, and Coexistence: American Soviet Cultural Relations 1917–1958*, Jefferson, N.C.: McFarland, 1983.

Parry, Dave, “It’s Not the Public Internet, It Is the Internet Public,” *Profound Heterogeneity* website, February 4, 2011. As of March 4, 2012:  
<http://profoundheterogeneity.com/2011/02/its-not-the-public-internet-it-is-the-internet-public/>

Parta, R. Eugene, *Discovering the Hidden Listener: An Empirical Assessment of Radio Liberty and Western Broadcasting to the USSR During the Cold War*, Stanford, Calif.: Hoover Institute Press, 2007.

patdollard.com, *Head of Russian Political Watchdog Group Arrested Ahead of Elections*, web page, December 3, 2011. Link no longer active. As of June 4, 2012:  
<http://patdollard.com/2011/12/head-of-russian-political-watchdog-group-arrested-ahead-of-elections/>

Peeters, Marga, *Demographic Pressure, Excess Labour Supply and Public-Private Sector Employment in Egypt: Modeling Labour Supply to Analyze the Response of Unemployment, Public Finances and Welfare*, MPRA Paper No. 31101, 2011, p. 7.

Pertsev, Andrey, "Social Media Brings People on the Streets," Itar-Tass, Russian website, July 12, 2011. As of March 12, 2012:

<http://www.firstnews.ru/news.policy/sotsialnye-seti-zovut-na-ulitsy/index.php?print=y>

Petersen, Kristian, "Usurping the Nation: Cyber-Leadership in the Uighur Nationalist Movement," *Journal of Muslim Minority Affairs*, Vol. 26, No. 1, April 2006.

Pilling, David, "China Crashes into a Middle Class Revolt," *Financial Times*, August 3, 2011. As of October 1, 2012:

<http://www.csmonitor.com/World/Asia-Pacific/2010/0209/China-sentences-quake-activist-Tan-Zuoren>

Pittaway, Mark, "The Education of Dissent: The Reception of the Voice of Free Hungary, 1951–1956," *Cold War History*, Vol. 4, No. 1, October 2003.

Polat, Rabia Karakaya, "The Internet and Political Participation: Exploring the Explanatory Links," *European Journal of Communication*, Vol. 20, December 2005.

Pollock, John, "Streetbook: How Egyptian and Tunisia Youth Hacked the Arab Spring," *MIT Technology Review*, August 23, 2011.

"POMED Notes: Economics, Youth, and Technology in the 'Arab Spring,'" *Project on Middle East Democracy*, March 23, 2012.

Posner, Michael H., Assistant Secretary, Bureau of Democracy, Human Rights, and Labor, and Jeffrey D. Feltman, Assistant Secretary, Bureau of Near Eastern Affairs, "U.S. Human Rights Policy Toward Iran and Syria," testimony before the House Foreign Affairs Subcommittee on the Middle East and South Asia, July 27, 2011. As of June 11, 2012:

<http://www.state.gov/j/drl/rls/rm/2011/169180.htm>

"Pravozashchitniki Obespokoyeny Sud'boy Samarskogo Golosa" ["Human Rights Activists Concerned About Fate of Samara Voices"], *Golos*, June 23, 2008 (file no longer available). As of March 15, 2012:

<http://golos.org/news/1982>

Preston, Jennifer, "Seeking to Disrupt Protesters, Syria Cracks Down on Social Media," *New York Times*, May 22, 2011.

"Prosecutors Accuse the 'Voice' of Violating Election Law," BBC Russian website, December 1, 2011. As of March 10, 2012:

[http://www.bbc.co.uk/russian/russia/2011/12/111201\\_golos\\_human\\_rights\\_activists.shtml](http://www.bbc.co.uk/russian/russia/2011/12/111201_golos_human_rights_activists.shtml)

Price, J. Hunter, "The New Media Revolution in Egypt: Understanding the Failures of the Past and Looking Towards the Possibilities of the Future," *Democracy and Society*, Vol. 7, No. 2, Spring 2010.

