A *Journal of Democracy* Book

•

SELECTED BOOKS IN THE SERIES

Edited by Larry Diamond and Marc F. Plattner

Poverty, Inequality, and Democracy (2012)
(with Francis Fukuyama)

Debates on Democratization (2010)

Democratization in Africa: Progress and Retreat (2010)

Democracy: A Reader (2009)

How People View Democracy (2008)

Latin America's Struggle for Democracy (2008)
(with Diego Abente Brun)

The State of India's Democracy (2007)
(with Sumit Ganguly)

Electoral Systems and Democracy (2006)

Assessing the Quality of Democracy (2005)
(Edited by Larry Diamond and Leonardo Morlino)

World Religions and Democracy (2005)
(with Philip J. Costopoulos)

Islam and Democracy in the Middle East (2003)
(with Daniel Brumberg)

Emerging Market Democracies: East Asia & Latin America (2002)
(Edited by Laurence Whitehead)

Democracy after Communism (2002)

Political Parties and Democracy (2001)
(Edited by Larry Diamond and Richard Gunther)

The Global Divergence of Democracies (2001)

Globalization, Power, and Democracy (2000)
(Edited by Marc F. Plattner and Aleksander Smolar)

Published under the auspices of
the International Forum for Democratic Studies

Liberation Technology

Social Media and the Struggle for Democracy

Edited by Larry Diamond and Marc F. Plattner

The Johns Hopkins University Press
Baltimore

Printed in the United States of America on acid-free paper

9 8 7 6 5 4 3 2 1

Chapters in this volume appeared in the following issues of the *Journal of Democracy:* chapter 1, July 2010; chapter 2, October 2010; chapters 4, 5, and 6, April 2011; chapter 8, July 2011. For all reproduction rights, please contact the Johns Hopkins University Press.

The Johns Hopkins University Press
2715 North Charles Street
Baltimore, Maryland 21218-4363
www.press.jhu.edu

Library of Congress Cataloging-in-Publication Data

Liberation technology : social media and the struggle for democracy / edited by Larry Diamond and Marc F. Plattner.
p. cm. — (A journal of democracy book)
Includes bibliographical references and index.
ISBN 978-1-4214-0567-4 (hdbk. : alk. paper) — ISBN 1-4214-0567-9 (hbk. : alk. paper) — ISBN 978-1-4214-0568-1 (pbk. : alk. paper) — ISBN 1-4214-0568-7 (pbk. : alk. paper) — ISBN 978-1-4214-0698-5 (electronic) — ISBN 1-4214-0698-5 (electronic)
1. Political participation—Technological innovations. 2. Democratization—Technological innovations. 3. Social media—Political aspects. I. Diamond, Larry Jay. II. Plattner, Marc F., 1945–

JF799.L53 2012
303.48'33—dc23

2012012206

CONTENTS

Acknowledgments vii

Introduction
Larry Diamond ix

I. Liberation vs. Control in Cyberspace

1. Liberation Technology
Larry Diamond 3

2. Liberation vs. Control: The Future of Cyberspace
Ronald Deibert and Rafal Rohozinski 18

3. International Mechanisms of Cyberspace Controls
Ronald Deibert 33

4. Whither Internet Control?
Evgeny Morozov 47

II. Liberation Technology in China

5. The Battle for the Chinese Internet
Xiao Qiang 63

6. China's "Networked Authoritarianism"
Rebecca MacKinnon 78

III. Liberation Technology in the Middle East

7. Ushahidi as a Liberation Technology
Patrick Meier 95

8. Egypt and Tunisia: The Role of Digital Media
Philip N. Howard and Muzammil M. Hussain 110

9. Circumventing Internet Censorship in the Arab World
Walid Al-Saqaf 124

10. Social Media, Dissent, and Iran's Green Movement
Mehdi Yahyanejad and Elham Gheytanchi 139

1

LIBERATION TECHNOLOGY

Larry Diamond

***Larry Diamond** is senior fellow at the Hoover Institution and the Freeman Spogli Institute for International Studies, director of Stanford University's Center on Democracy, Development, and the Rule of Law, and founding coeditor of the* Journal of Democracy. *This essay originally appeared in the July 2010 issue of the* Journal of Democracy.

In March 2003, police in Guangzhou (Canton), China, stopped 27-year-old Sun Zhigang and demanded to see his temporary living permit and identification. When he could not produce these, he was sent to a detention center. Three days later, he died in its infirmary. The cause of death was recorded as a heart attack, but the autopsy authorized by his parents showed that he had been subjected to a brutal beating.

Sun's parents took his story to the liberal newspaper *Nanfang Dushi Bao* (Southern Metropolis Daily), and its investigation confirmed that Sun had been beaten to death in custody. As soon as its report appeared on April 25, "newspapers and Web sites throughout China republished the account, [Internet] chat rooms and bulletin boards exploded with outrage," and it quickly became a national story.[1] The central government was forced to launch its own investigation and on June 27, it found twelve people guilty of Sun's death.

Sun's case was a rare instance in China of official wrongdoing being exposed and punished. But it had a much wider and more lasting impact, provoking national debate about the "Custody and Repatriation" (C&R) measures that allowed the police to detain rural migrants (typically in appalling conditions) for lacking a residency or temporary-living permit. In the outrage following Sun's death, numerous Chinese citizens posted on the Internet stories of their own experiences of C&R, and the constitutionality of the legislation became a hotly debated topic in universities. An online petition asking the Standing Committee of the National People's Congress to reexamine C&R quickly garnered widespread popular support, and in June 2003 the government announced that it would close all of the more than eight-hundred C&R detention centers.[2]

Sun's case was seen as a watershed—the first time that a peaceful outpouring of public opinion had forced the Communist Chinese state to change a national regulation. But Sun's case also soon became that of muckraking editor Cheng Yizhong, whom local officials jailed (along with three of his colleagues) in retaliation for their efforts to ferret out the wrongdoing that led to Sun's death. The legal defense that Xu Zhiyong mounted on behalf of the four journalists itself became a *cause célèbre*. As their fellow journalists launched an unprecedented campaign for their release, using among other means an Internet petition, Xu established a website, the Open Constitutional Initiative, to post documents and legal arguments about the case. All of this reflected a burgeoning *weiquan* ("defend-rights") movement. But while Cheng and his deputy editor were released from prison without charge, they lost their jobs and the authorities closed down Xu's site. Xu continued his work in defense of rights until July of last year, when his organization was shut down and he was arrested on politically motivated charges of tax evasion.

Optimists discern in these events a striking ability of the Internet—and other forms of "liberation technology"—to empower individuals, facilitate independent communication and mobilization, and strengthen an emergent civil society. Pessimists argue that nothing in China has fundamentally changed. The Chinese Communist Party (CCP) remains firmly in control and beyond accountability. The *weiquan* movement has been crushed. And the Chinese state has developed an unparalleled system of digital censorship.

Both perspectives have merit. Liberation technology enables citizens to report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom. But authoritarian states such as China, Belarus, and Iran have acquired (and shared) impressive technical capabilities to filter and control the Internet, and to identify and punish dissenters. Democrats and autocrats now compete to master these technologies. Ultimately, however, not just technology but political organization and strategy and deep-rooted normative, social, and economic forces will determine who "wins" the race.

Liberation technology is any form of information and communication technology (ICT) that can expand political, social, and economic freedom. In the contemporary era, it means essentially the modern, interrelated forms of digital ICTs—the computer, the Internet, the mobile phone, and countless innovative applications for them, including "new social media" such as Facebook and Twitter. Digital ICTs have some exciting advantages over earlier technologies. The Internet's decentralized character and ability (along with mobile-phone networks) to reach large numbers of people very quickly, are well suited to grassroots organizing. In sharp contrast to radio and television, the new ICTs are two-way and even multiway forms of communication. With tools such as Twitter (a social-networking and microblogging service allowing its users to send and read messages with up to 140 characters), a user can instantly reach hundreds or even thousands of "followers." Users are thus not just passive recipients but journalists, commentators, videographers, entertainers, and organizers. Although most of this use is not political, the technology can empower those who wish to become political and to challenge authoritarian rule.

It is tempting to think of the Internet as unprecedented in its potential for political progress. History, however, cautions against such hubris. In the fifteenth century, the printing press revolutionized the accumulation and dissemination of information, enabling the Renaissance, the Protestant Reformation, and the scientific revolution. On these foundations, modern democracy emerged. But the printing press also facilitated the rise of the centralized state and prompted the movement toward censorship.[3] A century and a half ago, the telegraph was hailed as a tool to promote peace and understanding. Suddenly, the world shrank; news that once took weeks to travel across the world could be conveyed instantly. What followed was not peace and freedom but the bloodiest century in human history. Today's enthusiasts of liberation technology could be accused of committing the analytic sins of their Victorian forebears, "technological utopianism" and "chronocentricity"—that is, "the egotism that one's own generation is poised on the very cusp of history."[4]

In the end, technology is merely a tool, open to both noble and nefarious purposes. Just as radio and TV could be vehicles of information pluralism and rational debate, so they could also be commandeered by totalitarian regimes for fanatical mobilization and total state control. Authoritarian states could commandeer digital ICTs to a similar effect. Yet to the extent that innovative citizens can improve and better use these tools, they can bring authoritarianism down—as in several cases they have.

Mobilizing against authoritarian rule represents only one possible "liberating" use of digital ICTs. Well before mobilization for democracy peaks, these tools may help to widen the public sphere, creating a more pluralistic and autonomous arena of news, commentary, and information. The new ICTs are also powerful instruments for transparency and accountability, documenting and deterring abuses of human rights and democratic procedures. And though I cannot elaborate here, digital ICTs are also liberating people from poverty and ill health: conveying timely information about crop prices, facilitating microfinance for small entrepreneurs, mapping the outbreaks of epidemics, and putting primary healthcare providers in more efficient contact with rural areas.[5]

Malaysia: Widening the Public Sphere

A crucial pillar of authoritarian rule is control of information. Through blogs (there are currently more than a hundred million worldwide), blog sites, online chatrooms, and more formal online media, the Internet pro-

vides dramatic new possibilities for pluralizing flows of information and widening the scope of commentary, debate, and dissent.

One of the most successful instances of the latter type is *Malaysiakini*, an online newspaper that has become Malaysia's principal alternative source of news and commentary.[6] As Freedom House has documented, Malaysia lacks freedom of the press. The regime (both the state and the ruling Barisan Nasional [BN] coalition) dominates print and broadcast media through direct ownership and monopoly practices. Thus it can shape what Malaysians read and see, and it can punish critical journalists with dismissal. Repressive laws severely constrain freedom to report, publish, and broadcast. However, as a rapidly developing country with high literacy, Malaysia has witnessed explosive growth of Internet access (and recently, broadband access), from 15 percent of the population in 2000 to 66 percent in 2009 (equal to Taiwan and only slightly behind Hong Kong).[7] The combination of tight government control of the conventional media, widespread Internet access, and relative freedom on the Internet created an opening for online journalism in Malaysia, and two independent journalists—Steven Gan and Premesh Chandran—ventured into it. Opponents of authoritarian rule since their student days, Gan and Chandran became seized during the 1998 *reformasi* period with the need to reform the media and bring independent news and reporting to Malaysia. Using about US$9,000 of their own money (a tiny fraction of what it would take to start a print newspaper), they launched *Malaysiakini* in November 1999. Almost immediately, they gained fame by exposing how an establishment newspaper had digitally cropped jailed opposition leader (and former deputy prime minister) Anwar Ibrahim from a group photo of ruling-party politicians.

From its inception, *Malaysiakini* has won a loyal and growing readership by providing credible, independent reporting on Malaysian politics and governance. As its readership soared, that of the mainstream newspapers fell. Suddenly, Malaysians were able to read about such long-taboo subjects as corruption, human-rights abuses, ethnic discrimination, and police brutality. Now the online paper posts in English about fifteen news stories a day, in addition to opinion pieces, letters, readers' comments, and daily satire (in *Cartoonkini*), plus translations and original material in Chinese, Malay, and Tamil. *Malaysiakini* reports scandals that no establishment paper would touch, such as massive cost overruns related to conflicts of interest at the country's main port agency and ongoing financial misconduct at the government-supported Bank Islam Malaysia. With the regime's renewed legal assault on Anwar Ibrahim, *Malaysiakini* is the only place where Malaysians can turn for independent reporting on the legal persecution of the opposition leader. In July 2008, it became Malaysia's most visited news site with about 2.5 million visitors per month. Yet, like many online publications worldwide, it still strives for financial viability.

