Part I Access Contested: Theory and Analysis

1 Access Contested

Toward the Fourth Phase of Cyberspace Controls

Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain

November 2009, Sharm el-Sheikh, Egypt. At a large conference facility in the middle of a desert landscape, the Internet Governance Forum (IGF) is in full swing. Thousands of attendees from all over the world, lanyards draped over their chests, bags stuffed with papers and books, mingle with each other while moving in and out of conference rooms. Down one hallway of the massive complex, a large banner is placed outside a conference room where a book launch is about to begin. The OpenNet Initiative (ONI) is holding a small reception to mark the release of its latest volume, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. As part of the planned proceedings, members of OpenNet Asia plan to show clips of a short documentary they have produced on information controls across Asia.

Before the event gets under way, an official from the United Nations—the forum's host—asks to speak to the ONI's Ron Deibert. The official is upset about the distribution of small pamphlets that invite attendees to the book reception, in particular about the reference to Tibet on the back (which he encircles in pen to make his point). He asks that no more such pamphlets be distributed. Deibert reluctantly agrees, since the event is about to begin.

But one incident leads quickly to another. An ONI research associate is now carrying the large banner back from the hallway, this time escorted by the same official, another official, and a security guard. The banner is placed on the floor while discussions take place. Deibert asks what the problem is now, to which the official replies that the reference to the "Great Firewall of China" is unacceptable to one of the state members and that the poster must be removed. An animated discussion follows, with people gathering. The growing crowd of onlookers pulls out mobile phones, snaps photos, starts rolling videos, and sends tweets out to the Internet about the furor. The security guards remove the banner from the book reception, and the event continues.

Following the reception, people assemble videos of the controversy and post them to YouTube. Press inquiries begin, and soon there are stories and posts about the event, including an image of the banner in question on BBC, CBC, and other news outlets around the world. What was a sleepy book reception has turned into a political melee.

Onlookers' accounts differ from those made by the IGF executive coordinator, Markus Kummer, and these differences stir up confusion. Kummer claims the reason the banner was removed had nothing to do with the reference to China, but rather that no banners or posters are allowed in the IGF, a claim that is clearly contradicted by dozens of other commercial banners spread throughout the massive complex.

The now-infamous IGF ONI book reception illustrates in one instance the current state of cyberspace contestation. Rather than overt censorship, a member state pressures UN officials at the IGF to remove a poster that alludes to practices (in this case, technical censorship) they would prefer not be mentioned. Meanwhile China is engaging in a forthright campaign to neutralize the IGF, pushing instead for Internet governance to be moved to a more state-exclusive forum. Perhaps not surprisingly, the IGF president seems loath to annoy the member state, perhaps for fear of stirring up yet more animosity toward the IGF. But the quiet show of authority does not go unchallenged—documented by dozens of social-media-enabled activists and attendees, accounts of the event ripple outward to become a media storm.

A little over a year later, events in Egypt take a dramatic turn as the country is embroiled in protests. The contests in the street are to an unknown degree organized over the Web and documented there, with the Egyptian authorities ordering all Internet service providers (ISPs) to shutter services.[1] While the country is effectively severed from the Internet, supporters of the Egyptian demonstrators worldwide share strategies on repairing the broken connections. Everything from ham radios and satellite phones to primitive dial-up connections is employed. Eventually, the Egyptian authorities relent on the blackout, but the contests in cyberspace continue. Egyptian authorities order the country's main cell phone carriers to send out mass SMS texts urging pro-Mubarak supporters to take to the streets and fight the assembled protestors.[2]

Digital technologies play an increasingly important role in terms of how we express ourselves and communicate with one another. Those who hold public office, along with those who speak to power, recognize the growing importance of the Internet and related technologies, which together forge the domain of cyberspace. It is now considered a domain equal in importance to land, air, sea, and space and is the medium through which commerce, education, hobbies, politics, and war all take place.

Not surprisingly, cyberspace has become an increasingly contested space—an object of geopolitical competition. This contestation is illustrated on a daily basis, from the formation of military cyber commands to the filtering of social media tools by repressive regimes to the creation of new tools and methods designed to circumvent them. The tussles over cyberspace are the result of a gradual entanglement of competing strategic interests mutually dependent on and targeting a common communications and information space. It bears constant reminding that the environment we are talking about is only several decades old, and in a short period of time it has gone through a massive growth that continues unabated.

Over the last eight years, through a pioneering interuniversity and public/private collaboration, we have been witness to these transformations and the growing struggles to shape and control cyberspace. Our collaboration started out animated by a simple and astonishingly unanswered puzzle: if someone connects to the Web in a country like China or Saudi Arabia, will that person experience the same Internet as a person connecting from Canada or the United States? We built a fairly elaborate methodology designed to answer this question, even as it evolved over time. Although we have documented with a good degree of precision the growing number of countries that attempt to filter access to information and services online, we have also observed an entirely different struggle to shape practices and norms around cyberspace. While it is still essential to have something like what we call a "gold standard" for testing Internet filtering on a comparative basis, the range of controls being exercised by a growing number of actors, as well as the resistance to those controls, present challenges to our research.

As with its predecessor, *Access Controlled*, which focused on member states of the Organization for Security and Cooperation in Europe, we take a regional view in *Access Contested,* focusing primarily on the cyberspace contests playing out in Asia. Although cyberspace can be viewed as an undifferentiated whole, it is important not to lose sight of important regional variations. Nowhere is the battle for the future of rights and freedoms in cyberspace more dramatically carried out than in the Asian region. At the epicenter of this contest is China—home to the world's largest Internet population and, in our view, the world's most advanced Internet censorship and surveillance regime. China struggles to balance national/cultural security and regime stability against the exploding aspirations of ethnic and social groups who strive for identity and recognition, and commercial ventures seeking connectivity to worldwide markets. The resistance to its controls ranges from grassroots human rights groups to corporate giants like Google. Recent revelations of cyber espionage, patriotic hacking, and theft of intellectual property have thrust China into a tense rivalry with regional and global powers, such as India and the United States.

The drama of security, identity, and resistance evident in China is played out across Asia, but in a form unique to each country's national context. India is an emerging information and communications technology (ICT) superpower but like China struggles to balance economic development, identity, and resistance through surveillance and censorship of its own. Burma is among the world's most repressive regimes and has shown a willingness to take drastic measures to control online dissent, including shutting down the Internet altogether during protests in 2007 known as the Saffron Revolution. In Thailand, street protests have spilled online, leading authorities to take unusually harsh measures to limit access to social networking and other mobilization services.

Throughout Asia, a diverse mixture of controls and local resistances has created a unique regional story around the contests to shape cyberspace. Most importantly, by

focusing on cyberspace contests in Asia we are taking a glimpse into the future. There is a major demographic shift in cyberspace under way, as the center of gravity of the Internet's population slowly shifts from the North and West to the South and East. These nations are entering into cyberspace with a much different set of customs, values, and state-society relations than those, like the United States and Europe, out of which the Internet was developed and first took shape. Just as West Coast Californian culture motivated the first generation of Internet practices and principles, so too should we expect the next phase of these practices and principles to reflect a different regional flavor.

Four Phases of Cyberspace Regulation

Since 2006 when we began our global comparative approach to Internet filtering research, we have mapped content-access control on the Internet in 70 states, probed 289 ISPs within those states, and tested Web access to 129,884 URLs. Based on the data we have collected and the work of other researchers asking similar questions, we argue that there are four phases of Internet access and content regulation. The phases are the "open commons" period, from the network's formation through about 2000; "access denied," through about 2005; "access controlled," through 2010; and "access contested," the phase we are now entering, which is the subject of this volume.

Phase 1: The Open Commons (the 1960s to 2000)

The first phase, roughly from the Internet's initial formation in the 1960s through about 2000, is the period of the "open commons." This phrase is intended to convey descriptive, predictive, and normative meanings. During this initial period of the network's development, the dominant theory about its regulation—to the extent that anyone was thinking seriously about regulation at all—was that the Internet itself was a separate space, often called "cyberspace." The concept of cyberspace melded the creativity of the science fiction writer with the aspirations of the democratic theorist dreaming of a fresh start. Up until the late 1990s, most states tended either to ignore online activities or to regulate them very lightly. When states did pay attention to activities online, they tended to think about and treat them very differently from activities in real space. While the idea of an open commons seemed to work as a description, it proved inaccurate as a prediction. Of course, on a normative level, there is still salience and widespread attachment to the concept of an open commons.

Though the era of the open commons as a description of cyberspace is long past, there are important elements of the theory behind it that persist today. For example, there is truth to the argument that the Internet allows us to hear more speech from

more people than ever before. The Internet can allow greater freedoms than citizens previously enjoyed, especially in closed regimes where the state controls the mainstream media. Governments can use the same technologies to increase openness and transparency in their operations. Moreover, cross-cultural understanding can flourish as never before, or so the theory goes, now that digital networks connect people from all around the world in new and important ways at very low cost. An individual in nearly any country on earth, assuming he or she has an Internet connection, can already access a vast store of information, much greater than what people a century ago could have imagined.

The great power of the Internet as a force for democratization is in collective action. Individuals can use these cheap technologies as organizing tools to pull others around them together and, through collective action, have a greater effect on a political process than they might have had otherwise. A vast amorphous set of communities known as the blogosphere cuts in and across political, ethnic, and other boundaries in a noisy but robust web of support for global civil society. However, any careful examination of the blogosphere and its subsets will demonstrate, too, that there are also problems associated with what people do in these spaces. This is true whether the context is the United States or Burma. Few would argue that there are sound reasons for any state to seek to restrict online speech and to practice increased surveillance, from child protection to routine law enforcement. While we celebrate the ways in which ICTs, whether digital or not, are useful to those who would bring democracy about around the world, it is equally important to realize that the same tools can be useful to those who would harm other people. Nearly all the problems that arise in offline space find their way into the online environment and in turn give rise to control strategies and contestation over them.

Though the rhetoric of the open Internet was (and remains, in some respects) compelling, it was inaccurate as a prediction. It was wrong in large measure because nothing in the technology is unrelated to human behavior. We have simply been wrapping our lives into this hybrid reality that is both virtual and analog—all of it "real"—at the same time. All the actions we take in using these technologies, whether on a virtual or a real platform, are effectively interconnected and could be regulated. As we have immersed more of our lives into cyberspace, the stakes have grown and the contests over those stakes and their related regulations have become more intense.

The technology of cyberspace is also not fixed in a way that lends itself to the sorts of predictions laid out by early enthusiasts. Indeed one of the hallmarks of cyberspace is its rapid cycles of innovations. It is a space characterized by powerful generativity—any of its millions of users can create software that ripples across the Internet with system-wide effects.[3] Whether these changes are benign or not, and regardless of their utility, these innovations ensure that cyberspace is in constant motion. At one level, the Internet's central characteristic is rapid change.

But the myth of openness that characterized this first phase remains an attractive model for citizens to collectively aspire to, even as it is carved up and colonized by powerful actors and competing interests. The core elements of an open commons have now become the touchstones for a set of constitutive principles to be shored up and defended, as opposed to assumed away as invincible. Perhaps ironically, what were once assumed to be the immutable laws of a powerful technological environment are now potentially fragile species in a threatened ecosystem.

Phase 2: Access Denied (2000 to 2005)

We call the second phase of Internet development, from roughly 2000 to 2005, the "access denied" period. During this second era, states and others came to think of activities and expression online as things that needed to be managed in various ways. The initial reaction to the mainstreaming of the Internet, by states such as China and Saudi Arabia, was to erect filters to block people from accessing certain information. In this second phase, governments shook off their laissez-faire approach to Internet regulation and began to intervene more assertively in cyberspace.

The world may appear borderless when seen from cyberspace, but sovereign state lines are in fact well established online, as is regional variation. It was the prospect of these lines emerging that formed the underlying rationale for the ONI as a joint research project among our respective institutions in 2002. We initially focused much of our research on states in the Middle East and North Africa, Asia, and Central Asia, where the world's most extensive filtering takes place. Our research has since come to cover states in every region of the world, including North America and Western Europe, where forms of speech regulation other than technical Internet filtering at the state level are the norm. A central component of our research is fieldwork conducted in situ. Two regional networks we helped form and continue to support—OpenNet Eurasia and OpenNet Asia—aim to monitor censorship and surveillance practices in their respective regions. OpenNet Eurasia was formed at the beginning of the ONI and consists of researchers, technologists, and lawyers from across the Commonwealth of Independent States (CIS). Building on our work in the CIS, we formed OpenNet Asia in 2007 through support from the International Development Research Centre. OpenNet Asia is composed of 14 academic and advocacy partners from 11 Asian countries. OpenNet Eurasia made key contributions to *Access Controlled*, and similarly we draw on contributions from members of OpenNet Asia in this volume to provide a grounded perspective on information controls in the region.

Filtering practices and policies vary widely among the countries we have studied. China continues to institute the most intricate and fast-acting filtering regime in the world, with blocking occurring at multiple levels of the network and covering content that spans a wide range of topic areas. Though its filtering program is widely discussed,

Singapore, by contrast, blocks access to only a handful of sites, each pornographic in nature. Most other states that we study implement filtering regimes that fall between the poles of China and Singapore, each with significant variation from one to the next. These filtering regimes are properly understood only in the political, legal, religious, and social context in which they arise.

The blocked content spans a wide range of social, religious, and political information. Our studies have combined a review of whether individual citizens could access sites in a "global basket" of bellwether sites to test in every jurisdiction across a variety of sensitive areas—akin to a stock index sorted by sector—as well as a list of Web sites likely to be sensitive in certain countries only. We found that in some instances governments justify their filtering by referring to one content category, such as pornography, while eliding the fact that other content categories were also being blocked. We also noted the tendency toward what we called "mission creep"—that is, once filtering systems were adopted for whatever reason, state authorities would be tempted to employ them to deal with other vexing public policy issues.[4] For example, while Pakistan began by blocking access to blasphemous content, it expanded its filtering regime to include Web sites of opposition groups and insurgencies.[5] We also discovered that governments tend to block local-language content more than that expressed in English, and locally relevant sources of information more than general global content.

The extent, locus, and character of Internet filtering vary from state to state and over time. Web filtering is inconsistent and prone to error. Numerous examples from our research noted the tendencies of overblocking and underblocking, whereby content is either missed or mistakenly included in block lists because of sloppy filtering techniques. What is hosted where is constantly changing (for example, IP addresses are often recycled for other uses while states' IP blocking lists are not updated), and Web content at any particular site is constantly changing, a fact that poses a problem for the censors. Mobile devices and social networks have further complicated the task of speech regulation online. No state we have yet studied, including China, seems able to carry out its Web filtering in a comprehensive manner (i.e., consistently blocking access to a range of sites meeting specified criteria). China appears to be the most nimble of the states that we have studied at responding to the shifting Web. This ability likely reflects a devotion of the most resources and political will to the enterprise of technical Internet filtering.

It would be a mistake to infer that Internet filtering is a phenomenon that takes place only in states with histories of hostility to free expression. Democratic states participate in extensive regulation of the Internet, just as authoritarian states do. We have documented Internet filtering in northern Europe, for instance, associated with child pornography. In the United States, the state regulates what children can see in libraries and schools, as one of many means of limiting access to information deemed to be harmful to them. One may feel differently about these child-protection measures

than one does about the blocking of activists' speech on the fringe of nondemocratic societies, but the practices involve similar technical mechanisms, as well as pitfalls, in both types of settings. These practices have made Internet filtering a growing and pervasive global norm.

Citizens with technical knowledge can generally circumvent filters that a state has put in place. Some states acknowledge as much: the overseer of Saudi Arabia's filtering program, under the state-run Internet Services Unit, admits that technically savvy users can simply not be stopped from accessing blocked content. Expatriates in China, as well as those citizens who resist the state's control, frequently find up-to-date proxy servers or virtual private-network services through which to connect to the Internet and through which they can evade filters in the process. While no state will ultimately win the game of cat-and-mouse with those citizens who are resourceful and dedicated enough to employ circumvention measures, a preponderance of users will never do so—rendering filtering regimes at least partially effective despite the obvious workarounds.

Some of the earliest theorizing about control in the online environment, from the open-commons period, suggested that such state-run control of Internet activity would not work.[6] States like China have proven that an ambitious regulatory body can, by devoting substantial technical, financial, and human resources, exert a large measure of control over what their citizens do online. If they want, states can erect digital gates at their borders, even in cyberspace, and can render these gates effective through a wide variety of modes of control. These controls have proven right the claims of Lawrence Lessig, Jack L. Goldsmith, Tim Wu, and others who have emphasized the extent to which the online environment can be regulated and the ways in which traditional international relations theory will govern in cyberspace as in real space.[7]

Phase 3: Access Controlled (2005 to 2010)

The third phase, from 2005 roughly to the present day, is the "access-controlled" phase. Access controlled characterizes a period during which states have emphasized regulatory approaches that function not only like filters or blocks, but also as variable controls. The salient feature of this phase is the notion that there is a large series of mechanisms (including those that are nontechnological) at various points of control that can be used to limit and shape access to knowledge and information. These mechanisms can be layered on top of the basic filters and blocks established during the previous era or implemented separately altogether in their absence.[8] They reflect a more nuanced understanding of the range of tools available to authorities to shape and control, as opposed to block, access to information and freedom of speech. Notoriously, such tools include the use of more "offensive" (compared to passive or defensive) methods, including computer network attacks, espionage, and the projection of ideas favorable to a state's strategic interests.

The mechanisms of the access-controlled period are more subtle and nuanced than the first-generation filtering and blocking mechanisms that they complement. These controls can change over time to respond to changing political and cultural environments that arise online and offline. Filtering mechanisms can be made to work "just in time," in order to block content and services at politically sensitive moments, as the Chinese government did in reaction to ethnic riots in the autonomous region of Xinjiang in 2009 or as the Egyptian regime did in extreme form in response to the January 2011 protests.[9]

Many states also use registration, licensing, and identity requirements to control what people do online and to create a climate of self-censorship. In some jurisdictions, in order to publish information lawfully on the Internet, one needs to register oneself with the state as a publisher. The first-order controls associated with censorship are combined with legal controls and surveillance, the effect of which is to ensure that those publishing online know that they are being watched and that the state is capable of shutting them down or putting them in jail. These methods of regulation, working in combination, are highly effective, both as a means of law enforcement and through a chilling effect on online speech.[10]

During this access-controlled period, states have also increased the number of control points that are possible on this network and their use. While the image of the "Great Firewall of China" is evocative and, to some extent, accurate as a description, it is misleading insofar as it tells only a small part of the story of control online, in China and elsewhere. States control the online environment not just at the national border, as information flows in and out of the state, but in many environments within states. For instance, in order to go into an Internet café to log on to the Internet in Burma, one has to establish one's identity and log in at the front of the store so that the proprietor can link online activities to a certain machine and IP address and period of time.[11] These registration and logging requirements are combined with surveillance cameras that are trained on computer users in Internet cafés. Law-enforcement officials, in turn, can monitor or later re-create the digital tracks of the large population of Internet users who rely upon Internet cafés, especially in developing countries where fast connectivity to the home is prohibitively expensive or nonexistent.

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 focus on cartoons of the Prophet Mohammed.[12] 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 video 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, "The government can take any decision to stop any activity that threatens national unity and integrity."[13]

Although many of these controls are initiated by states, other actors are implementing them either of their own accord or as a consequence of outsourcing. States themselves cannot implement the level of control that they seek over network activity directly, so their control strategies have expanded to include pressure on private-sector actors. Soon after China erected its Great Firewall, it became clear that this approach would not be sufficient as a means of exercising the extent and kinds of control that the state wanted to carry out over time. It has turned to private companies to do most of the blocking or the surveillance at the source, leading to a highly public, multiyear showdown between the state's regulators and the companies' executives.

While legal measures create the regulatory context for denial of access, for more immediate needs, authorities can make informal "requests" of private companies. Most often such requests come in the form of pressure on ISPs and online service providers to remove offensive posts or information that supposedly threatens "national security" or "cultural sensitivities." Google's 2010 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 running infrastructure to render services inoperative to prevent their exploitation by activists and opposition groups, as was the case in Egypt in January 2011. In some of the most egregious cases, such as the TOM-Skype case in China (discussed later in this section), 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.

For governments in both the developed and developing worlds, delegating censorship and surveillance to private companies keeps these controls on the front lines of the networks and among 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, cloud-computing services, Internet exchanges, and telecommunications companies—often drawing upon wide company discretion to implement a vague government mandate. Such a shift in the locus of controls raises serious issues of public accountability and transparency for citizens of all countries. In light of such regulations now creeping in the world over, 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. In the absence of government policies, Internet service providers, operators of social networking sites, and Web-hosting companies may make decisions based on business interests or on their own terms-of-service

agreements. Not surprisingly, these decisions can be inconsistent, ad hoc, and sometimes discriminatory against marginal or radical groups.

Disabling or attacking critical information assets at key moments in time—during elections or public demonstrations, for example—may be one of the most effective tools 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 thrive 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 ONI in Belarus, Kyrgyzstan, Tajikistan, Nepal, Burma, and most recently in Egypt.[14]

The attraction of just-in-time blocking to regulators is that information is disabled at key moments only, thus avoiding charges of Internet censorship and allowing for the perpetrators' plausible denial. In regions where Internet connectivity can be intermittent and unreliable, 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, it is nearly impossible to identify those responsible.

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 Fifty Cent Party (named for the amount of money its members are supposedly paid for each Internet post), patrols chat rooms and online forums, posting information favorable to the regime and chastising its critics.[15] In Russia, it is widely believed that the security services regularly coax hacker groups to fight for the motherland in cyberspace and may plant instructions on prominent nationalist Web sites and forums for hacking attacks.[16] In late 2009 in Iran, a shadowy

group known as the Iranian Cyber Army compromised Twitter and some key opposition Web sites, defacing the home pages with their own messages.[17] Although no formal connection to the Iranian authorities has been established, the groups responsible for the attacks posted proregime messages on the hacked Web sites and services.

Accessing sensitive information about adversaries is one of the most important tools for shaping political outcomes, so it should come as no surprise that great effort has been devoted to targeted espionage. In 2008 the Information Warfare Monitor discovered that TOM-Skype (the Chinese version of Skype) was actively collecting the logs and records of any text and voice calls placed to users, including full-text chat logs that contained politically sensitive keywords.[18] 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 (Web sites infected with viruses that target insecure browsers) is exploding along 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.[19]

The OpenNet Initiative's experiences in this third phase have proven to be challenging on a number of levels. Our methods were calibrated to check for basic Internet filtering as the primary mechanism of information shaping and denial. However, the hallmark of the access-controlled phase is the use of nontechnological methods of shaping cyberspace in combination with selective filtering. Many of these methods are based on social, as opposed to technical, means and do not lend themselves well to technical fingerprinting in ways that were more obvious in the access-denied phase, when our methods were born. In addition, some of the controls are applied selectively at key moments, when our testing regime may not be present, thus escaping our notice entirely. For the ONI to remain relevant, it must adapt to the exigencies of the new modes of cyberspace controls.

Phase 4: Access Contested (2010 and Beyond)

Today we are headed into a fourth phase that we call "access contested." Although the central characteristics of the previous phases remain relevant, the key notion of this phase, as outlined by Ronald Deibert and Rafal Rohozinski in chapter 2 of this volume, is that the contest over access has burst into the open, both among advocates for an open Internet and those, mostly governments but also corporations, who feel it is now legitimate for them to exercise power openly in this domain. There is, and will be more, pushback against some of these controls from civil society, supported in many instances by the resources of major governments, like the United States and the European Union. But that pushback is met by a more vigorous commitment by many

governments (including, ironically, the United States itself) to develop and refine offensive actions in cyberspace against adversaries, however they are defined.

There is an ongoing contest over what this hybrid environment will look like over time and a growing realization of the battle's stakes among all groups. Most importantly, as Deibert and Rohozinski argue, the contests reach down to the very inner workings of the Internet architecture and call into question principles and protocols that were once assumed away as noncontroversial as governments like China and Russia assert their interests for a different vision of cyberspace.

In chapter 9, Milton Mueller provides an analysis of China's international strategies for cyberspace, a component of its Internet control regime that is often overlooked but growing in importance. Unwilling to accept a cyberspace determined by others, particularly as the number of Chinese Internet users expands, China is asserting a more ambitious foreign policy for cyberspace. These strategies are naturally bumping up against others' interests but also finding support from like-minded governments and international organizations.

The growing centrality of online activities to life in general is the primary driver of cyberspace contests. From the perspective of Internet users, online activity is increasingly a part of everyday life—not a separate sphere to which they travel occasionally, as if on vacation. The metaphor of cyberspace as a space, akin to "real space," breaks down in this respect. The technological mediation of these activities changes some things—for instance, the technology brings with it specific affordances for the activist in getting her word out and the spy in snooping on Internet traffic as it passes—but it does not change the underlying dynamics of states, companies, individuals, and groups.

In accordance with this deep immersion, we are seeing cyberspace contests playing themselves out among institutions at all levels of society, including within those not otherwise known for extensive technical filtering practices. For example, although the Philippines is not a country that has a national Internet-filtering regime, Erwin A. Alampay, Joselito C. Olpoc, and Regina M. Hechanova show in chapter 6 how information controls in the country are exercised in a variety of institutions, such as places of work and study, often with greater effect than if they were imposed by government regulation. Likewise, chapter 4 by Heike Jensen, Jac sm Kee, Gayathri Venkiteswaran, and Sonia Randhawa provides an insight into how long-standing social norms, in this case those related to gender and sexuality, can affect cyberspace practices in a country like Malaysia, where national-level Internet filtering is minimal. In chapter 3, Vee Vian Thien takes a different tack on Malaysia, showing how heavy-handed state controls in the traditional sector, combined with intimidation and arrests, have unintentionally bolstered resistance from the blogosphere.

Her analysis is mirrored to a certain degree in chapter 5 by Pirongrong Ramasoota on cyberspace controls in Thailand. As Ramasoota shows, cyberspace contests are

particularly acute around major events and traumatic political episodes. Ramasoota documents how an emerging online public sphere in Thailand quickly became threatened following a military coup in the country with the introduction of more restrictive laws and regulations. However, civic groups have challenged these laws vigorously and through various methods in ways that demonstrate a continued vitality of the civil society sector.

In the access-contested phase, the regulation that states imposed in the earlier phases is giving rise to strong responses from civil society, from other states, and also from the private sector. Companies are implementing new strategies for coping with the spread of regulation and liability that they face as Internet intermediaries. And as we described, in response to mounting pressure from states including China and Vietnam, companies such as Google, Microsoft, and Yahoo! have joined together with human rights groups and academics to establish an organization, the Global Network Initiative, to help implement a code of conduct for handling such demands in a manner than upholds civil liberties.[20] And companies compete, directly and indirectly, in how extensively they carry out censorship online. Search engines, for instance, vary in terms of how and to what extent they filter keywords. Regulation online is increasingly a blend of the public and the private.[21] In her contribution to this volume (chapter 10), Rebecca MacKinnon compares pressures companies face in authoritarian China over surveillance and censorship to those in the democratic regimes of South Korea and India. Through this comparison she explores the challenges for corporate social responsibility and upholding universal principles of free expression and privacy in the region.

States, too, are now actively engaged in a contest with one another over cyberspace. Military officials increasingly think of the online environment as a strategic domain and a potential zone of warfare. The militarization of cyberspace indicates how states have built up offensive information-warfare capabilities in recent years.[22] 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 former Soviet Union countries. Two chapters look at these issues from different levels of analysis. In chapter 8, Nart Villeneuve and Masashi Crete-Nishihata trace the evidence around attacks on prominent Burmese-related independent media and reach some surprising conclusions that muddy the waters around attribution. For their part, Hal Roberts, Ethan Zuckerman, and John Palfrey take a more comprehensive view of the global situation regarding distributed-denial-of-service attacks against civil society groups and find the frequency and qualities of such attacks a growing concern (chapter 7).

Citizens around the world are beginning to awaken to some of these issues. Public reaction to Internet regulation also points to the contest that is beginning to play out in public arenas globally. For example, demonstrators in Pakistan in 2010 made plain

their disagreement with the state's decision to increase the incidence of Internet blocking.[23] China's mandate that hardware providers install Green Dam filtering software on new computers before they shipped met with substantial resistance and was pulled back.[24] The Malaysian state has publicly struggled with political pressure to start filtering.[25] Plans to institute state-mandated filtering in Australia were shelved after extensive public pushback.[26] The last chapter has yet to be written in the back-and-forth between Google and China about whether unfiltered search results can be presented to Chinese Internet users. And in contrast to most other examples, there appears to be vocal public support in favor of pornography filtering in Indonesia.[27] These and many other contests like them will play out in the years to come.

The perspective of most states on Internet regulation has changed substantially from where it began in the open-commons era. The premise today is not whether the Internet can be regulated, but rather how it must be regulated and how that regulation should be carried out most effectively. States have also come to realize that the activities of other states online need to be constrained in various respects. State interests in what transpires online—the activities of other states, private companies, individuals, and groups—have become much clearer over the past decade, and the competitions have become more intense as a result. As Deibert and Rohozinski emphasize, there is an arms race in cyberspace today between states and their adversaries.

The early theorizing about Internet regulation centered on the extent to which states could, and would, regulate the activities of individuals in cyberspace. This kind of state-to-individual regulation is a given today. Contests now concentrate not only on other kinds of regulation in which states are involved but also on those exercised by a multitude of other actors with a stake in cyberspace policies and practices. It is important to remember that most of cyberspace is owned and operated by private parties, and its protocols are developed and refined through processes that straddle the public and the private. As the frontline operators of the network, these actors are being asked or otherwise compelled to regulate the spaces they own and operate in ways that constitute a de facto exercise of authority. Not surprisingly, many of these companies are moving into spaces of public policy deliberation where such policies are likely to become more prominent features. It is not too far-fetched to think of companies like Google, Facebook, and Research in Motion having foreign policies. The same could be said of networks of civil society groups across all parts of the political spectrum. Cyberspace contestation is made up of a complex patchwork of competing interests and actors of all types. A key feature of the access-contested period will be the interplay and clash between these often-competing interests and values.

These contests among private and public actors reach deep into the heart of the very foundational principles upon which the Internet was formed. Almost everything is now up for grabs and open for debate. Reflecting the essentially contested nature of the space, some have even gone so far as to argue that the Internet itself should be

"reengineered" from the ground up, or that political authorities should have the capacity to turn it off entirely. As Deibert and Rohozinski claim in their chapter, one senses in these debates a watershed moment for the future of cyberspace. How it will all be resolved will have an enormous impact not just on global communications, but also on the future of democracy and human rights worldwide.

Notes

1. James Cowie, "Egypt Leaves the Net," Renesys, January 27, 2011, http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

2. Darren Pauli, "Vodaphone Sent Mubrark SMS Propaganda," ZDNet, February 4, 2011, http://www.zdnet.com.au/vodafone-sent-mubarak-sms-propaganda-339308969.htm.

3. Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); Jonathan Zittrain, *The Future of the Internet—And How to Stop It* (New Haven, CT: Yale University Press, 2008).

4. Ronald Deibert and Nart Villeneuve, "Firewalls and Power: An Overview of Global State Censorship of the Internet," in *Human Rights in the Digital Age,* ed. Mathias Klang and Andrew Murray (Portland, OR: GlassHouse, 2005), 111–125.

5. See the Pakistan country profile in this volume.

6. David Post, "Governing Cyberspace," *Wayne Law Review*, 23 (1996): 155–171.

7. Lessig, *Code and Other Laws of Cyberspace*; Jack L. Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (Oxford, UK: Oxford University Press, 2006); Jack L. Goldsmith, "Against Cyberanarchy," in *Who Rules the Net? Internet Governance and Jurisdiction,* ed. Adam Thierer and Clyde Wayne Crews, Jr. (Washington, DC: Cato Institute, 2003), 71–90.

8. Ronald Deibert and Rafal Rohozinski, "Beyond Denial: Introducing Next Generation Information Access Controls," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 3–12.

9. "China Shuts Down Internet in Xinjiang," OpenNet Initiative Blog, July 6, 2009, http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots; "Egypt's Internet Blackout: Extreme Example of Just-in-Time Blocking," OpenNet Initiative Blog, January 28, 2011, http://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking.

10. Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 24–28.

11. See the Burma country profile in this volume.

12. Reporters Without Borders, "List of Blocked Websites Gets Longer," May 20, 2010, http://en.rsf.org/pakistan-court-orders-facebook-blocked-19-05-2010,37524.html.

13. "YouTube Blocked in Bangladesh after Guard Mutiny," *Daily Telegraph*, March 9, 2009, http://www.telegraph.co.uk/news/worldnews/asia/bangladesh/4963823/YouTube-blocked-in-Bangladesh-after-guard-mutiny.html.