Pryaniki, Russian website, undated. As of August 14, 2012:

<http://www.pryaniki.org/>



Public Post, Russian website, undated. As of May 4, 2012:  
<http://www.publicpost.ru/>

Public Opinion Fund (FOM), "Exit Poll v Den' Vyborov v Gosdumu RF," Russian website, December 4, 2011. As of June 15, 2012:  
<http://fom.ru/partii/10270>

Puddington, Arch, *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty*, Lexington, Ky.: University Press of Kentucky, 2000.

Qasas, Faras, "Bashar al-Asad wa Tawsīfihī lil Sirā' al-Dā'ir fī Sūrīya" ["Bashar al-Asad and His Description of the Ongoing Conflict in Syria"], *Al-Arabiya.net*, November 30, 2011.

Rabasa, Angel, Cheryl Benard, Lowell H. Schwartz, and Peter Sickel, *Building Moderate Muslim Networks*, Santa Monica, Calif.: RAND Corporation, MG-574-SRF, 2007. As of May 9, 2013:  
<http://www.rand.org/pubs/monographs/MG574.html>

"Radio Liberty Profile 1964," Box 32, RFE-RL/CA, HIA 1964.

Rahimi, Babak, "The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran," *Communication Review*, Vol. 14, No. 3, September 2011.

Ralis, Maxis, Manager of Audience Research and Evaluation Department, *Three Years of RadLib Audience Research, Part 1*, October 1, 1959.

Reilly, James, *Strong Society, Smart State: The Rise of Public Opinion in China's Japan Policy*, New York: Columbia University Press, 2011.

"Results of the Election in Russia," elections.grakon.org website, undated. As of May 13, 2012:  
<http://elections.grakon.org/#>

Rich, Frank, "Wallflowers at the Revolution," *New York Times*, February 6, 2011.

Ridus, Russian website, undated. As of May 11, 2012:  
<http://www.ridus.ru/>

Rimensnyder, Sara, "Triangle Boy Howdy," Reason.com website, March 2002. As of February 19, 2013:  
<http://reason.com/archives/2002/03/01/triangle-boy-howdy>

Roberts, Hal, and Bruce Etling, "Coordinated DDOS Attack During Russian Duma Elections," Internet Democracy Blog, December 8, 2011. As of May 13, 2012:  
<http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/>

Rochon, Laurier, "The Dictator's Practical Internet Guide to Power Retention," Present Working Directory website, 2012. As of March 2, 2013:  
<http://pwd.io/guide/>

Rooydadnews.blogspot.com, Arabic website, undated. As of March 14, 2012:  
<http://rooydadnews.blogspot.com/>

RosAgit, Russian website, undated. No longer available. As of February 4, 2012:  
<http://www.rosagit.ru/>

Rugh, William, *Arab Mass Media: Newspapers, Radio, and Television in Arab Politics*, Westport, Conn.: Praeger, 2004.

Russian Public Opinion Research Center, "Miting 4 Fevralya na Bolotnoy Plohchadi: Rezulatyatyy Oprosa Uchastnikov (The February 4 Rally: Member Survey Results)," Russian web page, undated. As of February 15, 2012:  
<http://wciom.ru/index.php?id=459&uid=112492>

———, survey question, Russian web page, March 11, 2012. As of May 7, 2012:  
[http://wciom.ru/zh/print\\_q.php?s\\_id=814&q\\_id=57381&date=11.03.2012](http://wciom.ru/zh/print_q.php?s_id=814&q_id=57381&date=11.03.2012)

———, Public Opinion Survey, March 13, 2011.

———, "VTsIOM Puts Together a Collective Portrait of the Participants of the Russian Opposition Meeting," Russian web page, February 16, 2012. As of March 11, 2012:  
<http://tagilcity.ru/news/politics/vciom-sostavil-kollektivnyy-portret-uchastnika-mitinga-oppozicii.html>

"RuNet Organizuyet Massovye Protesty v Moskve y za Eye Predelami" ["RuNet Organizing Mass Protests in Moscow and Beyond"], CyberSecurity.ru, Russian website, December 8, 2011. As of June 28, 2013: <http://www.cybersecurity.ru/net/139444.html>

"Russian Social Network Rebuffs FSB Request to Close 'Opposition' Accounts—Spokesman," RIA News, December 8, 2011. As of May 7, 2012:  
[http://en.rian.ru/russia/20111208/169489984.html?utm\\_campaign=DTN+Russia:&utm\\_source=twitterfeed&utm\\_medium=twitter](http://en.rian.ru/russia/20111208/169489984.html?utm_campaign=DTN+Russia:&utm_source=twitterfeed&utm_medium=twitter)

Sands, Phil, "Syria Tightens Control over Internet," *National*, September 30, 2008. As of August 20, 2012:  
<http://www.thenational.ae/news/world/middle-east/syria-tightens-control-over-internet>

Schelling, Thomas, *The Strategy of Conflict*, Cambridge, Mass.: Harvard University Press, 1960.