While Malaysia today is no less authoritarian than when *Malaysiakini* began publishing a decade ago, it is more competitive and possibly closer to a democratic breakthrough than at any time in the last four decades. If a transition occurs, it will be mainly due to political factors—the coalescence of an effective opposition and the blunders of an arrogant regime. In addition, economic and social change is generating a better-educated and more diverse population, less tolerant of government paternalism and control. Polling and other data show that young Malaysians in particular support the (more democratic) opposition. But it is hard to disentangle these political and social factors from the expansion of the independent public sphere that *Malaysiakini* has spearheaded. In March 2008, the BN made its worst showing at the polls in half a century, losing its two-thirds parliamentary majority for the first time since independence. Facilitating this was the growing prominence of online journalism, which diminished the massive BN advantage in media access and "shocked the country" by documenting gross police abuse of demonstrators, particularly those of Indian descent.

Malaysiakini and its brethren perform a number of democratic functions. They report news and convey images that Malaysians would not otherwise see. They provide an uncensored forum for commentary and debate, giving rise to a critical public sphere. They offer space and voice to those whose income, ethnicity, or age put them on the margins of society. They give the political opposition, which is largely shut out of the establishment media, a chance to make its case. In the process, they educate Malaysians politically and foster more democratic norms. Many online publications and Internet blog sites perform similar functions in other semi-authoritarian countries, such as Nigeria, and in emerging and illiberal democracies. But is it possible for these functions to take root in a country as authoritarian as China is today?

Opening a Public Sphere in China

The prevailing answer is no: China's "Great Firewall" of Internet filtering and control prevents the rise of an independent public sphere online. Indeed, China's policing of the Internet is extraordinary in both scope and sophistication. China now has the world's largest population of Internet users—more than 380 million people (a number equal to 29 percent of the population, and a sixteen-fold increase since the year 2000). But it also has the world's most extensive, "multilayered," and sophisticated system "for censoring, monitoring, and controlling activities on the internet and mobile phones."[8] Connection to the international Internet is monopolized by a handful of state-run operators hemmed in by rigid constraints that produce in essence "a national intranet," cut off from anything that might challenge the CCP's monopoly on power.

Access to critical websites and online reporting is systematically

blocked. Google has withdrawn from China in protest of censorship, while YouTube, Facebook, and Blogspot, among other widely used sites, are extensively blocked or obstructed. Chinese companies that provide search and networking services agree to even tighter self-censorship than do international companies. When protests erupt (as they did over Tibet in 2008, for instance) or other sensitive political moments approach, authorities preemptively close data centers and online forums. Now the party-state is also trying to eliminate anonymous communication and networking, by requiring registration of real names to blog or comment and by tightly controlling and monitoring cybercafés. Fifty-thousand Internet police prowl cyberspace removing "harmful content"—usually within 24 to 48 hours. Students are recruited to spy on their fellows. And the regime pays a quarter of a million online hacks (called "50-centers" because of the low piece rate they get) to post favorable comments about the party-state and report negative comments.

Such quasi-Orwellian control of cyberspace is only part of the story, however. There is simply too much communication and networking online (and via mobile phones) for the state to monitor and censor it all. Moreover, Chinese "netizens"—particularly the young who are growing up immersed in this technology—are inventive, determined, and cynical about official orthodoxy. Many constantly search for better techniques to circumvent cybercensorship, and they quickly share what they learn. If most of China's young Internet users are apolitical and cautious, they are also alienated from political authority and eagerly embrace modest forms of defiance, often turning on wordplay.

Recently, young Chinese bloggers have invented and extensively lauded a cartoon creature they call the "grass mud horse" (the name in Chinese is an obscene pun) as a vehicle for protest. This mythical equine, so the narrative goes, is a brave and intelligent animal whose habitat is threatened by encroaching "river crabs." In Chinese, the name for these freshwater crustaceans *(hexie)* sounds very much like the word for Hu Jintao's official governing philosophy of "harmony"—a label that critics see as little more than a euphemism for censorship and the suppression of criticism. Xiao Qiang, editor of *China Digital Times,* argues that the grass mud horse

> has become an icon of resistance to censorship. The expression and cartoon videos may seem like a juvenile response to unreasonable rule. But the fact that the vast online population has joined the chorus, from serious scholars to usually politically apathetic urban white-collar workers, shows how strongly this expression resonates.[9]

In order to spread defiance, Chinese have a growing array of digital tools. Twitter has become one of the most potent means for political and social networking and the rapid dissemination of news, views, and withering satire. On April 22 at People's University in Beijing, three human-

rights activists protested a speech by a well-known CCP propaganda official, Wu Hao. Showering him with small bills, they declared, "Wu Hao, wu mao!" ("Wu Hao is a fifty-center!"). Twitter flashed photographs of the episode across China, delighting millions of students who revel in mocking the outmoded substance, tortured logic, and painfully crude style of regime propagandists.

When Google announced in late March 2010 it was withdrawing its online search services from mainland China (after failing to resolve its conflict with the government over censorship and cyberattacks), the Chinese Twitter-sphere lit up. Many Chinese were upset that Google would abandon them to the more pervasive censorship of the Chinese search-engine alternatives (such as Baidu), and they worried that the Great Firewall would block other services such as Google Scholar and Google Maps. Others suspected Google of doing the U.S. government's bidding. But the company's decision provoked a wave of sympathy and mourning, similar to what happened in January when Google first announced that it was considering withdrawing: "Citizen reporters posted constant updates on . . . Twitter, documenting the Chinese netizens who endlessly offered flowers, cards, poems, candles, and even formal bows in front of the big outdoor sign 'Google' located outside the company's offices in Beijing, Shanghai and Guangzhou."[10] Security guards chased the mourners away, declaring the offerings "illegal flower tributes." The term quickly spread in China's online forums, symbolizing the suppression of freedom.

The public sphere in China involves much more than "tweets," of course. Those often link to much longer blogs, discussion groups, and news reports. And many thought-provoking sites are harder to block because their critiques of CCP orthodoxy are subtler, elucidating democratic principles and general philosophical concepts, sometimes with reference to Confucianism, Taoism, and other strains of traditional Chinese thought that the CCP dares not ban. Full-scale blog posts (not subject to Twitter's severe length limits) are far likelier to criticize the government (albeit artfully and euphemistically). Rebecca MacKinnon finds that China's blogosphere is a "much more freewheeling space than the mainstream media," with censorship varying widely across the fifteen blog-service providers that she examined. Thus, "a great deal of politically sensitive material survives in the Chinese blogosphere, and chances for survival can likely be improved with knowledge and strategy."[11]

Despite the diffuse controls, China's activists see digital tools such as Twitter, Gmail, and filtration-evading software as enabling levels of communication, networking, and publishing that would otherwise be unimaginable in China today. With the aid of liberation technology, dissident intellectuals have gone from being a loose assortment of individuals with no specific goal or program to forming a vibrant and increasingly visible collaborative force. Their groundbreaking manifesto—Charter 08, a call

for nineteen reforms to achieve "liberties, democracy, and the rule of law" in China—garnered most of its signatures through the aid of blog sites such as *bullog.cn*. When Charter 08 was released online on 10 December 2008, with the signatures of more than three-hundred Chinese intellectuals and human-rights activists, the government quickly moved to suppress all mention of it. But then, "something unusual happened. Ordinary people such as Tang [Xiaozhao] with no history of challenging the government began to circulate the document and declare themselves supporters," shedding their previous fear. Within a month, more than five-thousand other Chinese citizens had signed the document. They included not just the usual dissidents but "scholars, journalists, computer technicians, businessmen, teachers and students whose names had not been associated with such movements before, as well as some on the lower rungs of China's social hierarchy—factory and construction workers and farmers."[12]

Officials shut down Tang's blog soon after she signed the Charter, and did the same to countless other blogs that supported it (including the entire *bullog.cn* site). But the campaign persists in underground salons, elliptical references, and subversive jokes spread virally through social media and instant messaging. One such joke imagines a testy Chinese president Hu Jintao complaining about the Charter's democratic concepts such as federalism, opposition parties, and freedom of association. "Where do they all come from?" he demands. His minions run down the sources and bring him the bad news: The troublesome notions can be traced to Mao Zedong, Zhou Enlai, the CCP, the official newspaper (the *Xinhua Daily*), and the constitution of the People's Republic itself. A flustered Hu wonders what to do. His staff suggests banning all mention of these names. "You idiots!" shouts Hu. "If you ban them, you might as well ban me too!" "Well," his staff retorts, "People do say that if they ban you, at least the Charter will be left alone."[13]

Monitoring Governance, Exposing Abuses

Liberation technology is also "accountability technology," in that it provides efficient and powerful tools for transparency and monitoring. Digital cameras combined with sites such as YouTube create new possibilities for exposing and challenging abuses of power. Incidents of police brutality have been filmed on cellphone cameras and posted to YouTube and other sites, after which bloggers have called outraged public attention to them. Enter "human rights abuses" into YouTube's search box and you will get roughly ten-thousand videos showing everything from cotton-growers' working conditions in Uzbekistan, to mining practices in the Philippines, to human-organ harvesting in China, to the persecution of Bahá'ís in Iran. A YouTube video of a young Malaysian woman forced by the police to do squats while naked forced the country's prime minister to call for an independent inquiry. When Venezuelan president Hugo Chávez forced Radio

Caracas Television off the air in May 2007, it continued its broadcasts via YouTube. No wonder, then, that authoritarian states such as Iran and Saudi Arabia completely block access to that video-posting site.

Across much of the world, and especially in Africa, the quest for accountability makes use of the simplest form of liberation technology: text messaging via mobile phone. (Mobile-phone networks have proven particularly useful in infrastructure-starved Africa since they can cover vast areas without requiring much in the way of physical facilities beyond some cell towers.) Around the world, the reach and capabilities of cellphones are being dramatically expanded by open-source software such as FrontlineSMS, which enables large-scale, two-way text messaging purely via mobile phones. In recent years, the software has been used over mobile-phone networks to monitor national elections in Nigeria and Ghana, to facilitate rapid reporting of human-rights violations in Egypt, to inform citizens about anticorruption and human-rights issues in Senegal, and to monitor and report civil unrest in Pakistan. A Kenyan organization, Ushahidi (Swahili for "testimony"), has adapted the software for "crisis-mapping." This allows anyone to submit crisis information through text messaging using a mobile phone, e-mail, or online-contact form, and then aggregates the information and projects it onto a map in real time. It was initially developed by citizen journalists to map reports of postelection violence in Kenya in early 2008, drawing some 45,000 Kenyan users. It has since been used to report incidents of xenophobic violence in South Africa; to track violence and human-rights violations in the Democratic Republic of Congo; and to monitor elections in Afghanistan, India, Lebanon, and Mexico.

The largest funder of both Ushahidi and FrontlineSMS is the Omidyar Network (ON), a philanthropic investment firm established six years ago by eBay founder Pierre Omidyar and his wife Pam. It extends into the worlds of political and social innovation the eBay approach: giving everyone equal access to information and opportunity to leverage the potential of individuals and the power of markets. This innovative effort—which comprises both a venture-capital fund directed at for-profit start-ups and a nonprofit grant-making fund—has committed more than $325 million in investments and grants in two broad areas: "access to capital" (microfinance, entrepreneurship, and property rights), and "media, markets and transparency" (which supports technology that promotes transparency, accountability, and trust across media, markets, and government). The ON supports national partners in Nigeria, Ghana, and Kenya that are using information technology to improve governance and free expression. These include Infonet—a web portal that provides citizens, media, and NGOs with easy-to-access information on national- and local-government budgets in Kenya—and Mzalendo, a comprehensive site that enables Kenyans to follow what their members of parliament are doing.

The ON's support for transparency initiatives also extends to other countries and to U.S.-based organizations. These include Global Integrity,

which harnesses the Internet and other sources of information in order to generate detailed assessments of corruption in more than ninety countries; and the Sunlight Foundation, which utilizes the Internet and related technology in order to make information about federal-government spending, legislation, and decision making more accessible to U.S. voters.

Mobilizing Digitally

One of the most direct, powerful, and—to authoritarian regimes—alarming effects of the digital revolution has been its facilitation of fast, large-scale popular mobilizations. Cellphones with SMS text messaging have made possible what technology guru Howard Rheingold calls "smart mobs"—vast networks of individuals who communicate rapidly and with little hierarchy or central direction in order to gather (or "swarm") at a certain location for the sake of protest. In January 2001, Philippine president Joseph Estrada "became the first head of state in history to lose power to a smart mob," when tens of thousands and then, within four days, more than a million digitally mobilized Filipinos assembled at a historic protest site in Manila.[14] Since then, liberation technology has been instrumental in virtually all of the instances where people have turned out *en masse* for democracy or political reform.