14. OpenNet Initiative, "Special Report Kyrgyzstan: Election Monitoring in Kyrgyzstan," April 15, 2005, http://opennet.net/special/kg/; OpenNet Initiative, "The Internet and Elections: The 2006 Presidential Election in Belarus (And Its Implications)," May 3, 2006, http://opennet.net/blog/2006/05/oni-releases-belarus-internet-watch-report; OpenNet Initiative, "Nepal," May 10, 2007, http://opennet.net/research/profiles/nepal; OpenNet Initiative,"Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," 2007, http://opennet.net/research/bulletins/013; OpenNet Initiative, "Tajikistan," December 1, 2010, http://opennet.net/research/profiles/Tajikistan; OpenNet Initiative Blog, "Egypt's Internet Blackout: Extreme Example of Just-in-Time Blocking."

15. David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review*, July 2008, http://feer.wsj.com/essays/2008/august/chinas-guerrilla-war-for-the-web.

16. Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace."

17. "'Iranian Cyber Army' Hits Twitter," BBC News, December 18, 2009, http://news.bbc.co.uk/2/hi/8420233.stm.

18. Nart Villeneuve, "Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform," Information Warfare Monitor, 2008, http://infowar-monitor.net/breaching-trust.

19. Google, "A New Approach to China," January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

20. Global Network Initiative, http://www.globalnetworkinitiative.org.

21. Jonathan Zittrain and John Palfrey, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 103–122; Colin Maclay, "Protecting Privacy and Expression Online: Can the Global Network Initiative Embrace the Character of the Net?" in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 87–108.

22. Ronald Deibert, "Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace," in *Digital Media and Democracy: Tactics in Hard Times,* ed. Megan Boler (Cambridge, MA: MIT Press, 2008), 152–157.

23. See the Pakistan country profile in this volume.

24. See the China country profile in this volume.

25. See the Malaysia country profile in this volume.

26. OpenNet Initiative, "Australia and New Zealand," 2010, http://opennet.net/research/australia-and-new-zealand.

27. OpenNet Initiative Blog, "Indonesia and Its Porn Troubles," August 6, 2010, http://opennet.net/blog/2010/08/indonesia-and-its-porn-troubles.

2 Contesting Cyberspace and the Coming Crisis of Authority

Ronald Deibert and Rafal Rohozinski

[Essentially contested concepts are] concepts the proper use of which inevitably involves endless disputes about their proper uses on the part of their users.
—W. B. Gallie[1]

In its short life span, the Internet has evolved from a laboratory research tool to a global immersive environment—called cyberspace—that encompasses all of society, economics, and politics. It is the communications environment in which all other activities are now immersed. From the beginning, one of its central characteristics has been its unusual dynamism—a characteristic facilitated by a distributed architecture formed around a basic common protocol. Typically, innovations can come from anywhere in the network, at any of its constantly expanding edge locations, and from any member of its exponentially increasing user base. As the network grows, so do the innovations—leading to yet more dynamism and unpredictability.

Over several phases of the Internet's evolution, however, a different pressure has begun shaping the character of cyberspace—the actions of major institutions, such as states and corporations. Originally conceived of as being too slow, cumbersome, and antiquated to deal with the swiftly evolving trajectory of digital media, states have moved rapidly to regulate, shape, intervene, and exercise power in cyberspace across all its spheres. There is now a burgeoning market for cyber security methods and services that has emerged as a consequence of, and contributor to, the securitization of cyberspace. These interventions have been met with growing resistance as users and others become aware of the stakes involved and as the struggles mount to preserve cyberspace as an open commons. Cyberspace has thus become an object of intense contestation in ways that have been unparalleled in its evolution. The impact is only just beginning to be felt but will have enormous consequences for its character and, by extension, for global politics.

In this chapter, we examine the increasing struggle for superiority and the competition for power, influence, and control that defines the contestation of cyberspace. We

lay out the major driving forces of cyberspace contests: the continued rapid expansion of cyberspace throughout all aspects of society, including the rapid rise of mobile access devices; a demographic shift from the North and West to the South and East as a new generation of digital natives outside the industrialized West logs on and brings with them a new set of values and interests and resistance to state and private-sector controls; the increasingly dynamic competition among states for influence in and through cyberspace, manifest in the creation of dedicated cyber armed forces and an arms race in cyberspace; and more aggressive measures taken by authoritarian and democratically challenged states to counter antiregime mobilization through offensive activities.

The contests we outline cannot be categorized in simple dualisms, but reflect a patchwork of competing interests and values. These contests are reaching down into the very inner workings of cyberspace, into areas previously assumed to be noncontroversial and immutable components of its core operating infrastructure. Everything is up for grabs as cyberspace opens itself up to intense debate, negotiation, and competitive struggle. Principles and rules that were once cherished and sacred have been questioned and challenged: from network neutrality, to basic peering and routing arrangements, to the legitimacy of denial-of-service and other offensive computer attacks. The contests in cyberspace that we outline, therefore, represent a serious crisis of political authority and legitimacy of existing norms, rules, and principles, as the emerging domain, along with the largely private-sector-controlled infrastructure on which it rests, clashes with the territorially based system of sovereign rule and widely varying perceptions of national interest and identity.

We conclude, however, on a relatively optimistic note. The crisis of authority in the domain opened up by contestation throws into question that entire edifice of cyberspace governance—from the infrastructure, to the code, to the regulatory realms. But in doing so, it also turns everything inside out, so to speak, laid bare for everyone to examine and begin again anew. Of course, such an opening presents serious risks for long-cherished principles and norms. But as they are questioned, an opportunity opens up for a comprehensive discussion of first principles: how the space should be defined and constituted, what behavior is appropriate for this space, and what should be the relationship, responsibilities, and rights of the actors who control it and the political jurisdictions through which it is embedded. Out of the rubble and chaos left in the wake of the perfect storm may arise an opportunity to rethink some conventional wisdom and assumptions that for too long have been taken for granted—not only about cyberspace, but also about the relationship between private and public authority, territory and political rule, and the character of global governance.

Drivers of Cyberspace Contestation

Driver 1: The Continuously Dynamic and Constantly Evolving Ecosystem of Cyberspace

It may seem obvious, but it is no less important a fact that cyberspace is deeply embedded in all aspects of life, growing continuously and dynamically. This growth and dynamism is one of the most important drivers of cyberspace contests. In a very short period of time cyberspace has moved from a research tool to which one connects to a space for online engagement separate from the "real world," to something that is all encompassing and all engrossing. We now depend on it for more of our daily activities, in the home, workplace, culture, politics, health, and other sectors. We store business and personal information on "clouds." We connect 24 hours a day through a continuously evolving range of devices. According to UN estimates, the number of SMS messages tripled from 2007 to 2010 to reach a staggering 6.1 trillion, with an average of close to 200,000 text messages sent every second.[2]

The Internet's infrastructure, relatively trivial at one time, has now become a critical component of society, economics, and politics, and ranked as one of the top security priorities for governments of the world. Downtime of a telecommunications network, even for a few minutes, can trigger huge financial losses for customers and clients. For example, even though Egypt has a relatively low Internet penetration rate of 24.3 percent,[3] the Organization for Economic Cooperation and Development estimated that the five-day shuttering of the Internet in early 2011 contributed to a loss of USD 90 million in direct revenues, and a substantially higher amount in secondary economic impacts for which it did not account.[4] It is noteworthy in this respect that the shuttering of the Internet did not initially include the Internet service provider (ISP) Noor, whose clients include the Egyptian stock exchange, five-star hotels, and corporate clients ranging from Coca-Cola to Pfizer.[5] Had the government shuttered that ISP at the same time as other providers, the losses would have been significantly larger.[6] In a more advanced industrialized setting, downtimes of minutes can cause major losses for the financial sector, including banks and stock exchanges.

Such an enormous shift from something separate to something so deeply immersive is going to raise the stakes for not only the rules of the game, but also the nature of the game itself, particularly around norms, rules, and principles that have previously been taken for granted or assumed away as noncontroversial. As more individuals, groups, and organizations become dependent on cyberspace, the clashes of interests, values, and ideologies become increasingly acute. There are more players with more at stake, and thus a more active interest in how regulatory and other shifts affect their strategic interests. Naturally, this creates conditions for disagreement and intense lobbying. What was once a tool for a relatively narrow segment of society (university

researchers) has over time become the infrastructure for all of society itself. Not surprisingly, the rules of the game, once considered sacred by an inner sanctum of technologists, are now up for grabs for all of global society.

It has become widely acceptable to refer to cyberspace as a "commons." But it is, in fact, a rather curious commons because it is one that is parceled up, owned and operated by a multitude of private-sector actors. Not surprisingly, part of cyberspace contestation involves the spotlighting of the conditions by which these companies mediate our experiences with it, an issue that has become more complex as the range of devices connecting to each other through common protocols expands. Consider, for example, debates over intermediary liability: whether private actors that control Internet services should be held responsible for the content that passes through their networks.[7] In the past, such debates centered mostly on one type of actor: ISPs or telecommunications carriers. Today, questions of intermediary liability are relevant to a wide range of companies and services, from cloud computing platforms, to online hosting companies, mobile phone devices, and online forums and video-sharing sites. As these market-based actors create, constitute, and control the spaces of the Internet, their activities come under increasing scrutiny, regulatory and other pressures, and legal oversight from a growing number of political jurisdictions. In cases like China, for example, intermediary liability is a sine qua non of operating within that political jurisdiction. Internet service providers and other companies are legally and otherwise compelled to police content associated with their service offerings. Such intrusive pressures are not surprising among authoritarian regimes. But even outside authoritarian contexts, the pressures bearing down on intermediary liability are growing, for copyright-protection and other reasons.[8] In many democratic industrialized countries, legislation has been proposed that puts greater burdens of liability on intermediaries for the content they manage for a variety of reasons, from concerns over copyright violations to antiterror and hate speech. In Italy, for example, Google executives found themselves facing criminal charges for failing to remove a video from YouTube that was deemed offensive by Italian prosecutors.[9] In India, laws have been passed that hold ISPs accountable for maintaining "public order, decency, and morality."[10]

There has also been a major shift in the way we conduct our communications experience, with a rapid change from fixed to wireless-enabled mobile devices. The number of mobile cellular subscriptions in the Asian region grew from 22.5 per 100 inhabitants in 2005 to 67.8 per 100 inhabitants in 2010.[11] The shift to mobile not only has made connecting to cyberspace more convenient, but also has increased the number and type of Internet-connected devices and thus points of potential control, resistance, and contestation. Mobile technologies have been behind some of the most spectacular examples of social mobilization, as demonstrated by SMS-enabled mass protests in Iran, Egypt, and elsewhere. With greater mobility and constant one-to-one connectivity it may seem intuitive to think that we are untethered and thus

increasingly empowered and free. But mobile connectivity also enhances the potential for fixing individual's communications with precision in time and space that would make the greatest tyrants of days past envious. For example, the latest (fourth-generation) mobile devices are standardly equipped to include metadata about the geolocational information of images and videos that are captured. Unwitting users who upload them to public Web sites and social networking platforms may not realize that the metadata can be harvested by anyone viewing the pictures and videos on those sites and services.

Not surprisingly, regimes aiming to control popular uprisings fueled by mobile technologies have turned to these and other methods to identify, isolate, and contain organizers and participants. These actions, in turn, have generated fear, intense scrutiny, widespread condemnation, and often very vocal criticism of the companies who operate the infrastructure and services and are forced or otherwise compelled in some manner to collude with the regimes.

For example, in Egypt in 2008, one of the country's largest cell phone carriers, Vodaphone, turned over information on users who employed the service to organize food protests. Later, in 2011, the company admitted that it had sent messages on behalf of state security services, encouraging Egyptians to take to the streets to counter the mass uprising in that country.[12] Both cases caused public outrage and calls for boycotts against the company from human rights and privacy advocates. Similarly, in a much-publicized set of squabbles, Research in Motion (RIM), the maker of the popular Blackberry device, has found itself facing demands from governments ranging from the United Arab Emirates to India and Indonesia for access to its encrypted data streams. In 2011, RIM agreed to implement content filtering on its Web browser in response to requests made by the Indonesian government to block pornography.[13] The controversy has brought about scrutiny into RIM's mobile architecture that otherwise would have likely never existed, pitted governments against each other, and generated criticism of RIM itself by human rights advocates suspicious that the company has made secret deals that violate due process and public accountability.[14] As cyberspace grows exponentially, embedding itself deeper into our everyday lives through a greater range of connected devices and services, the contests over the rules and protocols by which such a complex domain is organized naturally intensify as well.

Driver 2: A Demographic Shift in Cyberspace: Next-Generation Digital Natives

The massive growth, dynamism, and penetration of digital technologies are well known. What is less well known is that there is a major demographic shift occurring in cyberspace as the center of gravity of cyberspace users moves from the North and West to the South and the East. Although cyberspace was born in the United States and other Western industrialized countries, and thus embodies many of the values of

users from those regions, Internet users in places like China, India, Latin America, and Southeast Asia will soon dwarf these early adopting constituencies. With these new digital natives will come a different culture of governance and a new set of strategic interests. Although it is not assured that these values, norms, and interests will clash wholesale with the prevailing modes of cyberspace practices, they are bound to do so in various ways that will invariably lead to contestation. Already the signs of such contestation are visible and seem destined to grow in scale and importance.

Images and metaphors of cyberspace are a useful way to portray its dominant characteristics. William Gibson, the science fiction author who coined the term "cyberspace," paints a picture of the domain as a virtual reality matrix in which users would physically plug their minds into and escape into a world of "endless city lights receding."[15] The image evokes clean spheres and precise mathematical coordinates—like the contours of 3D computer graphics. Gibson was influenced by his experiences of the game arcades that peppered downtown Granville Street in Vancouver, Canada, where he lived. For many cyberspace users today, this consumerist abstraction is still the dominant impression.

Elsewhere, we have characterized cyberspace as a kind of gangster version of New York—private and public actors intermixing with criminals and quasi authorities in a myriad of overlapping rules and regulations.[16] For the next phase of its evolution, the more appropriate image is perhaps the *favela*, or the shantytown—which better describes from where the next billion cyberspace users are likely to come. The majority of new Internet users in 2010 came from the developing world.[17] While many Western analysts like to think of cyberspace as the realm of high-tech chrome and virtual light, it is in the back streets of the developing world, with its intermittent power, crowded Internet cafés, and burgeoning wireless access points, that the future of the Internet is now being forged.

These next-generation digital natives are very different from the ones that until now have ruled and shaped cyberspace. These digital natives are also emerging under much different contexts than those that applied to the Silicon Valley generation. For this next generation, the Internet has not been a public (and often free) resource that they have encountered in libraries, schools, offices, and living rooms. It is, rather, a relatively precious resource that has to be bought, built, or stolen, and carefully weighed against other competing expenses and needs. Whereas for the Silicon Valley generation the dream of cyberspace had to do with access to information, freedom of speech, social connections, and entrepreneurial flair, for the new digital natives cyberspace may be something completely different, as well as a means for following dreams that are otherwise thwarted in their local contexts. For these new digital natives, cyberspace may offer the best means not only for routing around structural barriers to socioeconomic advancement; it offers a way to gain access to global markets—and gain economic riches far in excess of those available locally. Such access does not

require venture capital or a leased office space and a large staff; it requires intelligence, boldness, and access to the Internet through a cheap consumer device.

Just as the social setting of universities and West Coast libertarian culture of the early Internet technologists influenced the constitutive values that informed cyberspace, so too will the much different social setting of the next generation of digital natives. At present, the Asian region comprises 42 percent of the world's Internet population (the most by region), but it ranks only sixth in terms of penetration rates at 21.4 percent, meaning that there is an enormous population yet to be connected, most of them young.[18] In China, for example, 60 percent of Internet users are under the age of 30.[19] According to the International Telecommunication Union (ITU), among the roughly 5.3 billion mobile subscriptions by the end of 2010, 3.8 billion are in the developing world.[20] It is important, although perhaps disturbing, to know that of the top 55 countries with the highest Internet penetration growth rates from 2008 to 2009,[21] 18 are considered by the United Nations to be the world's least developed countries, "representing the poorest and weakest of the international community."[22]

To understand the future of cyberspace, we need to understand the aspirations and needs of this next generation. From the crumbling tenements of the former Soviet Union, from the shantytowns of Nairobi, Manila, or Brazil, or from the crowded Internet cafés of Shanghai, a new wave of users is entering into the cyberspace domain. With them will come an entirely fresh suite of ideas, interests, and strategic priorities. Although not as wealthy in absolute terms, these actors are as smart and motivated as their Silicon Valley predecessors. And they are exploiting opportunities for economic advancement that follow different rules. At least a significant proportion of them realize that playing through the gray areas of sovereign state jurisdiction and the virtually endless methods of obfuscation can render law enforcement meaningless, allowing them to work in relative impunity in the profitable world of cybercrime (which we outline in the next section).

Not only are the demographic shifts that occur in cyberspace bringing new motivations and desires, but they are also bringing the weight of entire national collective identities and state interests hitherto largely absent or irrelevant to cyberspace governance issues. Although English has been the "operating system language" for the Internet since its inception, if present growth rates continue Chinese will be the dominant language on the Internet in five years.[23] Such a shift alone will have repercussions for how cyberspace is constituted as a public commons of information.[24] But more practically, it will begin (and already has begun) to put pressure on the governance of cyberspace routing. Already, the desire to encourage linguistic communities to express themselves online has triggered serious questions about how the systems that support them are managed and resources allocated, particularly around allocation and management of country top-level domains. What was once a purely technical

and then commercial issue has thus been transformed into a broader political and social question of forging, expressing, and maintaining collective identities.

As this demographic shift occurs, the contests over cyberspace will take on a different hue as the center of gravity of the user base moves South and East, away from the petri dish of experimentation out of which it emerged. The actors that represent the majority of users today, stakeholders from the South, the developing world, and the non-English segments of the net, will do more to shape the future of cyberspace than any discussions at the Pentagon or in policy circles in North America and Europe. To understand how and in what ways cyberspace will be characterized in years to come we need to think beyond the beltway, beyond Silicon Valley, and into the streets of Shanghai, Nairobi, and Tehran. The contests occurring in those spaces deserve our attention today, if for no other reason than that they provide a glimpse of the types of global issues that will drive cyberspace governance in the future.

Driver 3: The Dark Driver of Cyberspace Contestation—Cybercrime

A driver of cyberspace contestation, related in various ways to the previous two drivers, is the massive growth of cybercrime. Although cybercrime has formed a hidden shadow and a kind of evil doppelgänger to every step of the Internet's long history from its very origins, its growth has suddenly become explosive in recent years by virtually any estimate. According to the security company Sophos, its global network of labs received around 60,000 new malicious software (malware) samples every day in the first half of 2010; every 1.4 seconds of every day, a new malware sample arrives.[25]

The reasons for this sudden surge in cybercrime can be connected back to the previous two drivers. Our expanding and constantly evolving communications ecosystem of extensive social sharing of data, mobile networking from multiple platforms and locations, and increasing reliance on "clouds" and social networking services operated by thousands of companies of all shapes, sizes, and geographic locations has emerged with such swiftness that organizations and individuals have yet to adapt proper security practices and policies. While convenient and fun, this environment is also a dangerous brew and an opportunity structure ripe for crime and espionage to flourish. A largely hidden and massively exploding ecosystem is parasitically thriving off of insecure data-sharing practices and vulnerable browsers, servers, and Web sites.

Ever since the Internet emerged from the world of academia and into the world-of-the-rest-of-us, its growth trajectory has been shadowed by a gray economy that has thrived on the opportunities for enrichment that an open, globally connected infrastructure has made possible. In the early years, cybercrime was clumsy, consisting mostly of extortion rackets that leveraged blunt computer network attacks against online casinos or pornography sites to extract funds from frustrated owners. Over time, it has become more sophisticated, more precise: like muggings morphing into

rare art theft.[26] It has become one of the world economy's largest growth sectors—Russian, Chinese, and Israeli gangs are now joined by upstarts from Brazil, Thailand, and Nigeria—all of whom recognize that in the globally connected world, cyberspace offers stealthy and instant means for enrichment. Effecting a digital break-in of a Manhattan victim at the speed of light from the slums of Lagos or the terminal grayness of Moscow is elegant and rewarding—certainly more so than pulling a knife in the slums for a fistful of cash. It is a lot less risky too. Cybercrime has elicited so little prosecution from the world's law enforcement agencies it makes one wonder if a de facto decriminalization has occurred. Not surprisingly, it is seen as a safe yet challenging way out of structural economic inequality by the burgeoning number of educated young coders of the underdeveloped world.

What is most concerning, however, is that the market for the wares of the cybercriminal is expanding and broadening, moving from the dregs of identity theft and credit card fraud to the high-powered politics of interstate competition. As the Information Warfare Monitor has shown in the *GhostNet* and *Shadows in the Cloud* reports, and recent events in Iran, Burma, and Tunisia have demonstrated, the techniques of the cybercriminal are being redeployed for political purposes, including espionage and infiltration of adversaries.[27] With the recently revealed Stuxnet worm, developed to target the software used to control nuclear facilities in Iran, we have entered a new age where the techniques of cybercrime are being employed for advanced targeted warfare.[28]

The growth of cybercrime is much more than a persistent nuisance; it has become a highly ranked risk factor for governments, businesses, and individuals. The consequences for cyberspace contestation of this exploding threat vector are going to be numerous and wide-ranging, leading (among other things) to pressures for greater state regulation, intervention, and even exploitation—a fourth driver to which we now turn.

Driver 4: Assertions of State Power and National Identity in Cyberspace

The technological, demographic, and social shifts outlined previously are happening simultaneously with a sea change in the way that governments are asserting themselves in cyberspace. Whereas once the dominant metaphor of Internet regulation was "hands off," today the dominant descriptors involve intervention, control, and increasingly contestation. In our previous volume, *Access Controlled,* we outlined several generations of cyberspace control strategies employed by a growing number of states.[29] These strategies are now spreading virally, from regime to regime, as legitimate means to assert state power and control and disable adversaries. The types of assertions of state power vary, depending on the nature of the regime, but all states are approaching cyberspace in a much different way than they did a decade ago. They

are driven by the need to control dissent and opposition, protect and promote national identity and territorial control, or simply respond to the growing pressures to regulate cyberspace for copyright control, child protection, or antiterrorism measures. Among the most impressive drivers is the perceived need to develop armed-forces capabilities in cyberspace, which in turn has triggered an arms race in cyberspace. Naturally, such assertions of state power are generating countermovements and resistance from individuals, civil society groups, and other states, which in turn create conditions for multiple contestations.

Although there are many cases that have become emblematic of this complex dynamic, perhaps the most potent is that of Iran in 2009. Thirty years before, the country had experienced firsthand how small media could cause a revolution, in that case through distributed cassette tapes spreading the message of resistance on behalf of the Ayatollah Khomeini regime. During the summer of 2009, mass mobilization occurred rapidly following disputed elections and charges of widespread fraud. Protests spilled into the streets of Tehran and other urban centers, fueled by new technologies and connected to networks of support over global social networking sites and among civil society groups worldwide. An important catalyzing moment was the shooting death of Neda Agha-Soltan, whose murder was captured by amateur video loaded onto YouTube and other video-sharing sites, and then went viral on a global scale. The video and the colors of the Green Revolution became a symbol of democratic solidarity. For many in the Western press, academia, and the cognoscenti, the groundswell of support was evidence of the unstoppable might of social networks. It was not uncommon to see headlines referencing a "Twitter Revolution." At one point, members of the Obama administration reportedly lobbied Twitter to keep the service reliable and running in order to support the protests in the streets of Tehran.[30]

But in and around the street demonstrations and social networking, the authorities worked systematically to disable, disrupt, and neutralize opposition through a variety of means. At the most basic level, the regime employed first-generation controls of Internet filtering to block access to social networking services and the sites and tools used by dissidents and others to circumvent the controls. In and of themselves, these first-generation methods would easily have been bypassed and nullified had that been the limit of the Iranian regime's tool kit. However, the Iranian authorities had several other means at their disposal, employing the full range of second- and third-generation control techniques. They instituted new laws and regulations that prevented the use of circumvention technologies and the distribution of information threatening to the regime or insulting of Islam, which created an additional level of self-censorship and a climate of fear. Notably, the Iranian authorities defined content that was defiling Islam or insulting to the regime as "cybercrime."

More importantly, though, authorities began to employ more offensive, active techniques of information shaping and denial. The European telecommunications

company Nokia-Siemens had provided Iranians with high-grade surveillance and data-mining technologies that were employed with precision to identify communication networks and arrest individual protesters.[31] The Iranian authorities also harvested information from social networking sites, like Facebook and Twitter. It became quickly apparent that the very same technologies that were fueling dissidents and activists were being exploited with precision to identify, preempt, and disable them. A cloud of paranoia swept through Green Movement activists and their supporters as if a poisoned pill had been dropped into the well of social networking.

An even more ominous development was the emergence of a shadowy group known as the Iranian cyber army during the Green Revolution, which, in a very public fashion, began attacking opposition Web sites and hosting services connected to the revolution's supporters.[32] The evidence was not entirely clear at first, with the group making claims of support for the Iranian regime but leaving considerable speculation as to their actual attribution. Some more recent reports have surfaced providing circumstantial evidence linking the Iranian cyber army to the country's Revolutionary Guard. But whether evidence exists or not, the impact is clear enough: a menacing band of mercenaries took very vigorous offensive actions against adversaries.[33]

The Iranian case illustrates that cyberspace has become both a means and a battleground for intense, multivaried contestation. A revealing portrait of this complex space was recently undertaken in a joint analysis by Morningside Analytics and the Berkman Center for Internet and Society, which mapped the Iranian blogosphere.[34] The mapping shows the relative place and size of the conservatives and moderate/reformist components of Iranian cyberspace as represented by blogs, Web sites, and individuals. The main takeaway of this analysis is that cyberspace does not neatly or symmetrically line up in a sharp division between states and subjects. It is a complex domain of dynamic interaction, contestation, and conflict that involves links between segments of governments, the private sector, religious movements, and both civil and uncivil society. Big Brother may not be so big anymore: she can live next door. He can be your neighbor, the storekeeper down the street, your colleague from work, or the relatives who are living in Los Angeles or Toronto, as well as in Tehran.

It is important to emphasize that the newly invigorated cyberspace control strategies are not exclusive to authoritarian regimes like Iran. Some of the norms driving cyberspace controls are emanating from policies taken by liberal-democratic and advanced industrialized countries. Within these regimes, governments are developing wide-ranging and ambitious interventionist strategies in cyberspace, from the setting up of units within their armed forces dedicated to fighting and winning wars in cyberspace to introducing legislation on surveillance, data retention, and sharing. To give just one example, the *New York Times* recently reported that about 50,000 "national security letters" are sent out each year by U.S. law enforcement to companies in which

sealed requests are made to disclose information about its users, such as one recently made to Twitter for information about supporters of Wikileaks.[35]

It would be misleading to equate these policies with the types of pressures that such companies face in jurisdictions like Iran or Belarus where there are no meaningful checks and balances or spaces for an adversarial press to report on them without considerable risk. But they do provide a justification for such actions, albeit in a different context and wrapped in a different rationale. As the Iranian case illustrates, what is deemed cybercrime in one context can be translated into something entirely different in another, all under the rubric of legitimizing regulation of cybercrime as a global norm. Recently, for example, South Korea bolstered its capacity to enforce cybercrime laws that make it illegal to host pro–North Korean messages on Web sites and forums. Between January and June 2010, the new South Korean cybercrime team of the National Policy Agency forced Web site operators to delete 42,787 pro–North Korean posts from their Web sites—an increase from 1,793 deletions under the previous liberal Roh Moo-hyun administration in 2008.[36]

Assertions of state power in cyberspace mesh with one of the other drivers mentioned earlier: the demographic shift in cyberspace to the South and East. In these regions, many states have a well-established tradition of government intervention and state control, particularly of the mass media and the economy. Already having such a tradition in place, they are also coming into cyberspace at a much different historical juncture than the "early adopters" of the technology in the North and West. For the latter, cyberspace was either something to be cordoned from government intervention altogether or a mystery best left untouched. For the former, they are coming at cyberspace from the perspective of a much different security context surrounding cyberspace and a much greater understanding of its contested terrain. They are doing so building upon the knowledge and practices of prior experiments and are adopting and sharing best practices of information control and denial.

One area where these best practices may be increasingly shared and policies coordinated is among regional security organizations. Until recently, the Shanghai Cooperation Organization (SCO),[37] the Arab League,[38] the Gulf Cooperation Council (GCC),[39] the Association of Southeast Asian Nations (ASEAN), the North Atlantic Treaty Organization (NATO), and others had not dealt with cyberspace issues in a concerted fashion, but that situation is changing. Recently, there have been indications that regional security organizations may be harmonizing laws, practices, and doctrines around cyberspace operations. After its 2010 Lisbon Summit, for example, the NATO alliance affirmed a greater commitment to joint cyberspace operations and doctrine. Although the activities of some of the other regional organizations, like the SCO, are much more opaque, there is evidence of coordination around "information security" practices, including evidence of joint exercises to counter mass social mobilization. Reflecting a regime stability view of cyber security, an August 2009 SCO

summit approved a Russian proposal defining "information war" as an effort by a state to undermine another's "political, economic and social systems" including "mass psychologic [sic] brainwashing to destabilize society and state."[40] The GCC states have coordinated Internet policies perhaps the longest of the regional organizations. As far back as 1997, the GCC member states met to address the challenges for national security and "traditional practices and religious beliefs" of growing Internet connectivity. More recently, at the 2008 ITU Regional Cybersecurity Forum, held in Doha, representatives from the GCC were joined by Arab League states to discuss coordinated national security policies. The group issued a "Doha Declaration on Cybersecurity" at the conclusion, which emphasized the need for greater harmonization around cyberspace controls.[41]

Assertions of state power in cyberspace can exacerbate interstate rivalries and competition. After revelations of major breaches of the Indian national security establishment were made by the Information Warfare Monitor, for example, the Indian government stepped up its cyberwarfare and exploitation capabilities.[42] Legislation was even briefly proposed that would have legalized patriotic hacking in India in response to what was perceived to be a tolerance and exploitation of such activities in China.[43] The Indian government also took measures to restrict imports of high technology from China.[44] After the Operation Aurora attacks that compromised Google, the U.S. National Security Agency was called in to investigate the matter, and many inside and outside Congress pointed to the incident as a justification for an urgent expansion of offensive cyber capabilities.[45] Reflecting these sentiments, retired Air Force General Kevin P. Chilton argued that the United States should undertake a major and very public exercise of its offensive cyber capabilities for deterrent effects on other countries, presumably such as China.[46]

The militarization of cyberspace that we have described has touched off an arms race in the domain as governments and others rush to develop offensive capabilities. But it is also cultivating a normative milieu where offensive actions taken against adversaries and threats are given wider latitude and justification. Although within U.S. policy circles a tight lid is still kept on revelations of offensive cyber attacks, public discussions, like those of General Chilton, are becoming much more common. Likewise, although distributed denial of service (DDoS) attacks can be traced back decades, there has been a rash of more politically motivated ones, including those seemingly undertaken by or in support of governments against opposition groups and by citizens against states and corporations, such as the crowd-sourced Anonymous attacks directed against Tunisia and Egypt, and Visa, Mastercard, and Paypal.[47] In early 2011, in what will likely stand as one of the more brazen public hacks, Anonymous breached the servers of a security firm that was investigating its actions, called HBGary. The group defaced its Web site, took over the Twitter and LinkedIn accounts of some of its executives, and released more than 70,000 company e-mails into the public domain.[48]

Responses to this incident have yet to unfold, but seem certain to fuel more urgent calls to police cyberspace and control anonymity.

Driver 5: The Political Economy of Cyber Security

The assertion of state power in cyberspace is feeding into and in turn being driven by a massively exploding market for cyber security products and services. The size of this market is difficult to pinpoint with precision, in part because it is stretched across so many different economic sectors but also in part because a great deal of it is hidden within military and intelligence "black budgets" and withheld from public scrutiny. There are estimates that the global cyber security market is anywhere between USD 80 and 140 billion annually.[49] The market has triggered a major business restructuring and the emergence of a new cyber industrial complex, particularly in the United States where the market for products and services is the largest. Traditional military industrial giants like Northrup Grunman, Boeing, and Lockheed Martin have shifted to the cyber security markets, alongside a wide range of new niche players providing specialized services and tools.