Schramm, Wilbur, *A Communication Research Man Looks at Radio Liberation*, Radio Liberty, August 1957.

Schuler, Ian, "SMS As a Tool in Election Observation," *Innovations: Technology, Governance, Globalization*, Vol. 3, No. 2, Spring 2008.

Schwartz, Lowell, *Political Warfare Against the Kremlin: U.S. and British Propaganda Policy at the Beginning of the Cold War*, New York: Palgrave Macmillan, 2009.

Sennott, Charles, "Inside the Muslim Brotherhood, Part 1," Special Report: The Muslim Brotherhood's Role in the Egyptian Revolution," *Frontline* and *GlobalPost*, February 21, 2011.

Shirky, Clay, *Here Comes Everybody: The Power of Organizing Without Organizations*, New York: Penguin Group, 2008.

———, "The Political Power of Social Media: Technology, the Public Sphere, and Political Change," *Foreign Affairs*, January–February 2011. As of May 2012: <http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media>

Shpilkin, Sergei, "No Choice," *Esquire*, Russian website, December 1, 2011. As of May 8, 2012: <http://esquire.ru/elections>

———, "Election Statistics Examined," Herald, Russian website, December 10, 2011. As of February 4, 2012: [http://www.gazeta.ru/science/2011/12/10\\_a\\_3922390.shtml](http://www.gazeta.ru/science/2011/12/10_a_3922390.shtml)

"Sichuan Earthquake," *New York Times*, May 6, 2009. As of October 1, 2012: [http://topics.nytimes.com/topics/news/science/topics/earthquakes/sichuan\\_province\\_china/index.html](http://topics.nytimes.com/topics/news/science/topics/earthquakes/sichuan_province_china/index.html)

Skovgaard-Petersen, Jakob, "Islamic Fundamentalism in Arab Television: Islamism and Salafism in Competition," in Ulrika Martensson, Jennifer Bailey, Priscilla Ringrose, and Asbjorn Dyrendal, eds., *Fundamentalism in the Modern World*, Vol. 2, New York: I.B. Tauris, 2011.

Slon, Russian website, undated. As of March 4, 2012: <http://slon.ru/>

"Social Media: A Double-Edged Sword in Syria," *Reuters*, July 13, 2011.

Socialbakers.com, *Russia Facebook Statistics*, undated. As of July 11, 2012: <http://www.socialbakers.com/facebook-statistics/russia>

Soldatov, Andrei, "Vladimir Putin's Cyber Warriors," *Foreign Affairs*, December 9, 2011. As of June 3, 2012: <http://www.foreignaffairs.com/articles/136727/andrei-soldatov/vladimir-putins-cyber-warriors?page=show>

———, "In Ex-Soviet States, Russian Spy Tech Still Watches You," *Wired*, December 21, 2012.

Sosin, Gene, *Sparks of Liberty: An Insider's Memoir of Radio Liberty*, University Park, Pa.: Pennsylvania State University Press, 1999.

Srenberny, Annabelle, and Gholam Khibany, *Blogistan: The Internet and Politics in Iran*, London and New York: I.B. Tauris, 2010.

St. Petersburg for Fair Elections, “Who Would You Like to See Speak at the Rally on February 4 in St. Petersburg?” Facebook, January 10, 2012. As of June 4, 2012: <http://www.facebook.com/questions/294908370562062/>

Status, Richard, “East Berlin Demonstrations,” briefing of the Under Secretary for Psychological Strategy Board luncheon, June 17, 1953.

Stecklow, Steve, “Special Report: Chinese Firm Helps Iran Spy on Citizens,” Reuters, March 22, 2012. As of August 9, 2012: <http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322>

Storey, P.C., “Publicity and Propaganda Policy Towards the Soviet Union and the Satellites,” August 22, 1956.