Liberation technology figured prominently in the Orange Revolution that toppled the electoral authoritarian regime in Ukraine via mass protests during November and December 2004. The Internet newspaper *Ukrainskaya Pravda* provided a vital source of news and information about both the regime's efforts to steal the presidential election and the opposition's attempts to stop it. By the revolution's end, this online paper had become "the most widely read news source of any kind in Ukraine."[15] Website discussion boards gave activists a venue for documenting fraud and sharing best practices.[16] Text messaging helped to mobilize and coordinate the massive public protests—bringing hundreds of thousands to Kyiv's Independence Square in freezing weather—that ultimately forced a new runoff, won by the democratic opposition.

These digital tools also facilitated the 2005 Cedar Revolution in Lebanon (which drew more than a million demonstrators to demand the withdrawal of Syrian troops); the 2005 protests for women's voting rights in Kuwait; the 2007 protests by Venezuelan students against the closure of Radio Caracas Television; and the April 2008 general strike in Egypt, where tens of thousands of young demonstrators mobilized through Facebook.[17] In September 2007, the "Internet, camera phones, and other digital networked technologies played a critical role" in Burma's Saffron Revolution, so called because of the involvement of thousands of Buddhist monks. Although digital technology did little directly to mobilize the protests, it vividly informed the world of them, and revealed the bloody crackdown that the government launched in response: "Burmese citizens

took pictures and videos, many on their mobile phones, and secretly uploaded them from Internet cafes or sent digital files across the border to be uploaded." This international visibility may have saved many lives by inhibiting the military from using force as widely and brutally as it had in 1988.[18]

In China, pervasive text messaging has been a key factor in the mushrooming of grassroots protests. In 2007, an eruption of hundreds of thousands of cellphone text messages in Xiamen, a city on the Taiwan Strait, generated so much public dismay at the building of an environmentally hazardous chemical plant that authorities suspended the project.[19] The impact of the text messages was magnified and spread nationally as bloggers in other Chinese cities received them and quickly fanned the outrage. The technology is even seeping into North Korea, the world's most closed society, as North Korean defectors and South Korean human-rights activists entice North Koreans to carry the phones back home with them from China and then use them to report what is happening (via the Chinese mobile network).[20] In the oil-rich Gulf states, text messaging allows civic activists and political oppositionists "to build unofficial membership lists, spread news about detained activists, encourage voter turnout, schedule meetings and rallies, and develop new issue campaigns—all while avoiding government-censored newspapers, television stations, and Web sites."[21]

The most dramatic recent instance of digital mobilization was Iran's Green Movement, following the egregious electoral malpractices that appeared to rob opposition presidential candidate Mir Hosein Musavi of victory on 12 June 2009. In the preceding years, Iran's online public sphere had been growing dramatically, as evidenced by its more than "60,000 routinely updated blogs" exploring a wide range of social, cultural, religious, and political issues;[22] the explosion of Facebook to encompass an estimated 600,000 Persian-language users;[23] and the growing utilization of the Internet by news organizations, civic groups, political parties, and candidates.

As incumbent president Mahmoud Ahmedinejad's election victory was announced (complete with claims of a 62 percent landslide) on June 13, outraged accounts of vote fraud spread rapidly via Internet chatrooms, blogs, and social networks. Through Twitter, text messaging, Facebook, and Persian-language social-networking sites such as Balatarin and Donbleh, Iranians quickly spread news, opinions, and calls for demonstrations. On June 17, Musavi supporters used Twitter to attract tens of thousands of their fellow citizens to a rally in downtown Tehran. Internet users organized nationwide protests throughout the month, including more large demonstrations in the capital, some apparently attended by two to three million people. YouTube also provided a space to post pictures and videos of human-rights abuses and government crackdowns. A 37-second video of the death of Neda Agha-Soltan during Tehran's violent protests on

June 20 quickly spread across the Internet, as did other images of the police and regime thugs beating peaceful demonstrators. Neda's death and the distressing images of wanton brutality decimated the remaining legitimacy of the Islamic Republic domestically and internationally.

To date, the Green Movement illustrates both the potential and limits of liberation technology. So far, the Islamic Republic's reactionary establishment has clung to power through its control over the instruments of coercion and its willingness to wield them with murderous resolve. Digital technology could not stop bullets and clubs in 2009, and it has not prevented the rape, torture, and execution of many protestors. But it has vividly documented these abuses, alienating key pillars of the regime's support base, including large segments of the Shia clergy. While the regime has tortured dissidents to get their e-mail passwords and round up more opponents, the Internet has fostered civic and political pluralism in Iran; linked the opposition within that country to the Iranian diaspora and other global communities; and generated the consciousness, knowledge, and mobilizational capacity that will eventually bring down autocracy in Iran. A key factor affecting when that will happen will be the ability of Iranians to communicate more freely and securely online.

Breaking Down the Walls

Even in the freest environments, the new digital means of information and communication have important limits and costs. There are fine lines between pluralism and cacophony, between advocacy and intolerance, and between the expansion of the public sphere and its hopeless fragmentation. As the sheer number of media portals has multiplied, more voices have become empowered, but they are hardly all rational and civil. The proliferation of online (and cable) media has not uniformly improved the quality of public deliberation, but rather has given rise to an "echo chamber" of the ideologically like-minded egging each other on. And open access facilitates much worse: hate-mongering, pornography, terrorism, digital crime, online espionage, and cyberwarfare. These are real challenges, and they require careful analysis—prior to regulation and legislation—to determine how democracies can balance the great possibilities for expanding human freedom, knowledge, and capacity with the dangers that these technologies may pose for individual and collective security alike.

Still the overriding challenge for the digital world remains freedom of access. The use of Internet filtering and surveillance by undemocratic regimes is becoming both more widespread and more sophisticated. And some less-sophisticated efforts, using commercial filtering software, may block sites even more indiscriminately. Currently, more than three-dozen states filter the Internet or completely deny their citizens access.[24] Enterprising users can avail themselves of many circumvention technologies,

but some require installation of software and so will not be available if the Internet is accessed from public computers or Internet cafes; many of the Web-based applications are blocked by the same filters that block politically sensitive sites; and most of these means require some degree of technical competence by the user.[25] Not all circumvention methods protect netizens' privacy and anonymity, which can be a particularly acute problem when state-run companies provide the Internet service. The free software Tor, popular among Iranians, promises anonymity by "redirecting encrypted traffic through multiple relays . . . around the world," making it difficult for a regime to intercept a transmission.[26] But if it effectively monopolizes the provision of Internet service, a desperate regime such as Burma's in 2007 can always respond by shutting down the country's Internet service or, as Iran's government did, by slowing service to a paralyzing crawl while authorities searched electronic-data traffic for protest-related content.[27]

Even in liberal democracies, issues of access arise. Recently netizens worldwide—and the U.S. government—have become concerned over excessively broad legislative proposals in Australia that would force Internet service providers to blacklist a large number of sites for legal and moral considerations (including the protection of children). The Chinese practice of forcing Internet providers to assume liability for the content to which they provide access is seeping into European legal and regulatory thinking regarding the Internet.[28]

There is now a technological race underway between democrats seeking to circumvent Internet censorship and dictatorships that want to extend and refine it. Recently, dictatorships such as Iran's have made significant gains in repression. In part, this has happened because Western companies like Nokia-Siemens are willing to sell them advanced surveillance and filtering technologies. In part, it has also been the work of dictatorships that eagerly share their worst practices with one another. A host of new circumvention technologies are coming onto the market, and millions of Chinese, Vietnamese, Iranians, Tunisians, and others fervently want access to them. Rich liberal democracies need to do much more to support the development of such technologies, and to facilitate (and subsidize) their cheap and safe dissemination to countries where the Internet is suppressed. More could be done to improve encryption so that people in authoritarian regimes can more safely communicate and organize online. Breakthroughs may also come with the expansion of satellite access that bypasses national systems, if the cost of the satellite dishes and monthly usage rates can be reduced dramatically. Western governments can help by banning the export of advanced filtering and surveillance technologies to repressive governments, and by standing behind Western technology companies when dictatorships pressure them "to hand over Internet users' personal data."[29] And finally, liberal democracies should stand up for the human rights of bloggers, activists, and journalists who have been arrested for peacefully reporting, networking, and organizing online.

It is important for the United States to have declared, as Secretary of State Hillary Clinton did in a historic speech on 21 January 2010, that "We stand for a single Internet where all of humanity has equal access to knowledge and ideas." But the struggle for electronic access is really just the timeless struggle for freedom by new means. It is not technology, but people, organizations, and governments that will determine who prevails.

NOTES

The author thanks Anna Davies, Blake Miller, and Astasia Myers for their truly superb research assistance on this article; and also Lian Matias, Galen Panger, Tucker Herbert, Ryan Delaney, Daniel Holleb, Sampath Jinadasa, and Aaron Qayumi for their prior research assistance on this project.

1. Sophie Beach, "The Rise of Rights?" *China Digital Times*, *http://chinadigitaltimes.net/2005/05/rise-of-rights*.

2. Yongnian Zheng, *Technological Empowerment: The Internet State and Society in China* (Stanford: Stanford University Press, 2008), 147–51.

3. Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, Mass.: Belknap Press, 1983), 251.

4. Tom Standage, *The Victorian Internet* (New York: Berkley, 1998), 210, 213.

5. For various accounts, see *http://fsi.stanford.edu/research/program_on_liberation_technology*.

6. This account draws heavily from a student research paper conducted under my supervision: Astasia Myers, "*Malaysiakini:* Internet Journalism and Democracy," Stanford University, 4 June 2009.

7. Figures on the growth of Web use in Malaysia and China are available at *www.internetworldstats.com/stats3.htm*.

8. Freedom House, "Freedom on the Net: A Global Assessment of Internet and Digital Media," 1 April 2009, 34; available at *www.freedomhouse.org*.

9. Private email message from Xiao Qiang, May 2009. Quoted with permission.

10. S.L. Shen, "Chinese Forbidden from Presenting Flowers to Google," UPI Asia Online, 15 January 2010; available at *www.upiasia.com/Politics/2010/01/15/chinese_forbidden_from_presenting_flowers_to_google/4148*.

11. Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday*, 2 February 2009; available at *http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089*. See also Ashley Esarey and Xiao Qiang, "Below the Radar: Political Expression in the Chinese Blogosphere," *Asian Survey* 48 (September–October 2008): 752–72.

12. Ariana Eunjung Cha, "In China, a Grass-Roots Rebellion," *Washington Post*, 29 January 2009.

13. "Charter 08 Still Alive in the Chinese Blogosphere," *China Digital Times*, 9 February 2009.

14. Howard Rheingold, *Smart Mobs: The Next Social Revolution* (New York: Basic Books, 2003), 158.

15. Michael McFaul, "Transitions from Postcommunism," *Journal of Democracy* 16 (July 2005): 12.

16. Robert Faris and Bruce Etling, "Madison and the Smart Mob: The Promise and Limitations of the Internet for Democracy," *Fletcher Forum of World Affairs* 32 (Summer 2008): 65.

17. Cathy Hong, "New Political Tool: Text Messaging," *Christian Science Monitor*, 30 June 2005; Jóse de Córdoba, "A Bid to Ease Chávez's Power Grip; Students Continue Protests in Venezuela; President Threatens Violence," *Wall Street Journal*, 8 June 2007.

18. Mridul Chowdhury, "The Role of the Internet in Burma's Saffron Revolution," Berkman Center for Internet and Society, September 2008, 14 and 4; available at *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Chowdhury_Role_of_the_Internet_in_Burmas_Saffron_Revolution.pdf_0.pdf*.

19. Edward Cody, "Text Messages Giving Voice to Chinese," *Washington Post*, 28 June 2007.

20. Choe Sang-Hun, "North Koreans Use Cell Phones to Bare Secrets," *New York Times*, 28 March 2010. Available at *www.nytimes.com/2010/03/29/world/asia/29news.html*.

21. Steve Coll, "In the Gulf, Dissidence Goes Digital; Text Messaging is the New Tool of Political Underground," *Washington Post*, 29 March 2005.

22. John Kelly and Bruce Etling, "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere," Berkman Center for Internet and Society, April 2008; available at *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf*.

23. Omid Habibinia, "Who's Afraid of Facebook?" 3 September 2009; available at *http://riseoftheiranianpeople.com/2009/09/03/who-is-afraid-of-facebook*.

24. In addition to Freedom House, *Freedom on the Net*, see Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zitrain, *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008). For the ongoing excellent work of the OpenNet Initiative, see *http://opennet.net*.