It is important to underline that the political economy of cyber security not only responds to market demands, but is also a constitutive force that shapes and affects the realm of the possible, including strategic policy. New products and services, such as those providing deep packet inspection, surveillance and reconnaissance, data mining and analysis, filtering and throttling, and even computer network attack and exploitation present new opportunities for authorities and other actors that might never have been imagined. OpenNet Initiative research has tracked the sale of filtering technologies to authoritarian regimes for many years, but the market has expanded considerably.[50] Companies like Narus, for example, market products and technologies that allow precise identification and throttling of packets and protocols, including those used by censorship-circumvention projects and services. One of its products, Hone, parses through massive amounts of social networking data from disparate sources to connect individuals to separate accounts.[51] Its services came under scrutiny when it was revealed that its products were being employed to track dissidents and activists in Egypt and Saudi Arabia.[52] A growing number of firms now offer offensive computer network attack capabilities, which are being marketed as "solutions" for states and corporations.[53] Not surprisingly, the market can encourage the type of offensive actions against adversaries outlined earlier that push the boundaries of acceptable behavior online. For example, a Bollywood studio in India contracted a cyber security firm to engage in DDoS attacks against film download and torrent file trading sites.[54] As this type of market continues to expand, we should expect tools and services such as these to inform and drive state control practices.

Conclusion: Toward a Crisis of Authority

The drivers of cyberspace contestation outlined in the preceding sections reflect deep and powerful social forces that are not easily reversed. On the contrary, the momentum around each of these drivers of contestation is escalating and compounding daily. They are also mutually reinforcing. Although there are many implications of these contests, for cyberspace they reach down deep into and call into question some of its core constitutive norms, rules, and principles. Everything seems to be up for grabs. In such circumstances, it is fair to say that we have reached a point where cyberspace is an essentially contested space, to borrow a phrase form the philosopher W. B. Gallie. There is a crisis of authority in cyberspace, reflecting a fundamental disagreement about everything from acceptable behavior and rules of the road to the basis upon which the network itself is structured and governed globally.

In such circumstances, we should expect architectonic shifts—that is, alterations to the very nature of cyberspace itself that could change its character. Here it is important to emphasize that cyberspace is a human-made domain and therefore subject to a variety of technical rules and systems, all of which can be manipulated or subject to reversal and alteration. Such architectonic shifts could come by the introduction of shortsighted measures based out of fear and insecurity that have long-lasting and radical repercussions. One can see glimpses of such measures in disparate areas: in the growing number of cases of network disruption, from Nepal, China, Burma, Iran, and Egypt, as well as in "Internet kill switch" legislation proposals that would empower U.S. authorities to shut down the network in times of "crisis"; in discussions of mandatory Internet identity requirements and the abolition of online anonymity or discussions about reengineering the Internet; and most shockingly, in brazen offensive cyber attacks unleashed against supporters and detractors of Wikileaks, including theft and public release of proprietary e-mails. Principles and rules that were once considered fundamental and largely sacred have been subject to reexamination and questioning and outright dismissal—from network neutrality, to peering and domain name routing arrangements, to the legitimacy of DDoS and other types of offensive computer attacks.

It is against this backdrop that several developments on the horizon loom large and hold out the prospect for major design shifts in the architecture of cyberspace. According to many analysts, 2012 is the year in which the present IP addressing system, labeled IPv4, will run out of space and network operators and services will be required to adopt a new solution. The rapid expansion of Internet access in the Asian region is cited as one of the major factors contributing to the hasty exhaustion of the 4.3 billion spaces originally allocated in 1977.[55] At present, the main alternative to the existing system, IPv6, is one that offers much less anonymity and gives operators

of networks considerably more power to identity individuals connected to specific devices.

The shift to mobile devices was outlined earlier, but the point bears repeating here. At present and into the future, the majority of individuals will be accessing cyberspace through a handheld device. Though constituting a part of cyberspace, and often connecting through the Internet, mobile systems employ a unique architecture of routing, which offers an opportunity for network operators to build insularity from other networks, as well as to isolate users into segments in granular ways that previous devices, like PCs, could not. As more cyberspace use takes place through mobile networks, a new architecture may supersede and ultimately displace the existing one. When considered together, IPv6 and mobile ecosystems present probably the most important watershed moment for cyberspace design.

Another looming set of issues concerns mounting pressures toward territorialized Internet access. The trend toward cyberspace territorialization, which started with national technical filtering, is now being reinforced by economic strategies. Countries recognize that economic barriers can be just as effective, and offer a much lower political cost, than traditional censorship. Many are throwing state support behind national cyberspace development projects, which are now defined as a critical economic sector. For example, Kazakhstan and Tajikistan make available access to the Internet that is restricted to the national domain at a lower cost than access to the global Internet. Russia has determined that the construction of a national search engine is in that country's strategic interest.[56] China Mobile Communications and Xinhua News Agency have signed an agreement to create a homegrown search engine.[57] Iran proposed the creation of a national e-mail system as a competitor to Gmail that, while not meeting much support, shows the same strategic inclination.[58] National-level services and technologies like these can be justified as being in the national economic interest while also being easier to subject to political controls and regulations. They also complement the emergence of linguistic domains, which allow governments like China and Russia to control the registration of domains in national languages. Together, these further the severing of nonterritorial networks around which cyberspace has been constituted.

While these mutually reinforcing drivers certainly hold out a daunting prospect for the future of the cyberspace commons, there is a silver lining. With a deeply contested space comes a crisis of authority, and the entire edifice of cyberspace governance is thrown into question and laid bare for reexamination. A lid is lifted on the Internet, allowing for a closer examination of what goes on beneath the surface, including that which has been obscured by state secrecy or intellectual property concerns. Arguably, as cyberspace contestation continues apace, a growing number of citizens worldwide now can include in their daily lexicon issues of deep packet inspection, content filtering, encryption, and circumvention. What was once an arcane discussion restricted to engineers, intelligence agencies, and a small segment of policymakers is being

broadened into public-policy and popular circles. Although the prospects are strong that the present circumstances could see the introduction of radical and shortsighted measures, there is an equal opportunity for a discussion of "first principles" of cyberspace. With a crisis of authority, in other words, could come a constitutional moment for cyberspace.

Notes

1. W. B. Gallie, "Essentially Contested Concepts," *Proceedings of the Aristotelian Society,* 56 (1956): 167–198.

2. International Telecommunication Union (ITU), "ITU Estimates Two Billion People Online by End 2010: Access to Mobile Networks Available to Over 90% of World Population; 143 Countries Offer 3G Services," October 19, 2010, http://www.itu.int/net/pressoffice/press_releases/2010/39.aspx.

3. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 Figures, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

4. Organization for Economic Cooperation and Development (OECD), "The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt," February 4, 2011, http://www.oecd.org/document/19/0,3746,en_2649_33703_47056659_1_1_1_1,00.html.

5. Noor, "Clients," http://www.noor.net/Clients.aspx.

6. Noor was eventually shut down on January 31, 2011. Earl Zmijewski, "Egypt's Net on Life Support," Renesys Blog, January 31, 2011, http://www.renesys.com/blog/2011/01/egypts-net-on-life-support.shtml.

7. Ethan Zuckerman, "Intermediary Censorship," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 71–85.

8. Rebecca MacKinnon, "Will Google Stand Up to France and Italy, Too?" *The Guardian*, January 13, 2010, http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/13/google-china-western-internet-freedom.

9. Rachel Donadio, "Larger Threat Is Seen in Google Case," *New York Times,* February 24, 2010, http://www.nytimes.com/2010/02/25/technology/companies/25google.html.

10. Yamini Lohia, "Shackling the Net," *Times of India*, April 12, 2010, http://timesofindia.indiatimes.com/home/opinion/edit-page/Shackling-The-Net/articleshow/5784887.cms.

11. International Telecommunication Union (ITU), "Key Global Telecom Indicators for the World Telecommunication Service Sector," 2010 Figures, http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html.

12. Vodafone, "Statements—Vodafone Egypt," February 3, 2011, http://www.vodafone.com/content/index/press/press_statements/statement_on_egypt.html.

13. Reporters Without Borders, "BlackBerry Filters out Porn Sites in Response to Government's Demand," January 20, 2011, http://en.rsf.org/indonesia-blackberry-filters-out-porn-sites-20-01-2011,39371.html.

14. Ronald Deibert, "Cyberspace Confidential," *Globe and Mail*, August 6, 2010, http://www.theglobeandmail.com/news/opinions/cyberspace-confidential/article1665125.

15. William Gibson, *Neuromancer* (New York: Ace Books, 1984).

16. Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy*, 24, no. 1 (October 2010): 43–57.

17. The ITU estimated that in 2010, 162 million of the 226 million new Internet users in 2010 would be from developing countries. International Telecommunication Union, "ITU Estimates Two Billion People Online by End 2010," October 19, 2010, http://www.itu.int/net/pressoffice/press_releases/2010/39.aspx.

18. Internet World Stats, "World Internet Usage and Population Statistics," June 30, 2010, http://www.internetworldstats.com/stats.htm.

19. Paul Budde Communication Pty Ltd. "China—Key Statistics, Telecom Market, Regulatory Overview and Forecasts," July 7, 2010.

20. International Telecommunication Union, "ITU Estimates Two Billion People Online by End 2010," October 19, 2010, http://www.itu.int/net/pressoffice/press_releases/2010/39.aspx.

21. Internet World Stats, "The Internet Big Picture: World Internet Users and Population Stats," 2010, http://www.internetworldstats.com/stats.htm, accessed February 18, 2011.

22. According to the UN, least developed countries "represent the poorest and weakest of the international community. Extreme poverty, the structural weaknesses of their economies and the lack of capacities related to growth, often compounded by structural handicaps, hamper efforts of these countries to improve the quality of life of their people. These countries are also characterized by their acute susceptibility to external economic shocks, natural and man-made disasters and communicable diseases." Office of High Representative for Least Developed Countries, Landlocked Developing Countries and Small Island Developing States, "Least Developed Countries: About LDCs," http://www.unohrlls.org/en/ldc/25.

23. Alex Wilhelm, "Chinese: The New Dominant Language of the Internet [Infographic]," The Next Web, December 21, 2010, http://thenextweb.com/asia/2010/12/21/chinese-the-new-dominant-language-of-the-internet-infographic.

24. For further discussion, see Milton Mueller, "China and Global Internet Governance: A Tiger by the Tail," chapter 9 in this volume.

25. Sophos, "Security Threat Report: Mid-year 2010," White Paper, 24, https://secure.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-midyear-2010-wpna.pdf.

26. Joseph Menn, *Fatal System Error* (New York: Public Affairs, 2010).

27. Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, March 29, 2009, http://www.tracking-ghost.net/; Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud: An Investigation into Cyber Espionage 2.0*, April 6, 2010, http://shadows-in-the-cloud.net/; "Websites of Three Burmese News Agencies in Exile under Attack," *Mizzima News,* September 17, 2008, http://www.mizzima.com/news/regional/1052-websites-of-three-burmese-news-agencies-in-exile-under-attack.html; Alexis Madrigal, "The Inside Story of How Facebook Responded to Tunisian Hacks," *The Atlantic,* January 24, 2011, http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044; and Alexis Madrigal, "Most Sophisticated Malware Ever Targets Iran," *The Atlantic*, September 22, 2010, http://www.theatlantic.com/technology/archive/2010/09/most-sophisticated-malware-ever-targets-iran-possibly-state-backed/63420.

28. James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53.1 (2011), 23–40.

29. Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 15–34.

30. Sue Pleming, "U.S. State Department Speaks to Twitter over Iran," Reuters, June 16, 2009, http://www.reuters.com/article/2009/06/16/us-iran-election-twitter-usa-idUSWBT01137420090616.

31. Eddan Katz, "Holding Nokia Responsible for Surveilling Dissidents in Iran," Electronic Frontier Foundation, October 13, 2010, http://www.eff.org/deeplinks/2010/10/saharkhiz-v-nokia.

32. Hamid Tehrani, "Iran: Cyber Islamic Militarism on the March," Global Voices, February 19, 2010, http://globalvoicesonline.org/2010/02/19/iran-cyber-islamic-militarism-on-the-march.

33. Reports that were made in confidence to one of the authors of this chapter indicate that the Iranian cyber army had been able to penetrate deep into Green Revolution social movements through the use of sophisticated malware. If these reports are credible, and there is a good possibility that they are, the unquestioned assumption often made about the one-way impact of information and communications technologies (ICTs) on social and political liberation would need some serious qualification.

34. Bruce Etling and John Kelly, *Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere,* Berkman Center Research Publication No. 2008–01, 2008, http://cyber.law.harvard.edu/publications/2008/Mapping_Irans_Online_Public.

35. Noam Cohen, "Twitter Puts Spotlight on Secret F.B.I. Subpoenas," *New York Times,* January 1, 2011, http://www.nytimes.com/2011/01/10/business/media/10link.html?_r=1&partner=rss&emc=rss.

36. Lee Tae-hoon, "Censorship on Pro-NK Web Sites Tight," *Korea Times*, September 9, 2010, http://www.koreatimes.co.kr/www/news/nation/2010/09/113_72788.html.

37. The member states of the SCO are China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. India, Iran, Mongolia, and Pakistan are observers.

38. The member states of the Arab League are Algeria, Bahrain, Comoros, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, Palestine, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, the United Arab Emirates, and Yemen.

39. The member states of the GCC are the United Arab Emirates, Bahrain, Saudi Arabia, Oman, Qatar, and Kuwait.

40. Tom Gjelten, "Seeing the Internet as an "Information Weapon," National Public Radio, September 23, 2010, http://www.npr.org/templates/story/story.php?storyId=130052701&sc=fb&cc=fp.

41. International Telecommunication Union, "Arab Region Presses for Heightened Cybersecurity: Doha Declaration on Cybersecurity Adopted at ITU Forum," February 21, 2008, http://www.itu.int/newsroom/press_releases/2008/NP01.html; ITU Regional Cybersecurity Forum 2008, "Draft Meeting Report: ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop Doha, Qatar, February 18–21, 2008," (RWD/2008/01-E), February 21, 2008, http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-cybersecurity-forum-report-feb-08.pdf.

42. "Cyber War: Indian Army Gearing Up," *Times of India,* July 19, 2010, http://timesofindia.indiatimes.com/tech/news/internet/Cyber-war-Indian-Army-gearing-up/articleshow/6187297.cms.

43. Joji Thomas Philip and Harsimran Singh, "Spy Game: India Readies Cyber Army to Hack into Hostile Nations' Computer Systems," *Economic Times,* August 6, 2010, http://economictimes.indiatimes.com/news/news-by-industry/et-cetera/Spy-Game-India-readies-cyber-army-to-hack-into-hostile-nations-computer-systems/articleshow/6258977.cms.

44. Heather Timmons, "India Tells Mobile Firms to Delay Deals for Chinese Telecom Equipment," *New York Times*, April 30, 2010, http://www.nytimes.com/2010/05/01/business/global/01delhi.html.

45. John Markoff, "Google Asks N.S.A. to Investigate Cyberattacks," *New York Times*, February 4, 2010, http://www.nytimes.com/2010/02/05/science/05google.html?_r=1.

46. Bill Gertz, "Show of Strength Urged for Cyberwar," *Washington Times*, January 27, 2011, http://www.washingtontimes.com/news/2011/jan/27/show-of-strength-urged-for-cyberwar/?page=1.

47. Jose Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 163–181; Christopher R. Walker, "A Brief History of Operation Payback," Salon, December 9, 2010, http://mobile.salon.com/news/feature/2010/12/09/0.

48. Nate Anderson, "Anonymous vs. HBGary: The Aftermath," February 24, 2011, Ars Technica, http://arstechnica.com/tech-policy/news/2011/02/anonymous-vs-hbgary-the-aftermath.ars.

49. Deepa Seetharaman, "Arms Makers Turn Focus from Bombs to Bytes," Reuters, September 10, 2010, http://www.reuters.com/article/2010/09/10/us-aero-arms-summit-cybersecurity-idUSTRE6893EI20100910.

50. See, for example, Helmi Noman, "Middle East Censors Use Western Technologies to Block Viruses and Free Speech," OpenNet Initiative, July 27, 2009, http://opennet.net/blog/2009/07/middle-east-censors-use-western-technologies-block-viruses-and-free-speech.

51. Robert McMillan, "Narus Develops a Scary Sleuth for Social Media," IT World, March 3, 2010, http://www.itworld.com/internet/98652/narus-develops-a-scary-sleuth-social-media.

52. Ryan Singel, "Lawmaker Calls for Limits on Exporting Net-Spying Tools," *Wired*, February 11, 2011, http://www.wired.com/epicenter/2011/02/narus.

53. Dancho Danchev, "Should a Targeted Country Strike Back at the Cyber Attackers?" ZD Net, May 10, 2010, http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194.

54. John Leydon, "Bollywood 'Recruits DDoS Hired Guns to Fight Movie Pirates,'" *The Register*, September 10, 2010, http://www.theregister.co.uk/2010/09/10/bollywood_cyber_vigilantes_fight_movie_pirates.

55. Laurie J. Flynn, "Drumming Up More Addresses on the Internet," *New York Times*, February 14, 2011, http://www.nytimes.com/2011/02/15/technology/15internet.html?ref=technology.

56. "Russia Said to Be Developing National Search Engine—Vedomosti," Automated Trader, July 7, 2010, http://www.automatedtrader.net/real-time-dow-jones/3574/russia-said-to-be-developing-national-search-engine-_vedomosti.

57. Owen Fletcher, "The Chinese State Enters Online Search," *Wall Street Journal*, August 16, 2010, http://blogs.wsj.com/digits/2010/08/16/the-chinese-state-enters-online-search.

58. "Oh Lord: Why Iran's National Search Engine Will Likely Fail," Radio Free Europe/Radio Liberty, August 29, 2010, http://www.rferl.org/content/Oh_Lord_Why_Irans_National_Search_Engine_Will_Likely_Fail/2140725.html.

3 The Struggle for Digital Freedom of Speech

The Malaysian Sociopolitical Blogosphere's Experience

Vee Vian Thien

Beginning in July 2008, sodomy was featured in most Malaysian sociopolitical blogs and the headlines of Malaysian dailies for several months—a curious phenomenon given that a majority of Malaysians are either deeply religious or morally conservative, or a combination of both. Also, sodomy is a criminal offense in at least 78 countries including Malaysia.[1] The media interest was inspired by the unique identification of sodomy with the political career of a single man, Anwar Ibrahim. Anwar was charged with the offense once in 1998 when he held office as deputy prime minister of Malaysia, and again in 2008, as de facto leader of the opposition coalition, Pakatan Rakyat (PR). The timing of both trials could not be more significant. In 1998, the global spotlight was on Malaysia as host of the 1998 Commonwealth Games and for its upcoming 1999 general elections in the midst of the Asian financial crisis. On March 8, 2008, Anwar led PR to a new political dawn as a meaningful adversary to the ruling regime, Barisan Nasional (BN), in the 12th Malaysian general elections. For the first time in Malaysian history, PR stripped BN of its two-thirds majority in the federal parliament.[2]

The thriving, vibrant, and active Malaysian political blogosphere in its current form owes much to the Anwar sodomy saga. First, Anwar's trial attracted severe domestic and international criticism, which in combination with the Asian financial crisis created a hostile political atmosphere prior to the 1999 elections for his former mentor, the incumbent prime minister Dr. Mahathir Mohamad. Mahathir responded by pledging to boost Internet penetration in Malaysia through a series of programs.[3] Cumulatively, these programs effected changes necessary for the development of the Malaysian sociopolitical blogosphere. They laid the requisite physical infrastructure for access to broadband connection, that is, high-speed fiber-optic wires and ISPs, and trained a generation of "digital natives."[4]

Second, Anwar's swift coup-style removal from high political office stunned Malaysians into action. In 1998, they formed Reformasi, a grassroots movement protesting his dismal record that united disparate segments of civil society for the first time. This relatively diffuse, single-issue movement transformed into PR, a formidable opponent

to BN in 2008. Notably, on both occasions, PR and Reformasi relied heavily on the Internet to evade long-standing governmental control and surveillance of the mainstream media. The year 1998 saw the beginning of political activism on the Internet with the proliferation of pro-Reformasi Web sites.[5] In 2008, PR ran a successful campaign on blogs and Web sites, managing to elect blogger-politicians.[6] Third, because the constrained and censored mainstream media were unable to satiate the Malaysian public's hunger for details of Anwar's high-profile first sodomy trial, this news vacuum enabled Malaysiakini, an award-winning online news portal, to launch itself successfully into the role of a reliable and objective source of uncensored information.

Since 2008 the Malaysian government has made numerous attempts at asserting control over the relatively unfettered Internet, citing maintenance of racial harmony in ethnically diverse Malaysia as its regulatory justification.[7] These attempts, whether an extension of existing laws or a tabling of regulatory proposals, have been met with ferocious online resistance, especially by the Malaysian blogosphere. To date, the Malaysian government has backed down from its three most drastic regulatory proposals: implementation of a nationwide filter on the Internet, registration of bloggers, and identifying "professional" as opposed to "nonprofessional" bloggers. Although the government has not formally acknowledged these acts as a concession to online pressure, the concession can be inferred from the circumstances. This social pressure is significant in its context—the Malaysian government is not known for retracting or repealing unpopular measures, especially those infringing on civil liberties.[8]

Malaysian sociopolitical blogs, a subcategory of blogs on matters concerning the governance of state and socioeconomic concerns, figure prominently in the general Malaysian public consciousness and were especially influential in the run-up to the 2008 elections, according to a study conducted by Zentrum Future Studies, a media studies research group.[9] Zentrum's survey polled eligible voters between the ages of 21 and 41 during the election campaign period running from February 20 to March 5, 2008. Zentrum reported that 54.1 percent of 21,000 eligible voters in its nationwide sample designated the online media, that is, blogs and news portals like Malaysiakini, as their preferred source of information, as opposed to mainstream newspapers.[10] Of the 11,360 sampled voters who preferred online media, 58.5 percent ranked blogs as their primary source.[11] Blogs had a much stronger following among younger voters than their older counterparts, as figure 3.1 illustrates. Given their visibility, these blogs and their administrators have been the main Internet regulatory target of the Malaysian government.

This chapter situates the regulatory drama currently unfolding in Malaysia within the OpenNet Initiative theoretical framework of next-generation controls, as conceptualized by Ronald Deibert and Rafal Rohozinski in the context of the Commonwealth of Independent States (CIS).[12] It then identifies structural and normative features of the Malaysian political blogosphere that have enabled it to successfully contest the

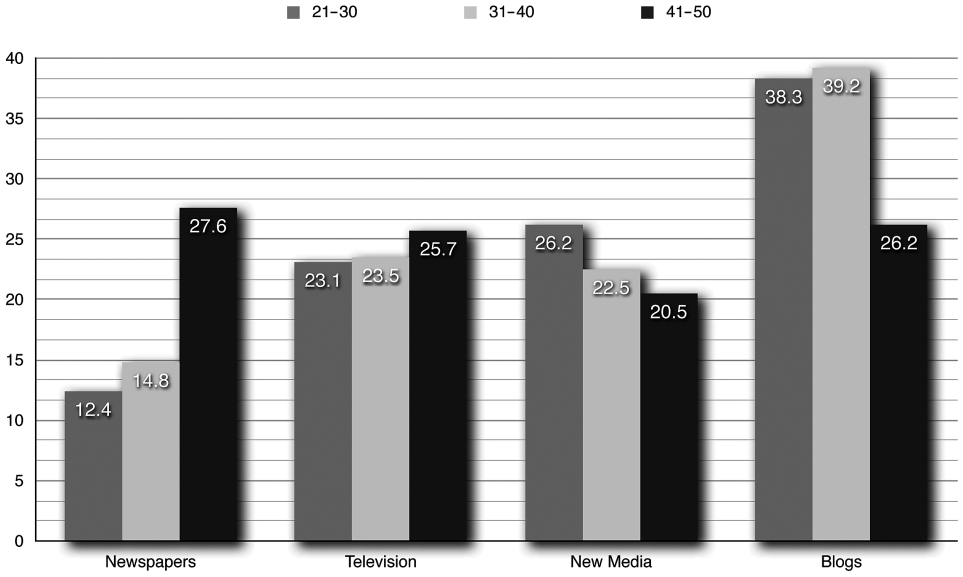

Figure 3.1
Age-based comparison of Malaysian voters' preferred media sources during the 2008 Malaysian general elections.
Source: Reproduced by permission from Zentrum Future Studies.

Malaysian government's imposition of *linear* regulatory measures, defined as traditional top-down imposition of state power. The chapter concludes by describing the recent emergence of third-generation controls in Malaysia and hypothesizing that it may be part of a wider shift toward subtler, covert, and, most importantly, *nonlinear*, participatory, and competitive forms of regulating the Internet in Malaysia. This shift in regulatory methodology also demonstrates the advent of a singular, unprecedented, bilateral dialogue between the Malaysian government and its regulatory subjects, namely, the sociopolitical blogosphere. I suggest that the direction of this conversation is still susceptible to influence by the Malaysian blogosphere.

Linear Regulatory Attempts: Hierarchical Top-Down Application of First- and Second-Generation Controls

Around 2007 the Malaysian government moved from publicly denouncing sociopolitical bloggers as untrustworthy to taking concrete steps against these vocal critics. In lieu of its well-known 1998 pledge of noncensorship of the Internet, the Malaysian government resorted mainly to second-generation controls.[13] It took a two-pronged approach in its attempt to extend traditional, unidirectional, top-down, and hence what I call

"linear," imposition of state power over cyberspace. First, it expanded its application of existing defamation, sedition, and "offensive content" laws to bloggers. Second, it proposed regulatory measures specifically targeted at bloggers or the Internet.

In January 2007, a landmark defamation suit was instigated by NSTP Corporation, a publication company with close ties to BN, against two prominent political bloggers.[14] Subsequently, the government began detaining blogger-critics under various national security laws from 2007 to 2008. Floods of complaints were also filed with the Malaysian Communications and Multimedia Commission (MCMC), the main Internet regulatory body, against sociopolitical bloggers for the criminal offense of posting "offensive content" online.[15]

Malaysian Internet service providers (ISPs) are required by law to comply with written requests from MCMC to assist in preventing the commission of criminal offenses, including the improper use of the Internet to circulate "offensive content."[16] On August 27, 2008, MCMC issued an order to all Malaysian ISPs to deny access to the controversial but popular Malaysia Today run by Raja Petra Kamarudin.[17] Only TMNet, the main Malaysian ISP, complied with this order, applying a domain-name block on Malaysia Today. This type of block is known as DNS tampering. It was significant for its unprecedented utilization of MCMC's broad statutory powers against a Web site for *offensive* as opposed to *fraudulent* content. The timing of the block also coincided with a highly symbolic parliamentary by-election in Permatang Pauh on August 26, 2008, which saw the official return of Anwar Ibrahim to parliament after his incarceration in 1998.

Subsequently, the two main distributed denial of service (DDoS)[18] attacks on Malaysia Today occurred in September 2009 and September 2010, after Raja Petra released stories on governmental corruption running to billions of ringgit that were corroborated by leaked classified documents.[19] As with the 2008 DNS block, these attacks were strategically timed, occurring when Internet traffic to the site was exceptionally high. Raja Petra has suggested that the intermittent and focused nature of the attacks indicates that its instigators were professional for-hire hackers.[20] Two other sites, Anwar Ibrahim's blog and Free Malaysia Today, an independent news portal, also reported DDoS attacks on September 10, 2010.[21]

In 2007, the Malaysian government announced plans to introduce two additional regulatory measures specific to the political blogosphere. First, a Singapore-styled registration scheme was proposed, which would have rendered registration compulsory for bloggers designated as "political" by MCMC.[22] In Singapore this scheme has arguably chilled online political speech. In 2001 the founder of a popular and active Singaporean political discussion board, Sintercom, chose to shut the site down upon receiving notification that Sintercom had been designated "political" because registration would hold him personally liable for *all* content appearing on Sintercom. This includes anonymous libelous comments, thus exposing him to the risk of ruinous

defamation suits.[23] Second, the government also proposed a labeling regime distinguishing government-backed "professional" from "nonprofessional" bloggers.[24] A third measure—far more drastic and wide-ranging than the first two—was announced on August 6, 2009. The Malaysian government declared plans to implement an Internet filter to curb access to pornography and "racially inflammatory" material. Reuters reported that a filter tender was issued to software companies on the same day.[25]

2007–2010: The Blogosphere's Backlash

Within hours of service of a defamation suit against Jeff Ooi and Ahiruddin Attan by NSTP, a blog dedicated solely to their cause was launched, a fund set up, and a solidarity logo "Bloggers United" mushroomed all over the Malaysian blogosphere.[26] After Nathaniel Tan became the first blogger to be detained under national security laws in Malaysia, a forum was held on July 20, 2007, to protest his arrest. The "Say 'NO!' to a Police State in the Malaysian Blogosphere" forum drew an audience of more than 150 individuals, and its panelists included many of the same individuals who rallied in support of Ooi and Attan, the first indicator of continuity in collective action by the blogosphere.[27]

When news of MCMC's order to ISPs to block Malaysia Today broke in 2008, in addition to resounding condemnation of the block, methods of circumventing the DNS block were posted immediately on other political blogs. The September 2010 DDoS attack on Malaysia Today was ultimately futile as copies of documents that the attack was apparently intended to block reappeared on another blog. Despite the 2009 and 2010 DDoS attacks, older Malaysia Today articles were shared on other sociopolitical blogs, mirroring the response to the DNS block in 2008.[28]

Responding to First- and Second-Generation Regulatory Proposals

The government's registration-of-bloggers scheme was reported on April 4, 2007. On April 5, 2007, a group of core sociopolitical bloggers met in person, formed an unregistered society of bloggers, the National Alliance of Bloggers (NAB), and elected its pro tem committee.[29] Members of NAB and other bloggers presented a unanimous front in condemning both registration and labeling proposals.[30] NAB organized a gathering on May 19, 2007, and hosted the forum "Blogs and Digital Democracy" five months later on October 3, 2007. Although ministerial statements indicate that the government was still contemplating new laws as of July 2007,[31] no draft legislation was ever reported, and by May 2009 the information minister affirmed that no new laws would be introduced against bloggers.[32] Anecdotal evidence and an observation of the chronology of events indicate that the fierce and quick-fire backlash by political bloggers, combined with widespread criticism, was at the very minimum a significant factor in

the government's decision to retract its regulatory plans. Following 2009 proposals of a Malaysia-wide Internet filter, politicians and civil-society activists greeted this proposal with furious criticism on the blogosphere. Less than a week later, the Malaysian government retreated from this proposal, contradicting a Reuters report that it had already issued tenders to software companies.[33]

A Malaysian Form of "Flash Mobs": Continuity in the Blogosphere's Collective Action

In October 2010 police reports were lodged against three popular political blogs for postings alleging corruption involving the information minister, coincidentally a long-time critic of Malaysian bloggers.[34] These provided the impetus for another "real-world" mobilization of sociopolitical bloggers. A week after the police reports were filed, a group of bloggers, including former members of NAB, met in person and resolved to replace NAB with Bloggers for Malaysia (BfM), whose objectives are significantly less ambitious than NAB's, perhaps in response to the difficulties faced by NAB in obtaining consensus on universal standards of blogger conduct. Instead, BfM focuses on simply looking out for bloggers.[35] Both NAB and BfM share much in common with "flash mobs," powerful groups that form and dissolve rapidly. Much like NAB's relative dormancy after the initial uproar over legislative proposals in 2007, there has been little reported action by BfM since October 21, 2010. However, the distinguishing feature of these Malaysian "flash mobs" lies in the continuity of their identity and composition.

The Wider Roles of the Malaysian Sociopolitical Blogosphere

In addition to gaining electoral visibility in 2008 and contesting linear regulatory proposals between 2007 and 2010, the Malaysian political blogosphere plays several other roles often associated in developed democracies with the mainstream press.

Blogs as the Fifth Estate

Falling through an Internet loophole in licensing and registration regimes that constrain the Malaysian mainstream media, Malaysian bloggers have taken it upon themselves to act as watchdogs of the government.[36] They report on issues omitted by the mainstream media, set the public agenda in doing so, and provide refreshing, alternative viewpoints. For example, in early 2003, East Asia was afflicted by the fatal severe acute respiratory syndrome (SARS) epidemic. Fearing widespread panic, the Malaysian government required the mainstream media to downplay reporting on the issue, prompting a frustrated Jeff Ooi to comb the Internet for international sources, collating and posting his findings on his blog, Screenshots. Unexpectedly, Screenshots

became a central hub for information on SARS, propelling Ooi's blog to international and domestic prominence.

Blogs as Catalysts for Mobilizing General Collective Action

One of the most highly visible accomplishments of the Malaysian blogosphere is its ability to rally huge protests and mobilize collective action. In a country where a gathering of three or more persons could constitute an assembly, thereby requiring a police permit, rallies, protests, and riots are rare.[37] From independence in 1957 until the emergence of the sociopolitical blogosphere circa 2005, there have been three major instances of riots. By contrast, civil society marched to protest on five separate occasions in 2007. All five were heavily publicized and coordinated by means of the Malaysian Internet and blogosphere, including the BERSIH rally calling for fair and clean elections, which attracted tens of thousands of protestors.