———, “BBC Russia Service May–September 1956,” September 12, 1956.

“Suqūt al-Shuhada’ Mundhu Sabāh wa Janāza al-Shahīd al-Halabī Tahawwulat ila Muzhāhara Hāshida Ghayr Masbūqa” [“Fallen Martyrs Since this Morning and the Funeral of a Martyr Morphs into an Unprecedented Mass Demonstration”], *Suriya Mustaqbal*, December 26, 2011.

Sunstein, Cass R., *Republic.com*, Princeton, N.J.: Princeton University Press, 2002.

———, “Neither Hayek nor Habermas,” *Public Choice*, Vol. 134, 2008.

“Survey of Blocked Uyghur Websites Shows Xinjiang Still Cut Off from the World,” Reporters Without Borders website, October 29, 2009. As of February 13, 2013:

<http://en.rsf.org/china-survey-of-blocked-uyghur-websites-29-10-2009,34859>

Svoboda, Raido, “U Assotziatzi Golos Izyali Documenty dlya Nablyudeniya za Vyborami v Orle” [“Golos Observes Document Seizures in Election”], *Golos*, February 14, 2010 (file no longer available). As of March 14, 2012:

<http://golos.org/news/3187>

“Syrian Youth Breaks Through Internet Blocks,” Institute for War and Peace Reporting, June 3, 2008. As of August 3, 2012:

<http://www.isn.ethz.ch/isn/Digital-Library/Articles/Detail/?lng=en&id=88422>

syrianrevolution.org, Arabic website, undated. As of March 29, 2012:

[http://syrianrevolution.org/?page\\_id=20692](http://syrianrevolution.org/?page_id=20692)

Tang, Lijun, and Peidong Yong, “Symbolic Power and the Internet: The Power of a ‘Horse,’” *Media, Culture, and Society*, Vol. 33, No. 5, 2011.

Tarek, Sherif, “Egypt’s Ultras: Politically Involved But Not Politically Driven, Yet,” *abramonline*, January 16, 2012.

Taubman, William, *Khrushchev: The Man and His Era*, New York: W.W. Norton and Company, 2003.

Taylor, Julie E., "Prophet Sharing: Strategic Interaction Between Muslim Clerics and Middle Eastern Regimes," *Journal of Islamic Law and Culture*, Vol. 10, No. 1, April 2008.

Techinasia.com, *China Internet Penetration Map*, web page, January 17, 2012. As of March 2, 2012:

<http://www.techinasia.com/china-Internet-penetration-map>

Thompson, Clive, "Google's China Problem (and China's Google Problem)," *New York Times*, April 6, 2006. As of October 1, 2012:

[http://www.nytimes.com/2006/04/23/magazine/23google.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2006/04/23/magazine/23google.html?pagewanted=all&_r=0)

Tian, Xiao, *Battle for Freedom in Chinese Cyberspace*, unpublished manuscript, May 2006. As of August 20, 2012:

<http://www.Interefreedom.org/files/Research/battle-for-freedom-in-chinese-cyberspace.pdf>

Tilly, Charles, *From Mobilization to Revolution*, Reading, Mass.: Addison-Wesley, 1978.

"Timeline: Egypt's Revolution," *al-Jazeera*, February 14, 2011.

Tor Metrics Portal, website, undated. As of June 22, 2012:

<https://metrics.torproject.org/>

Tor Project, Number of Connections from China to the Tor Network, undated. As of September 27, 2009:

<https://metrics.torproject.org/users.html?graph=direct-users&start=2010-01-01&end=2013-06-05&country=cn&events=off#direct-users>

———, Number of Connections from Russia to the Tor Network, undated. As of June 3, 2013:

<https://metrics.torproject.org/users.html?graph=direct-users&start=2009-01-01&end=2012-08-22&country=ru&dpi=72#direct-users>

———, Number of Connections from Syria to the Tor Network, undated. As of June 3, 2013:

<https://metrics.torproject.org/users.html?graph=direct-users&start=2010-01-01&end=2013-06-05&country=sy&events=off#direct-users>

———, Number of Connections from Egypt to the Tor Network, undated. As of June 4, 2013:

<https://metrics.torproject.org/users.html?graph=direct-users&start=2010-01-01&end=2013-06-04&country=eg&events=off#direct-users>

Torproject.org, "Tor Partially Blocked in China," September 27, 2009. As of June 23, 2012:

<https://blog.torproject.org/blog/tor-partially-blocked-china>

Tucker, Joshua, "Enough! Electoral Fraud, Collective Action Problems, and Post-Communist Color Revolutions," *Perspectives on Politics*, Vol. 53, No. 5, September 2007.