25. University of Toronto Citizen Lab, "Everyone's Guide to By-Passing Internet Censorship," September 2007; available at *www.civisec.org/guides/everyones-guides*.

26. Center for International Media Assistance, National Endowment for Democracy, "The Role of New Media in the 2009 Iranian Elections," July 2009, 2; available at *http://cima.ned.org/wp-content/uploads/2009/07/cima-role_of_new_media_in_iranian_elections-workshop_report.pdf*.

27. Rory Cellan-Jones, "Hi-Tech Helps Iranian Monitoring," BBC News, 22 June 2009. Available at *news.bbc.co.uk/2/hi/technology/8112550.stm*.

28. Rebecca MacKinnon, "Are China's Demands for Internet 'Self-Discipline' Spreading to the West?" McClatchy News Service, 18 January 2010; available at *www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html*.

29. Daniel Calingaert, "Making the Web Safe for Democracy," *ForeignPolicy.com*, 19 January 2010; available at *www.foreignpolicy.com/articles/2010/01/19/making_the_web_safe_for_democracy*.

2

LIBERATION VS. CONTROL: THE FUTURE OF CYBERSPACE

Ronald Deibert and Rafal Rohozinski

Ronald Deibert *is professor of political science and director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto.* ***Rafal Rohozinski*** *is a principal with the SecDev Group and former director of the Advanced Network Research Group of the Cambridge Security Programme. They are cofounders of the OpenNet Initiative and the Information Warfare Monitor. Their forthcoming book is* Ghost in the Machine: The Battle for the Future of Cyberspace. *The following essay is adapted from their "Cyber Wars" in the* Index on Censorship *(2010), available at* www.indexoncensorship.org. *This version originally appeared in the October 2010 issue of the* Journal of Democracy.

Every day there seems to be a new example of the ways in which human ingenuity combines with technology to further social change. For the Green Movement in Iran, it was Twitter; for the Saffron Revolution in Burma, it was YouTube; for the "color revolutions" of the former Soviet Union, it was mobile phones. No matter how restrictive the regulations or how severe the repercussions, communities around the world have exhibited enormous creativity in sidestepping constraints on technology in order to exercise their freedoms.

Looking at the seemingly endless examples of social innovation, one might easily assume that cybertechnologies possess a special power, that they are "technologies of liberation."[1] No other mode of communication in human history has facilitated the democratization of communication to the same degree. No other technology in history has grown with such speed and spread so far geographically in such a short period of time. Twitter, to take just the latest cyberapplication as an example, has grown from an average of 500,000 tweets a quarter in 2007 to more than four-billion tweets in the first quarter alone of 2010. The continual innovations in electronic communications have had unprecedented and far-reaching effects.

Yet some observers have noted that the very same technologies which give voice to democratic activists living under authoritarian rule can also be harnessed by their oppressors.[2] Cybercommunication has made possible some very extensive and efficient forms of social control. Even in democratic countries, surveillance systems penetrate every aspect of life, as people implicitly (and perhaps unwittingly) consent to the greatest invasion of personal privacy in history. Digital information can be easily tracked and traced, and then tied to specific individuals who themselves can be mapped in space and time with a degree of sophistication that would make the greatest tyrants of days past envious. So, are these technologies of freedom or are they technologies of control?

This dichotomy is itself misleading, however, as it suggests a clear-cut opposition between the forces of light and the forces of darkness. In fact, the picture is far more nuanced and must be qualified in several ways. Communications technologies are neither empty vessels to be filled with products of human intent nor forces unto themselves, imbued with some kind of irresistible agency. They are complicated and continuously evolving manifestations of social forces at a particular time and place. Once created, technologies in turn shape and limit the prospects for human communication and interaction in a constantly iterative manner. Complicating matters further is the inescapable presence of contingency. Technical innovations may be designed for specific purposes but often end up having wildly different social uses and effects than those intended by their creators. Yet these "alternative rationalities"— systems of use based on local culture and norms, particularly those that originate outside the developed world—often become the prevailing paradigm around which technologies evolve, until they in turn are disrupted by unanticipated uses or new innovations.[3]

The concepts of "liberation" and "control" also require qualification. Both are socially constructed ideas whose meaning and thus application can vary widely depending on the context in which they appear. Different communities work to be free (or "liberated") from different things—for example, colonial rule or gender or religious discrimination. Likewise, social control can take many forms, and these will depend both on the values driving them as well as what are perceived to be the objects of control. Countless liberation movements and mechanisms of social control coexist within a shared but constantly evolving communications space at any one time. This makes any portrayal of technology that highlights a single overarching characteristic biased toward either liberation or control seem fanciful.

This social complexity is a universal characteristic of all technological systems, but it is especially marked in the communications arena for several reasons. Processes of globalization, which are both products of and contributors to cyberspace, intensify the mix of actors, cultures, in-

terests, and ideas in the increasingly dense pool of communications. Although it may seem clichéd to note that events on one side of the planet can ripple back at the speed of light to affect what happens on the other side, we must not underestimate the proliferation of players whose actions help to shape cyberspace and who in turn are shaped by their own interactions within cyberspace. This "dynamic density" also accelerates the pace of change inherent in cyberspace, making it a moving target.[4] Innovations, which potentially may come from any of the millions of actors in cyberspace, can occur daily. This means that rather than being a static artifact, cyberspace is better conceptualized as a constantly evolving domain—a multilevel ecosystem of physical infrastructure, software, regulations, and ideas.

The social complexity of cyberspace is compounded by the fact that much of it is owned and operated by thousands of private actors, and some of their operations cross national jurisdictions. Guided by commercial principles, these enterprises often make decisions that end up having significant political consequences. For example, an online chat service may handle or share user data in ways that put users in jeopardy, depending on the jurisdiction in which the service is offered. Such considerations are especially relevant given the current evolution toward "cloud computing" and software-as-a-service business models. In these models, information and the software through which users interact are not physically located on their own computers but are instead hosted by private companies, often located in faraway jurisdictions. As a result, we have the curious situation in which individuals' data are ultimately governed according to laws and regulations over which they themselves have no say as citizens. This also accelerates existing trends toward the privatization of authority.[5]

Although the decisions taken by businesses—the frontline operators in cyberspace—play a critical role, cyberspace is also shaped by the actions of governments, civil society, and even individuals. Because corporations are subject to the laws of the land in which they operate, the rules and regulations imposed by national governments may inadvertently serve to carve up the global commons of information. According to the OpenNet Initiative research consortium, more than forty countries, including many democracies, now engage in Internet-content filtering.[6] The actions of civil society matter as well. Individuals, working alone or collectively through networks, can create software, tools, or forms of mobilization that have systemwide implications—not all of them necessarily benign. In fact, there is a hidden subsystem of cyberspace made up of crime and espionage.

In short, the actions of businesses, governments, civil society, criminal organizations, and millions of individuals affect and in turn are affected by the domain of cyberspace. Rather than being an ungoverned realm, cyberspace is perhaps best likened to a gangster-dominated version of New York: a tangled web of rival public and private authori-

ties, civic associations, criminal networks, and underground economies. Such a complex network cannot be accurately described in the one-dimensional terms of "liberation" or "control" any more than the domains of land, sea, air, or space can be. Rather, it is composed of a constantly pulsing and at times erratic mix of competing forces and constraints.

Liberation: From What and for Whom?

Much of the popular reporting about cyberspace and social mobilization is biased toward liberal-democratic values. If a social movement in Africa, Burma, or Iran employs a software tool or digital technology to mobilize supporters, the stories appear throughout the global media and are championed by rights activists.[7] Not surprisingly then, these examples tend to be generalized as the norm and repeated without careful scrutiny. But social mobilization can take various forms motivated by many possible rationales, some of which may not be particularly "progressive."[8] Due to both media bias and the difficulties of conducting primary research in certain contexts, these alternative rationalities tend to be obscured from popular view by the media and underexplored by academics.[9] Yet they are no less important than their seemingly more benign counterparts, both for the innovations that they produce and the reactions that they generate.

Consider, for example, the enormous criminal underworld in cyberspace. Arguably at the cutting edge of online innovation, cybercriminals have occupied a largely hidden, parasitic ecosystem within cyberspace, attacking the insecure fissures that open up within this constantly morphing domain. Although most cybercrime takes the form of petty spam (the electronic distribution of unsolicited bulk messages), the sophistication and reach of cybercriminals today are startling. The production of "malware"—malicious software—is now estimated to exceed that of legitimate software, although no one really knows its full extent. About a million new malware samples a month are discovered by security engineers, with the rate of growth increasing at a frightening pace.

One of the more ingenious and widespread forms of cybercrime is "click fraud," whereby victims' computers are infected with malicious software and redirected to make visits to online pay-per-click ads operated by the attackers. Although each click typically generates income on the order of fractions of a penny, a "botnet" (a group of thousands of infected computers referred to as "zombies") can bring in millions of dollars for the criminals.

One such cybercriminal enterprise called Koobface (an anagram of Facebook) exploits security vulnerabilities in users' machines while also harvesting personal information from Facebook and other social-networking services. It creates thousands of malicious Facebook ac-

counts every day, each of which is then directed toward click fraud or malicious websites that prompt the download of Trojan horses (malware downloads that appear legitimate). With the latter, Koobface can extract sensitive and confidential information such as credit-card account numbers from the infected computers of unwitting users, or deploy the computers as zombies in botnets for purposes of distributed computer-network attacks. Like the mirror universe on the television series *Star Trek,* in which parallel Captain Kirks and Spocks were identical to the originals except for their more malicious personalities, these phony accounts are virtually indistinguishable from the real ones. The Koobface enterprise demonstrates extraordinary ingenuity in social networking, but directed entirely toward fraudulent ends.

Just as software, social-networking platforms, and other digital media originally designed for consumer applications may be redeployed for political mobilization, innovations developed for cybercrime are often used for malicious political activity. Our research reveals the deeply troubling trend of cybercrime tools being employed for espionage and other political purposes.

Twice in the last two years, the Information Warfare Monitor has uncovered major global cyberespionage networks infiltrating dozens of high-level political targets, including foreign ministries, embassies, international organizations, financial institutions, and media outlets. These investigations, documented in the reports "Tracking *GhostNet*" and "Shadows in the Clouds," unearthed the theft of highly sensitive documents and the extensive infiltration of targets ranging from the offices of the Dalai Lama to India's National Security Council. The tools and methods used by the attackers had their origins in cybercrime and are widely available on the Internet black market.[10] Indeed, "Gh0st Rat," the main device employed by the cyberespionage network, is available for free download and has been translated into multiple languages. Moreover, although the networks examined in both studies are almost certainly committing politically motivated espionage rather than crime per se, our research suggests that the attackers were not direct agents of government but were probably part of the Chinese criminal underworld, either contracted or tolerated by Chinese officials.

Likewise, the OpenNet Initiative analyzed the cyberattacks waged against Georgian government websites during the August 2008 war with Russia over South Ossetia. The computers that were harvested together to mount distributed denial-of-service attacks were actually botnets already well known to researchers studying cybercrime and fraud, and had been used earlier to attack pornography and gambling sites for purposes of extortion.[11]

The most consistent demonstrations of digital ingenuity can be found in the dark worlds of pornography, militancy, extremism, and

hate. Forced to operate in the shadows and constantly maneuvering to stay ahead of their pursuers while attempting to bring more people into their folds, these dark networks adapt and innovate far more rapidly and with greater agility than their more progressive counterparts. Al-Qaeda persists today, in part, because of the influence of jihadist websites, YouTube channels, and social-networking groups, all of which have taken the place of physical meeting spaces. Just as disparate human-rights groups identify with various umbrella causes to which they belong through their immersion in social-networking services and chat platforms, so too do jihadists and militants mobilize around a common "imagined community" that is nurtured online.

Perhaps even more challenging to the liberal-democratic vision of liberation technology is that much of what is considered criminal and antisocial behavior online increasingly originates from the young online populations in developing and postcommunist countries, many of whom live under authoritarianism and suffer from structural economic inequalities. For these young "digital natives," operating an email scam or writing code for botnets, viruses, and malware represents an opportunity for economic advancement. It is an avenue for tapping into global supply chains and breaking out of conditions of local poverty and political inequality—itself a form of liberation.

In other words, regardless of whatever specific characteristics observers attribute to certain technologies, human beings are unpredictable and innovative creatures. Just because a technology has been invented for one purpose does not mean that it will not find other uses unforeseen by its creators. This is especially true in the domains of crime, espionage, and civil conflict, where innovation is not encumbered by formal operating procedures or respect for the rule of law.

