# JOURNAL OF DEMOCRACY

*October 2010, Volume 21, Number 4  $12.00*

## Democratization and Development

*Alejandro Toledo* ▪ *Thomas Carothers*
*Brian Levy* ▪ *Kenneth Wollack & K. Scott Hubli*

## Liberation vs. Control in Cyberspace

*Ronald Deibert & Rafal Rohozinski*

## What Does Democracy Mean?

*Michael Bratton* ▪ *Tianjian Shi & Jie Lu* ▪ *Larry Diamond*
*Fares Braizat* ▪ *Yun-han Chu & Min-hua Huang*

*April Longley Alley* on Yemen's Multiple Crises
*Mark Thompson* on the Philippines
*Richard Madsen* on Religion in China
*Nic Cheeseman* on African Elections

## Success Stories from "Emerging Africa"

*Steven Radelet*

# LIBERATION VS. CONTROL: THE FUTURE OF CYBERSPACE

*Ronald Deibert and Rafal Rohozinski*

***Ronald Deibert** is associate professor of political science and director of 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. Together they are the founders of the Information Warfare Monitor and the OpenNet Initiative. The following essay is adapted from their* Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace *(MIT Press, 2010), coedited with John Palfrey and Jonathan Zittrain.*

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 cyber-technologies 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 cyber-application 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] Cyber-communication 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?

***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 authorities, civic associations, criminal networks, and underground economies.***

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, interests, 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 authorities, 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, cyber-criminals have occupied a largely hidden, parasitic ecosystem within cyberspace, attacking the insecure fissures that open up within this constantly morphing domain. Although most cyber-crime takes the form of petty spam (the electronic distribution of unsolicited bulk messages), the sophistication and reach of cyber-criminals 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 cyber-crime 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 cyber-criminal 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 accounts 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 cyber-crime are often used for malicious political activity. Our research reveals the deeply troubling trend of cyber-crime tools being employed for espionage and other political purposes.

Twice in the last two years, the Information Warfare Monitor has uncovered major global cyber-espionage 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 cyber-crime and are widely available on the Internet black market.[10] Indeed, "Gh0st Rat," the main device employed by the cyber-espionage 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 cyber-attacks 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 cyber-crime 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* economic 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 cyber-crime 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 cyber-criminal 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 cyber-security 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 cyber-security.

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 companies, 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 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 systemwide 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), patrol 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 cyber-domain 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, Rafal Rohozinski, John Palfrey, and Jonathan Zittrain, 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.htm.*

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.*