Tufekci, Zeynep, "As Egypt Shuts Off the Net: Seven Theses on Dictator's Dilemma," Technosociology website, January 28, 2011. As of July 11, 2012: <http://profoundheterogeneity.com/2011/02/its-not-the-public-internet-it-is-the-internet-public/>

Ungerleider, Neal, "Iran Cracking Down Online with 'Halal Internet,'" *Fast Company*, April 17, 2011. As of June 4, 2012: <http://www.fastcompany.com/1748123/iran-cracking-down-online-halal-internet>

United Nations Conference on Trade and Development, *ICT Policy Review: Egypt, Switzerland*, United Nations Publication, 2011.

"United Russia Wins 48.5 Percent; KPRF, LDPR, and Just Russia Also Win Duma Seats: Exit Poll" (in Russian), *RIA News*, December 4, 2011. As of June 28, 2013: <http://ria.ru/politics/20111204/506565506.html>

U.S. Central Intelligence Agency, *The World Factbook—Literacy*, web page, statistics for 2010, undated. As of August 20, 2012: <https://www.cia.gov/library/publications/the-world-factbook/fields/2103.html>

———, *The World Factbook—Country Comparisons, Population*, web page, statistics for 2012, undated. As of July 2012: <https://www.cia.gov/library/publications/the-world-factbook/geos/wz.html>

———, Office of Current Intelligence, "CIA Comment on East Berlin Uprising," June 17, 1953.

U.S. State Department, *Bureau of Democracy, Human Rights, and Labor (DRL) Programs* web page, undated. As of August 9, 2012: <http://www.state.gov/j/drl/p/>

U.S. Treasury Department, "Fact Sheet: New Executive Order Targeting Human Rights Abuses via Information Technology," April 23, 2012.

"Users," Tor Metrics Portal website, undated. As of November 4, 2012: <https://metrics.torproject.org/users.html?graph=direct-users&start=2009-01-01&end=2012-08-22&country=ru&dpi=72#direct-users>

Verma, Sonia, "How a Brutal Beating and Facebook Led to Egyptian Protests," *Globe and Mail*, January 26, 2011.

VTsIOM—See Russian Public Opinion Research Center.

Warrick, Joby, "Iran Reportedly Aiding Syrian Crackdown," *Washington Post*, May 27, 2011.

Wee, Sui-Lee, "China Says It Will Shut Plant as Thousands Protest," Reuters website, August 14, 2011. As of October 1, 2012:  
<http://www.reuters.com/article/2011/08/14/us-china-protests-idUSTRE77D0EK20110814>

"What Are You Allowed to Say on China's Social Network?" IEEE Spectrum, June 2011. As of September 1, 2012:  
<http://www.chinadigitaltimes.net/2011/06/121482/>

White House, "Statement by the President on Syria," Washington, D.C., April 22, 2011. As of November 4, 2012:  
<http://www.whitehouse.gov/the-press-office/2011/04/22/statement-president-syria>

White House Executive Order, "Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology," Washington, D.C.: April 23, 2012. As of December 14, 2012:  
<http://www.whitehouse.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer>

Wines, Michael, "China Expands Program Requiring Real-Name Registration Online," *New York Times*, January 18, 2012. As of October 1, 2012:  
<http://www.nytimes.com/2012/01/19/world/asia/china-expands-program-requiring-real-name-registration-online.html>

Wisner, Frank, "White House Inquiry Concerning the Performance of RIAS," memorandum to Charles Douglas Jackson, July 20, 1953.

Woodard, George, "Poland," from Session Three: Impact of the Broadcasts: Jamming and Audiences, in the *Report on the Impact of Cold War Broadcasting*, a conference organized by the Hoover Institution and the Cold War International History Project of the Woodrow Wilson International Center for Scholars at Stanford University, October 13–16, 2004.