Blogs as Instructive Platforms of Expression

The mainstream Malaysian media steer clear of many pertinent political issues that are racially charged for fear of revocation of their printing licenses or of prosecution for sedition. By contrast, the blogosphere is strident and transparent about the "racial perspectives" taken, by both bloggers and readers who leave comments. However, "racially inflammatory" online content has not disrupted public order to date and is increasingly less commonplace, suggesting that the blogosphere may act as a "safety valve," a place to air grievances peaceably without resorting to violence and to discuss racial relations without descending to name calling.[38]

The Janus-Faced Malaysian Sociopolitical Blogosphere: A Medium of Communication and a Peer-Production System of Political Discourse

The question of how the Malaysian blogosphere has coordinated successful pushback against linear governmental regulatory attempts raises a related question of how it resolves the problem of information overload. Put simply, if anyone with access to the Internet can speak, how is anything meaningful being said or heard? The answer to both queries lies in unique features of the Malaysian political blogosphere.

Physical Clustering of Malaysian Sociopolitical Bloggers

In a 2006 study, Jun-E Tan and Zawawi Ibrahim report that Malaysian bloggers are geographically clustered.[39] An overwhelming 63.3 percent of them are located in Selangor and Kuala Lumpur, which is unsurprising given that this is the heartland of

Malaysia's IT-development projects and demographically has the highest percentage of top earners.[40] A 2008 study by Brian Ulicny reports that the active Malaysian sociopolitical blogosphere probably consists, at most, of 500 to 1,000 bloggers, "with a small, very active core of about 75 to 100 bloggers."[41] Based on the size of the political blogosphere and the geographical clustering of bloggers, the core community seems relatively easy to mobilize on short notice, especially if it is based on relationships that predate the blogosphere.

The Strength and Importance of Real-World Networks in Malaysia

There is a high degree of coincidence between the blogging community and civil-society activists in Malaysia, attributable in part to the initial lack of Internet censorship in the country. Political bloggers' demographics corroborate this overlap even further. A 2010 study by Brian Ulicny, Christopher J. Matheus, and Mieczyslaw M. Kokar observes that although 26.7 percent of their sample of random Malaysian bloggers are students, they make up a mere 5.9 percent of sociopolitical bloggers.[42] Also, the age range is correspondingly higher for this subset of Malaysian political bloggers, at an average age of 31.9 as opposed to the average of 20.5 for the sample of random Malaysian bloggers.[43]

A considerable number of top Malaysian sociopolitical bloggers are public figures in their capacity as civil-society activists, politicians, or prominent journalists. In a sample of 46 of the top sociopolitical blogs, drawn from a combination of the 2006 and 2010 studies, 34 bloggers reveal their identities. Of these, at least 20 fall within one of the three categories mentioned earlier. In addition, civil society strongly supports bloggers. The National Press Club hosted both 2007 and 2010 meetings establishing NAB and BfM, respectively. Also, the four Bloggers Universe Malaysia events to date have been jointly coordinated by NAB and the Center for Policy Initiatives, a nonprofit reformist think tank populated by bloggers.

Several propositions can be extrapolated from these observations and data. The higher median age of most sociopolitical bloggers provides a partial explanation for sustained participation within the blogosphere—Malaysian political bloggers are unlikely to be transitory college students. The significant number of these bloggers who were public figures prior to blogging accounts for the blogosphere's visibility, with its speakers drawing on their existing offline audiences. The remarkably rapid and impassioned responses by the blogosphere to regulatory proposals are unsurprising when juxtaposed against the Internet's intimate and multifaceted relationship with civil society. A comparison with Singapore illustrates the final point. By contrast to the thriving and active Malaysian sociopolitical blogosphere, its Singaporean counterpart is less visible and vocal despite Singapore's vastly superior Internet penetration rate. This contrast is especially stark when one compares Internet political activism during the countries' respective general elections, Singapore in 2006 and Malaysia in

2008. One academic reports the difference like this: "In the case of Singapore, the Internet merely exerted *some* pressure on the preexisting laws and state-imposed norms governing free speech; in contrast, in Malaysia, the Internet was a major contribution to what has been described as a 'political tsunami' during the recent general election."[44] Even allowing for Singapore's tighter online controls, election-specific regulations disallowing political videos and podcasts, and lack of explosive political scandals, academics attribute the general disparity to the preexisting strength of the offline Malaysian civil society.[45]

The observation that the success of the Malaysian sociopolitical blogosphere owes much to the existing civil society movement suggests another identifying feature of Malaysian sociopolitical bloggers: their motivations are nonpecuniary and social-psychological in nature.[46] Tan and Ibrahim report that most political bloggers cite influencing public opinion and performing a civic duty as their rewards for blogging.[47] This finding is highly relevant because it rationalizes the vehement rejection of the 2007 proposed labeling regime. To these pundits, political blogging is less attractive when government incentives are introduced because it reduces the social-psychological rewards they derive from blogging. They could be perceived as hypocritical and less credible for accepting government-backed labels while claiming to act as watchdogs of an administration accused of corruption.

On the basic premise that rewards have to outweigh costs for people to act, up until 2007 participation in the Malaysian sociopolitical blogosphere came at a low cost, because infrastructure remained inexpensive with Malaysia's aggressive IT policy. However, from 2007, the combined threats of defamation suits, detention, and MCMC persecution have raised the cost of blogging significantly, as was made evident by Raja Petra's drastic step of fleeing the country to avoid repeated incarceration. Nevertheless, the Malaysian political blogosphere remains vibrant, active, and responsive, with Raja Petra continuing to contribute from abroad in spite of the high personal costs of his participation.

Norms: The Invisible "Glue" That Binds the Malaysian Sociopolitical Blogosphere

The final missing piece of the puzzle of necessary and sufficient factors for the Malaysian blogosphere's sustained existence lies in the presence of norms. Tan and Ibrahim report that Malaysian political bloggers believe that it is *right* to double-check one's sources, that it is *better* to identify oneself openly, and that it is *wrong* to hurl racial abuse in comment boxes.[48]

The distinction between norms and social practices lies in the internal perspective of obligation, an expectation of nonlegal sanctions. One *expects* social sanctions for noncompliance with the regular practice of removing one's hat in church but not for failure to attend the cinema on a weekly basis.[49] Norms can be further subdivided into two categories.[50] Abstract norms rely on full internalization and unanimous

endorsement by participants of a social practice.[51] By contrast, concrete norms need only a desire for esteem, a much shallower mode of internalization, which in turn enables easier amendment or abandonment of these concrete norms without overall destruction of the abstract norms from which they stem.[52] This conceptual distinction has powerful explanatory force for the Malaysian sociopolitical blogosphere. From a combination of general observations and the 2006 and 2010 studies mentioned earlier, I argue that there are four abstract norms supported by a total of twelve concrete norms in the Malaysian blogosphere. The four abstract norms are as follows.

Responsible Blogging Tan and Ibrahim report that Malaysian bloggers are, in general, not exceedingly conscientious about the veracity of facts in their postings.[53] By contrast, 63.0 percent of *sociopolitical* bloggers interviewed in 2006 claim to double-check facts before posting.[54] This practice is supported by two concrete norms: the "see-for-yourself" norm of linking to original materials and the norm of disclosing one's real-life identity. This abstract norm's operation is illustrated by Anwar Ibrahim's 2007 allegations of political tampering with judicial nominations. These claims were accepted by bloggers once they had viewed a corroborating video clip uploaded by Anwar.[55]

Expectation of Bias Readers are ultimately responsible for checking the truthfulness of blog posts and making their own judgments on credibility. Out of 476 readers polled by Tan and Ibrahim who trust blogs, merely 13.2 percent admit to "strongly trust[ing]" these blogs.[56] This distrust is grounded in the subjective practice of blogging, commencing with what *bloggers* care about most, in sharp distinction to objective, neutral, public-interest reporting by professional journalists. This feeds into two separate concrete norms. First, bloggers are expected to disclose their ideologies and motivations. Second and correspondingly, readers are expected to be the final judge of content quality once bloggers have made their relevant disclosure. Criticisms of MCMC proceedings against Nose4News, a popular satirical blog known for its outlandish mock reports, demonstrate this abstract norm in practice. The blogosphere defended the blogger by pointing to clear disclaimer notices on Nose4News as sufficient discharge of the blogger's responsibilities to his readers.

Inclusivity This abstract norm has enabled relatively unknown individuals, such as Jeff Ooi, to join the ranks of A-list sociopolitical bloggers. Inclusivity is highly significant in two ways. First, it maintains conversations between bloggers and readers, albeit weighted in favor of the blogger. Bloggers are expected to enable the comment function on their blogs and to consider readers' contributions as potential sources of information. Second, as between bloggers, a concrete norm of mutual links, whether in-line citation or the maintenance of blogrolls, sustains the existence of a community of political bloggers through clustering. The conceptual distinction between abstract and concrete norms is most relevant here. Based on a sample I created of 46 of the most popular A-list political blogs, 19 do not maintain blogrolls. Nine of these belong

to blogger-politicians, some of whom kept blogrolls prior to the 2008 elections. This omission may stem from a risk-adverse political calculation, but it does not substantially weaken the overarching abstract norm of inclusivity.

Another concrete norm stemming from inclusivity is the granular and heterogeneous nature of participation in the blogosphere.[57] "Granular" means that the degree of contribution to discourse in the political blogosphere can be as minimal or extensive as one is able to make it. Contributions are also "heterogeneous"—the *type* of contribution made depends on the blogger's expertise or interest. For example, Haris Ibrahim as a trained lawyer posts on legal issues, and Tony Pua, now an elected MP, blogged almost exclusively on education in the past.

Topicality The value articulated by this abstract norm is that the determinative criteria for mutual- or cross-linking are the quality, relevance, and subject matter of the materials, not simply how well-connected they already are.[58] It is manifested in three concrete norms. First, political bloggers are expected to be motivated by nonpecuniary rewards. Second, listing in a blogroll is based on the host blogger's judgment on topicality, which is crucial in race-divided Malaysia. Most significantly, topicality is embodied in the third concrete norm requiring removal of racial slurs from blogs. These comments are not considered valuable contribution to political discourse, and racial tensions are universally acknowledged to be especially damaging in Malaysia (table 3.1).[59]

Table 3.1

SUMMARY OF ABSTRACT AND CONCRETE NORMS IN THE MALAYSIAN SOCIOPOLITICAL BLOGOSPHERE

Abstract Norms	Concrete Norms
1. "Responsible blogging"	• Double-check one's facts before posting online. • "See for yourself" links to original source • Reveal one's identity where possible.
2. Expectation of bias	• Disclosure of blogger's ideologies, motivations, or intentions • Readers are the ultimate judge of content quality.
3. Inclusivity in participation	• Permit comments to be left by readers. • Grant consideration to readers' e-mails/comments as potential sources of materials. • Mutual links encouraged by maintaining blogrolls and mutual citation • Granularity and heterogeneity are expected in contributions.
4. Topicality	• Incentive for blogging not pecuniary, but passion • If a blogroll is maintained, sites are selected based on topicality or language, not race. • Bloggers are responsible for removing racist comments, posts, and trolls.

The Malaysian Sociopolitical Blogosphere: A Peer-Production System of Political Discourse

The Malaysian blogosphere mobilizes collective action effectively and avoids plunging into a chaotic abyss of information overload by operating as a self-organizing, networked, peer-production system of political discourse. It operates much like Wikipedia insofar as it is decentralized and dependent on social cues over market prices, and its participants are motivated by social-psychological rewards. The blogosphere's topological features and norms organize the production of political conversations through a three-step process of intake, filtration, and synthesis.[60]

Intake The first step of this system of production is the intake of material. Überblogs function as central points of entry for information. Bloggers' main sources of information are online news portals, other blogs, and readers' e-mails. In addition, the elected politicians among Malaysian A-list bloggers will often have firsthand information on parliamentary proceedings or regulatory proposals. Although Malay is the official language in Malaysia, many Malaysian A-list bloggers act as links out to foreign blogs. These bloggers are linguistic bridges, translating English posts to Malay and vice versa. This practice is evident in my sample of 46 of the most popular Malaysian sociopolitical bloggers. More than half, 56.5 percent, cross-link across languages, and 32.6 percent of these blogs are themselves bilingual. Also, politician bloggers have a vested interest in maintaining multilingual blogs to reach a broader electorate base.

Filtration The relevance of content is assessed by the posting bloggers who make judgments congruent with the norms of topicality and responsible blogging. Accreditation by fellow bloggers is an important aspect of the filtration mechanism. Although readers ultimately determine the reliability of a post for themselves, the blogosphere assists this process through a form of peer review reliant on "signals." The norms of topicality and responsible blogging together maintain a pool of vocal and vigilant individuals who will make their disagreement, if any, with a speaker-blogger's views known. Corroborative posts and/or the lack of contradictory posts thus form the first signal. The next two signals are general indicators of approval—listing on a blogroll is a personal stamp of approval by the listing blogger, and hit counters form a crude indicator of any one blog site's popularity.

The blogosphere's filtration mechanism played a visible role during the campaign season of a 2010 federal by-election. The Hulu Selangor by-election saw "blogwars" explode between BN and PR supporters over circulation of "evidence" that PR's Muslim candidate consumed alcohol. When the grainy photograph first emerged on two pro-BN blogs, discerning and unaffiliated sociopolitical bloggers immediately began commenting on the awkwardness of the candidate's arms in that photograph. Eventu-

ally, these unaffiliated bloggers located the original undoctored photograph from a newspaper clipping, concluding the debate over its authenticity.

Synthesis The final stage of peer production in the blogosphere lies in synthesizing the material into blog posts. The stability of this stage depends on bloggers abiding by the norms of verification and the expectation of bias. Additionally, the concrete norm of granularity and heterogeneity is triggered at this stage, when bloggers delve into as much depth as they want on a particular topic or take a particular spin on it. Note also the continuing responsibility of bloggers to monitor comments and remove racist slurs.

Cycling back to the two questions I asked at the outset of this discussion (How does the Malaysian sociopolitical blogosphere successfully coordinate pushback against linear, unidirectional regulatory attempts and fulfill the wider roles ascribed to it?), we must recall the relevant baseline. The Malaysian mainstream media suffer two major weaknesses; they are heavily censored and are divided by language. Unlike the mainstream media, the blogosphere emerged free from licensing regimes and thus has not been forced to adopt a similarly strong norm of self-censorship. Also, while multilingual columns in Malaysian daily papers are rare, a majority of the top Malaysian sociopolitical bloggers serve as linguistic bridges. The plotted link structure of the Malaysian political blogosphere by Ulicny, Matheus, and Kokar in figure 3.2 indicates this relationship. It also suggests that there is no extreme BN/PR polarization problem (yet) akin to the Republican/Democratic divide in the U.S. blogosphere.

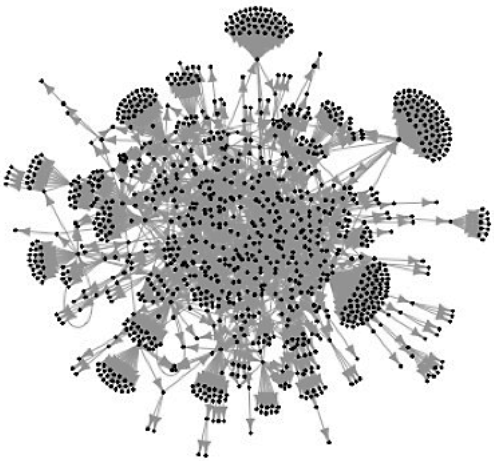

Figure 3.2
Link structure of the Malaysian sociopolitical blogosphere as of 2010.
Source: Reproduced by permission from Brian Ulicny, Christopher J. Matheus, and Mieczyslaw M. Kokar, "Metrics for Monitoring a Social-Political Blogosphere," IEEE Computer Society 34 (2010).

Because the blogosphere is a decentralized peer-production system, individual detentions and defamation suits did not cripple the system as a whole, nor could the government assert comprehensive control by usurping centralized corporate ownership. In addition, more people are speaking to each other through the medium of the Malaysian blogosphere across racial and linguistic divides that exist offline. Existing real-world relationships, networks, and civil-society activism provide a strong starting point of publicity for the political blogosphere that has been enhanced and sustained by norms. With the relative geographical proximity of Malaysian sociopolitical bloggers, these factors cumulatively enable rapid, powerful responses both online and offline to linear regulatory attempts.

A Shift Away from Linear Regulation: Third-Generation Controls

It would be a misstatement to describe BN as still being the underdog in the digital race for votes.[61] After its 2008 debacle of losing the Internet war, the incumbent BN that still controls the Malaysian federal government has demonstrated a willingness to compete for cyberspace. Recent governmental actions indicate an inception of third-generation controls that are competitive, participatory, and nonlinear. Instead of traditional, unidirectional imposition of state power on the regulatory target, these measures focus on counterinformation strategies where the state is an active player competing for online reader attention. Such measures can broadly be divided between general and election-specific measures.

Most BN politicians launched their own Facebook pages, blogs, and Twitter accounts after 2008. Joining a global trend of e-transparency, the Malaysian government launched MyProcurement.com in April 2010. MyProcurement.com is an online portal displaying all nonclassified governmental tenders and successful bids. This is a peculiarly bold and risky move because these contracts form a recurrent theme in Malaysian corruption scandals. MyProcurement.com has received mixed reviews and has led to further uncovering of corruption by PR politicians. Another notable example of online engagement occurred in August 2010. Thousands of Malaysians responded to the prime minister's invitation on his blog 1Malaysia for suggestions and comments on the 2011 national budget that was due to be tabled before Parliament.

There has also been a significant increase in anonymous disruptive attacks on both PR and independent blogs. "Cybertroopers" is now a common Malaysian catchphrase. It was coined around 2007 and refers to pro-BN Internet activists who actively monitor the Malaysian political blogosphere for antigovernmental postings. Cybertroopers are often accused of being responsible for online attacks on PR politicians. For example, on August 31, 2010, a doctored photograph depicting a Chinese PR minister slaughtering a cow during the Ramadan month of fasting was circulated online. It was thought to be the work of a BN cybertrooper and was quickly identified as a doctored image.

The intention behind circulation of the photograph was clear: it was an attempt at rupturing relations between PR's component non-Muslim and Muslim parties.[62]

Post-2008 by-elections have seen PR, BN, and independent political bloggers all establish event-specific blogs.[63] These blogs exist for a limited period of time but are updated very regularly for that short campaigning period leading to the by-election. Blogs affiliated with PR and BN post comprehensive information on their offline schedules and event venues, while their independent counterparts tend to provide neutral commentary on the candidates. Recently, Malaysiakini reported unconfirmed rumors of a BN-cybertrooper fund, valued at MYR 10 million (almost USD 3.3 million), reserved for an upcoming Sarawak state election.[64] BN has unequivocally adopted an antipodal position to Internet campaigning and the "trustworthiness" of blogs in the years since its dismissive and ultimately costly stance in 2008.

Conclusion

The battle for control of Malaysian cyber-informational space is far from over, and its lines have shifted dramatically since the 2008 general elections. By contrast to the pre-2008 identification of online activism with civil society or PR, there is now a perceived three-way cleavage in the Malaysian sociopolitical blogosphere between BN supporters, PR supporters, and independent commentators. However, even so-called BN-affiliated bloggers have not escaped the government's heavy-handed reliance on existing laws criminalizing sedition or "offensive content." One explanation for NAB's reformation as BfM on thinner grounds of commonality lies in the inadequacy of political affinity as a shield from governmental persecution. Both PR-controlled state governments and BN's federal administration have filed numerous MCMC complaints against bloggers, regardless of political identity.

The recent surge of third-generation controls against the Malaysian sociopolitical blogosphere suggests two emerging patterns. First, there is a growing governmental preference for covert, subtle, and mostly nonlinear forms of *general* Internet regulatory controls in Malaysia. Although detention of Malaysian bloggers has ceased since 2008, there has been a less-publicized exponential increase in the number of MCMC proceedings against bloggers and independent news portals.[65] I consider MCMC action to be a subtler, albeit linear, form of control because its reasons for action are not necessarily traceable to the state—it is statutorily empowered to act on its own initiative or on receipt of complaints from individuals.[66] Further, this general movement is also reflected by the shift in the *type* of technical attacks launched against blogs and independent news portals. Following public outcry against the 2008 DNS block on Malaysia Today, all subsequent denial-of-access incidents affecting blogs and portals have been DDoS attacks. Because it is nearly impossible to trace the source of these attacks, blame cannot be attached to the state with any certainty.

The blogosphere is less able to respond effectively to these new measures than to overt, linear regulatory controls. For example, MCMC's broad interpretation of its statutory powers is harder to utilize as a rallying point to mobilize the masses, when compared to the state's 2007 overwhelmingly disproportionate reliance on national security laws to detain bloggers. Similarly, the blogosphere could neither marshal technical resources to effectively resolve DDoS attacks nor concentrate criticism on state actors to attract international sympathy, unlike its public campaign to evade the DNS block. Although the blogosphere uncovered original photographs in the incidents involving circulated doctored images, criticism was limited to and directed against pro-BN bloggers when no direct state-link was conclusively established.

Reasons for this shift are manifold. One view rests on a cynical assumption that the Malaysian government's actual goal is to extend existing state control over the mainstream media to the Internet. By this account, the shift is simply the result of a discovery that nonlinear controls have the twofold benefits of efficacy and a lower political price, as they are inherently more difficult to attribute to the state—which is especially appealing to the embattled BN administration. An opposite interpretation sees these controls as a positive sign of increased engagement between the state and its subjects. Regardless of which view is taken, the pivotal point here is that the government *has* changed tack. Its change is significant in the historical context because the Malaysian government is rarely swayed by public pressure. For example, the most widely circulated newspaper, *The Star*, was once a vocal critic of the Malaysian government. The state responded swiftly in 1987, revoking *The Star*'s publishing license in a concerted strike against growing political dissent. When reinstated several months later, *The Star* was and remains a pale version of its former self. Thus the Malaysian government's willingness to react and adapt to the blogosphere's resistance, regardless of its motivations for doing so, is unique.

My second suggestion is that there is now a dialogue between the state and the political blogosphere. A combination of factors has created fertile ground for the Malaysian blogosphere to take deep root in its current form in the Malaysian public consciousness. They range from the inadvertent, such as a decade-old pledge not to censor the Internet and BN's current political vulnerability, to the unexpected, such as the continuing Anwar sodomy saga and the fervency of online civil society activism. Arguably, the blogosphere has more successfully contested linear forms of governmental control than any other nonstate actor, forcing the Malaysian government to engage in an asynchronous dialogue. The script of this colloquy is as follows: the government initiated contact by attempting to impose hierarchical control over the blogosphere and was met with ferocious resistance. This prompted the state to retreat and rechannel its efforts instead through subtler means and competing with its own information campaign. Features of the sociopolitical blogosphere that enabled this initial exchange may now work to its disadvantage. For example, its decentralized

structure, low barriers to entry, and norm of inclusivity mean that BN supporters cannot be excluded despite their flouting the norm of responsible blogging by initiating vicious, unfounded attacks on non-BN bloggers. The ball is now in the political blogosphere's court; if it wishes to develop positive aspects of this conversation, the blogosphere needs to innovate and evolve in order to seize the lead in the precious, but increasingly precarious, dialogic space it has managed to create.

Notes

1. International Lesbian, Gay, Trans and Intersex Association, "World: Illegality of Male to Male Relationships," http://ilga.org/ilga/en/article/about_ilga.

2. See the Malaysia country profile in this volume for further details.

3. These programs include the Multimedia Super Corridor, described in further detail in the Malaysia country profile in this volume.

4. John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books, 2008), 1–15, define "digital natives" as people born after 1980 who "all have access to networked digital technologies. And they all have the skills to use those technologies" (1).

5. Agus Sudibyo, "Reformasi According to Malaysiakini," *Southeast Asian Press Alliance*, May 12, 2010, http://www.seapabkk.org/announcements/fellowship-2004-program/46-reformasi-according-to-malaysiakini.html.

6. See the Malaysia country profile in this volume for further details.

7. Ibid.

8. See, for example, the government's insistence on going ahead with deeply unpopular plans to build another megatower in Malaysia; "Anti–100 Storey Tower Group Calls for 'Cake Party,'" November 15, 2010, Malaysiakini, http://www.malaysiakini.com/news/148257. Note in particular its persistent refusal to repeal the draconian Internal Security Act, which permits detention without trial, despite long-running calls for its abolishment. Amnesty International, "Malaysian Parliament Should Abolish Internal Security Act," September 4, 2008, http://www.amnesty.org/en/news-and-updates/news/malaysian-parliament-should-abolish-internal-security-act-20080905.

9. Zentrum Future Studies Malaysia, "Pilihanraya umum Malaysia ke 12: Pengaruh kepercayaan terhadap media dan kesannya terhadap bentuk dan corak pengundian Malaysia—Tumpuan pada kumpulan responden 21–41 tahun" [12th Malaysian general elections: The extent of faith in the media and its effect on Malaysian voting shapes and patterns—Focus on the age group of 21–41 of respondents] (Edisi PDF untuk rujukan dan naskah lengkap kajian [PDF edition for reference and a complete study]), http://www.scribd.com/doc/8751281/Zentrum-Studies-Pru12. (The group was headed by Associate Professor Abu Hassan Bin Hasbullah of the University of Malaya.)

10. Calculated from data available in Zentrum, "Pilihanraya umum," 5 Jadual 4 [Table 4].

11. Ibid.

12. Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 22–28.

13. For more details, see the Malaysia country profile in this volume.

14. Ibid.

15. Ibid.

16. Malaysian Communications and Multimedia Act 1998, sec. 263(2).

17. On August 27, 2008, MCMC issued an order to all Malaysian ISPs to deny access to Malaysia Today. As of 6:00 p.m. local time that day, only TMNet subscribers reported problems accessing the site—other ISPs' subscribers were still able to access the site. The DNS block lasted less than two weeks. The government decided to lift the ban on September 11, 2008, but detained Malaysia Today's administrator, Raja Petra Kamarudin, the following day. See generally, Debra Chong and Shannon Teoh, "Cyberspace Crackdown Limited to Malaysia-Today Website . . . for Now," *Malaysian Insider*, August 28, 2008, http://www.malaysianbar.org.my/legal/general_news/cyberspace_crackdown_limited_to_malaysia_today_website_for_now.html; Sim Leoi Leoi and Florence A. Samy, "MCMC Told to Unblock Malaysia Today (Update 2)," *The Star*, September 11, 2008, http://thestar.com.my/news/story.asp?file=/2008/9/11/nation/20080911145128&sec=nation. Note also that some commentators classify Malaysia Today as a news portal because it aggregates news from other sources. For my purposes, Malaysia Today is counted as a blog because Raja Petra self-identifies as a blogger. In addition, his *views*, not the site's aggregation of news, are arguably the main attraction of Malaysia Today.

18. For further details on DDoS attacks, see Hal Roberts, Ethan Zuckerman, and John Palfrey, "Interconnected Contests: Distributed Denial of Service Attacks and Other Digital Control Measures in Asia," chapter 7 in this volume.

19. On September 15, 2009, after Raja Petra posted a story on an MYR 12.5 billion (approximately USD 4 billion) corruption case involving the prime minister, which he corroborated by releasing PDFs of leaked classified cabinet documents, "suspicious activity" was reported attacking the site on the next day, September 16, 2009. The first round of hacking damaged the site on September 17, 2009, but the site's technical team managed to permit access to Malaysia Today by 6:00 p.m. local time. Subsequently, DDoS attacks ranging from 227 to 835 Mbps from proxy servers crippled the site's Singaporean node with the overwhelming traffic on the next day. See Raja Petra Kamarudin, "The Attacks on Malaysia Today," Malaysia Today, September 29, 2009, http://www.malaysia-today.net/archives/27311-the-attacks-on-malaysia-today-udpated-with-chinese-translation. A year later, Raja Petra again released a slew of documents from August 15 to August 27, 2010, this time on a controversial governmental buyback of Malaysian Airlines at the same price at which it was privatized, despite the MYR 8 billion (USD 2.6 billion) in losses accumulated

during its privatized state. DDoS attacks began on September 7, 2010, after his posting of another story on corruption involving the prime minister on September 5, 2010. Malaysia Today was inaccessible for 24 hours on September 7, 2010, and was intermittently inaccessible for seven days until September 14, 2010. See Malaysia Chronicle, "Fears for RPK's Safety as Attacks on Malaysia Today Continue," September 14, 2010, http://www.malaysia-chronicle.com/2010/09/attacks-on-malaysia-today-continue.html.

20. Raja Petra, "The Attacks," http://www.malaysia-today.net/archives/27311-the-attacks-on-malaysia-today-udpated-with-chinese-translation.

21. Neville Spykerman, "Cyber Attack: Anwar's Blog Latest to Be Hit," Malaysian Insider, September 10, 2010, http://www.themalaysianinsider.com/malaysia/article/fmt-malaysia-today-not-accessible-after-attacks.

22. "Bloggers May Have to Reveal Identities," Malaysiakini, April 5, 2007, http://www.malaysiakini.com/news/65558.

23. T. H. Tan, "Sintercom Founder Fades Out of Cyberspace," *Straits Times*, August 22, 2001. Note that Sintercom has since reemerged as Newsintercom, but its reincarnation is hosted abroad and run by anonymous administrators.

24. "Zam Recommends Labels for Bloggers," Malaysiakini, May 5, 2007, http://www.malaysiakini.com/news/66854.

25. Niluksi Koswanage and Royce Cheah, "Update 1—Malaysia Plans Internet Filter, Tougher Controls," Reuters, August 6, 2009, http://www.reuters.com/article/2009/08/06/malaysia-internet-idUSSP39843320090806.

26. Jeff Ooi, "Bloggers Legal Fund Being Finalised," Screenshots, January 24, 2007, http://asiancorrespondent.com/6403/bloggers-legal-fund-being-finalised/.

27. Joyce Tagal, "A Resounding NO to Police State," Malaysiakini, July 20, 2007, http://malaysiakini.com/news/70200.

28. Examples of these routing-round posts include "Three Ways to Access Blocked Malaysia Today," Liewcf.com, August 28, 2008, http://www.liewcf.com/3-ways-to-access-blocked-malaysia-today-3835/, and "How to Access Malaysia Today by Proxy and Beat the Block," Uppercaise, September 20, 2009, http://uppercaise.wordpress.com/2009/09/20/proxy-bookmarks-for-malaysia-today/.

29. Jeff Ooi, "Register the Bloggers? NAB and BUM," Screenshots, April 6, 2007, http://asiancorrespondent.com/6201/register-the-bloggers-nab-bum/.

30. Jeff Ooi, "MarinaM on Blogging 101 for Lame Politikus," Screenshots, May 9, 2007, http://asiancorrespondent.com/6107/marinam-on-blogging-101-for-lame-politikus/.

31. "Nazri Warns Bloggers Face Harsh Laws," Malaysiakini, July 25, 2007, http://malaysiakini.com/news/70375. (It was alleged that the government was "looking at formulating new laws to allow it to monitor and act against offending bloggers.")

32. "Rais Decries Dodgy Enforcement of Blogging Laws," Malaysiakini, May 13, 2009, http://malaysiakini.com/news/104230. (Rais Yatim, the Malaysian information minister, declared that existing laws were adequate to prosecute and regulate bloggers, but was critical of the enforcement of these laws.)

33. Niluksi Koswanage, "Malaysia to Cancel Internet Filter Study—Source," Reuters, August 12, 2009, http://in.reuters.com/article/2009/08/12/malaysia-internet-idINKLR52289420090812?pageNumber=1.

34. Cecilia Victor, "Rais Yatim Lodges Report over Allegations against Son," *Malay Mail*, October 12, 2010, http://www.mmail.com.my/content/52046-rais-yatim-lodges-report-over-allegations-against-son.

35. Tony Yew, "Bloggers for Malaysia," Bloggers for Malaysia, October 21, 2010, http://bloggersformalaysia.blogspot.com/.

36. Note that this "loophole" may soon be closed, as legislative amendments are being proposed to extend licensing requirements to online news portals and blogs. See the Malaysia country profile in this volume for further details.

37. Malaysian Police Act 1976, sec. 27.

38. Xiang Zhou, "The Political Blogosphere in China," *New Media and Society* 11 (2009): 1017 (referring to M. Jiang, "Authoritarian Deliberation: Public Deliberation in China," paper presented at sixth annual Chinese Internet Research Conference, Hong Kong, June 13–14, 2008).

39. Jun-E Tan and Zawawi Ibrahim, *Blogging and Democratization in Malaysia: A New Civil Society in the Making* (Petaling Jaya, Malaysia: SIRD, 2008).