Enclosing the Commons: Next-Generation Controls

Arguments linking new technologies to "liberation" must also be qualified due to the ongoing development of more sophisticated cyberspace controls. Whereas it was once considered impossible for governments to control cyberspace, there are now a wide variety of technical and nontechnical means at their disposal to shape and limit the online flow of information. Like the alternative rationalities described above, these can often escape the attention of the media and other observers. But these control mechanisms are growing in scope and sophistication as part of a general paradigm shift in cyberspace governance and an escalating arms race in cyberspace.

To understand cyberspace controls, it is important first to consider a sea-change in the ways in which governments approach the domain. During the "dot-com" boom of the 1990s, governments generally took a hands-off approach to the Internet by adhering to a *laissez-faire* eco-

nomic paradigm, but a gradual shift has since occurred. While market ideas still predominate, there has been a growing recognition of serious risks in cyberspace.

The need to manage these risks has led to a wave of securitization efforts that have potentially serious implications for basic freedoms.[12] For example, certain security measures and regulations have been put in place for purposes of copyright and intellectual-property protection. Although introduced as safeguards, these regulations help to legitimize government intervention in cyberspace more generally—including in countries whose regimes may be more interested in self-preservation than in property protections. If Canada, Germany, Ireland, or another industrialized democracy can justifiably regulate behavior in cyberspace in conformity with its own national laws, who is to say that Belarus, Burma, Tunisia, or Uzbekistan cannot do the same in order to protect state security or other national values?

The securitization of cyberspace has been driven mainly by a "defensive" agenda—to protect against threats to critical infrastructures and to enable law enforcement to monitor and fight cybercrime more effectively. There are, however, those who argue that "offensive" capabilities are equally important. In order to best defend key infrastructures, the argument goes, governments must also understand how to wage attacks, and that requires a formal offensive posture. Most of the world's armed forces have established, or are in the process of establishing, cyber-commands or cyberwarfare units. The most ambitious is the U.S. Cyber Command, which unifies U.S. cyber-capabilities under a separate command led by General Keith Alexander of the National Security Agency. Such an institutional innovation in the armed forces of the world's leading superpower provides a model for similar developments in other states' armed forces, who feel the need to adapt or risk being left behind.

Not surprisingly, there have been a growing number of incidents of computer-network attacks for political ends in recent years, including those against Burmese, Chinese, and Tibetan human-rights organizations, as well as political-opposition groups in the countries of the former Soviet Union. It would be disingenuous to draw a direct line between the establishment of the U.S. Cyber Command and these incidents, especially since many of these practices have been pioneered through innovative and undeclared public-private partnerships between intelligence services in countries such as Burma, China, and Russia and their emergent cybercriminal underclasses. Yet it is fair to argue that the former sets a normative standard that allows such activities to be tolerated and even encouraged. We should expect these kinds of attacks to grow as governments explore overt and declared strategies of offensive action in cyberspace.

Further driving the trend toward securitization is the fact that private-sector actors, who bear the brunt (and costs) of defending cyberspace's

critical infrastructures against a growing number of daily attacks, are increasingly looking to their own governments to carry this burden as a public good. Moreover, a huge market for cybersecurity services has emerged, estimated to generate between US$40 and $60 billion annually in the United States alone. Many of the companies that now fill this space stand to gain by fanning the flames of cyberwar. A few observers have questioned the motivations driving the self-serving assessments that these companies make about the nature and severity of various threats.[13] Those criticisms are rare, however, and have done little to stem fear-mongering about cybersecurity.

This momentum toward securitization is helping to legitimize and pave the way for greater government involvement in cyberspace. Elsewhere, we have discussed "next generation" controls—interventions that go beyond mere filtering, such as those associated with the Great Firewall of China.[14] Many of these controls have little to do with technology and more to do with inculcating norms, inducing compliant behavior, and imposing rules of the road, and they stem from a multitude of motivations and concerns. Any argument for the liberating role of new technologies needs to be evaluated in the wider context of these next-generation controls.

Legal measures. At the most basic level, government interventions in cyberspace have come through the introduction of slander, libel, copyright-infringement, and other laws to restrict communications and online activities.[15] In part, the passage of such laws reflects a natural maturation process, as authorities seek to bring rules to cyberspace through regulatory oversight. Sometimes, however, it also reflects a deliberate tactic of strangulation, since threats of legal action can do more to prevent damaging information from surfacing than can passive filtering methods implemented defensively to block websites. Such laws can create a climate of fear, intimidation, and ultimately self-censorship.

Although new laws are being drafted to create a regulatory framework for cyberspace, in some cases old, obscure, or rarely enforced regulations are cited *ex post facto* to justify acts of Internet censorship, surveillance, or silencing. In Pakistan, for example, old laws concerning "blasphemy" have been used to ban access to Facebook, ostensibly because there are Facebook groups that are centered around cartoons of Muhammad.[16] Governments have also shown a willingness to invoke national-security laws to justify broad acts of censorship. In Bangladesh, for example, the government blocked access to all of YouTube because of videos clips showing Prime Minister Sheikh Hasina defending her decision to negotiate with mutinous army guards. The Bangladesh Telecommunications Commission chairman, Zia Ahmed, justified the decision by saying: "[T]he government can take any decision to stop any activity that threatens national unity and integrity."[17] In Lebanon,

infrequently used defamation laws were invoked to arrest three Facebook users for posting criticisms of the Lebanese president, in spite of constitutional protections of freedom of speech.[18] In Venezuela, several people were arrested recently after posting comments on Twitter about the country's banking system. The arrests were made based on a provision in the country's banking laws that prohibits the dissemination of "false information."[19] Numerous other examples could be cited that together paint a picture of growing regulatory intervention into cyberspace by governments, shaping and controlling the domain in ways that go beyond technical blocking. Whereas at one time such regulatory interventions would have been considered exceptional and misguided, today they are increasingly becoming the norm.

Informal requests. While legal measures create the regulatory context for denial, for more immediate needs, authorities can make informal "requests" of private companies. Most often such requests come in the form of pressure on Internet service providers (ISPs) and online hosting services to remove offensive posts or information that supposedly threatens "national security" or "cultural sensitivities." Google's recent decision to reconsider its service offerings in China reflects, in part, that company's frustration with having to deal with such informal removal requests from Chinese authorities on a regular basis. Some governments have gone so far as to pressure the companies that run the infrastructure, such as ISPs and mobile phone operators, to render services inoperative in order to prevent their exploitation by activists and opposition groups.

In Iran, for example, the Internet and other telecommunications services have slowed down during public demonstrations and in some instances have been entirely inaccessible for long periods of time or in certain regions, cities, and even neighborhoods. While there is no official acknowledgement that service is being curtailed, it is noteworthy that the Iranian Revolutionary Guard owns the main ISP in Iran—the Telecommunication Company of Iran (TCI).[20] Some reports indicate that officials from the Revolutionary Guard have pressured TCI to tamper with Internet connections during the recent crises. In authoritarian countries, where the lines between public and private authorities are often blurred or organized crime and government authority mingle in a dark underworld, such informal requests and pressures can be particularly effective and nearly impossible to bring to public account.

Outsourcing. It is important to emphasize that cyberspace is owned and operated primarily by private companies. The decisions taken by those companies about content controls can be as important as those taken by governments. Private companies often are compelled in some manner to censor and surveil Internet activity in order to operate in a particular jurisdiction, as evidenced most prominently by the collusion

of Google (up until January 2010), Microsoft, and Yahoo in China's Internet censorship practices. Microsoft's Bing, which tailors its search engine to serve different countries and regions and offers its services in 41 languages, has an information-filtering system at the keyword level for users in several countries. According to research by the OpenNet Initiative's Helmi Noman, users located in the Arab countries where he tested are prevented from conducting Internet searches relating to sex and other cultural norms in both Arabic and English. Microsoft's explanation as to why some search keywords return few or no results states, "Sometimes websites are deliberately excluded from the results page to remove inappropriate content as determined by local practice, law, or regulation." It is unclear, however, whether Bing's keyword filtering in the Arab world is an initiative of Microsoft or whether any or all of the Arab states have asked Microsoft to comply with local censorship practices and laws.[21]

In some of the most egregious cases, outsourced censorship and monitoring controls have taken the form either of illegal acts or of actions contrary to publicly stated operating procedures and privacy protections. This was dramatically illustrated in the case of Tom-Skype, in which the Chinese partner of Skype put in place a covert surveillance system to track and monitor prodemocracy activists who were using Skype's chat function as a form of outreach. The system was discovered only because of faulty security on the servers operated by Tom Online. In May 2009, the Chinese government introduced new laws that required personal-computer manufacturers to bundle a filtering software with all of the computers sold in the country. Although this was strongly resisted by many companies, others willingly complied. While this requirement seems to have faded over time, it is nonetheless indicative of the types of actions that governments can take to control access points to cyberspace via private companies.

Access points such as Internet cafes are becoming a favorite regulatory target for authoritarian governments. In Belarus, ISPs and Internet cafes are required by law to keep lists of all users and turn them over to state security services.[22] Many other governments have similar requirements. In light of such regulations, it is instructive to note that many private companies collect user data as a matter of course and reserve the right in their end-user license agreement to share such information with any third party of their choosing.

Presumably, there are many still undiscovered acts of collusion between companies and governments. For governments in both the developed and developing worlds, delegating censorship and surveillance to private companies keeps these controls on the "frontlines" of the networks and coopts the actors who manage the key access points and hosting platforms. If this trend continues, we can expect more censorship and surveillance responsibilities to be carried out by private com-

panies, carrier hotels (ISP co-location centers), cloud-computing services, Internet exchanges, and telecommunications companies. Such a shift in the locus of controls raises serious issues of public accountability and transparency for citizens of all countries. It is in this context that Google's dramatic announcement to end censorship of its Chinese search engine should be considered a watershed moment. Whether other companies follow Google's lead, and how China, other countries, and the international community as a whole will respond, are critical open questions that may help to shape the public accountability of private actors in this domain.

"Just-in-time blocking." Disabling or attacking critical information assets at key moments in time—during elections or public demonstrations, for example—may be the most effective tool for influencing political outcomes in cyberspace. Today, computer-network attacks, including the use of distributed denial-of-service attacks, can be easily marshaled and targeted against key sources of information, especially in the developing world, where networks and infrastructure tend to be fragile and prone to disruption. The tools used to mount botnet attacks are now thriving like parasites in the peer-to-peer architectures of insecure servers, personal computers, and social-networking platforms. Botnets can be activated against any target by anyone willing to pay a fee. There are cruder methods of just-in-time blocking as well, such as shutting off power in the buildings where servers are located or tampering with domain-name registration so that information is not routed to its proper destination. This kind of just-in-time blocking has been empirically documented by the OpenNet Initiative in Belarus, Kyrgyzstan, and Tajikistan, as well as in numerous other countries.

The attraction of just-in-time blocking is that information is disabled only at key moments, thus avoiding charges of Internet censorship and allowing for plausible denial by the perpetrators. In regions where Internet connectivity can be spotty, just-in-time blocking can be easily passed off as just another technical glitch with the Internet. When such attacks are contracted out to criminal organizations, determining attribution of those responsible is nearly impossible.

Patriotic hacking. One unusual and important characteristic of cyberspace is that individuals can take creative actions—sometimes against perceived threats to their country's national interest—that have system-wide effects. Citizens may bristle at outside interference in their country's internal affairs or take offense at criticism directed at their governments, however illegitimate those governments may appear to outsiders. Those individuals who possess the necessary technical skills have at times taken it upon themselves to attack adversarial sources of information, often leaving provocative messages and warnings behind. Such

actions make it difficult to determine the provenance of the attacks: Are they the work of the government or of citizens acting independently? Or are they perhaps some combination of the two? Muddying the waters further, some government security services informally encourage or tacitly approve of the actions of patriotic groups.

In China, for example, the Wu Mao Dang, or 50 Cent Party (so named for the amount of money its members are supposedly paid for each Internet post), patrols chatrooms and online forums, posting information favorable to the regime and chastising its critics. In Russia, it is widely believed that the security services regularly coax hacker groups to fight for the motherland in cyberspace and may "seed" instructions on prominent nationalist websites and forums for hacking attacks. In late 2009 in Iran, a shadowy group known as the Iranian Cyber Army took over Twitter and some key opposition websites, defacing the home pages with their own messages. Although no formal connection to the Iranian authorities has been established, the groups responsible for the attacks posted pro-regime messages on the hacked websites and services.