Wooldridge, Jeffrey, *Cross-Sectional and Panel Data Analysis*, Cambridge, Mass.: MIT Press, 2002.

World Bank, World Development Indicators, ComScore, "Russia Has Fastest Growing Internet Population in Europe," press release, August 27, 2008. As of March 18, 2012:  
[http://www.comscore.com/Press\\_Events/Press\\_Releases/2008/08/Russia\\_Internet\\_Growth](http://www.comscore.com/Press_Events/Press_Releases/2008/08/Russia_Internet_Growth)

World Bank, World Development Indicators and Global Development Finance, web page, 2011. As of October 2, 2012:  
<http://databank.worldbank.org/data/Views/VariableSelection/SelectVariables.aspx?source=World%20Development%20Indicators%20and%20Global%20Development%20Finance>

Yang, Guobin, *The Power of the Internet in China: Citizen Activism Online*, New York: Columbia University Press, 2009.

- Yeltsin, Boris, *In Country and the World*, RL program, August 24, 1991.
- York, Jillian C., and Trevor Timm, "Satphones, Syria, and Surveillance," Electronic Frontier Foundation website, February 23, 2012. As of August 13, 2012:  
<https://www.eff.org/deeplinks/2012/02/satphones-syria-and-surveillance>
- Zakharov, Alexey, "How Many Votes in the Parliamentary Election Observers Saved," Slon.ru, December 7, 2011. As of December 4, 2012:  
[http://slon.ru/russia/nezavisimye\\_nablyudateli\\_spasli\\_10\\_golosoov\\_na\\_parlamentskikh\\_vyborakh-722685.xhtml](http://slon.ru/russia/nezavisimye_nablyudateli_spasli_10_golosoov_na_parlamentskikh_vyborakh-722685.xhtml)
- Zaks, Russian website, undated. As of December 2, 2012:  
<http://www.zaks.ru/>
- Zhang, Anna, "Public Outrage Mounts over Train Wreck's Botched Rescue," *Forbes*, July 27, 2011. As of October 1, 2012:  
<http://www.forbes.com/2011/07/27/china-train-crash-opinions-contributors-rescue-xiang-weiyi.html>
- Zheng, Yongnian, *Technological Empowerment: The Internet, State, and Society in China*, Stanford, Calif.: Stanford University Press, 2008.
- Zhuo, Xiaolin, Barry Wellman, and Justine Yu, "Egypt: The First Internet Revolt?" *Peace Magazine*, Vol. 27, No. 3, July–September 2011.
- Ziadeh, Radwan, "The Double Edged Sword of Social Media," *Mark*, July 21, 2011.
- Zimmerman, William, "Mobilized Participation and the Nature of the Soviet Dictatorship," in James R. Millar, ed., *Politics, Work, and Daily Life in the USSR: A Survey of Former Soviet Citizens*, New York: Cambridge University Press, 1987.
- Zuckerman, Ethan, "Meet the Bridgebloggers," *Public Choice*, Vol. 134, Nos. 1–2, August 2008.



**T**he Internet has become a new battleground between governments that censor online content and those who advocate freedom to browse, post, and share information online for all, regardless of their place of residence. This report examines whether and how furthering Internet freedom can empower civil society vis-à-vis public officials, make the government more accountable to its citizens, and integrate citizens into the policymaking process. Using case studies of events in 2011 in Egypt, Syria, China, and Russia, researchers focus on the impact of Internet freedom on freedom of assembly, freedom of expression, and the right to cast a meaningful vote, all of which are the key pillars of political space. Researchers analyze the mechanisms by which Internet freedom can enhance the opportunities to enjoy these freedoms, how different political contexts can alter the opportunities for online mobilization, and how, subsequently, online activism can grow out into offline mobilization leading to visible policy changes. To provide historical context, researchers also draw parallels between the effects of Radio Free Europe/Radio Liberty programs in the Soviet Union during the Cold War and the ongoing efforts to expand Internet freedom for all. The report concludes by discussing implications for the design of Internet freedom programs and other measures to protect “freedom to connect.”



NATIONAL DEFENSE RESEARCH INSTITUTE

[www.rand.org](http://www.rand.org)

\$32.95