40. Ibid., 44.

41. Brian Ulicny, "Modeling Malaysian Public Opinion by Mining the Malaysian Blogosphere" (First International Workshop on Social Computing, Behavioral Modeling and Prediction, Phoenix, AZ, April 2008), http://vistology.com/papers/VIS-SBP08%20.pdf.

42. Brian Ulicny, Christopher J. Matheus, and Mieczyslaw M. Kokar, "Metrics for Monitoring a Social-Political Blogosphere," *IEEE Computer Society* 34 (2010): 34–44, 36 (table 1).

43. Ibid.

44. Hang Wu Tang, "The Networked Electorate: The Internet and the Quiet Democratic Revolution in Malaysia and Singapore," *Journal of Information Law and Technology* 2 (2009): 3.

45. Cherian George, "The Internet's Political Impact and the Penetration/Participation Paradox in Malaysia and Singapore," *Media, Culture and Society* 27, no. 6 (2005): 903, DOI: 10.1177 (general observation); Tang, "The Networked Electorate," 10–11 (elections-specific). For an interesting flipside analysis of the online replication of offline relationships and networks, see Heike Jensen, Jac sm Kee, Gayathri Venkiteswaran, and Sonia Randhawa, "Sexing the Internet: Censorship, Surveillance, and the Body Politic(s) of Malaysia," chapter 4 in this volume.

46. For an in-depth analysis and discussion of social-psychological motivation and the diversity of motivations for action, see Yochai Benkler, "Coase's Penguin," *Yale Law Journal* 112 (2006): 371–446.

47. Tan and Ibrahim, *Blogging*, 52.

48. Ibid., 50–60.

49. H.L.A. Hart, *The Concept of Law* (Oxford, UK: Oxford University Press, 1994), 9–11.

50. Richard McAdams, "The Origin, Development, and Regulation of Norms," *Michigan Law Review* 96 (1997): 378–381.

51. Ibid.

52. Ibid.

53. Tan and Ibrahim, *Blogging*, 55.

54. Ibid.

55. Nathaniel Tan, "Audio Clip Further Incriminates Mahathir, Vincent Tan and VK Lingam," Jelas.info (blog), September 19, 2007, http://jelas.info/2007/09/19/.

56. Tan and Ibrahim, *Blogging*, 61 (figure 5.4).

57. I borrow and build on Yochai Benkler's definition of "granularity" and "heterogeneous," first used in the context of commons-based peer-production systems, that is, *Wikipedia* and *Slashdot*. See Benkler, "Coase's Penguin," 378–379.

58. Yochai Benkler, *The Wealth of Networks* (New Haven, CT: Yale University Press, 2006), 253.

59. See the Malaysia country profile in this volume for further details.

60. Benkler, *Wealth*, 254.

61. "Alternative Media: BN vs. PR—Who's Winning?" *Malaysian Digest*, March 15, 2010, http://www.malaysiandigest.com/features/2541-alternative-media-bn-vs-pr-who-is-winning.html. (The report finds BN having more Twitter and Facebook fans overall at 19,596 and 164,335 as opposed to PR's 17,176 and 109,472.)

62. PR's component parties include the mostly non-Muslim Democratic Action Party (DAP) and the Parti Islam Se-Malaysia (PAS), an Islamist political party.

63. See generally, Gabrielle Chong, "By-elections Cyber War Escalates," Malaysiakini, March 28, 2009, http://malaysiakini.com/news/101175.

64. Leven Woon Zheng Yang, "PBB Denies RM10 Mil Cybertrooper Fund," Malaysiakini, December 21, 2010, http://malaysiakini.com/news/151367.

65. See the Malaysia country profile in this volume for further details.

66. Malaysian Communications and Multimedia Act 1998, sec. 68, 69, and 70.

4 Sexing the Internet

Censorship, Surveillance, and the Body Politic(s) of Malaysia

Heike Jensen, Jac sm Kee, Gayathry Venkiteswaran, and Sonia Randhawa

The scholarly investigation of digital censorship and surveillance has moved from an initial focus on fact finding—what was filtered, who was under surveillance, and how this was accomplished technologically—to more contextualized investigations of the political, economic, and social dimensions of specific censorship and surveillance practices. A gender-sensitive approach is arguably more important now than ever for fully understanding the meanings and struggles over censorship and surveillance regimes. For instance, consider the central finding reported by Jonathan Zittrain and John Palfrey: "The Internet content blocked for social reasons—commonly pornography, information about gay and lesbian issues, and information about sex education—is more likely to be the same across countries than the political and religious information to which access is blocked."[1] Why should this be the case? And which logic has encouraged the common suppression of such disparate content?

The logic at issue is the logic underlying the nation-state and its task of perpetuating itself through the reproduction and renegotiation of its internal social hierarchies. We use Malaysia as a case study to point out some of these dimensions of national reproduction, tied as they are to the reproduction of citizens within national borders. At issue here is a nation's patriarchal policing of gender roles and their appropriate forms of (potentially procreative) sexuality, from an overall heteronormativity to finely tuned divisions based on class, race, region, and other salient markers.[2] This policing has been increasingly transferred to the digital realm, because this space has in unprecedented ways accommodated both the proliferation of alternative takes on the established gender and sexual order and the policing of citizens through censorship and surveillance.

Gender-sensitive research is thus urgently needed in this field of study, and our exploratory chapter is meant to chart some of the prime issues that need to be tackled.[3] To begin with, a change of perspective is required to see that the social issues in digital censorship and surveillance are not "soft" and relatively unimportant compared to "hard" issues such as political or religious persecution, but are in fact the central matters that go directly to the root of the social fabric. Attention to the reproduction

of gender and sexuality within the framework of the nation-state is essential for understanding the morality debates that have increasingly come to dominate discussions about Internet governance and digital censorship and surveillance. Such a focus is essential because different kinds of political and economic tensions within a nation-state can be mediated by contesting morality issues and related gender and sexual issues in the digital realm.

Employing a gender lens fundamentally shifts the very definitions of censorship and surveillance to include a basic lack of freedom of expression and privacy. It shows how most women and many disenfranchised men have been kept from contributing to the public sphere by social and economic structures and agents other than state censors, and how many women have been placed under surveillance by their social peers rather than state agents. In drawing attention to these circumstances, a gender lens generates a more comprehensive understanding of the agents of censorship and surveillance, showing that the state is only one among several entities and institutions that systematically hinder specific groups of people from expressing themselves freely or from enjoying a self-determined degree of privacy.

Such an augmented understanding of censorship, surveillance, and its agents is crucial for understanding the precise stakes and scope of state-initiated censorship and surveillance systems. It additionally creates a useful familiarity with agents beyond the state precisely at a time when there is growing evidence that nonstate actors have become increasingly recruited by certain states to carry out undercover censorship and surveillance missions. This practice was identified by Ronald Deibert and Rafal Rohozinski as "next-generation information controls."[4]

Similarly, as it is becoming increasingly obvious that the absence of state-imposed digital censorship and surveillance in a nation does not mean that all its citizens enjoy freedom of expression and privacy, research needs to dig deeper into the multilayered mechanisms that regulate speech and privacy. Such conditions can be illustrated quite well by our case study of Malaysia. While we could not detect any state-level Internet filtering in Malaysia when we conducted the testing for the OpenNet Initiative (ONI) in 2008 and 2009,[5] and previous ONI testing had similarly not yielded any evidence of Internet filtering,[6] censorship and surveillance have nevertheless played important roles. Before looking through a gender lens on recent developments in this field in Malaysia and in particular focusing on the significance of sexuality and morality for its body politic, we will provide further methodological grounding to our framework and hypotheses.

Agents of Censorship and Surveillance

Following the logic of international human rights law such as the International Covenant on Civil and Political Rights (ICCPR), state authorities are the agents that may

potentially curb their citizens' freedom of expression and privacy. In reality, however, distinct sociopolitical entities can be crucial agents in censorship and surveillance. Regarding regulation including censorship, Lawrence Lessig has developed a useful model that identifies the interrelated levels of norms, laws, markets, and architecture.[7] Laws constrain through the punishment they threaten; norms constrain through the stigma a community imposes; markets constrain through the price that they exact; and architectures, including hardware and programming code, constrain through the physical burdens or obstacles they impose.[8] Lessig makes the point that norms, markets, and architectures may generate their own regulatory effects, or they may be regulated by laws and thus pass on this state regulatory endeavor indirectly.

Jean K. Chalaby's work adds important dimensions of censorship to those identified by Lessig.[9] Most notably, she also recognizes media administration as well as outright state violence. Media administration includes obligations to obtain licenses, registrations, or authorizations and the requirement to deposit financial guarantees for entities wanting to establish media. Tactics of state violence encompass arbitrary arrests or physical attacks, and violent forms of censorship can also be exercised by nonstate agents, either at the behest of authorities or on their own. In fact, as recent research by the ONI in the Commonwealth of Independent States has shown, indirect and at times unlawful forms of Internet censorship instigated by states seem to play an increasing role. These next-generation information controls are often kept secret by states and may be outsourced to private or even illegally operating networks, including botnets that commit denial-of-service attacks. Next-generation controls even go beyond blocking content and services and include outsourced information campaigns designed to mislead, intimidate, fragment, confound, or hinder those perceived as enemies of the state.

Implicit in much of the literature addressing censorship is thus a definition that is not restricted to the suppression of content already produced. Censorship also means erecting enough hurdles to systematically keep specific content from reaching a social group, either at all or in a meaningful way, or to keep people from producing content in the first place. Experiences of censorship can in turn lead to self-censorship—the "slow internalization of the mechanisms of suppression."[10]

Surveillance, like censorship, can be instigated and carried out by different actors. States generally practice surveillance with the same rationales they cite for censorship, that is, to enhance national security and maintain order. They do so either directly, often within legal frameworks, or indirectly by requiring other actors to collaborate in surveillance, most notably media administrators, businesses, software writers, and other social entities. Big market players are also important agents of surveillance in their own right, and their motive is profit maximization, either by selling data trails left by customers or by using these data trails for marketing and advertising. Software writers may also be considered as autonomously involved in surveillance, at least to

Table 4.1

AGENTS, LEVELS, AND FORMS OF CENSORSHIP AND SURVEILLANCE

	State Censorship	Nonstate Censorship	State Surveillance	Nonstate Surveillance
Laws	Direct	n/a	Direct	n/a
Violence	Direct	Direct	n/a	n/a
Administration	Indirect	Direct	Indirect	n/a
Business	Indirect	Direct	Indirect	Direct
Norms/society	Indirect	Direct	Indirect	Direct
Architecture, including code	Indirect	Direct	Indirect	Direct

the extent that they voluntarily offer or embed surveillance functions in their programming. Finally, private individuals engage in surveillance on their own, often in accordance with social norms. The dimensions of censorship and surveillance just discussed are systematized in table 4.1.

The Malaysian Nation

Turning to our exploratory case study of Malaysia, to apply a gender lens first of all requires us to "defamiliarize" ourselves with the nation-state as the unit of analysis that has become self-evidently applied in much of the research on digital censorship and surveillance.

The nation-state has traditionally been defined by a sovereign government ruling over the permanent population living within its demarcated territory, and it has thus been principally concerned with organizing people and boundaries.[11] In Malaysia, race relations have significantly textured the social, political, cultural, and economic makeup of the nation. Formal politics have been contested on the grounds of ethnic interests, and the singular ethnic conflict that occurred on May 13, 1969,[12] has resulted in two national policies[13] that continue to define a nation that is artificially split into two. Although the 27.6 million[14] population of Malaysia consists of a plurality and hybridity of ethnicities and backgrounds, formally Malaysians are hailed as either *bumiputera*[15] or *non-bumiputera*—each constituting roughly half the total population. The two groups form a hierarchy in which the *bumiputera*—Malays constitutionally defined as Muslims,[16] together with some 70 groups and subgroups of indigenous peoples—are afforded a privileged position in the constitution.[17]

The state is compelled to reify the differences between the two categories of citizenship to maintain and manage the continued legitimization of its hierarchy. Gender

and sexuality are at the heart of this process. Ideologically, sexual norms and the enforcement of moral cultures serve to define the boundaries between different categories of citizen-subjects. Quite materially, these ideologies are meant to guide and police procreative (hetero-) sexuality and women's reproductive choices. The body thus becomes both a figurative and a real site for social order and control, where gender, sexuality, ethnicity, and religion are relationally constituted through and in each other.

The regulation of sexuality plays an important role in establishing the moral rights and supremacy of a particular ethnicity, which in turn helps to solidify the differences between the groups. At times of flux, the policing of these boundaries becomes accentuated. Paying attention to how sexual speech, discourse, and acts are regulated and placed under surveillance can provide important indicators on current national concerns and uncover the directions that censorship and surveillance will take.

Beyond the significance of gender and sexuality for internal stratification within the nation, these concepts are also central for the ideology of the nation as a whole. The national collective identity, or, in Benedict Anderson's influential terminology, the "imagined community," is usually based on the ideologies of the privileged groups in the nation.[18] Notably, the nation has often been imagined as female, evoking the hegemonic ideals of femininity favored by the ruling classes. Nationalism concurrently is described by Inderpal Grewal and Caren Kaplan as "a process in which new patriarchal elites gain the power to produce the generic 'we' of the nation. The homogenizing project of nationalism draws upon female bodies as the symbol of the nation to generate discourses of rape, motherhood, sexual purity, and heteronormativity."[19]

But what about real women? How are they situated in Malaysia? There is still a substantial gender disparity in terms of health, politics, and economic development. This can be seen in Malaysia's low Gender Empowerment Measure (GEM) ranking, coming in at 68 out of 109 countries, and its Gender Development Index (GDI) that ranks lower (76) than its Human Development Index (66).[20] These rankings point to systemic and structural barriers for women's equal opportunities and access to resources, which are also reflected in terms of decision-making positions. Women made up only 27.3 percent of senators in 2009, and only 10.4 percent of members of Parliament.[21] The figures do not improve much in the private sector, with only 6.1 percent of women participating at boardroom levels in the corporate sector.[22] As a result, women are significantly removed from most decision-making processes, including determining the boundaries of acceptable and unacceptable expression in the public sphere.

Media, the Internet, and Gendered Publics

A prime tool for the ideological creation of any nation has been the establishment of its public sphere, in relation to which freedom of expression and censorship have

generally been theorized. The public sphere has always been created and maintained by media, from earlier mass media/news media to the more recent Internet. In Malaysia, the flow of information, speech, and expression has traditionally been tightly regulated in multiple ways with respect to the mass media. Regulation has included a monopoly over institutions of mass media,[23] stringent and punitive licensing administration,[24] numerous laws[25] and reiterative cautions on the possible recurrence of ethnic conflicts like the one of May 13, 1969.[26] Jointly, these measures have effectively circumscribed speech perceived as "sensitive" and threatening to disrupt social relations. Self-censorship has consequently been widely practiced, from members of the mass media to the everyday person.[27]

Although the development of the Internet in Malaysia was expressly promoted by the state in the late 1990s to catalyze the nation into fully developed status,[28] it has simultaneously destabilized governmental control over the flow of information and expression in the public domain. To attract foreign investment in the Multimedia Super Corridor (MSC) and to mitigate the government's reputation for exercising strict state control of the information and communications public domain, consultations were held with several key industry leaders including Microsoft and IBM. Business here acted as an anticensorship agent, and the MSC Bill of Guarantees that came out of these consultations included the promise that there would be no censorship of the Internet.[29] This was supported through Article 3(3) of the Malaysia Communications and Multimedia Act (MCMA)—the primary piece of legislation that regulates the Internet—which expressly states that "nothing in this Act shall be construed as permitting the censorship of the Internet."[30]

Given this formal guarantee, the Internet became a unique "public" space in Malaysia. Although stemming from economic interest, this relative freedom presented opportunities for civil society to engage in and proliferate the public discourse with previously prohibited speech and information. Several alternative news sites have sprung up since the late 1990s to early 2000s, among them Malaysiakini,[31] Malaysia Today,[32] and more recently, Malaysian Insider[33] and The NutGraph.[34] They are maintained by "technopreneurs," bloggers, and journalists aiming to fill the palpable gap of independent and unbiased information not directed by the ruling political party.[35] New sites also include community sites for people of diverse and marginalized sexualities.

It may also be noted that as Internet access began to proliferate in Malaysia, not only men but also a large number of women gained access. From 2000 to 2008, the percentage of the population with Internet access grew from 15 to nearly 70 percent.[36] Data collection on access to the Internet and infrastructural reach has often not been gender-disaggregated, but the latest survey conducted in 2008 on household use[37] of the Internet[38] stated only a slight difference between the percentage of male home users (51.9 percent) and female home users (48.1 percent).

Nevertheless, the general predominance of men as principal communicators in the public sphere has not been successfully challenged in the course of the rise of the Internet. In particular, the most influential bloggers tend to be men.[39] What consequently has also remained largely intact, despite the new communicators' claims to "unbiased" information, is the "male definition of news value."[40] It means that the public sphere of politics as well as other spheres of "hard news" such as the economy, finance, and science have remained defined as masculine or, to be more precise, defined as "neutral" from a male point of view.

The global pervasiveness and longevity of this gender imbalance in both offline and online news, as well as national variations of it, have been traced by the Global Media Monitoring Project (GMMP), conducted every five years since 1995 in all parts of the globe.[41] The gender disparity in terms of what constitutes "newsworthiness" is reflected in the 2010 Malaysia GMMP report, where women make up only 15 percent of all news subjects compared to men, who make up 85 percent.[42] The report also found that women were more likely to be featured as celebrities, homemakers, students, activists, teachers, and nonmanagement workers, whereas men were more likely to be represented as royalty, politicians, government officials, police officers, diplomats, and service professionals. This result clearly indicates that gender stereotypes predominate.

The censorship of women and their points of view has come about through their structural and ideological exclusion from the public sphere and its media, but it has also happened more directly through the use of sexist language and threats of sexual violence. Both strategies to silence women's speech continue to thrive on the Internet. Take for instance, Pamela Lim's experience on a popular Web site, http://www.loyarburuk.com, which provides a platform for discussing current topics in Malaysia. On October 10, 2010, she posted a video of two police officers who she claimed had behaved in an intimidating manner after stopping her car and asking her for a bribe to overlook an alleged traffic offense.[43] This video post received an unprecedented number of hits on the site and more than 700 comments. A majority of the comments that disagreed with her action were made up of personal attacks and employed racist and sexist language to condemn her act of citizen journalism. For example, one of the comments read, "Oh pammy, you remind me of my f*ck buddy a couple of years ago. A real 'miss-know-it-all.' She just couldn't shut up even if she tried. There was really only one way to keep her quiet and yes, she was a guzzler!"[44]

Here we find a pattern common to many media, in which women as a gender group tend to be predominantly confronted with attempts of censorship by nonstate actors. Meanwhile the state might even promote equal opportunities, but without striking at the commercial, social, and normative roots of gender-based discrimination, these initiatives generally do not go far. This is why authors like Sharzad Mojab see the "censorship of feminist knowledge" as a root problem, stating, "I believe that the

subtlest censorship is denying feminist knowledge a visible role in the exercise of power. The state, Western and non-Western, rules through privileging androcentric knowledge as the basis for governance."[45]

The Malaysian state did try to encroach on the Internet to bring it more in line with the tight restrictions on "traditional" media. This effort has led to a situation in which the Internet is free from censorship only from the point of view of Internet law and, as ONI found, free from systematic Internet filtering.[46] Meanwhile, existing and non-Internet-specific laws such as the Sedition Act,[47] Official Secrets Act,[48] Internal Security Act,[49] and Defamation Act[50] have been used to restrict the kinds of content and speech that are allowed online. However, given the laws' reputation as tools of state repression and intimidation, their application was swiftly critiqued (and amplified over the Internet) by civil-society actors as constituting a breach of the initial promise of a censorship-free Internet.

This response presented a dilemma for the state, augmented by new and irrefutable evidence that the leading political group itself was actually at stake. The 2008 general elections in Malaysia saw the ruling coalition lose two-thirds of its majority in Parliament for the first time since the nation's independence. The Internet was credited with playing a significant role in the outcome of this election, providing a relatively freer and more independent avenue for information exchange and dissemination, and even fund-raising.[51] This signaled a time of transformation, in which the established social order was threatened by a new form of political engagement that appeared to reject familiar race-based politics.

It is at such points of status and boundary anxieties that the policing of sexuality becomes pronounced, so that a restoration of the symbolic cohesion and social order is attempted through reinstating the integrity of the material and sexed body, with its accompanying morality discourse. The apparent "free flow" of the Internet has become increasingly scrutinized and regulated vis-à-vis the subject of sexuality. Two major state strategies can be identified in this regard, to which we turn in the next section.

Sexualizing Censorship and Surveillance

The first strategy consisted of a consolidation of state power over the Internet through a reconfiguration of the government machinery responsible. In 2009 newly elected Prime Minister Mohd Najib Razak formed the Ministry of Information, Communications, and Culture (KPKK). The communications sector was removed from the Ministry of Energy, Water, and Communications, and merged with the highly powerful Ministry of Information and, interestingly, the Ministry of Unity, Culture, Arts, and Heritage. This change clearly signaled that information and communications technology (ICT) was no longer seen as primarily a matter of infrastructure as it had been in the late 1990s. Instead, its role in shaping the nation and its internal boundaries through

information exchange, discourse proliferation, and expression was being recognized. Consequently, it has become anchored to the state machineries responsible for both the "hard" aspects of intelligence and state propaganda (information) and the "soft" aspects of arts and culture. This change also means that the minister who presently holds such a wide ambit of power is also responsible and much empowered under the MCMA.

The second strategy involved attempts to create a sense of moral legitimacy for Internet regulation by infusing it with a paternalistic framework of sexuality. Again, this strategy was attempted because other tactics of state censorship were met with harsh public criticism. In the early months of 2009 there were increased prosecutions under various pieces of legislation including the MCMA for the publication of materials online. Section 233 of the MCMA makes it an offense to transmit, create, or solicit any content that is "obscene, indecent, false, menacing or offensive in character with the intent to annoy, abuse, threaten or harass another person."[52] For the first time in its history, it was used to convict an Internet user for posting a comment on a Web site that was deemed insulting to the monarchy. A hefty fine of MYR 10,000 (USD 3,000) was imposed with the expressed rationale of acting as a deterrent and warning to members of the public from freely posting their thoughts online.[53] In view of the political transformations during that period, this fine significantly challenged the credibility of the act.

At the same time, a huge public debate was raised on the issue of online privacy in response to an incident where private photographs of a popular female public official from the opposition party were posted online as a tactic to shame or discredit her, an increasingly common practice in the "Web 2.0" context in many parts of the world.[54] The incident rendered visible the lack of laws against sexual harassment (both online and offline). However, instead of taking any steps to finally legislate on a sexual harassment bill or a data protection act—both having been in the pipeline for almost a decade—the same Section 233 of the MCMA was put forward as providing viable legal remedy for the protection of women against online sexual harassment, or blackmail by spouses who threaten to publish private and sexualized photographs online.[55]

This disregard for the actual recommendation by women's rights groups,[56] together with the wide interpretation of the law, indicate that the goal is not so much to realize and protect women's rights on the Internet as to strengthen the scope of the MCMA and to recover its moral legitimacy. It is also interesting to note that censorship was being proposed as a viable measure to counter the public invasion of a woman's privacy. After being mooted since 1998, the Personal Data Protection Bill 2010 was finally passed on April 5. However, the scope of the law is limited to the processing of personal data in commercial transactions, and the government is exempted from its purview. This provision effectively compromises its potential to act as an effective counterbalance to the impact of surveillance and self-censorship.

Religious material[57] and material related to sexuality[58] published online in Malaysia are also subjected to scrutiny.[59] Advocates and organizations that defend the rights of Muslim women, such as Sisters in Islam (SIS), face constant attacks because they not only directly challenge the power of the state overdefining "Islam," but they do so from a standpoint of gender equality and women's rights. In 2008, SIS's publication on progressive interpretations of Islam was banned,[60] and its Web site has been repeatedly compromised[61] since the opposition Islamic political party (PAS) called for an investigation and ban of the organization in 2009.[62]

However, due to the "informal" nature of such censorship efforts, which confirm a trend found by ONI's research,[63] they are rarely visible in reporting or documented in efforts to monitor the space for public expression and information exchange. Yet it is clearly evident that these censorship efforts respond to the perceived threats to the nation's constitution posed by groups such as SIS and their promotion of alternative discourses on gender, sexuality, and religion.

Finally, in August 2009, in synchronicity with the global thematic trends of Internet content regulation, the KPKK minister announced the government's intention to implement Internet filtering to reduce "Malaysian children's exposure to online pornography."[64] Despite renouncing the proposal after being met with alarm by content producers, in particular alternative online media providers and bloggers, the minister acknowledged that the Malaysian Communications and Multimedia Commission (MCMC) has been tasked to find appropriate solutions to the as-yet-unsubstantiated claim of the threat to children's safety from pornography.[65] This development presents a merging of both technical and discursive solutions in regulating the unruly online space.

Even though business acted as promoters of free speech in the consultations for the MSC Bill of Guarantees, industry self-regulation does not necessarily by extension equate with free speech. When the Communication and Multimedia Content Forum (CMCF) was formed by the MCMC together with industry players, academics, civil-society organizations, and selected prominent individuals, it developed a content code that includes provisions promoting rights-based and nondiscriminatory forms of content. However, application of the code is voluntary, and it appears that private companies prefer to implement their own individual policies and guidelines to meet potential concerns and liability. In fact, particularly with regard to sexual content, private companies have become central, autonomously acting agents of censorship, whose sustained background actions have both "normalized" this censorship as any company's "right" and have largely shielded it from public scrutiny and debate.

For example, the Web hosting company Exabytes changed its policy in May 2008 to prohibit "adult content" on their servers. This ban included Web sites "related to gay and lesbian"[66] content, conflating pornographic content with any type of content produced by, about, or for an already peripheral and discriminated-against section of society. However, after several complaints about this policy, the explicit mention of

"gay and lesbian" was removed and replaced with the company's overriding right to decide what falls under the "adult" category. Internet service providers (ISPs) also appear to act as moral guardians by blocking access to sites with sexual content, such as pornography-sharing sites like YouPorn[67] and RedTube,[68] as well as Gutter-Uncensored,[69] a site that solicits and publishes private videos and images that are sexual in nature, including those of local celebrities and politicians. These blockings have remained almost unnoticed beyond the sites' users, who share advice on how to circumvent them.[70] The augmented censorship role of the private sector, along with the limited redress that ordinary users have, creates a power imbalance that is strangely reminiscent of the power imbalance between the traditional mass media and their audience. How the ISPs' censorship role in the area of sexuality relates to the various stakes of the state in this regard remains to be seen.

As a last example, cases surrounding the Malaysian national identity card MyKad offer interesting insights into how programming code has been used to discipline citizens and how the data constituting gender, race, and religion are assigned and controlled through laws, culture, and norms in order to police sexualities and desires. The MyKad contains personal data (name, date of birth, address, race, and religion), photo identification, and a biometric fingerprint. It is required for any formal transaction, and every Malaysian is obligated to carry it.[71] As a result, the MyKad potentially enables the government to comprehensively place individuals under surveillance. But, in addition, the card is the digital artifact that defines and produces, and in fact attempts to "freeze," the Malaysian citizen-subject in socially acceptable positions. This fact is evident in several cases of Malaysian citizens attempting to get the data in their MyKads changed, notably after conversions from Islam or after sex-reassignment surgery. In all cases, the individual struggles over self-definition and citizenship rights became a symbolic site for the struggle over what constitutes the nation and its internal social hierarchy and order, as it is coded through race, religion, and appropriate heterosexual contracts between citizens.[72]

Conclusion

In our Malaysian case study, we have illustrated how recent, publicly available information about the development of the Internet and its regulation at various levels and through various means acquires a fuller meaning when analyzed in a gender-sensitive framework and with attention to gender indicators for this country. The overall framework we have proposed for our interpretation posits that the maintenance of the body politic within a nation requires the disciplining of women and men along specific heterosexual and gender lines, interarticulated with other social hierarchies. The public sphere and its mass media, including the Internet, have constituted a vital area in which this disciplining is negotiated, particularly around notions of sexuality and morality.

Censorship by the state and by other entities constitutes an important form of intervention in this ideological battle, and the Malaysian case has provided evidence for the overall trend in several countries, as traced by ONI testing, that direct and sustained, state-ordered filtering of the Internet may not play a crucial role in this context and may in fact be much less important than other mechanisms of censoring and silencing people employed by state actors as well as nonstate actors. In addition, the deployment of a moralistic discourse of the state's duty to regulate sexuality has become the central framework employed by the state to distract from and thus negotiate tensions between the economic objectives of Internet development in the country and the Internet's disturbing capacity to shape and disrupt ideas of the Malaysian nation and its citizens.

The Malaysian case illustrates the clash between the potential power of the Internet to instigate far-reaching economic and social changes on the one hand and the established power of political and social elites on the other hand, which tries to perpetuate itself under new conditions. Under these conditions, the initial promise of a Malaysian Internet free from censorship was not upheld by the state, which has increasingly encroached upon this medium through a variety of direct and indirect means. These include the application of peripheral laws to rein in transgressive discourse, as well as administrative procedures and identity-based surveillance designed to foster a culture of self-censorship and conformity with gender and sexual rules. Further gender-sensitive research into censorship and surveillance, in Malaysia and elsewhere, would be welcome to unearth more of the inner workings of such negotiations, as well as the circumstances and factors that may complicate these processes and could theoretically also spur many unintended consequences in the gender and sexual order of a nation.

Notes

1. Jonathan Zittrain and John Palfrey, "Internet Filtering: The Politics and Mechanisms of Control," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 35.

2. Heteronormativity refers to the privileging of heterosexuality through institutions, structures of understanding, and practical orientations. See Lauren Berlant and Michael Warner, "Sex in Public," *Critical Inquiry* 24, no. 2 (1998): 548.

3. This chapter was written by the OpenNet-Asia Gender Research Framework development team, coordinated by the Association of Progressive Communications, Women's Networking Support Programme, in partnership with the Centre for Independent Journalism, Malaysia. The full framework is available at http://www.genderit.org.

4. Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert,

John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 22–28.

5. However, there have been individual cases of sites being blocked, especially by TMNet—Malaysia's main ISP. A widely known "just-in-time" blocking example is of the popular sociopolitical blog http://www.MalaysiaToday.com, which was blocked during an important by-election in 2008 that saw the return of the opposition party's de facto leader (see Vee Vian Thien, "The Struggle for Digital Freedom of Speech: The Malaysian Sociopolitical Blogosphere's Experience," chapter 3 in this volume). More sustained and less noticed blocking has targeted popular sites featuring sexual content, discussed later.

6. See the Malaysia country profile in this volume for further details.

7. Lawrence Lessig, *Code Version 2.0* (New York: Basic Books, 2006). See chapter 11 and especially 123 and 234.

8. Ibid., 123–124. Lessig explains that protection as well as regulation has been exercised at these levels.

9. Jean K. Chalaby, "New Media, New Freedoms, New Threats," *International Communication Gazette* 62, no. 1 (2000): 19–29.

10. Brinda Bose, "The (Ubiquitous) F-Word: Musings on Feminism and Censorships in South Asia," *Contemporary Women's Writing* 1, no. 1/2 (2007): 17–18.

11. Anne McClintock, Aamir Mufti, and Ella Shohat, eds., *Dangerous Liaisons: Gender, Nation, and Postcolonial Perspectives* (Minneapolis: University of Minneapolis Press, 1997).

12. On May 13, 1969, existing racial tensions sparked a series of violent clashes between the Malay, Chinese, and Indian communities in Kuala Lumpur. This unrest led to the declaration of a state of emergency and the suspension of Parliament. See Martin Vengadesan, "May 13, 1969: Truth and reconciliation," *The Star*, May 11, 2008, http://thestar.com.my/lifestyle/story.asp?file=/2008/5/11/lifefocus/21181089; Wong Chin Huat, "Watershed elections of 1969," *The Sun*, July 26, 2007, http://may131969.wordpress.com/2008/09/27/watershed-elections-of-1969.

13. Economic Planning Unit, New Economic Policy, Prime Minister's Department, Malaysia, 1971.

14. Department of Statistics Malaysia, "Preliminary Count Report, Population and Housing Census, Malaysia, 2010," last accessed April 20, 2011, http://www.statistics.gov.my/portal/index.php?option=com_content&view=article&id=350%3Apreliminary-count-report-population-and-housing-census-malaysia-2010&catid=102%3Apreliminary-count-report-population-and-housing-census-malaysia-2010&lang=en.

15. The term *bumiputera* (literally "sons of the earth") was introduced through the New Economic Policy, and is in reference to Article 153(1) of the Federal Constitution.

16. Article 160 of the Federal Constitution defines "Malay" as "a person who professes the religion of Islam, habitually speaks the Malay language, conforms to Malay custom [sic]."