Targeted surveillance and social-malware attacks. Accessing sensitive information about adversaries is one of the most important tools for shaping political outcomes, and so it should come as no surprise that great effort has been devoted to targeted espionage. The Tom-Skype example is only one of many such next-generation methods now becoming common in the cyber-ecosystem. Infiltration of adversarial networks through targeted "social malware" (software designed to infiltrate an unsuspecting user's computer) and "drive-by" Web exploits (websites infected with viruses that target insecure browsers) is exploding throughout the dark underbelly of the Internet. Among the most prominent examples of this type of infiltration was a targeted espionage attack on Google's infrastructure, which the company made public in January 2010.

These types of attacks are facilitated by the careless practices of civil society and human-rights organizations themselves. As Nart Villeneuve and Greg Walton have shown in a recent Information Warfare Monitor report, many civil society organizations lack simple training and resources, leaving them vulnerable to even the most basic Internet attacks.[23] Moreover, because such organizations generally thrive on awareness-raising and advocacy through social networking and email lists, they often unwittingly become compromised as vectors of attacks, even by those whose motivations are not political per se. In one particularly egregious example, the advocacy group Reporters Without Borders unknowingly propagated a link to a malicious website posing as a Facebook petition to release the Tibetan activist Dhondup Wangchen. As with computer network attacks, targeted espionage and social-malware attacks are being developed not just

by criminal groups and rogue actors, but also at the highest levels of government. Dennis Blair, the former U.S. director of national intelligence, recently remarked that the United States must be "aggressive" in the cyberdomain in terms of "both protecting our own secrets and stealing those of others."[24]

A Nuanced Understanding

There are several theoretical and policy implications to be drawn from the issues we raise. First, there needs to be a much more nuanced understanding of the complexity of the communications space in which we operate. We should be skeptical of one-dimensional or ahistorical depictions of technologies that paint them with a single brush. Cyberspace is a domain of intense competition, one that creates an ever-changing matrix of opportunities and constraints for social forces and ideas. These social forces and ideas, in turn, are imbued with alternative rationalities that collide with one another and affect the structure of the communications environment. Unless the characteristics of cyberspace change radically in the near future and global culture becomes monolithic, linking technological properties to a single social outcome such as liberation or control is a highly dubious exercise.

Second, we must be cautious about promoting policies that support "freedom" software or other technologies presented as magic solutions to thorny political problems. Early on, the Internet was thought to be a truly democratic arena beyond the reach of government control. Typically, the examples used to illustrate this point related to heavy-handed attempts to filter access to information, which are relatively easy to bypass. This conventional wisdom has, in turn, led to efforts on the part of governments to sponsor "firewall-busting" programs and to encourage technological "silver bullets" that will supposedly end Internet censorship once and for all. This viewpoint is simplistic, as it overlooks some of the more important and powerful next-generation controls that are being employed to shape the global commons. Liberation, freedom, and democracy are all socially contested concepts, and thus must be secured by social and political means. Although the prudent support of technological projects may be warranted in specific circumstances, they should be considered as adjuncts to comprehensive strategies rather than as solutions in and of themselves. The struggles over freedom of speech, access to information, privacy protections, and other human-rights issues that now plague cyberspace ultimately pose political problems that are grounded in deeply rooted differences. A new software application, no matter how ingenious, will not solve these problems.

Third, we need to move beyond the idea that cyberspace is not regulated or is somehow immune to regulation. Nothing could be further from the truth. If anything, cyberspace is overregulated by the multitude of actors whose decisions shape its character, often in ways that lack transparency and public accountability. The question is not *whether* to regulate cyberspace, but rather *how* to do so—within which forum, involving which actors, and according to which of many competing values. The regulation of cyberspace tends to take place in the shadows, based on decisions taken by private actors rather than as a result of public deliberation. As the trend toward the securitization and privatization of cyberspace continues, these problems are likely to become more, rather than less, acute.

Finally, for the governance of cyberspace to be effective, it must uncover what is going on "below the surface" of the Internet, largely invisible to the average user. It is there that most of the meaningful limits on action and choice now operate, and they must be unearthed if basic human rights are to be protected online. These subterranean controls have little to do with technology itself and more to do with the complex nature of the communications space in which we find ourselves as we enter the second decade of the twenty-first century. Meaningful change will not come overnight with the invention of some new technology. Instead, it will require a slow process of awareness-raising, the channeling of ingenuity into productive avenues, and the implementation of liberal-democratic restraints.

NOTES

1. Larry Diamond, "Liberation Technology," *Journal of Democracy* 21 (July 2010): 70–84.

2. Elia Zureik et al., eds., *Surveillance, Privacy, and the Globalization of Personal Information* (McQuill-Queen's University Press, 2010).

3. Our conception of "alternative rationalities" is inspired by Ulrich Beck et al., *Reflexive Modernization* (Cambridge: Polity, 1994). The concept of alternative rationalities has its origins in Max Weber's work and is further developed in critical and postmodern theories.

4. For the concept of "dynamic density," see John Gerard Ruggie, "Continuity and Transformation in the World Polity: Toward a Neorealist Synthesis," *World Politics* 35 (January 1983): 261–85.

5. A. Claire Cutler, Virginia Haufler, and Tony Porter, *Private Authority and International Affairs* (New York: SUNY Press, 1999).

6. Ronald J. Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge: MIT Press, 2010).

7. See, for example, "Iran's Twitter Revolution," *Washington Times,* 16 June 2009; available at *www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution.*

8. Chrisanthi Avgerou, "Recognising Alternative Rationalities in the Deployment of Information Systems," *Electronic Journal of Information Systems in Developing Countries* 3 (2000); available at *www.ejisdc.org/ojs2/index.php/ejisdc/article/view/19.*

9. Rafal Rohozinski, "Bullets to Bytes: Reflections on ICTs and 'Local' Conflict," in Robert Latham, ed., *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security* (New York: New Press, 2003), 222.

10. Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0,* JR03-2010, 6 April 2010; Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network,* JR02-2009, 29 March 2009.

11. Ronald Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 South Ossetia War," ms. forthcoming.

12. Ronald Deibert and Rafal Rohozinski, "Risking Security: The Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4 (March 2010): 15–32.

13. Stephen Walt, "Is the Cyber Threat Overblown?" *Foreign Policy,* 3 March 2010; available at *http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.*

14. Deibert et al., *Access Controlled.*

15. The following section draws from an earlier article of ours: "Cyber Wars," Index on Censorship, March 2010; available at *www.indexoncensorship.org/2010/03/cyber-wars-technology-deiber.*

16. See *http://en.rsf.org/pakistan-court-orders-facebook-blocked-19-05-2010,37524.html.*

17. See *www.telegraph.co.uk/news/worldnews/asia/bangladesh/4963823/YouTube-blocked-in-Bangladesh-after-guard-mutiny.html.*

18. See *www.guardian.co.uk/commentisfree/libertycentral/2010/jul/03/lebanon-facebook-president-insult.*

19. See *www.latimes.com/technology/sns-ap-lt-venezuela-twitter,0,6311483.story.*

20. "IRGC Consortium Takes Majority Equity in Iran's Telecoms," 5 October 2009, *www.zawya.com/story.cfm/sidv52n40-3NC06/IRGC%20Consortium%20Takes%20Majority%20Equity%20In%20Iran%26rsquo%3Bs%20Telecoms.*

21. See *http://opennet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabian-countries.*

22. See *http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article1391469.ece.*

23. See *www.infowar-monitor.net/2009/10/0day-civil-society-and-cyber-security.*

24. See *www.govinfosecurity.com/p_print.php?t=a&id=1786.*

3

INTERNATIONAL MECHANISMS OF CYBERSPACE CONTROLS

Ronald Deibert

***Ronald Deibert** is professor of political science and director of the Canada Centre for Global Security Studies and the Citizen Lab at the University of Toronto's Munk School of Global Affairs. He is a cofounder and a principal investigator of the OpenNet Initiative and Information Warfare Monitor projects. His forthcoming book (with Rafal Rohozinski) is* Ghost in the Machine: The Battle for the Future of Cyberspace.

One of the burgeoning areas of Internet research is the study of cyberspace controls—the implementation of government-mandated or privately implemented filtering, surveillance, and other means of shaping cyberspace for strategic ends. Whereas it was once assumed that cyberspace was immune to government regulation because of its swiftly changing nature and distributed architecture, a growing body of scholarship has shown convincingly how governments can shape and constrain access to information and freedom of speech online within their jurisdictions.

Today, more than thirty countries engage in Internet filtering, not all of them authoritarian regimes.[1] Internet-surveillance policies are now widespread and bearing down on the private-sector companies that own and operate the infrastructure of cyberspace, including Internet Service Providers (ISPs). Likewise, a new generation of second- and third-order controls complements filtering and surveillance, creating a climate of self-censorship.[2] There is a very real arms race in cyberspace that threatens to subvert the Internet's core characteristics and positive network effects.

The study of cyberspace controls has tended to focus on the nation-state as the primary unit of analysis, and has examined the deepening and widening of these controls within domestic contexts. For example, the leading international research organization dedicated to studying Internet filtering—the OpenNet Initiative (ONI)—has published an annual

series of country and regional reports that are based on an empirical examination of country-level controls.[3] Its reports have become touchstones for information and analysis of Internet filtering and are important empirical contributions to the study of cyberspace controls.

Largely unexamined so far, however, are the *international* dynamics by which such controls—and the resistance to them—may spread. These dynamics and mechanisms are important to consider because states do not operate in a vacuum; they are part of an international system that has important implications for what they do and how they behave. This can have both "positive" and "negative" characteristics.[4] In a positive sense, states learn from and imitate each other. They borrow and share best practices, skills, and technologies. They take cues from what like-minded states are doing and implement policies accordingly.

On the negative side, states compete against one another. Their perceptions of adversarial intentions and threats can affect the decisions that they take. This dynamic has been characterized in the international-relations literature as the logic of the "security dilemma." One can see this logic at work today in the domain of cyberspace with the development of national military capabilities to fight and win wars in cyberspace.

The international system also comprises transnational actors—namely, civil society networks and private-sector firms—that serve as conduits and propagators of ideas and policies. Civil society networks educate users within countries about best practices and networking strategies, and operate largely irrespective of national boundaries.[5] The networks that tend to get the most attention are those promoting human rights, such as access to information, freedom of speech, and privacy rights. These networks come in a variety of shapes and sizes. Some are independent and largely grassroots in origin; others have been drawn into a support structure synchronized to the foreign-policy goals of major powers such as the United States and the European Union. But very few of them, especially the more important ones, operate only in a domestic policy setting.

Private-sector actors are responsive to and seek to develop commercial opportunities across national boundaries, and they are increasingly a part of the international system's mechanisms and dynamics of cyberspace controls. Particularly relevant in this respect is the cybersecurity market, estimated at up to US$80 billion annually. Commercial providers of networking technology have a stake in the securitization of cyberspace and can inflate threats to serve their more parochial market interests.[6] Private actors also own and operate the vast majority of the infrastructure and services that we call cyberspace. For that reason alone, the decisions that they take can have major consequences for the character of cyberspace worldwide. It is not too far a stretch to argue that some companies have the equivalent of "foreign policies" for cyberspace, in some ways going beyond individual governments in terms of scope and influence.

In this chapter, I first provide a brief summary of prior research on cyberspace controls, drawing primarily from the experiences of the ONI. I then lay out a research framework for the study of international mechanisms and dynamics of cyberspace controls. The aim is not to provide an exhaustive analysis of these mechanisms and dynamics as much as it is to sketch out a conceptual and analytical framework for further research. I lay out several areas where such mechanisms and dynamics might be found and investigated further. I turn in the conclusion to a consideration of some of the reasons why further research in this area is important for the study of cyberspace.

From Access Denied to Access Controlled

Studies of cyberspace controls have developed and matured as these practices have spread worldwide. Early in the Internet's history, it was widely assumed that the Internet was difficult for governments to manage and would bring about major challenges to authoritarian forms of rule. Over time, however, these assumptions have been called into question, as governments (often in coordination with the private sector) have erected a variety of information controls. It is now fair to say that there is a growing norm worldwide for national Internet filtering, although the rationale for implementing filtering varies widely from country to country.

Some justify Internet filtering to control access to content that violates copyright, exploits children, or promotes hatred and violence. Other countries filter access to content related to minority rights, religious movements, political opposition, and human-rights groups. Levels of government transparency and accountability as well as the filtering methods themselves vary broadly across the globe. Invariably, the private-sector actors who own and operate the vast majority of cyberspace infrastructure are being compelled or coerced to implement controls on behalf of states. In short, a sea change has occurred over the last decade in terms of cyberspace controls. But how did these norms of cyberspace control spread internationally?

