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.

RAND 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.

Cover design by Dori Gordon Walker
Cover images by Thinkstock

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

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.[1] 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[2]—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. [3] 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

[1] Fergus Hanson, "Internet Freedom: The Role of the U.S. State Department," in *Baked in and Wired: eDiplomacy @ State*, Brookings, October 25, 2012.

[2] 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.

[3] 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 nonpolitical 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 nondemocratic 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 Ultrasurf. Pwning computers is difficult to counter, but care in downloading, 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 nondemocratic 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.