Federal Constitution (as of June 1, 2007) (Petaling Jaya, SDE: International Law Book Series, 2007), 198.

17. Article 153(1), Federal Constitution (as of June 1, 2007) (Petaling Jaya, SDE: International Law Book Series, 2007), 188.

18. Benedict Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (New York: Verso, 1983).

19. Inderpal Grewal and Caren Kaplan, "Postcolonial Studies and Transnational Feminist Practices," *Jouvert: A Journal of Postcolonial Studies* 5, no. 1 (2000), available at http://english.chass.ncsu.edu/jouvert/v5i1/grewal.htm (accessed October 4, 2009), paragraph 6.

20. "Human Development Report 2009—Country Fact Sheets—Malaysia," n.d., last accessed October 20, 2010, available at http://hdrstats.undp.org/en/countries/country_fact_sheets/cty_fs_MYS.html.

21. Zulkifli Abd Rahman, "30% Quota for Women in Decision-Making Posts," *The Star*, July 4, 2009, last accessed 20 October 2010, available at http://www.anugerahcsrmalaysia.org/2009/07/04/30-quota-for-women-in-decision-making-posts.

22. Sam Haggag, "Women at Work," *Malaysian Business*, April 1, 2010, last accessed October 20, 2010, at http://findarticles.com/p/articles/mi_qn6207/is_20100401/ai_n53096425.

23. For one of the most comprehensive surveys conducted to date, see Article 19 and SUARAM, *Freedom of Expression and the Media in Malaysia* (Kuala Lumpur: Article19 and SUARAM, 2005).

24. Print media are tightly controlled through the Printing Presses and Publications Act, and the majority of newspapers are owned directly or indirectly by political parties.

25. Laws that have an impact on freedom of expression include the Sedition Act, the Official Secrets Act (OSA), the Internal Security Act (ISA), the Defamation Act, and the Penal Code (Article 19 and SUARAM, *Freedom of Expression, and the Media in Malaysia*).

26. Vengadesan, "May 13, 1969: Truth and reconciliation"; Huat, "Watershed elections of 1969."

27. See note 24.

28. Roger W. Harris, "Malaysia's Multimedia Super Corridor—An IFIP WG 9.4 Position Paper," 1998, last accessed January 20, 2010, available at http://is2.lse.ac.uk/ifipwg94/pdfs/malaymsc.pdf.

29. Point 7 of the Bill of Guarantees states simply, "ensure no internet censorship," last accessed January 20, 2010, available at http://www.mscmalaysia.my/topic/MSC+Malaysia+Bill+of+Guarantees.

30. Laws of Malaysia, Act 588—Malaysia Communications and Multimedia Act, 1998 (incorporating all amendments up to January 2006).

31. Available at http://www.malaysiakini.com.

32. Available at http://www.malaysia-today.net.

33. Available at http://www.themalaysianinsider.com.

34. Available at http://www.thenutgraph.com.

35. For an analysis of the emergence of the Malaysian sociopolitical blogosphere, see Vee Vian Thien, "The Struggle for Digital Freedom of Speech," chapter 3 in this volume.

36. Statistics culled from ITU and MCMC, published by Internet World Statistics, "Malaysia Internet Usage and Telecommunications Reports," last accessed January 20, 2010, available at http://www.internetworldstats.com/asia/my.htm.

37. This constitutes a large part of all Internet use, with 39.4 percent of all subscriptions being for home use.

38. SKMM, "Household Use of the Internet Survey—Statistical Brief Number Seven," 2008, http://www.skmm.gov.my/link_file/facts_figures/stats/pdf/HUIS08_02.pdf.

39. Brian Ulicny, Christopher J. Matheus, and Mieczyslaw M. Kokar, "Metrics for Monitoring a Social-Political Blogosphere: A Malaysian Case Study," *Internet Computing* 14, no. 2 (2010): 36.

40. Gaye Tuchman, *Making News: A Study in the Construction of Reality* (New York: Free Press, 1978), 138.

41. See the self-description on the home page, last accessed October 15, 2009, available at http://www.whomakesthenews.org/gmmp-background.html.

42. National Report: Malaysia (Global Media Monitoring Project 2010), last accessed October 20, 2010, available at http://www.whomakesthenews.org/images/stories/restricted/national/Malaysia.pdf.

43. Pamela Lim, "Police Intimidation Caught on Video" (video), LoyarBurok, October 10, 2010, http://www.loyarburok.com/the-system/bolehland/video-police-intimidation-caught-on-video.

44. Ibid. See comments section.

45. Shahrzad Mojab, "Information, Censorship, and Gender Relations in Global Capitalism," *Information for Social Change* 14 (2001–2002), http://www.libr.org/isc/articles/14-Mojab.html.

46. See the Malaysia country profile in this volume for further details.

47. For example, see R.S.N. Murali, "Reckless Bloggers Can Be Prosecuted," *The Star*, August 18, 2009, http://thestar.com.my/news/story.asp?file=/2009/8/18/nation/4540459&sec=nation.

48. For example, see SEAPA, "Blogger Arrested under Official Secrets Act, Another under Investigation; Symptomatic of Clampdown on Online Expression, Says SEAPA," IFEX, July 16, 2007, http://www.ifex.org/malaysia/2007/07/16/blogger_arrested_under_official/.

49. For example, see Committee to Protect Journalists, "Malaysian Blogger Jailed for Two Years under Security Act," September 23, 2008, http://www.cpj.org/2008/09/malaysian-blogger-jailed-for-two-years-under-secur.php.

50. For example, see "Malaysian Blogger Charged with Criminal Defamation," Committee to Protect Journalists (CPJ), July 23, 2008, http://www.unhcr.org/refworld/country,,CPJ,,MYS,4562d8cf2,48a5754433,0.html.

51. Tommy Thomas, "Election 2008: Crossing the Rubicon," Aliran, April 30, 2008, http://aliran.com/720.html?.

52. Laws of Malaysia, Act 588—Malaysia Communications and Multimedia Act, 1998 (incorporating all amendments up to January 2006).

53. Jacqueline Ann Surin, "Fined RM 10,000 for Insulting Sultan," The Nutgraph, March 13, 2009, http://thenutgraph.com/fined-rm10000-for-insulting-sultan.

54. Lee Yuk Peng, Wani Muthiah, Loh Foon Foong, and Sim Leoi Leoi, "Nude Pix Scandal Hits PKR Rep (Update 7)," *The Star*, February 16, 2009, http://thestar.com.my/news/story.asp?file=/2009/2/16/nation/20090216115814&sec=nation.

55. "Privacy: Does It Exist in Malaysia? Is It Time to Legislate?" Malaysian Bar, http://www.malaysianbar.org.my/human_rights/privacy_does_it_exist_in_malaysia_is_it_time_to_legislate_.html.

56. NGO Shadow Report Group, "NGO Shadow Report on the Initial and Second Periodic Report of the Malaysian Government: Reviewing the Government's Implementation of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)," 2005, http://www.iwraw-ap.org/resources/pdf/Malaysia_SR.pdf.

57. Committee to Protect Journalists, "Malaysian Blogger Jailed for Two Years under Security Act," September 23, 2008, http://www.cpj.org/2008/09/malaysian-blogger-jailed-for-two-years-under-secur.php.

58. For example see "Malaysia Says NO to Internet Porn—But What's Wrong with Health Sites?" Softpedia, June 30, 2005, http://news.softpedia.com/news/Malaysia-Says-NO-to-Internet-Porn-4044.shtml.

59. For example see "Stern Warning to Those Who Violate Laws on Net," *The Star*, August 20, 2009, http://thestar.com.my/news/story.asp?file=/2009/8/20/nation/4556160&sec=nation.

60. An SIS publication entitled *On Muslim Women and the Challenges of Islamic Extremism* was banned by the Home Ministry in 2008, under Section 7 of the PPPA, on the grounds that it was "prejudicial to public order," as reported by Lisa Goh, "Book Ban Is Irrational and against Constitution: SIS Lawyers," *The Star*, October 28, 2009, http://thestar.com.my/news/story.asp?file=/2009/10/28/nation/20091028201322&sec=nation. SIS challenged the order, and in the High Court quashed the Home Ministry's ban on January 25, 2009. *SIS Forum (Malaysia) v. Dato Seri Syed Hamid Albar bin Syed Jaafar Albar* [2009].

61. Interview of the authors with Mas Elati, communications officer of Sisters in Islam, October 18, 2009.

62. "42 'Deeply Disturbed' Groups Urge PAS to Recant Call to Ban SIS," *The Star*, June 14, 2009, http://thestar.com.my/news/story.asp?file=/2009/6/14/nation/4117613&sec=nation.

63. Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace."

64. "Najib: Govt Will Not Censor the Internet (Update)," *The Star*, August 7, 2009, http://thestar.com.my/news/story.asp?file=/2009/8/7/nation/20090807143305&sec=nation.

65. Ibid.; Mazwan Nik Anis, "Govt to Study 'Negative Impact' of the Net," *The Star*, August 13, 2009.

66. A copy of an e-mail by Exabytes that details this policy is reproduced in a blog that followed the protest by various individuals about the change in policy (last accessed January 20, 2010), available at http://lainie.tabulas.com/2008/04/25/i-will-not-like-it-if-your-website-host-is-exabytes./.

67. Available at http://www.youporn.com.

68. Available at http://www.redtube.com.

69. Available at http://www.gutteruncensored.com.

70. See Gutteruncensored.com "How to Access Gutteruncensored.com from Malaysia?" Facebook page, last accessed January 9, 2011, available at http://www.facebook.com/topic.php?uid=71689381800&topic=9595; "Accessing Youporn, Gutter Uncensored or Other Blocked Websites within Malaysia," Programming-Is-Fun.com, September 18, 2008, http://www.programming-is-fun.com/2008/09/accessing-yourpon-from-malaysia.html.

71. Annie Freeda Cruez, "Malaysians Told: Carry ICs or Risk Detention," *New Straits Times*, May 14, 1998.

72. See Jane Perez, "Once Muslim, Now Christian and Caught in the Courts," *New York Times*, August 24, 2006, http://www.nytimes.com/2006/08/24/world/asia/24malaysia.html; "Sex Change Won't Validate Same Gender Marriage: Tan," Daily Express Newspaper Online, November 15, 2005, http://www.dailyexpress.com.my/news.cfm?NewsID=38393. In the case of *Wong Chiou Yong v. Pendaftar Besar/Ketua Pengarah Jabatan Pendaftaran Negara* [2005] 1 CLJ 622, the High Court ruled that Wong, a female-to-male transsexual, could not alter the gender assigned to his identity card after his sex-change operation without an act of Parliament.

5 Internet Politics in Thailand after the 2006 Coup

Regulation by Code and a Contested Ideological Terrain

Pirongrong Ramasoota

In 2009, Thailand joined the rank of "a new enemy of the Internet," according to Reporters Without Borders.[1] This status is ironic, given the fact that the country's name means "land of the free" in Thai. This development marked a significant regress from a decade earlier when there was no cyber law and no regulator, only open Internet architecture and freedom as the central norm among first-generation Thai Internet users. Despite economic doldrums that followed a financial meltdown in 1997, freedom of expression and freedom of information in Thailand were markedly stable in the late 1990s.[2] The Thai Internet regulatory landscape gradually shifted, however, first with the establishment of the Ministry of Information and Communication Technology (MICT)[3] in 2002, which introduced the first Internet filtering policy, and later with the passing of the computer crime law in 2007, following the September 2006 military coup that overthrew the country's longest-ruling civilian administration in modern Thai history.

The period following the 2006 coup saw Thai politics bitterly divided between two opposing camps: red-shirted supporters[4] of the self-exiled former prime minister, Thaksin Shinawatra, who was ousted from power on charges of corruption and for disloyalty to the crown; and those who back the country's "network monarchy"[5]—a loose alliance of the palace, the military, the ruling Democrat Party, and the People's Alliance for Democracy (PAD), or the "yellow shirts."[6] This contest has also exhibited itself in the online sphere as powerful members of the network monarchy exercised control over Internet communication to maintain political stability while red-shirt dissidents and their supporters evaded and resisted the control through circumvention and online civic mobilization. Notably, the new computer crime law has been a potent force in constraining the behavior of Internet users as well as service providers through the new regulatory framework it imposes. In the postcoup years, the lèse-majesté offense—insulting the monarchy—has also been increasingly used to charge anyone writing or posting material deemed to be defamatory of Thailand's King Bhumibol Adulyadej or the royal family, and in blocking Internet content or shutting down Web sites.

In *Codes and Other Laws of Cyberspace*, Lawrence Lessig notes that four major regulatory elements are at play in Internet regulation—social norms, markets, technology (what he calls architecture), and law. Each of these elements, he argues, can directly limit individuals' actions in cyberspace through the different type of constraint each imposes, or they may work in combinations to constitute the "code" that regulates Internet users' behavior, that is, "regulation by code."[7] Norms constrain through the stigma that a community imposes; markets constrain through the price they exact; architecture constrains through the physical burdens it imposes; and law constrains through the punishment it threatens. Lessig emphasizes that architecture is the most sensible and influential modality of regulation. Nevertheless, he also notes that law can also change the regulation of architecture, especially when architecture (how the network is built and designed) is changed in order to realize a particular social end.

To extend Lessig's notion of regulation by code a bit further, a classical Marxist theory of ruling ideology is relevant if one considers the Internet beyond its role as conduit technology and thinks more deeply about its content and communication dimensions. In Internet-restrictive countries, "code" writers tend to shape the Internet as a means to promote a certain set of views and ideas—the ideology of the ruling class—and to exclude alternative or opposition ideas or views.

Drawing on this theoretical framework, this chapter examines the recent evolution of Internet filtering in Thailand, focusing in particular on the period following the September 19, 2006, coup and on the regulation of political content and communication. I address two main questions: (1) What are the major regulatory modalities in the Thai Internet filtering regime in the post-2006-coup era, and what are their major consequences for Internet stakeholders? (2) What are the reactions from civil society, and what mechanisms for addressing Internet filtering issues have emerged in Thailand?

The study relies on extensive analysis of laws and related policies, as well as in-depth interviews with stakeholders, policymakers, regulators, and members of civil society related to Internet regulation in Thailand. The discussion shows how the Internet in Thailand has turned into a contested terrain for competing values since the political change in 2006. What had been evolving as an emerging online public sphere became threatened and eroded in the postcoup years with the introduction of content-restrictive cybercrime law, an ID-enabled architecture, and the buttressing of a dominant social norm, which together constitute a schematic regulation by "code." However, civic groups and conscientious users who do not condone this controlling scheme have resisted it by projecting freedom and transparency as underlying values while challenging the legitimacy of Internet filtering and censorship through different means. While the contested nature of these Internet politics is not exactly equivalent to the color-coded politics that Thailand has been infamous for in recent years, there are definitely strong connections and shared implications.

Background

While Internet filtering has been actively practiced in Thailand since 2002, it did not become a political issue until after the military coup d'état of September 19, 2006.[8] The coup overthrew the highly popular Prime Minister Thaksin Shinawatra[9] and marked the beginning of a tumultuous chapter in Thai political history. In the aftermath of the coup, the self-exiled Thaksin and his red-shirt supporters have exploited the Internet as a primary channel for political communication.[10] Meanwhile, much political expression in Thailand has resorted to cyberspace, which has enjoyed relatively greater freedom of expression than have other forms of mass media. While broadcast media in Thailand have historically been controlled through state monopoly of the airwaves,[11] and print media generally had a lukewarm attitude toward the coup,[12] throughout the postcoup period (which international observers call color-coded politics for its red and yellow shirts), the Internet has emerged as a major public sphere.[13] Different online political forums, online newspapers, and political Web sites have become important platforms for expression, exchanges, and debates that represent a wide spectrum of political ideologies and orientations. As a result, authorities have increasingly zeroed in on Internet content as a target for censorship and surveillance in the post-2006-coup period.

Since September 2006, Thailand has seen four different governments led by four different prime ministers. The first postcoup PM was an appointee of the military junta, the Council for National Security (CNS), while the other three were MPs elected in 2007. The fourth prime minister—Abhisit Vejjajiva, leader of the Democrat Party, rose to power after the abrupt dissolution of the People's Power Party (PPP)[14] in late 2008, and the subsequent shift of alliance by a major faction in the preceding coalition government. The Democrat-led government, which was approved by the yellow shirts (the PAD) and the network monarchy, appeared to be brokered in by the military, and this alleged political illegitimacy was consistently used as a rationale by the United Front of Democracy against Dictatorship (UDD) in staging a series of protests against the Democrat-led government in 2009 and 2010.

In March to May 2010, when the red shirts took Bangkok in a protest calling for parliament's dissolution and a fresh election, the survival of the Abhisit government was again put to the test. Repeated negotiations failed to set an election date. The protests escalated into prolonged violent confrontations between the protesters and the military, and attempts to negotiate a ceasefire failed. More than 90 civilians and scores of soldiers were killed, with a total of more than 2,100 injured by the time the military successfully cracked down on the protesters on May 19. However, unrest rapidly spread throughout Thailand as red-shirt supporters clamored for justice. Many of these grievances were pouring out into cyberspace through social media where many dissidents were active.

Despite assuming office under unusual circumstances—over doubts regarding his government's sustainability and amid grievances against government mismanagement of the 2010 bloody crackdown—Abhisit completed his second year of administration with powerful backing still intact. In 2011 he was continuing to pursue his proclaimed goals of national reform and reconciliation.

To a number of observers and political experts, Thailand's wrenching political struggle over the past few years also boils down to another daunting question—the fate of the country after the end of the ailing 83-year-old King Bhumibol Adulyadej's reign. Other than the issues of support for Thaksin and the September 19, 2006, coup's legitimacy, Thai politics has also been polarized around loyalty to the monarchy. The right-wing conservatives and pro-status-quo forces in the military and current government, the main core of the network monarchy, are insecure and fearful of what will happen after the king passes from the scene.[15] During these dubious times, cases of lèse-majesté, involving prosecution of alleged insults to the immediate royal family, have dramatically increased. Critics see charges of lèse-majesté as an effective means to silence dissent, including on the Internet.

Insofar as online political communication is concerned, lèse-majesté has been the keyword in clamping down alternative viewpoints and in blocking Web sites related to Thaksin or the UDD (the red shirts). On more than one occasion, Abhisit and the Democrat-led government publicly announced that any lèse-majesté speech would not be tolerated offline or online. As part of their much-publicized policy to promote national reconciliation, the Abhisit-chaired cabinet approved a new agency in June 2010 to look after violations of the Computer-Related Offenses Act, in particular to protect and take care of the royal institution.[16]

This complex context is necessary for a nuanced understanding of the Internet-filtering regime in post-2006-coup Thailand. At least three regulatory elements can be delineated in this emerging filtering scheme: law, architecture, and social norms.

Law, Architecture, and Social Norms: Primary Regulators of the Thai Internet Filtering Regime

Law, architecture, and social norms are the dominant forms of regulation in Thailand's post-2006 Internet filtering regime. While Internet industry operators play a role, their regulatory influence emanates largely from the enforcement of law.

Law: Computer Crime Law and Lèse-Majesté

From September 2006 until the end of 2009, Thailand saw four different governments, two periods of massive political unrest, persistent insurgency, and an unprecedented

level of political polarization. In this highly volatile context, four major legal measures have been used to control online communication:

1. The Council for Democratic Reform's Order No. 5/2549 (2006)[17] on the Ministry of Information and Communication Technology's control of information disseminated through information technology systems (known as the CDR's Order No. 5).
2. The Computer-Related Offenses Act B.E. 2550 (2007).
3. The Emergency Decree on Government Administration in a State of Emergency B.E. 2548 (2005) and the Internal Security Act B.E. 2551 (2007).
4. Lèse-majesté provisions.

Since the CDR's Order No. 5 was enforced concurrently with martial law in the period immediately after the coup, it will not be discussed here.

The Computer-Related Offenses Act B.E. 2550 (2007)

The Computer-Related Offenses Act B.E. 2550, better known as the Computer Crime Law, was the very first legislation to be passed by the CNS-appointed National Legislative Assembly (NLA), an interim legislature after the coup.[18] Although the initial drafting of the law began in 1996, it was not actually passed until 2007, following an international controversy in April 2007 when the junta-appointed minister of MICT banned video clips deemed insulting to the Thai king and threatened to sue YouTube for carrying them. This threat of a lawsuit came after failed requests to YouTube to take down the problematic clips.[19]

Since its enactment, the computer crime law has been controversial, particularly its negative implications for online freedom of expression. Unlike conventional cybercrime law, which does not regulate content,[20] the Thai Computer-Related Offenses Act classifies content offenses committed on a computer as another major offense category in addition to offenses committed against computer systems or computer data. Section 14 of the law defines offenses as the import into a computer system of

- forged or false computer data, in a manner that is likely to cause damage to a third party or the public.
- false data in a manner likely to damage national security or to cause public panic.
- data constituting an offense against national security under the penal code; and pornographic data in a manner that could be publicly accessible.[21]

According to recently published research on online censorship through law and policy in Thailand, two major types of offenses can be delineated from prosecution charges filed under the 2007 Computer-Related Offences Act:[22] (1) offenses against computer systems or data and (2) offenses against content published online. Statistics in the three years since the new law came into effect show that 45 cases fall into the first

Table 5.1

STATISTICS OF OFFENSES CHARGED UNDER THE COMPUTER-RELATED OFFENSES ACT B.E. 2550 (2007) FROM JULY 2007 TO JULY 2010

Types of Offenses	Number of Cases	Percentage
Offenses related to computer system	45	24.32
Offenses related to content	128	69.19
Cannot be clearly categorized	12	6.49

Source: Suksri, Sawatree, et al., *Situational Report on Control and Censorship of Online Media through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: Heinrich Böll Foundation Southeast Asia, 2010).

type (24.32%), 128 cases into the second type (69.19%), and 12 cases (6.49%) cannot be clearly categorized, as shown in table 5.1.

The data in table 5.1 show that the main emphasis in the enforcement of the new law is on content regulation rather than computer crimes that use computers as tools or aim at computer system as targets. National security is the main keyword for content offenses, most likely because it includes lèse-majesté (insulting the royal family), which is a taboo and a serious crime in Thai society.

The law also imposes severe sanctions for violators. For offenses against computer systems or computer data, the penalties include imprisonment of between six months and 20 years and/or a fine of between THB 10,000 (approximately USD 300) and 300,000 THB (approximately USD 9,036) while penalties for content offenses range from imprisonment for up to five years and/or a fine of up to THB 100,000 (approximately USD 3,012).[23]

Furthermore, the law grants broad powers to officials to investigate and gather evidence of a suspected offense committed by computer. Rather than suggesting the least intrusive action that will support their investigation, the law allows broad-based surveillance, censorship, and control of Internet-based activities. Competent officials, who are appointed by the minister of ICT, are authorized to do a range of things including summoning alleged parties to appear; requesting information and evidence; duplicating, decrypting, censoring, and accessing computer information; and confiscating or "freezing" computer systems.

In addition to granting these powers, the enforcement of the Computer-Related Offenses Act has important consequences for the regulation of Thai cyberspace, as follows:

1. *Legalizing blocking of Internet content*

Prior to the passing of the computer crime law, blocking of Internet content, which has been practiced since 2002 by the MICT, was always criticized for lack of legal

grounds. Critics have alluded to constitutional provisions that guarantee freedom of expression when attacking the blocking's illegality. For instance, the first clause in section 45 of the constitution reads, "A person shall enjoy the liberty to express his or her opinion, make speeches, write, print, publicize, and make expression by other means." The section goes on to prohibit the shutdown of media outlets like newspapers and broadcasting. While the Internet is never addressed in this constitutional provision, many cyber libertarians still see the Internet as a form of mass media that warrants the same protection. But with the passing and enforcement of the new computer crime law, blocking of Internet content is now legalized, falling as it does under the category of an offense. As section 20 of the law reads:

> In case the offences according to this law involve the publicizing of computer information that may have negative implications to national security as indicated in Part II of this law or as prescribed in 1/1 of the penal code or which may violate public order or good morals of the people, the competent officials, with approval from the appointed Minister, may petition, with supporting evidence, to the court within the jurisdiction, to halt the spread of such computer information.
>
> If the court issues an order to block the spread of information as in clause 1, competent officials may block the spread of that information themselves or request service providers to block the spread of that information.[24]

As a result, Internet filtering, which was a controversial issue in the past, is now considered legal. Since the act first came into effect, the MICT has applied section 20 to order thousands of Web sites alleged to contain lèse-majesté or pornographic materials to be blocked. Cracking down on lèse-majesté content has been identified as the MICT's policy priority.[25]

While the law specifies that a court warrant is mandatory, the actual enforcement has not been entirely strict. Based on interviews conducted as part of this study with selected Internet service providers, "requests for cooperation" from government agencies like the MICT and the Department of Special Investigation (DSI) do not always come furnished with court orders. The usual objectives of such requests are obtaining log files of Internet traffic, blocking problematic Web sites, and deleting problematic postings in online discussion forums. The requests often plainly make reference to provisions in the Computer-Related Offenses law, but without court orders. Although many service providers have qualms about blocking Internet content, they do not have any option but to comply.

2. *Indirect regulation via intermediary providers and self-censorship of online content providers*

The computer crime law enables the state to regulate intermediary providers who in turn regulate users. Section 15 of the law creates the burden of intermediary liability by imposing the same penalty on offenders as on intermediaries, regardless of prior

knowledge or intent. It claims that "any service providers [who] knowingly or unknowingly support or allow offenses indicated in Section 14 to be committed in the computer or system under his control *shall receive the same penalties as offenders under Section 14*"[26] (my emphasis).

According to the law, no distinction is made between network providers who act as mere conduits and content providers who actually host content in the way they are held liable for harmful or illegal content. Whether or not the providers have actual knowledge of the content in question or whether they quickly remove the content after becoming aware of it does not grant any immunity. However, the law does not extend liability to search engines and portals that provide links to illegal content.

Because of this intermediary liability enforcement, Internet intermediaries—network and content alike—have set up new measures to regulate content and in the process are passing regulatory constraints onto users. These measures are summarized in table 5.2.

Keeping a log file of Internet traffic is intended for investigation purposes, but the real target is the identity of users. In Thailand, where a civil registration system has been an inherent part of society for almost a century, it is relatively easy to pair IP addresses with citizen identification, since all service applications require the 13-digit citizen-identification number. While larger operators like Internet service providers (ISPs) can integrate this legal requirement into their existing operation, smaller providers—operators of Web sites, Web-hosting services, online discussion forums, and providers of institutional servers—have to set up some new form of identification and certification clearance system that makes users' network access conditional on providing credentials. In the case of Internet cafés, since they do not provide network service, customers are required to sign their names and citizen IDs in a logbook before using the service.

Meanwhile, medium to large organizational servers—academic institutions, companies, government agencies, and some Internet cafés—that provide Internet access

Table 5.2

SERVICE PROVIDERS' NEW REGULATORY MEASURES THAT CREATE INDIRECT REGULATION OF USERS AS A RESULT OF THE COMPUTER-RELATED OFFENSES ACT

New Content Regulation Measures Passed by Intermediaries Due to the 2007 Computer-Related Offenses Act
1. Keeping a log file of Internet traffic, including users' IP addresses, for 90 days
2. Identification and certification clearance requirement for users at institutional servers and for subscribers to online discussion forums
3. Installing filtering software at organizational servers to enable content filtering
4. Setting up a 24-hour monitoring system for online discussion forums
5. Incorporation of provisions of the law into codes of ethics/practice and terms of services

are increasingly installing filtering software on their systems, using a keyword or groups of keywords as criteria. Filtering criteria depend mainly on the policy of each organization, but the types of content offenses provided in the computer crime law are usually included.

Internet service providers also administer surveillance on interactive Web sites like online discussion forums and chat rooms that have registered IP addresses under their networks. For instance, CAT Telecom, a major ISP, administers this content-monitoring scheme through an in-house unit called Internet Data Center (IDC). An IDC staff member will periodically examine exchanges in online discussion forums, particularly political forums. If lèse-majesté content is found, IDC will inform the moderators of the particular online forum and give them 30 minutes to remove the content. If the content is not deleted within that time, CAT Telecom will block access to the IP address that hosts the online discussion forum.

As for operators of online discussion forums themselves, a 24-hour monitor of postings on the forum has been in place since the law came into force. While moderators of such forums make it part of their daily routine to remove illegal or harmful content, most feel reluctant and view the new law with much apprehension. The Web moderator of Prachatai (http://www.prachataiwebboard.com), Chiranuch Premchaiporn, who is now awaiting trial on intermediary liability charges filed under this law, described the main effect of the law being "a transfer of censorship from state agencies to webmaster, with the law as choker."[27] The late Somkiat Tangnamo,[28] webmaster of http://www.midnightuniv.org, admitted that he self-censored on lèse-majesté to an unprecedented level during the Abhisit government's rule. Evidently, self-censorship has become the prevalent practice for moderators of online forums, particularly politically oriented ones. See table 5.3 for a summary of such self-censorship/regulation practices during the post-coup period.

Although there has not yet been a study to examine online citizen reporters and their reaction to Internet filtering, related research shows that bloggers engaged in citizen journalism regulate content through codes of practice. In the case of OK Nation Blog, a popular journalistic blog, member bloggers develop their own sets of codes and practices, which closely observe provisions in the computer crime law and related laws like lèse-majesté.[29] In effect, legal provisions are incorporated into citizen reporters' codes and thereby become a framework for the self-regulation of bloggers.

The Emergency Decree on Government Administration in State of Emergency B.E. 2548 (2005) and the Internal Security Act B.E. 2551 (2007)

The Emergency Decree was passed in 2005 during the Thaksin administration, with the main objective of quelling the endemic insurgency in Southern Thailand. The

Table 5.3

SUMMARY OF SELF-CENSORSHIP PRACTICES IN ONLINE POLITICAL DISCUSSION FORUMS IN THE POST-2006-COUP PERIOD

Name of Online Discussion Forum	Self-Censorship/Self-Regulation Practices
www.midnightuniv.org	After lifting of the ban on the Web site in the days following the coup, the webmaster changed the site's comment-posting procedure by having all the posters send him an e-mail message rather than posting directly onto the forum so that he could filter all the postings firsthand. The practice, however, put off many regular visitors to the forum, which became a read-only forum without direct interaction among the forum users. Lèse-majesté has been the key criterion in monitoring postings, with particular sensitivity noted during the coup-installed government and the Abhisit Vejjajiva government.
www.prachathaiwebboard.com	Working staff have taken turns to maintain 24-hour monitoring of the forum to keep the postings under close watch, with lèse-majesté content a top priority. A distributed system of content monitoring was set up to enable Web moderators and users (with membership longer than one month) to mutually develop a watch list of problematic postings by flagging them. Web moderators look into the watch list and make final judgments about which postings ought to be deleted.
www.pantip.com* (Rajdamnoen room)	Webmaster installed a one-person-one-account regulation system in which each member has to register with a citizen ID number. Only registered members are eligible to post in the forum. This way, all members/posters know that they are traceable. Web site policy states that the Web moderator has the right to remove all postings regardless of direction (positive or negative) related to the royal family.

*www.pantip.com, or *pantip* for short, is a popular Web site that specializes in online forums. Its many forums and chat rooms encompass almost all topics of common interest, ranging from politics, science, sports, and fashion to entertainment. Its political online forum is named Rajdamnoen after a major thoroughfare in Bangkok where the Democracy monument is located and where many historic prodemocracy street protests took place. Transliterated in Thai, *pantip* means a thousand tips. The name derived from Pantip Plaza, a very famous computer mall in Bangkok.

Internal Security Act (ISA) B.E. 2551 was passed in November 2007 by the military-installed legislature—the NLA. The ISA establishes an Internal Security Operations Command (ISOC), directed by the prime minister and the commander-in-chief of the army. The ISOC has the power to have relevant government officials implement any action or withhold the implementation of any action.

Both laws have imposed far-reaching restrictions on the right to free expression, peaceful assembly, and freedom of movement, and the right to a fair judicial process. During the political turmoil in April 2009, both laws were invoked on more than one occasion in certain districts of Bangkok during demonstrations by the United Front of Democracy against Dictatorship (UDD). The enforcement of these laws enabled the MICT and other government agencies to exercise broad-based censorship and surveillance of the media, including the Internet.

During the "Red Shirt Protests" from April to May 2010, a significant number of red-shirt sites were targeted and blocked, following a block list issued under the Emergency Decree that ordered 36 Web sites to be filtered. During this period ONI conducted tests on two major ISPs—state-run TOTNET and TRUE, a private telecommunications conglomerate. The testing found blocked sites under common content categories in both ISPs as follows: free expression and media freedom, gambling, political reform groups, and social networking. However, TOTNET was found to have filtered almost twice the number of sites (29 URLs) than TRUE and more content categories. For example, anonymizer and circumvention sites were blocked by TOTNET but not by TRUE. Significantly, neither TRUE nor TOTNET filtered the entire block list, with TOTNET blocking only 10 URLs from the list and TOTNET filtering this same set and an additional 13 for a total of 23 URLS.[30] Meanwhile, community radio stations and cable television stations were raided, and satellite television stations' signals were cut off.[31] While it is in effect, the Emergency Decree supersedes all other laws. It has been attacked by critics as an authoritarian piece of legislation that allows unprecedented state control.