The most authoritative research on Internet filtering is from the ONI, which uses a combination of technical interrogation, field research, and data-analysis methods to test for filtering in more than sixty countries on an annual basis.[7] The ONI's methods were developed very much in response to the predominant question circulating at the time of its inception (2002): Could governments control access to information online within their jurisdictions? To answer this question, the ONI built a global-level, but nationally based, testing regime. Researchers from the ONI download specially designed software that connects back to databases

at the University of Toronto. The databases contain categorized lists of URLs, domains, keywords, and Internet services that are tested on a regular basis across each of the major ISPs of each of the countries under consideration. The categorized lists are broken down into two main groups: 1) a global list, which is tested in all countries and is used as a basis to make comparative judgments across countries; and 2) a "local" or "high-impact" list that contains URLs, domains, and keywords that are relatively unique to a particular country context and are suspected of being targeted for filtering in that jurisdiction.

The ONI reports provide a "snapshot" of accessibility at the time of testing from the perspective of national information environments. Among the findings of the ONI is that Internet filtering is growing in scope, scale, and sophistication. The latest ONI reports indicate that more than thirty countries engage in some form of Internet filtering, a growing number of them being democratic, industrialized countries. The ONI has also presented evidence of the range of techniques that states employ to filter access to information. Some of the nondemocratic regimes that engage in Internet filtering do so using commercial filtering products developed in the United States. Others have developed more homegrown solutions.

The ONI has also captured the range of transparency practices through its research. Some states provide "block pages" for banned content that explain the rationale and legal basis for the blocking; others provide only error pages, some of which are misleading and meant to obscure the states' intentions. The ONI has also subjected Internet services to scrutiny, in particular comparing the results obtained from major search engines by requests in different countries. This has helped to expose the collusion of Internet companies with regimes that violate human rights, while putting pressure on those companies to become more accountable.

Recently, ONI researchers have described growing trends away from "Chinese-style" firewall-based filtering to more subtle and fluid forms of information control.[8] The ONI describes these as "next-generation" methods of cyberspace controls; they include pressures on the commercial sector, outsourcing controls to private actors, and more offensive methods, such as just-in-time attacks on key information sources and targeted malware against opposition or adversarial groups. ONI researchers have noted that these new and subtle forms of information control challenge the ONI's core methodology and are difficult to document empirically.

International Mechanisms and Dynamics

What is missing from the ONI's research, as well as from the growing body of scholarship on cyberspace controls, is a consideration of the *international* mechanisms and dynamics of such controls. The field of

international relations is premised on the notion that there are factors that affect state behavior at the international systemic level. Put simply, states are embedded in an international order that affects what they do and how they do it. Although some of this scholarship has been rightly criticized in the past for reifying the international system and ignoring domestic-level processes, it nonetheless identifies an important dimension of political behavior that needs to be considered.[9] States' policies are formed in interaction with other states in the international system. However much domestic struggles and local threats motivate what states do, their interactions with one another, their perceptions of adversarial actions and intentions, and their placement in the international order matter as well.

International institutions. The most obvious places to look for such international dynamics are the main forums of Internet governance: the International Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union (ITU), the Internet Governance Forum (IGF), and others. These international institutions are important touchstones for the identification of the mechanisms and dynamics that interest us here.[10] They have been studied by scholars of Internet governance who have examined the stakeholders, processes, and policy outputs of these various forums in detail for many years.[11] Yet these institutions are increasingly under new pressures as governments assert themselves more forcefully in cyberspace. As a consequence, the main issues that are addressed in these forums are changing, and previously unpoliticized or mostly technical issues are becoming the objects of intense political competition. These institutions, which may have been dismissed in the past as irrelevant or overly technical, deserve renewed attention from scholars, if only because some governments are now taking them seriously as vectors of policy formation and propagation.

For example, a loose coalition of like-minded countries has begun to develop strategic engagements with international institutions such as the ITU and the IGF in ways that are quite novel. Most strikingly, Russia and the Russian-speaking countries of the former Soviet Union have adopted a wide-ranging engagement with these forums to promote policies that synchronize with national-level laws related to information security.[12] Recently, China has explicitly stated not only that states have sovereign control over national information space, but also that global cyberspace should be governed by international institutions operating under the United Nations.[13] Not surprisingly, policies reflecting these views have been vocally supported by Hamadoun Touré, the secretary-general of the ITU, who has called for a state-based cyberarms-control treaty that would imply significant renationalization of the Internet.[14] He has also been a vocal supporter of India, Indonesia, the United Arab Emirates (UAE), and other countries that have pressured companies like

Research In Motion (RIM), the Canadian maker of Blackberry products, to share encrypted data under the rubric of national-security protections.[15] Every year since 1998, Russia has put forward resolutions at the United Nations to prohibit "information aggression," which is widely interpreted to mean ideological attempts—or the use of ideas—to undermine regime stability.[16] At least 23 countries now openly support Russia's interpretation of information security.

Sometimes engagement at these forums is intended to stifle or stonewall instead of to promote certain policies. For example, Chinese delegations have been quite prominent at IGF meetings, ironically as a means to stall this forum from gaining credibility and to undermine the broadening of Internet governance to civil society and other nonstate stakeholders. At the November 2009 IGF meeting in Egypt, for example, UN security officials disrupted a book launch of the ONI's recent volume, *Access Controlled*, because the Chinese delegation objected to a poster that contained a reference to the "Great Firewall of China."[17] The propagation of norms internationally can be facilitated not only by promoting them but also by the obstruction of contrary tendencies.

What is perhaps most interesting is that the international institutions whose missions are primarily focused on the technical coordination of the Internet—ICANN, the Internet Assigned Numbers Authority (IANA), and the regional naming authorities—have become increasingly politicized and subject to securitization pressures. For example, attendees at recent meetings of regional Internet registries have noticed the presence of government military and intelligence personnel in ways that are largely unprecedented. Governments whose strategic interests are oriented around legitimization of national controls are viewing these technical forums, once generally ignored except by specialists, as important components of a broader, more comprehensive policy engagement. For example, a coalition of Russian-speaking countries, supported by China and India, has put forward a proposal through a submeeting of the ITU to give governments veto power over ICANN decisions.[18]

Generally speaking, these countries are seen as attempting to reassert the legitimacy of national sovereign control over cyberspace by promoting such a norm at international venues. Ironically, in other words, international institutions are perceived by policy makers of these countries as vehicles of nationalization.

Policy coordination through regional organizations. Although international institutions are important conduits of norm propagation and legitimization, they can also be unwieldy and diffuse. As a consequence, coalitions of like-minded states are increasingly operating through more manageable lower-level organizations, such as regional institutions. Some of these forums attract little attention and meet in relative obscurity. Thus the actions that they take rarely see the light of day and are

ignored or overlooked by activists and others concerned with Internet freedom and cyberspace governance. But the participants treat them seriously and use them as vehicles of policy coordination and information-sharing.

One example is the Shanghai Cooperation Organization (SCO), a regional organization made up of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan.[19] India, Iran, Mongolia, and Pakistan have observer status, and Belarus and Sri Lanka are considered "dialogue partners." Iran is engaged in the SCO but prevented from formally joining because of UN sanctions. It is considered an active participant in the SCO summits, however, which have been held regularly throughout the region since the early 2000s. The SCO aims to share information and coordinate policies around a broad spectrum of cultural, economic, and security concerns, among them cyberspace policies. In 2010, the SCO issued a statement on "information terrorism" that drew attention to the way in which these countries have a shared and distinct perspective on Internet-security policy. The SCO has also engaged in joint military exercises and missions, described by some observers as simulations of how to reverse "color" revolutions and popular uprisings.[20] Unfortunately, the SCO's meetings tend to be highly secretive affairs and thus not easily subject to outside scrutiny. But they are likely to become important vehicles of policy coordination, giving unity, normative coherence, and strength to the individual countries beyond the sum of their parts.

Bilateral cooperation. Norms can diffuse internationally in the most direct way by governments sharing resources and expertise with each other in bilateral relationships. There has been longstanding speculation that China and Chinese companies are selling technology to regimes that import China's filtering and surveillance system. For example, officials from China's IT ministry recently visited Sri Lanka, ostensibly to offer advice on how to filter the Internet.[21] These discussions and arrangements are rarely transparent, however, and are typically shrouded in the type of secrecy that accompanies matters of national security, law enforcement, and intelligence. They are likely to become more important vehicles for the promotion of these states' strategic interests as they seek to propagate practices internationally that are supportive of their own domestic policies.

Informal Mechanisms

Although these forums and bilateral relations are important, by no means do they exhaust the dynamics and mechanisms of cyberspace controls at play in the international system. Here it is important to underline the many different means by which norms, behaviors, and policies are propagated internationally. Although formal sites of governance such as

those above are important, norms can propagate through the international system in a variety of ways. Norm diffusion is the process through which norms are socialized and shared and then become internalized, accepted, and implemented by national actors. This process is uneven and mixed, and can vary in different contexts depending on the depth to which the norm penetrates societies. Norms enter into and are accepted into national contexts depending on preexisting belief systems of a national society that support or constrain their acceptance. Norms can be propagated internationally by norm entrepreneurs (transnational actors, NGOs, and businesses acting as conveyor belts or conduits) or through imitation, learning, socialization, and competition.[22] The latter processes are often difficult to document empirically because of their epistemic or cognitive foundations, but they are important factors in explaining the spread and adoption of policies such as Internet filtering. To understand the growth of cyberspace controls over the last decade, we need to better understand the mechanisms and dynamics of this diffusion internationally.

Imitation and learning. Among international-relations theories of all stripes, there is a basic understanding that government policies are formed on the basis of dynamic relations with other states in the international system.[23] Governments are outward-looking as much as they are inward-looking. When one government sees another doing something, pressures may build to do likewise or risk being left behind. Studies of learning and imitation in the field of international relations offer a number of hypotheses and data that can be collected and imported into the study of cyberspace controls.[24] A wealth of anecdotes suggests that this is a potentially fruitful area of inquiry.

In the most elemental sense, states learn from and imitate each other's behaviors, practices, and policies. They borrow and share best practices, skills, and technologies. They take cues from what like-minded states are doing and implement policies accordingly. Fear and "self-help" are among the most important and perennial drivers of imitation and learning. States implement policies based on reactions to what other governments are doing for fear of being left behind or overtaken by adversaries. A current example of such a dynamic can be seen clearly in the rush by many countries to pressure RIM to cooperate with local law-enforcement and intelligence agencies. After the UAE went public with its concerns that RIM might have made an arrangement with the U.S. National Security Agency that the UAE wanted extended to its own security services, numerous other governments chimed in and joined the queue, including Bahrain, India, Indonesia, and Saudi Arabia.[25]

The most intense forms of imitation and learning occur around national-security issues because of the high stakes and urgency involved. For example, in reaction to revelations of Chinese-based cyberespionage against U.S. companies and government agencies, Dennis Blair, the former U.S. director of national intelligence, argued that the United States needs to be more aggressive in stealing other countries' secrets. After major compromises to the Indian national-security and defense establishment were traced back to the Chinese criminal underground, some members of the Indian government proposed legislation to give a safe haven and stamp of approval for Indian hackers to do the same.[26] India also blocked imports of Chinese telecommunications equipment, and moved swiftly to set up cyberwarfare capabilities within its armed forces.[27] In what will be no surprise to international-relations theorists, we are now entering into a classic "security-dilemma," arms-race spiral in cyberspace, as dozens of governments look to other states' actions to justify the need to set up or bolster offensive cyberwarfare capabilities. The message sent by the establishment of the U.S. Cyber Command cannot be overemphasized in this regard. Such an institutional innovation in the armed forces of the world's largest superpower sends a major signal to the international defense community.

The imitation and learning process is not uniform, but mixes with national interests and local culture to create a warp and woof.[28] Governments can look to other states in the international system to lend legitimacy to slightly modified or even altogether different policies. For example, after the United States and other industrialized countries adopted antiterror legislation, many countries of the Commonwealth of Independent States (CIS) did likewise. Their policies, however, were much more far-reaching and oriented toward the stifling of minority-independence and political-opposition movements and the shoring up of regime stability rather than to fighting international terrorism.

A similar process can be seen in the spread of cybercrime and copyright-protection legislation. Under the umbrella of an international norm intended for one purpose, states can justify policies and actions that serve more parochial aims. Russia and other authoritarian regimes have used the excuse of copyright policing to seize opposition and NGO computers—in at least once instance with the assistance of companies like Microsoft.[29] Similarly, the now widespread belief that it is legitimate to remove videos containing "offensive" information from websites can be interpreted broadly in various national contexts. Pakistani authorities have repeatedly pressured video-hosting services to remove embarrassing or politically inflammatory videos under this rubric.