Lèse-Majesté Provisions

Lèse-majesté—damaging or defaming the king and royal family—has been the single offense most frequently applied by the Thai authorities against Internet users and service providers under the computer crime law, largely because of the postcoup political crisis. Lèse-majesté provisions in Thai law include sections 8 and 9 of the 2007 constitution and section 112 of the penal code. Section 8 of the 2007 constitution notes that "the King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action."[32]

Lèse-majesté is also classified under Offenses Relating to the Security of the Kingdom in Thailand's penal code. It has always been part of the code and rarely subject to change since its inception in 1957. Thai authorities treat lèse-majesté as a matter of national security, and cases of lèse-majesté usually entail severe punishment. This fact is evident in section 112 of the penal code, which reads, "Whoever defames, insults, or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years."[33] The royalist Democrat government, which has ruled since late 2008, recently proposed to Parliament a legal amendment that will raise prison sentences for lèse-majesté to a maximum of 25 years. The amendment will also add a maximum fine of one million baht (about USD 28,500). Currently, lèse-majesté carries no fine.

An analysis of legal prosecutions related to Internet content since the 2006 coup shows that lèse-majesté was the leading offense. When bringing charges of defaming the monarch on the Internet, the police will usually cite section 14 of the computer crime law together with section 112 of the penal code, since the offense is covered by provisions in both pieces of legislation. See table 5.4 for analysis of prominent cases of Internet content offenses during the post-2006-coup period.

Of all the content offenses charged, the only unresolved case is that of Chiranuch Premchaiporn, webmaster of Prachatai. The interesting point about Chiranuch's case is that she was first charged with only the computer crime law under an intermediary liability charge because the alleged lèse-majesté comment was posted by a forum user and not by herself. However, in September 2010 she was arrested on multiple charges including lèse-majesté for an interview published on the Web site in 2008 with a man who was arrested and charged with lèse-majesté for refusing to stand up during the royal anthem in a movie house.[34]

It should be noted that lèse-majesté cases have also increased offline. From 2008 to 2009, at least four cases were charged, alongside those in cyberspace:

- A local man, Chotisak Onsoong, went to a movie and refused to stand up while the royal anthem played before the movie. He was later arrested after the movie operator reported him to the police for an act deemed an insult to the king.[35]
- An Australian man, Harry Nicolaides, was arrested and sentenced to three years in prison for having published a book that defames the crown prince.[36] He later received a royal pardon and was immediately deported to Australia.
- Political science professor Giles Ungpakorn was summoned for questioning for an alleged lèse-majesté charge. He later fled to England, for fear of not getting a fair trial.[37]
- Political activist Daranee Chancheongsilapakul, also known as Da Torpedo, was convicted of lèse-majesté and sentenced to a combined jail term of 18 years. Daranee reportedly made a series of inflammatory speeches against the king and the 2006 coup at one of the red-shirt political rallies.[38]

Table 5.4

SUMMARY OF LEGAL CASES AND OFFENSES RELATED TO INTERNET CONTENT DURING THE POST-2006-COUP PERIOD

Date of Incident	Type of Offense Allegedly Committed	Summary of Incident	Legal Measures Taken
September 2007	Lèse-majesté (section 8 of the constitution, and section 112 of the penal code); input into a computer system of data that were an offense against national security or terrorism according to the criminal code [section 14(3) of the Computer-Related Offenses Act]	An alleged lèse-majesté comment against the monarchy on the now-defunct political forum Web site www.propaganda.forumotion.com by a man using the pseudonym of Praya Pichai. The man was brought into custody and jailed for two weeks but charges could not be filed for lack of evidence.	The Web site was shut down and Praya Pichai faced ten years of continued surveillance and a threatened prison term if he posts a political comment online again.
April 2008	Input into a computer system of pornographic computer data that are accessible to the public [section 14(4)] of the Computer-Related Offenses Act	Owner of 212 café online forum was arrested for hosting a link to a pornographic Web site. At the arrest time, the police could not specify the problematic URL of the link. Although the forum webmaster immediately shut down the Web site, a month later, the police raided his home office and appropriated his servers and computer devices.	The forum owner was summoned to appear at a police station and to submit the names and contact list of all the forum's clients (about 28,000 people). He eventually spent one night in jail and later posted bail for THB 100,000 (USD 3,250).
January 2009	Lèse-majesté (section 8 the constitution, section 112 of the penal code), input into a computer system of computer data that is an offense against national security or terrorism according to the penal code [section 14(3) of the Computer-Related Offenses Act]	A blogger was arrested and convicted for having uploaded royally defaming materials on the www.youtube.com Web site. He was held in custody for three months before a lèse-majesté verdict was announced in April, resulting in a ten-year imprisonment. In June 2010 his petition for a royal pardon was answered and he was released from prison.	The police (through the high-tech crime unit and DSI) kept the convicted blogger on surveillance for about six months before the arrest.

Continued

Table 5.4

(continued)

Date of Incident	Type of Offense Allegedly Committed	Summary of Incident	Legal Measures Taken
March 2009	Intermediary liability or consent/ negligence of operators for offenses to be committed (section 15 of the Computer-Related Offenses Act)	Webmaster of the independent online newspaper www.prachatai.co.th was arrested because alleged lèse-majesté comments were posted on the Web site's online discussion forum at www.prachataiwebboard.com—though she said that she had removed them immediately after the first notice from the police. She is currently undergoing trial.	Prior to the arrest, Prachathai had reportedly received "requests" from the military to remove from its Web site articles and commentaries on the monarchy and the military.
November 2009	Import of false computer data that could threaten national security or cause public panic [section 14(2) of the Computer-Related Offenses Act)	Two brokers were arrested for having posted information on two political online forums—www.prachataiwebboard.com and www.sameskyboard.org. One of the postings was a translation of a Bloomberg news service article on a rumor about the king's deteriorating health. The postings allegedly helped the market to plunge 7 percent during trading on October 14 and 15, 2009. However, the webmaster of www.prachataiwebboard.com contradicted the police theory that the two brokers were helping spread the rumors for financial gain by confirming that both were long-standing members of the forum.	High-tech crime division and DSI have been keeping both political forums under constant surveillance throughout the postcoup period. When the suspects were arrested, their apprehension was in the context of a stock market manipulation. But a police official in charge did mention that their spreading of rumors took place on "two politically problematic and controversial Web boards."

Table 5.4

(continued)

Date of Incident	Type of Offense Allegedly Committed	Summary of Incident	Legal Measures Taken
September 2010	Lèse-majesté (section 112 of the penal code); inciting unrest by publication (section 116 of the penal code); input into a computer of system computer data that are an offense against national security or terrorism according to the penal code [section 14(3) of the Computer-Related Offenses Act]; and intermediary liability or consent/ negligence of operators for offenses to be committed (section 15 of the Computer-Related Offenses Act)	Webmaster of www.prachatai.co.th was stopped at an immigration checkpoint and arrested at Bangkok International Airport after returning from the Internet at Liberty 2010 conference in Budapest, Hungary. Her arrest warrant was based upon an interview published in www. prachatai.co.th about a man who was charged with lèse-majesté for failing to stand up for the royal anthem in a movie theater in 2008.	The arrestee was bailed out on THB 200,000 (USD 6,600) bail. She was expected to report to Khon Kaen provincial police station, where the arrest warrant was issued, once a month until the case is either dismissed or filed to the public prosecutor.

Architecture: From Automatic URL Filtering to an ID-Enabled Cyberspace

Automatic URL Filtering

After the September 2006 coup, the MICT was faced with mounting complaints over lèse-majesté cases, which were reportedly mushrooming on anticoup and pro-Thaksin Web sites. The existing IP-based filtering at ISP levels, based on block lists circulated by MICT, was deemed ineffective and was also criticized for overblocking. The interim minister of ICT thus revisited the idea of an automatic Internet filtering system, which was discussed in the later years of the Thaksin administration but did not materialize. As a result, a feasibility study was carried out, and a pilot project was commissioned to local researchers. The new automatic filtering system was installed at the level of international Internet gateway (IIG),[39] which is a higher level of networking than national Internet exchange (NIX) or ISPs.[40] All IIGs under CAT Telecom Plc were the first to be installed with the new automatic filtering system, since CAT Telecom is a state enterprise and reports directly to the MICT. The filtering technology was developed by a group of computer-engineering researchers at the Bangkok-based Kasetsart University. The URL filtering technique was originally developed to filter out unwanted content such as spam but could also be used to filter Web access by blocking at application layers or at URL levels.[41] The system began a trial run in 2008 and has been fully operational since early 2009.

Essentially, the URL filtering technique uses what Robert Faris and Nart Villeneuve call proxy-based filtering strategies.[42] Internet traffic passing by the filtering system is reassembled, and the specific HTTP address being accessed is checked against a list of blocked URLs or blocked keywords in the URL. When users attempt to access these URLs, they are subsequently blocked. But instead of showing an MICT block page indicating that the site has been blocked (as would be the case of IP blocking at ISP level), the new system has created a block page that looks like the browser's default error page, possibly to disguise the fact that the government is blocking these sites.

ID-Enabled Cyberspace

Largely because of enforcement of the computer crime law, online service providers (OSPs)—those that host social networking services, blogs, and Web sites—have increasingly set up a system that enables "traceability regulation."[43] To access content and services on these Web sites, users are required to provide some sort of identification or certification first. Using traceability regulation as a framework, we surveyed popular local online services like online discussion forums, blogs, social networking services, portals, and online newspapers. The results are shown in table 5.5.

Table 5.5

IDENTIFICATION AND CERTIFICATION REQUIREMENTS OF SELECTED ONLINE SERVICES

Type/Name of Web site	Identification/ Certification upon Login	Identification/Certification upon Registration			Remark
	User Name/ Password	E-mail	13-Digit Citizen ID	Name/ Address/ Phone	
Online discussion forums					
pantip.com	√	√	√	√	Member registration requires citizen ID and a personal photo
mthai.com	√	√			
forum.serithai.net	√	√			
Blog					
blogging.com	√	√	√	√	Membership bundled with that of pantip.com
exteen.com	√	√	√		
oknation.net	√	√	√	√	Member registration requires citizen ID and a personal photo
blogger.com	√				Login via Google account
gotoknow.org	√	√		√	Member registration requires real name
asiancorrespondent .com	√	√			English-language blog. Covers politics and situation in southern part of Thailand. Provides analyses of news from the *Bangkok Post* and *The Nation.*
Social networking service (SNS)					
facebook.com	√	√			

Continued

Table 5.5

(continued)

Type/Name of Web site	Identification/ Certification upon Login: User Name/ Password	Identification/Certification upon Registration: E-mail	13-Digit Citizen ID	Name/ Address/ Phone	Remark
Twitter.com	√	√			
Hi5.com	√	√			
MySpace.com	√	√		√	Member registration requires name and birth date
Portal					
hunsa.com	√	√	√	√	Does not require citizen ID. User will be entered into "lucky draw" and able to join online auction if citizen ID is provided.
sanook.com	√	√			
kapok.com	√	√			
th.yahoo.com	√	√		√	Member registration requires name and birth date
Online newspaper					
thairath.co.th	√	√	√	√	Membership is required to search historical news
manager.co.th	√	√		√	Member registration requires name, birth date, and postal code
posttoday.com	√	√			Member registration requires name and birth date

Table 5.5
(continued)

Type/Name of Web site	Identification/ Certification upon Login: User Name/ Password	Identification/Certification upon Registration: E-mail	13-Digit Citizen ID	Name/ Address/ Phone	Remark
komchadluek.net	√	√	√	√	Membership is required to receive e-newsletter and to post comments on the news
Others (video and photo sharing, satellite TV)					
voicetv.co.th	√	√		√	Member registration requires name and birth date
youtube.com	√	√			Can watch and upload video clips
flickr.com	√	√		√	Automatically registered with Yahoo account

The most minimal forms of identification and certification required in all surveyed OSPs are user name and password for logging into the system. For registration, all providers require an e-mail address as a precondition for access, while some require name, address, and phone number, and a few require the 13-digit citizen identification number. In any case, it is apparent that an architecture of identification has been established in the Thai cyberspace as a result of the new computer crime law.

Social Norms: A Benevolent and Inviolable Kingship

While lèse-majesté may sound peculiar to non-Thais, it has been a deep-seated concept in Thai culture for centuries. The monarchy has always been a central institution in Thai society. Despite the 1932 revolution that changed the governing regime from absolute monarchy to constitutional monarchy, the king was still allowed to exercise sanctioning prerogatives of legitimization. At that time, the first constitution was regarded as a royal gift, while the throne was generally viewed as holding a position

of moral superiority over the new political leadership. This view still appears to prevail today.

In past and present constitutions, the monarch, as the head of state, has these privileges:

1. He is to be unreservedly respected: his person is inviolable, and he is not subject to the jurisdiction of the courts.
2. He is the Head of the State.
3. He is the soul of the nation and the font of national harmony.
4. He is above politics.
5. He is politically neutral, without aligning with any political group or party.
6. He can do no wrong (constitutionally).

Furthermore, the Thai conception of kingship is a combination of the Hindu divine right of *deva raja* and the Buddhist patriarchal kingship in which the king rules according to the law or dharma. Therefore, the legitimacy of the monarch is derived not only from divine right but also from his own conduct and commendable deeds. The present king, Bhumibol Adulyadej, who is now the world's longest-reigning monarch, has been credited for his lifelong dedication to rural development and the livelihoods of his poorest subjects. He is thus well loved and respected by the general Thai public. In 2006 on the 60th anniversary of his coronation, the entire country glowed yellow as loyal supporters of the king donned special yellow royal shirts in celebration everywhere throughout the year.

With exceptional privileges, conceptual dominance, and public reverence, the Thai monarchy has been used as a source of legitimacy in Thai politics. A former prime minister (1957–1963) and military dictator, Field Marshal Sarit Thanarat, made extensive use of the monarchy to legitimize his regime both domestically and internationally. This legitimization often happens at the expense of free speech. In the past, dissidents who were charged with lèse-majesté were usually social critics or those who openly resented military involvement in politics. Meanwhile, filers of lèse-majesté suits were typically from the military.

Traditionally, the monarchy has been identified as one of the core values to be protected under national security, which includes three things—the monarchy, religion (Buddhism), and the Thai nation. Any attempt to undermine these so-called three pillars of Thai society would be viewed as a threat to national security. As these core values are usually fused together, it is not uncommon for a show of disrespect, including criticism of the king, to be interpreted as "unpatriotic."

There has always been tension between free speech and royalism in Thailand, but never has the anxiety been so great as in the age of the Internet and a time of foreseeable royal succession. With the borderless and robust nature of the Internet, it is no longer feasible to keep the king virtually beyond criticism in the virtual world. But no

matter how futile and ultraconservative lèse-majesté filtering may appear to some liberal people, there are those who support it and even participate in monitoring Web sites and reporting lèse-majesté to authorities. Statistics released by the MICT show that the greatest number of complaints received on Internet content had to do with lèse-majesté.[44]

Reaction from Civil Society and Mechanisms for Addressing Internet Filtering

In response to Internet filtering issues, members of civil society have reacted in a number of ways and used varying strategies to deal with new regulatory constraints. Members of civil society also contest what they conceive to be the government's abuse of power and violation of free speech online.

Online Security Caution

According to interviews with selected civil society activists, tightening up security in their online use seems to be the top strategy in coping with authorities' censorship and surveillance. This approach was manifested most frequently in their technological choice. For instance, a few Internet advocacy activists said they deliberately gave up the more popular Windows platform and opted instead for Linux as an operating system. Some also chose to disable the conversation-recording feature of Gtalk and turn on the secure access feature (SSL) in Gmail. The majority are very cautious about their passwords. Not only do they keep their passwords as their most confidential information, but they also change passwords frequently. Their choice of password is also crucial. One online activist said he avoided words in the dictionary and used multiple layers of password protection. In using social media like Facebook or Twitter, a few activists noted that they exercise more caution in accepting friends or in setting the circle to which their personal information will be accessible. Similarly, in using online discussion forums, these activists are careful in posting comments and in registering their personal information to the Web sites. Usually, they do not give anything beyond their e-mail address to avoid being identified.

Evasion and Circumvention

When it comes to Web censorship, a number of users wishing to access blocked Internet content can find easy ways around it by using proxy or VPN or using Google translate or Google cache. But with Web 2.0 applications and social media, things are a bit more complicated to get around. At this level, OSPs that rent out server space to a large number of Web site developers and operators of social media platforms are becoming increasingly important as intermediary censors for online content. Ethan

Zuckerman refers to OSPs' role in Internet filtering as "intermediary censorship."[45] They have become important choke points for Web users who publish content on Web servers they do not control. Such censorship is observed in at least three online political discussion forums that the research team studied in the postcoup period. These findings are summarized in table 5.6.

The summary in table 5.6 clearly shows that because a number of smaller Internet providers rely on them to publish content, OSPs can be powerful entities in controlling online speech. But the same summary also shows that this newer generation of Internet publishers is savvy enough to circumvent such intermediary filtering systems by exploiting alternative hosting services overseas. While this strategy may not solve their problem entirely—since the state can still block through URL-filtering at the IIG level—it still suggests that cyber citizens make efforts to redress the problem with whatever technological options are available.

Campaigning for Local and International Support

Based on interviews with civil society members, their most immediate concern about Internet filtering in Thailand is the new computer crime law. To them, the new law is more of an effort by the after-coup government to curb threats against national security and the monarchy, rather than to stop cybercriminality. In response to arrest cases under this very law, several rights-based groups have campaigned in support of the arrestees. The most obvious case is that of Chiranuch Premchaiporn, who has been arrested twice with charges under the same law. (See details about Chiranuch's arrest in table 5.4.) Because Chiranuch is a member of the prominent online freedom advocacy group—the Thai Netizen Network (TNN)[46]—her case has been continuously reported in Prachatai (until it was blocked by the emergency decree during the red-shirt crisis of March to May 2010) and in other alternative online media including mailing lists of TNN. Ever since Chiranuch's first arrest in March 2009, campaigns to support her and Internet freedom, using her case as a rallying point, have been growing steadily.

First, only the TNN and alliance organizations like Campaign for Popular Media Reform (CPMR)[47] and Freedom against Censorship Thailand (FACT)[48] joined forces. Gradually, other local human rights nongovernmental organizations (NGOs) joined the campaign to free Chiranuch (also known by her nickname Jiew) by submitting an open letter seeking the immediate dropping of charges against her and dissuading public prosecutors from pursuing trial. These include the Network of Human Rights Lawyers, the Project on Legal Environment, and the Association for Civil Rights and Liberties. Subsequently, the circle grew to more regional participation with the Southeast Asian Press Alliance (SEAPA), Southeast Asian Media Legal Defense (SEAMLD), which is a regional spin-off from the global Media Legal Defense Initiative (MLDI),

Table 5.6

SUMMARY OF ONLINE SERVICE PROVIDERS' ROLE AS INTERMEDIARY CENSORS OF ONLINE DISCUSSION FORUMS IN THAILAND

Name of Online Discussion Forum	Intermediary Censorship Experience	Reaction
www.midnightuniv.org*	The Web-hosting company from which the forum rented server space was blocked during the aftermath of the coup and discontinued service to the forum thereafter.	Forum moderator decided to change to a new Web-hosting company and introduced a new filtering system for forum postings.
www.prachataiwebboard.com†	During the period of intense political conflict in 2008–2009, the contracted Web-hosting company decided to terminate service to the Prachatai online forum, evidently out of fear of the political sensitivity of the forum's content.	Webmaster decided to separate hosting services used for the online newspaper and for the online political discussion forum. The latter moved to rent from an overseas Web-hosting service, to avoid blocking problem.
www.sameskyboard.org‡	The contracted Web-hosting service company was reportedly pressured by the MICT to abruptly halt service for www.sameskybooks.org/ and its other online services. The MICT's interference also wiped out the affiliated online forum—www.sameskyboard.org—and all the database kept by the online publisher for the previous five years.	The editor of the www.sameskybooks.org/ publicly condemned MICT for their alleged interference and opened a temporary Web site and a new online forum. Later, the service shifted to an overseas hosting company for all its online services.

*The site www.midnightuniv.org, known as Midnight University, is a leading alternative educational Web site that compiles academic resources on various sciences including social science and anthropology. The site also provides a forum for the public to exchange opinions on matters of interest. A group of progressive-minded academics, a number of whom are from Chiang Mai University, run this Web site and the political discussion forum attached to it. After the 2006 coup, www.midnightuniv.org attracted a lot of media attention because it represented very rare voices in society that condemned the coup and denounced the postcoup (2007) constitution.

†The site www.prachatai.co.th, or Prachatai for short, is an online newspaper that is very famous for its leftist and highly critical political standing. Prachatai is also openly anti-2006-coup. Founded in 2004 by a well-known social activist, it aims to be an independent medium free from state control, after the model of the famous Minda News (http://www.mindanews.com) in the Philippines. Prachatai's initial funding was allocated by the Thai Health Promotion Foundation. Later, when the foundation blacklisted it for probing into the foundation's spending, its supporter shifted to overseas sources such as the Rockefeller Foundation and Open Society Institute. Prachatai also runs a famous left-wing online discussion forum—www.prachataiwebboard.com, of which the political room is most popular.

‡The site www.sameskyboard.org, or samesky for local users, is a popular left-wing online political discussion forum attached to www.sameskybooks.com, an online site of local publishers of *Samesky* magazines. *Samesky* magazine is well-known for its progressive and critical viewpoints on politics and society.

and Asian Human Rights Commission (AHRC), among others. At the time of writing (October 2010), a global campaign to support Chiranuch was well under way, with leading media advocacy and human rights organizations such as the Electronic Frontier Foundation (EFF), Committee to Protect Journalists (CPJ), International Court of Justice (ICJ), Open Society Institute (OSI), Human Rights Watch (HRW), and Amnesty International involved. These organizations' main criticism is directed at Thailand's censorship policy and its impact on human rights and free speech, especially in cyberspace. Both the new computer crime law and lèse-majesté have been criticized as tools to suppress dissent and persecute political opponents.

After Chiranuch's second arrest in September 2010, a wider circle of Internet users promoted her cause through social media. Examples include a campaign using "free jiew" as a tag on the popular micro-blogging site Twitter (https://twitter.com/search?q=%23freejiew); blogs dedicated to the cause (http://freejiew.blogspot.com); and a platform set up by Digital Democracy to receive donations in support of her bail (http://digitaldemocracy.chipin.com/free-jiew).

Public Advocacy and Policy Lobbying

Alongside campaigning for support at local and international levels for Chiranuch's case, civil society organizations have also been active in advocating for public awareness about Internet restrictions in Thailand. In fact, advocacy work through public education has been the core work of the TNN, of which Chiranuch is a founding member. For the past two years, TNN has been at the forefront in organizing meetings, seminars, and public forums on issues related to Internet freedom. For instance, in August 2010, TNN, together with Media 4 Democracy and SEAPA, organized a high-profile seminar on the Computer-Related Offenses Act, on its third anniversary. A former information minister, an online newspaper webmaster, a popular blogger, a media watch representative, and Chiranuch herself shared comments on the computer crime law's impact on democratization in Thailand. The common sentiment is that restrictive law and careless enforcement during political polarization will contribute negatively to democracy because self-censorship becomes the rule for safety, hence deterring debate and the climate of opinion that are so fundamental to democracy.

In addition to public education, civil society has also used policy lobbying as another avenue to redress Internet control issues. In early 2009, several rights groups, including TNN, CPMR, and FACT, submitted an open letter to current Thai Prime Minister Abhisit Vejjajiva demanding an amendment of the computer crime law to make it more transparent and less politically motivated. Although Abhisit stressed civil liberties in his inauguration speech in December 2008, he has ruled out a repeal of the computer crime law.

Ambivalence and Indifference

In contrast to the stance and strategies taken by NGOs and activists, key institutional bodies responsible for human rights in Thailand are not only slow in responding to complaints about impediments to freedom from enforcement of the new computer law, but they have also been ambivalent in the face of lèse-majesté and the protection of national security. According to the chairperson of the National Human Rights Commission (NHRC), a post-1997 reform independent organization, the MICT's Internet blocking is a new challenge for many organizations, including NHRC. There are still few complaints at NHRC about Internet filtering as a violation of the freedom of expression—compared to other more pressing issues such as exploitation of natural resources, abuse of power, and governmental malpractice. The complicated nature of the Internet has also contributed to Thai institutions' limited understanding of the seriousness of the situation.

The NHRC usually refers ICT-related complaints, including online blocking, to the National Telecommunications Commission (NTC), an independent telecommunications regulator and now interim regulator of broadcasting. While acknowledging that violations of freedom do exist on the Internet, the NHRC also admitted they lack the necessary technical and legal expertise to deal with the problem.

Apart from the NHRC, another avenue where people can address Internet filtering issues is through human-rights-related commissions attached to the House of Parliament and the Senate. However, an interview with one chairperson of such a commission—the House commission on human rights, freedom, and consumer protection—revealed a rather conservative stance. Absolute freedom, this person argued, can threaten national security, especially when it involves the monarchy. The reverence of the monarchy, he stressed, is unique to Thai society and shall not be compromised at any cost. In this light, the new computer crime law is a justified effort by the government to properly regulate Internet use by balancing freedom of expression with national security. The chairperson feels that the judicial system is always open for online civil rights groups to tap if the rights to communicate and freedom of expression online are violated by the law.

Conclusion

At a glance, the politics of Internet filtering in Thailand may only reflect the larger political struggle between pro- and anti-Thaksin forces or between pro- and antimonarchy forces. But a closer examination yields another type of politics beyond the dominant color-coded politics. This politics of the Thai Internet code involves a subtle relationship between different elements in the regulation of Thai cyberspace.

In the post-2006-coup experience, the Computer-Related Offenses Act of 2007, a product of the coup-installed legislature, appears to be a major driving force in shaping the cyber experience in Thailand. A number of new regulatory practices have resulted, including the following:

- Legalizing of blocking at network levels.
- Indirect regulation by intermediary providers, which gave rise to intermediary censorship by online service providers and self-censorship of online content providers.
- Creating an ID-enabled architecture that promotes traceability regulation.
- Incorporating censorship into the cyber community's code of practice.
- Self-censorship by users in the online public sphere.

Other laws such as the Emergency Decree, the Internal Security Act of 2007, and lèse-majesté laws also help intensify regulatory restraints with the elements of surveillance and punishment. Gradually, Internet operators—network, service, and content—and Internet users in Thai society have learned to integrate these legal provisions into their cyber behavior. While it is true that lèse-majesté law has been in existence since 1957, its actual enforcement or looming possibility of enforcement has never been as evident as in the present period. I for one still remember the early days of the Internet in the early 1990s in which Thai Net users exchanged opinions on the future of the monarchy on Bulletin Board Service (BBS) using anonymous e-mails. The Internet was free and unregulated because it was difficult to identify the user or poster of comments. This is no longer true in Thai cyberspace, since everyone is now visible and traceable through the new ID-enabled architecture.

Notably, the increased transparency of the Thai Internet is made possible by indirect regulation from the new law. As users are forced to give self-authenticating facts to service providers in order to gain access to the Net, they have contributed directly to the regulation of their own behavior in cyberspace. The new law has changed the regulation of architecture through design constraints that condition netizens' access to cyberspace.

Meanwhile, automatic URL filtering, which involves more subtle filtering design than IP blocking, has also led to a greater technical capability to deny access to information resources while reducing the possibility of blockers being discovered. Though not directly related to the new law, this new technological design has indeed made filtering more malleable and more effective.

The law and the architecture aside, social norms also have a powerful role to play in the Thai politics of Internet filtering. The respect and reverence for the monarchy, particularly for the current king who has reigned for more than 62 years, is a deep-rooted norm in Thai society. Whether lèse-majesté is legitimate or not may be a moot point. What is clear is that this enigmatic norm carries with it high sensitivity in cyberspace as well as in the "real" world. Alongside the increase in prosecution cases

related to lèse-majesté speech online and offline, there has also been growing evidence of participatory forms of censorship—by service providers, content operators, and users—against lèse-majesté. While this participatory censorship is partly a consequence of the climate of fear arising from the new computer law and strict enforcement of lèse-majesté law, the law is not an isolated cause. After all, as Lessig rightly notes, norms constrain through the stigma that a community imposes, while law constrains through the punishment it threatens. In the Thai scenario, both elements apply.

Post-2006 Thailand is an interesting time and place to study Internet censorship and control. In this unique context, an ideological struggle is being played out between the old norm of preserving the sanctity of a revered institution that unites the nation and the new norm of free speech that could disrupt national order. If this ideological contest continues, we are likely to see more filtering, more cyber surveillance, more cyber policing, and more "rule of law" being used to suppress and undermine human rights and free speech online. In the meantime, civil society will employ more tools and options to circumvent politically motivated censorship through wider and higher circles of advocacy, to ultimately prove that freedom is not a crime.

Notes

1. Reporters Without Borders, "Is Thailand a New Enemy of the Internet?" January 12, 2009, http://en.rsf.org/thailand-is-thailand-a-new-enemy-of-the-12-01-2009,29945.

2. This was a result of the 1997 reform-oriented constitution that promoted transparency, accountability of government, and people's rights, liberties, and participation.

3. The Ministry of Information and Communication Technology (MICT) was set up as part of the bureaucratic reform introduced by Thaksin Shinawatra, then the new prime minister. From its inception, the MICT's main policy has been Internet regulation. This began with introducing filtering through the unit called "Cyber-inspector," aimed largely at pornographic content. Later in 2003, the MICT passed regulatory measures to regulate online gaming in response to moral panic in Thai society.

4. The "red shirts" is the informal name for the United Front of Democracy against Dictatorship (UDD), a major political organization in the post-coup period. Members of the UDD are known for wearing red clothes during antigovernment protests. Established in 2006 as Democratic Alliance against Dictatorship (DAAD), the main objective of the red shirts then was to fight against its arch rival—the People's Alliance for Democracy (PAD)—and to support the ousted former Prime Minister Thaksin Shinawatra. Supporters of the UDD are largely rural grassroots people who benefited from Thaksin's populist welfare policy, but also include the urban middle class who admire Thaksin's business-oriented administrative policy and action.

5. Duncan McCargo, "Political Outlook: Thailand," *Regional Outlook* (2010–2011), 54–58.

6. The People's Alliance for Democracy (PAD) originated from the mass movements preceding the September 2006 coup that ousted Thaksin from the premiership. The PAD, also known as the yellow shirts, spent much of 2008 protesting against two successive Thaksin-nominated governments—led by the late Samak Sundaravej and Somchai Wongsawat (Thaksin's brother-in-law)—that arose from the December 2007 election. The PAD's 190-day protest in 2008 was marked by the seizure of the Government House and the Suvarnabhumi International Airport in Bangkok, which had devastating and lasting effects on the Thai economy. In 2009, leaders of the PAD entered electoral politics by establishing the New Politics Party.

7. Lawrence Lessig, *Codes and Other Laws of Cyberspace* (New York: Perseus, 1999), 15–30.

8. This coup took place after a 15-year interval. The previous coup was staged in 1992 by the so-called National Peace-Keeping Council (NPKC), led by then Supreme Commander-in-Chief General Sunthorn Kongsompong. The NPKC overthrew General Chatichai Choonhavan, a civilian prime minister, who led a coalition government for less than two years.

9. Thaksin Shinawatra, founder of the Thai Rak Thai (TRT) Party, was a famous telecommunications tycoon, having made his fortune from satellite and mobile phone concessions through Shin Corporation. Thaksin was also a popular political leader who led the longest democratic and civilian rule—six years—in contemporary Thai history. Thaksin's popularity was largely attributed to populist policies that featured income redistribution, cheap health care, microcredit schemes, and many policy innovations in support of globalization and neoliberal economy. Thaksin is not well liked by a large number of urban or middle-class voters who are repulsed by his arrogance, authoritarian tendencies, and policy discrepancy while in power. He was also widely accused of disloyalty to the crown, an accusation that was largely used as a justification for the September 19, 2006, coup.

10. For instance, Thaksin reportedly launched and managed www.thaksinlive.com on his own before moving on to social media like Facebook and Twitter with http://twitter.com/Thaksinlive, in addition to making periodic video-linked appearances via satellite at the red-shirts' rallies. In late 2009, his family launched an Internet television site called Voice TV, which can be accessed on the Web at http://www.voicetv.co.th.