Some regimes that are geographically remote appear to be learning from one another's "best practices" when it comes to dealing with cyberspace controls over opposition groups. For example, a growing list of countries have banned SMS and instant-messaging services prior to national crises or significant events such as elections or public demonstrations. Although it is possible that each of these countries is doing

so in isolation, it seems more likely that they have been inspired by the actions of other countries. Cambodia,[30] Egypt,[31] India,[32] Iran,[33] Mozambique,[34] and Turkmenistan,[35] have all disabled SMS and text messaging during or leading up to recent elections, events, and public demonstrations as a way to control social mobilization.

Imitation and learning are major components of norm propagation, but they are processes that are difficult to document empirically. Unless government representatives or policy makers specifically point to an instance or act from which they are drawing inspiration, imitation and learning processes can be obscure and have to be deduced from behavior.

Commercial conduits. Norms can spread internationally via private actors, in particular companies offering a service that supports the norm. For example, a major market for cybersecurity tools and technologies has exploded in recent years, estimated at between $60 and 80 billion annually. Companies are naturally gravitating to this expanding market in response to commercial opportunities. But they can also influence the market itself by the creation of products and tools that present new opportunities for states. There are, for example, a wide range of new products that offer "deep packet inspection" and traffic-shaping capabilities, even though such activities are contrary to fading norms of "network neutrality." There are also companies that offer services and products designed for offensive cybernetwork attacks. Naturally, the principals of these companies have a vested interest in ensuring that the market continues to expand, which can, in turn, influence government policies.

The market for surveillance and offensive computer operations that has emerged in recent years was preceded by a relatively smaller market for filtering technologies. The latter were developed initially to serve business environments but quickly spread to governments looking for solutions for Internet-censorship demands. ONI research throughout the 2000s documented a growing number of authoritarian countries using U.S.-based commercial-filtering products, including Smartfilter in Iran and Tunisia, Websense in Yemen, and Fortinet in Burma. Some of these products appear to have been tailored to meet the unique requirements of authoritarian regimes. For example, the Websense product had built-in options for filtering categories that included human-rights and non-governmental organizations. In one case, a PowerPoint presentation by Cisco (the maker of telecommunications-routing equipment) surfaced which made the argument that a market opportunity had presented itself for the company to work in collusion with China's security services.[36] Commercial solutions such as these can help to structure the realm of the possible for governments. Whereas in the past it might have been difficult or even inconceivable to engage in deep packet inspection or keyword-based filtering on a national scale, commercial solutions open

up opportunities for policy makers looking to deal with vexing political problems on a fine-grained scale.

International Vacuums (*horror vacui*)

One of the least obvious mechanisms of norm propagation is the absence of restraints. Policies and behaviors can spread internationally when there are no countervailing safeguards or checks. Norm diffusion through the absence of restraints might be likened to the principle of nature abhorring a vacuum. Practices and behaviors fill a void in the policy arena. This mechanism is perhaps the most difficult to pin down empirically because it lacks any identifiable source or location. Yet it may be among the most important international dynamics of cyberspace controls.

One might hypothesize that norm diffusion via the absence of restraints is most amenable to the diffusion of "bad" norms precisely because there are no countervailing restraints. For example, the spread of cybercrime and the blurring of cybercrime and espionage can be explained in part by the ways in which the perpetrators are able to exploit fissures in the international system. Bad actors act globally and hide locally in jurisdictions where state capacity is weak and they are beyond the reach of the victims' local law enforcement. Some governments, through their *inaction,* may even be deliberately cultivating a climate favorable for crime and espionage to flourish. For example, major cyberespionage networks and acts of cybercrime have been traced back to China, Russia, and other countries that take few or, at best, symbolic measures in response, in part because of the strategic benefits that accrue to these countries from the flourishing of those activities. These governments can reap windfalls from the ecology of crime and espionage through the black market while maintaining a relatively credible position of plausible deniability.[37]

Focusing on the international dynamics and mechanisms of cyberspace controls is important for several theoretical and practical reasons. First, there are unique processes that occur at the international level that are distinct from what happens domestically. These mechanisms and dynamics help to explain why a norm for Internet filtering and surveillance is spreading internationally. States do not operate in isolation; they are part of a dense network of relations that influences their decisions and actions. Without considering these mechanisms and dynamics, we may miss some of the more important explanations for growing cyberspace controls, which have until now been primarily attributed to domestic-level causes. The framework laid out above is meant to be a first step in identifying some of the most important sources of those mechanisms and dynamics.

The focus on the spread of cyberspace controls, as outlined here, may offer an important contribution to the study of international norm diffu-

sion more generally. Up until now, scholarship in this area has been focused almost entirely on the propagation and diffusion of "good" norms, such as landmine and chemical-weapons bans, the abolition of slavery, and the spread of democratic values.[38] The examples laid out here show that the propagation and diffusion of "bad" norms can happen along the same lines, employing some of the same mechanisms and dynamics. Further research into the spread of cyberspace controls may shed light on some unique mechanisms and dynamics employed by authoritarian and competitive authoritarian regimes. It is sometimes assumed that these governments are by definition inward-looking and have an aversion to internationalism and multilateralism. Some of the examples pointed to here show that, to the contrary, these regimes have very active international and regional engagements that are likely to continue to grow.

Finally, a focus on international mechanisms and dynamics underscores the iterative and relational quality of state behavior. States' actions and behaviors are formed very much in response to other states' decisions, often in unintended ways. This observation has important policy implications for democratic industrialized countries. The policies that these governments implement may be used by authoritarian regimes to legitimize their actions at home in ways considerably different than democratic countries originally intended. Unfortunately, there is not a lot that can be done to guard against this dynamic. But it is important to be aware of it and recognize it when it occurs. General statements about the "war on terror" or "copyright controls" can be turned into excuses for a broad spectrum of nefarious actions by authoritarian regimes. These dynamics also underscore the importance of consistency, transparency, and accountability on the part of democratic regimes. For example, shortly after U.S. secretary of state Hillary Clinton admonished governments for pressuring RIM to collude with security services, the Obama administration introduced legislation that would put in place precisely the same procedures as those requested by India, Saudi Arabia, the UAE, and others. Governments are embedded in an international system and thus a dynamic network of relations. One cannot understand the spread of cyberspace controls without understanding its international mechanisms and dynamics.

NOTES

1. Ronald J. Deibert et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008).

2. Ronald J. Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010).

3. The author is one of the founders and principal investigators of the ONI.

4. By "positive" and "negative," I do not mean to imply a normative judgment of the policies, but rather to describe the processes around which policies are formed.

5. Margaret E. Keck and Kathryn A. Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca: Cornell University Press, 1999).

6. Stephen M. Walt, "Is the Cyber Threat Overblown?" ForeignPolicy.com, 30 March 2010, available at *http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.*

7. See *http://opennet.net.*

8. Deibert et al., *Access Controlled.*

9. For criticism along these lines, see Robert O. Keohane, ed., *Neorealism and Its Critics* (New York: Columbia University Press, 1986).

10. For a discussion of how international organizations can influence state behavior in ways not intended as part of their original design, see Michael Barnett and Martha Finnemore, "The Politics, Power and Pathologies of International Organizations," *International Organization* 53 (Autumn 1999): 699–732,

11. See, in particular, Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge: MIT Press, 2010).

12. Policy statement made by Igor Shchegolev, Russian minister of telecommunication and mass communications, on 4 October 2010 at the International Telecommunication Union plenipotentiary conference in Guadalajara, Mexico, available at *www.itu.int/plenipotentiary/2010/statements/russian_federation/shchegolev-ru.html.*

13. See Brenden Kuerbis, "Reading Tea Leaves: China Statements on Internet Policy," Internet Governance Project, 8 June 2010, available at *http://blog.internetgovernance.org/blog/_archives/2010/ 6/8/4548091.html.*

14. Tim Gray, "U.N. Telecom Boss Warns of Pending Cyberwar," *TechNewsDaily,* 10 September 2010, available at *www.msnbc.msn.com/id/39102447/ns/technology_and_science-security.*

15. "RIM Should Open Up User Data: UN Agency," CBC News, 2 September 2010, available at *www.cbc.ca/money/story/2010/09/02/rim-user-data-un.html.*

16. Tom Gjelten, "Seeing the Internet as an 'Information Weapon,'" NPR, 23 September 2010, available at *www.npr.org/templates/story/story.php?storyId=130052701&sc=tw&cc=share.*

17. Jonathan Fildes, "UN Slated for Stifling Net Debate," BBC News, 16 November 2009, available at *http://news.bbc.co.uk/2/hi/technology/8361849.stm, accessed 6 Oct. 2010.*

18. Gregory Francis, "Plutocrats and the Internet," CircleID, 4 October 2010, available at *www.circleid.com/posts/20101004_plutocrats_and_the_internet.*

19. See Andrew Scheineson, "The Shanghai Cooperation Organization," Council on Foreign Relations, 24 March 2009, available at *www.cfr.org/publication/10883/shanghai_cooperation_organization.html.*

20. Richard Weitz, "What's Happened to the SCO?" *The Diplomat,* 17 May 2010, available at *http://the-diplomat.com/2010/05/17/what's-happened-to-the-sco/.*

21. Bandula Sirimanna, "Chinese Here for Cyber Censorship," *Sunday Times,* 14 February 2010, *www.sundaytimes.lk/100214/News/nws_02.html.*

22. Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52 (Autumn 1998): 887–917.

23. Kenneth N. Waltz, *Theory of International Politics* (Reading, Mass.: Addison-Wesley, 1979); and Keohane, *Neorealism and Its Critics*.

24. Benjamin E. Goldsmith, "Imitation in International Relations: Analogies, Vicarious Learning, and Foreign Policy," *International Interactions* 29, no. 3 (2003): 237–67.

25. "Factbox: BlackBerry Under Fire from States Seeking Access," Reuters, 13 August 2010, *www.reuters.com/article/2010/08/13/us-blackberry-access-factbox-idUSTRE67B22T20100813*.

26. Harsimran Singh and Joji Thomas Philip, "Spy Game: India Readies Cyber Army to Hack into Hostile Nations' Computer Systems," *Economic Times*, 6 August 2010, available at *http://articles.economictimes.indiatimes.com/2010-08-06/news/27590170_1_computer-systems-spy-game-hackers*.

27. Rhys Blakely, "India Blocks Deals with Chinese Telecoms Companies over Cyber-Spy Fears," *Times Online*, 10 May 2010, available at *http://citizenlab.org/2010/05/india-blocks-deals-with-chinese-telecoms-companies-over-cyber-spy-fears/*.

28. For a general discussion, see Jeffrey Legro, "Which Norms Matter? Revisiting the 'Failure' of Internationalism," *International Organization* 51 (Winter 1997): 31–63.

29. Clifford J. Levy, "Russia Uses Microsoft to Suppress Dissent," *New York Times*, 22 September 2010.

30. Prerna Mankad, "Cambodia Bans Text Messaging," ForeignPolicy.com, 30 March 2007, *http://blog.foreignpolicy.com/posts/2007/03/30/cambodia_bans_text_messaging*.

31. See *www.almasryalyoum.com/en/news/restrictions-placed-sms-messages-avert-promoting-anti-regime-incitations*.

32. Harmeet Shah Singh, "India's Top Court Delays Decision on Holy Site," CNN, 23 September 2010, available at *http://edition.cnn.com/2010/WORLD/asiapcf/09/23/india.holy.verdict/index.html*.

33. Nazila Fathi, "Iran Disrupts Internet Service Ahead of Protests," *New York Times*, 11 February 2010, available at *www.nytimes.com/2010/02/11/world/middleeast/11tehran.html?ref=global-home*.

34. Janet Gunter, "Mozambique: Government Interference in SMS Service," *Global Voices*, 21 September 2010, available at *http://advocacy.globalvoicesonline.org/2010/09/21/mozambique-government-interference-in-sms-service/*.

35. Annasoltan, "Technology and Tradition Are Not Enemies: Agent.mail.ru Banned in Turkmenistan!" 1 September 2010, available at *http://www.neweurasia.net/media-and-internet/technology-and-tradition-are-not-enemies-agentmailru-banned-in-turkmenistan*.

36. Brad Reese, "Powerpoint Presentation Appears to Implicate Cisco in China," *NetworkWorld*, available at *www.networkworld.com/community/node/27957*.

37. See Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," joint report, 6 April 2010.

38. One exception is Ryder McKeown, "Norm Regress: US Revisionism and the Slow Death of the Torture Norm." *International Relations* 23 (March 2009): 5–25.