11. Up until 2001 when the first community radio station aired, all broadcast frequencies—524 for radio and six for national television stations—were controlled by state agencies. Major controllers of the airwaves include the Department of Public Relations (PRD), the Mass Communication Organization of Thailand (MCOT), and the Ministry of Defense, mainly through the army.

12. The Thai printed press, which has always been an important institution in shaping public opinion and setting public agenda, came under heavy criticism for condoning the coup. Notably, three leaders of professional media organizations/associations were appointed by the junta to be in the National Legislative Assembly (NLA), an interim legislature. Also, the printed media were able to push for the passage of a liberal print notification law to replace the draconian and authoritarian print law during the NLA term.

13. According to a nationwide survey of Internet users in 2009 by the National Electronics and Computer Technology Center (NECTEC), Thailand has 18.3 million Internet users, of which 1.8 million are broadband users.

14. The PPP shared the same fate as its predecessor—the TRT Party—when it faced dissolution by a ruling from the Constitutional Tribunal in November 2008 over charges of election fraud.

15. Thitinand Pongsudhirak, "The Search for a New Consensus," *Journal of International Security Affairs,* no. 17 (Fall 2009), http://www.securityaffairs.org/issues/2009/17/pongsudhirak.php.

16. Available at http://www.bangkokpost.com/tech/computer/39215/ministers-sign-computer-related-crime-mou.

17. Immediately after the coup, the coup makers made themselves known to the public as the Council for Democratic Reform under Constitutional Monarchy but usually used Council for Democratic Reform (CDR) as a shorter title. Later they changed the name to Council for National Security, or CNS.

18. The Computer-Related Offenses Act (also referred to as the cybercrime or computer crime act) was in the pipeline since 1992, involving several changes and draft versions.

19. "Thais to Sue Google over King Video" Al Jazeera, May 8, 2007, http://english.aljazeera.net/news/asia-pacific/2007/05/2008525131444839889.html.

20. For example, the Council of Europe's Cybercrime Convention, which is the main international standard in this field and provides a guideline for the development of national legislation as well as a framework for international cooperation, does not address content regulation but instead calls for self-regulation or coregulation in relation to Internet content. Council of Europe, Convention on Cyber Crime CETS No. 185, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

21. Translation of the Computer-Related Offenses Act, Vol. 124, Section 27 KOR., Royal Gazette, 18 June 2007, p. 7. Available at http://www.itac.co.th/index.php?option=com_content&view=article&id=90.

22. Sawatree Suksri, et al., *Situational Report on Control and Censorship of Online Media through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: Heinrich Böll Foundation Southeast Asia, December 8, 2010), http://www.boell-southeastasia.org/downloads/ilaw_report_EN.pdf.

23. Sinfah Tunsarawuth and Toby Mendel, *Analysis of the Computer Crime Act of Thailand*, http://www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

24. Translation of the Computer-Related Offenses Act, Vol. 124, Section 27 KOR., Royal Gazette, 18 June 2007, p. 7. Available at http://www.itac.co.th/index.php?option=com_content&view=article&id=90.

25. "Web Censoring Needs a Debate," *Bangkok Post*, January 6, 2009, http://www.bangkokpost.com/opinion/opinion/9202/.

26. Translation of the Computer-Related Offenses Act, Vol. 124, Section 27 KOR., Royal Gazette, 18 June 2007, p. 7. Available at http://www.itac.co.th/index.php?option=com_content&view=article&id=90.

27. Interview with Chiranuch Premchaiporn and the author.

28. Somkiat Tangnamo passed away in July 2010.

29. Nida Moryadee, "OK Nation Blog as Citizen Journalism," unpublished master's thesis, Chulalongkorn University, 2009, 2–12.

30. See the Thailand country profile in this volume for further details.

31. Reporters Without Borders, "Government Uses State of Emergency to Escalate Censorship," April 8, 2010, http://en.rsf.org/thailand-government-uses-state-of-emergency-08-04-2010,36968.

32. Translation of Constitution of the Kingdom of Thailand B.E.2550 (2007). Available at http://www.isaanlawyers.com/constitution%20thailand%202007%20-%202550.pdf.

33. Translation of Thai Penal Code B.E. 2499 (1956), Section 112. Available at http://thailaws.com/law/t_laws/tlaw50001.pdf.

34. Standing during the royal anthem in a movie theater is a customary practice in Thailand to show respect and allegiance to the king.

35. "Thailand: Moviegoer Faces Prison for Sitting during Anthem," *New York Times*, April 24, 2008, http://query.nytimes.com/gst/fullpage.html?res=9506E1DF1E31F937A15757C0A96E9C8B63&fta=y.

36. "Aussie Author Gets Three-Year Sentence for Lèse-Majesté," *Bangkok Post*, January 20, 2009, http://www.bangkokpost.com/news/local/10026/aussie-author-gets-three-year-jail-sentence-for-lese-majeste.

37. "Lèse-Majesté Suspect Flees," *Bangkok Post*, February 10, 2009, http://www.bangkokpost.com/news/local/136371/lese-majeste-suspect-flees.

38. "Eighteen Years in Jail for Da Torpedo," *Bangkok Post,* August 28, 2009.

39. Based on data of the National Electronic and Computer Technology Center (NECTEC), Thailand has six international Internet gateways (IIGs): CAT Telecom Plc, TOT Plc, TRUE Corporation, Thai Telephone and Telecommunications (TT&T), ADC, and CS Loxinfo. These six IIGs also serve as National Internet Exchange (NIX). Of these six IIGs, two—CAT Telecom Plc and TOT Plc—are former state enterprises and monopoly telecommunications companies that have been corporatized, while two others—TRUE and TT&T—are long-time telecommunications concessionaires. Only ADC and CS Loxinfo are new market entrants and fully private entities. NECTEC's data also show that only 20 ISPs are actually carrying regular Internet traffic despite the fact that more than 40 ISPs hold licenses to operate.

40. Of the 20 operating ISPs, half are semiconcessionaires, as 35 percent of their shares are by default held by CAT Telecom, the long-standing international carrier monopoly. Although CAT Telecom's shares are wholly controlled by the Ministry of Finance, the corporatized state enterprise is under the bureaucratic structure of another government agency—MICT. This bureaucratic structure also helps explain the line of control in monitoring and filtering Web sites in Thailand. A number of ISPs are not under this bureaucratic structure, however. These are new operators that emerged as a result of a telecommunications reform process that has been ongoing since

the 2004 establishment of the National Telecommunications Commission (NTC), the country's first independent regulator of telecommunications. NTC has been issuing licenses for telecommunications services and Internet services since 2005. So far, a total of 130 licenses have been issued for telecommunications service and 132 for Internet. This description, therefore, reflects a two-tiered structure of Internet regulation. On one side, there are the pre-reform semiconcessionaires who are highly liable to CAT Telecom, which answers directly to MICT. On another side, there are the postreform ISPs that operate under licenses issued by NTC. This structure leads to somewhat of a double standard in Internet regulation and filtering.

41. URL filtering is one of the Web-content-filtering techniques. Content filters act on either the content or the information contained in the network packet header or body. URL filtering focuses on the URL and is suitable for blocking a Web page or sections of Web sites. There are two common approaches for URL filtering—pass-through filtering and pass-by filtering. Unlike pass-through filtering in which network traffic (a stream of packets) must pass through the filtering engine (firewall, proxy, or application gateway) for content inspection and can cause extra delay, pass-by filtering network packets do not have to "go through" the filtering engine. The filtering engine normally connects to a mirror port of a switch/gateway and passively monitors packets that pass through the switch (hence the term *pass-by*). Pass-by filtering is more flexible and therefore chosen for the Thai URL filtering system.

42. Robert Faris and Nart Villeneuve, "Measuring Global Internet Filtering," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 87.

43. Lawrence Lessig describes "traceability regulation" as a requirement by the state for service providers to employ software that facilitates traceability by making access conditional on the users' providing some minimal level of identification. Lessig, *Codes and Other Laws of Cyberspace*.

44. Warapong Theprongthong, "Content Regulation of Political Online Discussion Forums, after the Enforcement of the Computer-Related Offenses Act 2007," unpublished master's thesis, Chulalongkorn University, 2010, 54.

45. Ethan Zuckerman, "Intermediary Censorship," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 71–85.

46. Thai Netizen Network (TNN) is an interest group of Internet users who gathered to advocate on five basic principles—right to access information, freedom of expression, right to privacy, self-regulation, and creative commons—for online media. The group was founded in 2008 and comprises mainly people of the Net generation from various occupational backgrounds. See Thai Netizen Network, http://thainetizen.org.

47. Campaign for Popular Media Reform (CPMR), formerly the Committee to Monitor the Implementation of Article 40, was founded in 1997 by networks of academics, nongovernment organizations, mass-media practitioners, and civic media groups. These founders have played an active role in campaigning and participating in the course of Thai media reform since 1992.

CPMR's objective is to democratize communication in Thailand by promoting the transparency of media structure and the creation of a public sphere for communication. See Campaign for Popular Media Reform, "About Us," http://www.media4democracy.com/eng/about_us.html.

48. Freedom against Censorship Thailand (FACT) describes itself on its Web site as "a network of people who disagree with state censorship. We are a member organization in the Global Internet Liberty Campaign (GILC) and the Global Internet Freedom Consortium and cooperate with 200+ organisations around the world." See Freedom against Censorship Thailand, "About," http://facthai.wordpress.com/about.

6 Competing Values Regarding Internet Use in "Free" Philippine Social Institutions

Erwin A. Alampay, Joselito C. Olpoc, and Regina M. Hechanova

The Internet is used within institutions to expand access to knowledge, to improve communications, to manage information, or to increase productivity. But users also download movies, write blog posts, and chat with friends. In other words, people do not always use the Internet for the original purpose for which an institution provided it. Though it is value neutral, there are often competing values in the intentions of those who use Internet technology in an organization: between openness and control, privacy and security, participation and efficiency. These competing values are not necessarily emphasized equally, and may differ from unit to unit, even within the same type of institution. Emphasizing one value can hamper the pursuit of another, depending on the context and structures influencing an organization's choice.[1] Quinn and Rohrbaugh in their model on competing values, for instance, hypothesize that common tensions arise out of internal versus external issues, and between concern for control and a desire for flexibility.[2]

Since information systems can be designed for a range of purposes, it is relatively easy to observe how competing values lead to tensions in access and use. In the case of the Internet, how it is used and adopted within institutions also undergoes similar contestations, even in countries such as the Philippines, where access to it is relatively unfettered.[3]

This chapter explores three institutions in the Philippines: the government, educational institutions, and private corporations. Through a series of case studies, we analyze how these institutions struggle with implementing policies on Internet use, while highlighting competing values among stakeholders on how to take advantage of the benefits that the Internet provides. These cases highlight some of the issues, concerns, and competing views with respect to using Internet facilities in the workplace that emerged from two separate surveys conducted by OpenNet Asia in 2008–2009. The first survey collected the views of information and technology managers and human resources managers on why they provided Internet in the workplace and how they monitored and disciplined employees. The second survey investigated the same issues from the perspective of the employees. Comparing the views of both sides,

patterns of dispute regarding the online space the organization provided were evident: one side tried to control use (e.g., monitoring; disciplining for misuse, etc.), while the other side explored the boundaries of the space (e.g., performing tasks not originally intended, deliberately circumventing policies that restrict use).

The first set of cases deals with how the current government uses new media. Governments see in new media the opportunity to encourage citizen participation and a venue for more transparent government. The second set of cases involves educational institutions. It analyzes universities internally providing Internet access to increase access to online knowledge, while at the same time trying to regulate what students access. The last set of cases analyzes corporations and how they tackle Internet abuse by employees, and their ways to control external stakeholders whose use of the Internet also has an impact on how these organizations are perceived.

These cases are analyzed using Quinn and Rohrbaugh's model, which describes four important values that differ in their preference for control (controlling versus flexibility) and locus (internal versus external), namely: internal process value, open system value, rational goal value, and human relations values. Internal process value emphasizes control and internal focus while stressing information management, communication, and stability. Rational goal, in contrast, focuses on the external and on control, using terms like *plans* and *productivity*. Human relations values the flexibility provided, while focusing on the internal and stressing better cohesion, morale, and human resources. Finally, open systems also look at the external and how to provide the organization with flexibility, while stressing growth, resource acquisition, and external support.[4]

Three Philippine institutions illustrate how competing values apply in contested Internet use: government, schools, and corporations. In these cases, clear positions, protocols, or policies have yet to take hold. In each venue, different sides debate the balance of how the Internet can or should be used by or within these institutions. These incidents, in turn, help define their respective institutions' future policies. Although not as dramatic as the contestations that occur at the international level, they nonetheless touch on similar themes: security, control, privacy, access to information, transparency, and freedom of speech.

Government Bureaucracy: Using the Internet for Participation, Transparency, and Efficiency

The new administration of President Benigno Aquino III won the May 2010 elections, which were partly fought through new media. Political candidates made use of social media including Facebook, YouTube, Twitter, and text messages on mobile phones. Since new media helped the administration get elected, the government eventually wanted to harness it for governance.

However, there are mixed sentiments regarding its utility in government service. A newly elected congressman, Federico Quimbo, through House Resolution 184, claims that "unabated and unregulated use of the Internet by government officials and employees during office hours adversely affects their productivity and the quality of service they provide." He estimates that all 900,000 state workers use government computers for at least two hours every day for unauthorized online social networking activities, and that the government stands to lose an estimated PHP 103,158,000 (approximately USD 2.3 million) every month from electricity expenses alone. He also claims that the Home Development Mutual Fund, where he previously served as president and chief executive officer, gained a significant increase in profit from PHP 2.7 billion (just over USD 61 million) in 2001 to PHP 9.8 billion (USD 221 million) in 2009 when it regulated the use of the Internet.[5] While this purported gain is difficult to prove as due solely to well-regulated Internet use, such sentiments on better organizational regulation are not unique to government institutions. In an OpenNet Asia survey of Philippines organizations in 2008, 77 percent of respondents said they had some restrictions in Internet access, of which more than half (51 percent) reported blocking social networking sites.

The Aquino administration, however, has a different perspective. It believes that Congress does not have to pass a law regulating the use of social networking sites like Facebook and Twitter in government offices. The heads of government departments and agencies are left to "state their policies on social media if the productivity of the employees is affected by their use of social networking sites."[6] In fact OpenNet Asia's organizational survey found that almost two-thirds of government agencies already had a form of Internet use policy in place. This includes policies on permissible sites to visit, use of Yahoo! Messenger, and access to social networking sites. About half of all government agencies restrict use of Yahoo! Messenger, while a third do not allow Skype, and 8 percent prohibited use of e-mail. Overall, use of social networking applications in the office or workplace was the third most common application blocked after pornography and gaming.[7]

Upon assuming office the new administration created a group specifically tasked with managing new media.[8] Their motivation in doing this was to be more transparent, obtain feedback, and get the sentiments of the public. However, because using new media for governance is relatively uncharted in the Philippines, the hard lessons of how to actually make them work as an instrument for state and civil society exchanges and discussion are just becoming evident.

The following is among the first cases of how the new administration used online social networks in a very prominent national issue. The case involves the events and investigation surrounding an ill-fated rescue of 25 tourists held hostage in a bus in Manila that led to the death of eight Hong Kong nationals.

Failed Rescue of Hong Kong Nationals

On August 23, 2010, a tourist bus with 25 people mainly from Hong Kong was hijacked by a disgruntled police officer recently dismissed from the service. The hostage drama unfolded before the eyes of the public and was made more spectacular by a zealous press. When negotiations fell apart, the hostage taker started firing shots, which forced the police to launch an assault. The hostage taker was killed in the final police assault, along with eight Hong Kong tourists.[9]

As the event was unfolding, it was broadcast live over national television and online. Hong Kong's chief executive, Donald Tsang, tried to contact President Aquino. However, even though the president had an official telephone, mobile phone, and e-mail and had a new media staff that presumably made him accessible on Twitter and Facebook, Tsang was unable to connect with him as the crisis was escalating. In the hours after the surviving hostages had been rescued, the president visited the site of the carnage, and his pictures and message were again beamed through various media, including the Internet.

This very open coverage is typical in the Philippines, where press freedom is highly valued and the media are considered an active influence in keeping government in check. This particular coverage, however, was also seen as contributing to the breakdown of negotiations, and also led to negative sentiments, not only from local citizens but also from Hong Kong residents, which was all documented in many social media, including the president's official Facebook page.[10]

To their credit, President Aquino's social media team initially did not filter the angry postings by Chinese residents to his Facebook account during the highly emotional and tragic events. Some of the messages posted said:

"Shame on you and your government. Tender your resignation now."

"*Maaari po sana na paki training ang mga kapulisan at ang SWAT team o kaya naman sibakin na po lahat. . . . nakakakahiya sa international community ang daming namatay* [Please either train the SWAT teams or fire them all. It is embarrassing to the international community that many people died.]."

"Your incompetence of leading your untrained stupid police force caused such a tragedy."

"We Hong Kong people are very angry for your comments. Please apologize to those who were affected."

"He's [President Aquino's] slowly killing our country coz [sic] of his stupidity."

"You see, our president is a retard who has done nothing but smirk in front of the TV cameras after all that has happened."

The administration's openness, in this case, allowed people to vent anger, as it was meant to do. At one point, Aquino's new media team had to change his profile picture from a smiling one (which some found offensive or insensitive given the situation)

to a more solemn pose. Eventually, as some postings became more offensive and were deemed "below-the-belt" attacks on the president, some of the comments posted on his Facebook page were filtered.[11]

Subsequently, the government created an independent commission headed by the secretary of justice, called the Incident Investigation and Review Committee (IIRC), to look into the apparent systemic failure in the hostage incident. The president promised that all those found accountable by the commission would be charged and punished.

After two weeks of hearings, the IIRC submitted an 82-page report that found ten officials liable for administrative and criminal sanctions. Three close supporters of the president were among those included in the recommendations. According to Malou Mangahas of the Philippine Center for Investigative Journalism, the president wanted palace lawyers to first review the report and, if possible, strike out the names of three of his close allies. He was quoted as saying, "*Napatapang 'ata masyado ah. Bakit kasama pa sila* Puno, Lim, *at* Verzosa?" [It's too strongly worded. Why are we implicating Puno, Lim, and Verzosa?][12]

The administration then announced that a copy would be first supplied to the Chinese government as a form of courtesy, but promised to publish the complete report in time on the Office of the President's Web site (http://www.op.gov.ph), and quickly uploaded pages 1 to 60 of the report. However, it did not include the subsequent 22 pages that had the committee's conclusions on accountability or its recommendations and highlights of the report.

As these two cases illustrate, the government's intent to use the Internet for opening discussions and more transparency has not been completely fulfilled. For the former goal, there are fears that unfettered regulation could potentially lead to greater discord and disharmony rather than better understanding. For the latter, sociopolitical considerations still factor into what gets said.

Educational Institutions

Internet access is becoming a fundamental need in schools and universities, since it provides students with access to more knowledge and information.[13] As a result, access to the Internet in schools is becoming a norm, despite negative and unwanted experiences that result from its use.[14]

Access and Availability

Among educational institutions in the Philippines surveyed, 73 percent provided Internet access to everyone (faculty, students, and employees), while the rest had provisional access depending on the person's role in the institution.[15]

The degree to which the Internet is provided in Philippine schools varies, especially when considering the costs attached to it. For some, especially in private schools, the cost is already embedded in other fees. For others, the cost of using computers and the Internet is part of individual courses, with limited time use, any excess of which entails additional payments.

Access can also vary depending on the kind of user and the manner in which she or he obtains access. Some universities provide stand-alone computers with Internet access that do not require individual passwords to log on. In these cases, individual use of computer terminals cannot be effectively monitored. In other schools, students have to register their computer unit or log on using university-issued accounts, requirements that make it easier for dedicated information technology departments to monitor online use.

Restriction, Privileges, and Appropriate Use

Varying restrictions are implemented in educational institutions. For instance, generally, all of the universities in the OpenNet Asia organizational survey agree that access to pornography should be blocked.

However, for liberal arts programs, especially those with fine arts and literature courses, pornography can be a contentious issue. In some specific cases, technical tests conducted for OpenNet Asia in 2008 in the Philippines reveal that some sites that clearly have LGBT content were blocked. These include http://www.gayhealth.com, which promotes the belief that "lesbian, gay, bisexual and transgender men and women need and deserve their own source for health information," and http://www.samesexmarriage.ca, a Canadian site that advocates for equal rights for same-sex couples. Regardless of the reasons for the blocking of these sites, the danger in censoring sites is that decisions are dependent on the discretion of gatekeepers and, at times, are left to purely automated systems that cannot discriminate between sites.[16]

Some universities provide some leeway with these restrictions by giving users temporary access to blocked content provided that they give justification for why they want to access a Web site. In the OpenNet Asia survey study one university noted that it grants requests for temporary access provided that it is for research and instruction purposes. However, student respondents in a focus group found this process cumbersome, especially when action on the request takes time (if it comes at all) and when access can be alternatively obtained from public Internet cafés or from private Internet accounts. The same university has relaxed restrictions for its faculty, giving them access to alternative proxy servers. However, faculty members have to register in order to gain such access. Hence, people surrender certain liberties, which in this case may be privacy, in order to be included and gain privileges.[17] In fact, a computer science professor interviewed says that once a person logs on to the university network, that

person's account can already be monitored, whether he or she uses the university-issued e-mail or commercial e-mail.

Another issue among universities regarding Internet usage pertains to accessing "high-bandwidth" consumer sites. OpenNet Asia testing conducted in a state university found YouTube and subsequently news content such as http://youtube.com/AlJazeeraEnglish and http://youtube.com/zamboangajournal blocked. The reason for this block, at the time of testing, was bandwidth concerns. In larger campuses with bigger student populations, the quality of Internet access varies. Some students complain that the quality of Internet access also varies within the same building. These quality issues were a network infrastructure problem, whereby quality diminishes with distance from the source. In other instances, there are individual units and colleges that provide wireless access independently, and in these cases they provide layers of restrictions in addition to those that the university already provides.

A recent study on the Filipino youth's digital media use found research and schoolwork to be the most common use for the Internet.[18] However, the same study found accessing entertainment and YouTube ranked second. As a result, one university proposed regulating high-bandwidth sites. Its recommendation was based on its internal Internet traffic report in 2008 that showed that six of the top 20 sites being accessed by its users pertained to online videos and downloading/file-sharing sites (table 6.1).[19] The proposed restriction, however, was not accepted by the student body. The students argued that since they are already paying fees for the service and since the cost of bandwidth was actually going down, funds should not be a problem if additional bandwidth is necessary.

These examples illustrate how Internet use in schools is developing rapidly, and how much is to be learned on how to make it effective and safe for students to use. Even though there is no prescriptive remedy to ensure Internet responsibility, schools find they cannot rely on a single solution.[20]

Corporations

Corporations recognize the impact on and contribution to their business of information technology like the Internet and "smart phones." A study on Philippine organizations revealed that 65 percent of employers provide Internet access to all their employees. Employers cited the importance of technology in enabling communication, enhancing productivity among employees, and obtaining information.[21]

There are also data to suggest that employee use can include unproductive, negligent, illegal, and counterproductive activities. In an OpenNet Asia survey that was distributed to 1,033 employees in 86 companies all over the Philippines, respondents were asked if they "know of any employee being disciplined due to violation of Internet use policy at work."[22] They were then asked to explain some details about the

Table 6.1

TOP SITES BROWSED IN A PHILIPPINE UNIVERSITY WHERE INTERNET ACCESS IS UNREGULATED

	Web Site	Bytes	Percent	Description/Remarks
1	http://veoh.com	28,660,474,919	13.29	Online videos
2	University home page (total)	17,656,553,028	8.19	Probably default home page of browsers
3	Google (total)	17,415,538,849	8.08	Various Google pages (aggregated)
4	http://onemanga.com	16,933,337,623	7.85	Japanese anime Web site
5	http://yimg.com	15,645,486,702	7.26	Yahoo! images server (provides the images in the main Yahoo! pages)
6	Facebook (total)	10,940,882,497	5.07	Social networking Web site
7	http://googlevideo.com	9,873,551,602	4.58	Online videos
8	http://vo.llnwd.net	7,558,115,507	3.51	Peer-to-peer networking
9	http://rapidshare.com	6,316,262,412	2.93	File-sharing/downloading site
10	http://megavideo.com	6,046,856,378	2.80	Online videos (like YouTube)
11	Yahoo! (total)	5,088,233,299	2.36	Various Yahoo! pages (aggregated)
12	http://multiply.com	4,340,471,199	2.01	Personal blogging/social networking Web site
13	http://liveupdate.symanteclive update.com	4,209,346,563	1.95	Symantec update services
14	http://animemagicbox.com	4,083,513,115	1.89	Japanese anime Web site
15	http://myspace.com	3,561,970,100	1.65	Personal blogging/social networking Web site
16	http://megaupload.com	3,389,124,492	1.57	File-sharing/downloading site
17	http://node1.otakuworks.net	3,321,871,362	1.54	Japanese anime Web site
18	http://tudou.com	3,297,361,598	1.53	Online videos (like YouTube, Chinese version)
19	http://friendster.com	3,251,756,770	1.51	The original social networking Web site
20	*.l.google.com	2,692,012,762	1.25	Top Google cache server (but counted in item 3)
	Totals	174,282,720,777	80.84	

violation and any sanction imposed. Eleven percent, or 114, of the respondents reported knowing of a coworker who committed some technology abuse at work. Out of the 114 respondents, 73 gave details about the type of Internet-use-related abuse. The top two technology abuses or violations were "pornography related" and "downloading of video files, audio files, or unauthorized applications."[23]

Thus, like other employers across the globe, Filipino employers are at risk. They struggle to balance the productive uses of information and communication technologies for saving time and enhancing productivity, while also trying to curtail the abuses that can threaten their internal security and lead to legal liabilities.[24] At the same time, the experiences of employers highlight tensions in corporate values—equal treatment/benefits versus cost, privacy versus security, and freedom of expression versus risk of defamation.

Equal Treatment versus Cost

The use of policies to regulate information and communications technology (ICT) use is still not widespread among Philippine organizations. Less than half (48 percent) have an ICT-use policy in place. These policies typically cover the use of the Internet, e-mail, and instant-messaging applications. A minority have policies on mobile phone use (16 percent) and use of camera phones (11 percent).[25]

Beyond the existence of policy, a dilemma appears to be emerging in its implementation. On one hand, there is a need for any policy to apply to all members of an organization. On the other hand, actually implementing the policy uniformly may place an organization at a bigger risk. This dilemma appears to be especially salient in the case of pornography.

In the case of Company A (a bank) two incidents of accessing pornography were mentioned. The first was a case of an employee directly caught by the president of the company. The president happened to pass by his cubicle and saw the employee viewing a pornographic movie. The employee was terminated on the same day.

The second incident occurred during the height of a sex video release involving some popular show-business personalities. The IT security director of the bank was directed by the president to investigate the downloading of these videos in their system. Since they kept audit logs of Web sites that their employees visit and any Internet activities that they engage in, employees caught during the audit would be sanctioned according to the company's policies. With his investigation, the IT security director informed the president that should the prescribed sanctions be imposed on those who were caught, more than half of the company's management committee would not be present in the next board meeting. In the end, the president decided to release a memo informing everyone that a number of employees had been caught during the audit and a stern warning was issued (instead of termination).

Access to Information versus Security

The Internet has become a valuable resource for Philippine organizations and workers in obtaining information. A previous study revealed that one of the most popular reasons for using the Internet is research.[26] Yet the value of providing employees access to information is also tempered with concerns about security. Companies are facing bigger and bigger risks from viruses and malicious programs that are intentionally or unintentionally downloaded while employees are online. Companies also lose some level of productivity because the large size of some files can clog up the bandwidth, degrade the network, and consume valuable corporate storage space.

In qualitative responses from the employee survey, employees mentioned that those who were caught were downloading movie files (e.g., TV series or pornographic movies), music files, or pirated/unlicensed software. These files were then stored or installed on their work computer or, in the case of one incident, stored on the shared drive of the whole company. Employees who were caught downloading files were warned, suspended, or put on probation depending on the number of times they were caught downloading files that were considered unauthorized by the company.

To deal with the tension of access versus security, one approach of employers is to place restrictions on Internet use. For example, the OpenNet Asia survey reveals that 58 percent of employers block specific sites (although for 37 percent, blocked sites can be accessed if permission is requested). For a quarter of employers, accessible sites are dependent on the nature of their job (23 percent) or are limited to specific computers (21 percent).[27]

Freedom of Expression versus Risk of Defamation

Information and communication technology is used to facilitate communication, whether within the organization or between the organization and its publics. One emerging tension emerging from this communication is that freedom of expression can create a space for defamation, especially in the case of blogs.

Data show that a fifth of organizations surveyed by Lingao and Tordecilla already have ICT policies pertaining to personal blog postings.[28] These policies are also more common among financial and manufacturing firms. However, this is an emerging policy area among all types of organizations, as illustrated by the two following cases.

The first case is the first libel suit against a Philippine blog. It was filed in August 2005 against the institutional blog of the Philippine Center for Investigative Journalism (PCIJ) by Jonathan Tiongco. He filed six libel suits against the PCIJ, including one case for sedition. All of them were related to the posting of the "Hello Garci" audio recordings in PCIJ's institutional blog. These recordings were supposed conversations

between then-president Gloria Macapagal-Arroyo and a commissioner for elections regarding vote manipulations in the presidential election. The Supreme Court threw out the petition to remove the recordings in October that year and said the constitutional right to free expression was paramount, even if it was just in a blog.[29]

The second case involved Pacific Plans, Inc. (PPI), an educational savings firm that offers educational plans to families. In 2005 the company was in near collapse and applied for rehabilitation with the Makati Regional Trial Court in 2005. The court issued a stay order on April 12, 2005, that allowed PPI to stop payment of tuition fee benefits to the traditional, open-ended plan holders and unilaterally substitute what its educational plan holders considered a patently disadvantageous scheme without any consultation with them. As an immediate reaction to this unexpected and unconscionable move of PPI, parents (plan holders) who converged at Kamagong Street in Makati on April 14, 2005, began to mobilize to be heard, and the Parents Enabling Parents (PEP) Coalition was born.

As a result, the Yuchengco group of companies and Pacific Plan holders are locked in a legal battle in connection with the savings firm's admission of financial difficulty, making it hard pressed to honor its commitment to fund the education of its 34,000 plan holders.

The Yuchengcos filed the libel case on October 18, 2005, before the city prosecutor of Makati City in connection with the alleged "highly defamatory" article posted by PEP members on its PEP Coalition blog alleging mismanagement and mishandling of their fund.[30] The case was later dismissed by a Makati court and by the court of appeals.

Blogging-related controversies are of course not just a concern among private corporations, but also a problem in public institutions as well as schools. In a public high school in the Philippines, for instance, a principal handed a ten-day suspension to four students as a penalty for posting a blog critical of her and other school officials. The principal argued that the blog postings were damaging to her role as principal and to the school and that they caused alarm to the school's alumni. She then imposed a penalty that she said was based on the school's rules and regulations.[31]

Student editors' guilds protested, calling the suspension a form of campus repression that undermined students' rights to freedom of speech and expression. The Commission on Human Rights chairman was also of the opinion that the students' rights may have been violated. The Department of Education eventually stepped in to rescind the order and transferred the principal.[32]

In these three cases, it is apparent that legal measures and harassment are being implemented to curtail freedom of expression. Even though the first two cases were dismissed from court, from an organizational perspective, legal costs of employee postings are very real concerns. Posting on an internal corporate blog, for instance, can be sensitive and potentially damaging because it has an institutional name attached to it. Likewise, external blogs of consumer groups can also become a public

relations problem. All types of organizations are therefore becoming more wary of what occurs in the blogosphere.

Conclusion

The issues highlighted in the cases in this chapter illustrate the struggle to balance different objectives with competing values with regard to the Internet in the Philippines (figure 6.1).

The Internet can be used internally to strengthen internal systems and communications, just as it can be used externally to support communications with clients and obtain knowledge from outside the organization. Likewise, it can be used to control not only information, but also members of an organization, since it allows institutions to monitor their members. Similarly, with the increasing mobility of new devices and ever-expanding content online, the Internet also offers flexibility to members of organizations, assuming that institutions providing access to these services allow them to be used in this manner.

The problem, as the cases illustrate, occurs when institutions or their stakeholders want to use the Internet for purposes that conflict, contradict, or compete with another purpose. For instance, government prioritizes both national security and transparency and encourages external support through people's participation. However, these are inherently competing values, with the former being internally focused and requiring greater control, while the latter is focused externally and encourages more flexibility in its use. Similar contradictions were seen in how schools provide access to the vast knowledge in the Internet, and yet want to control how their students use that knowledge because of harmful content.

Resolving Competing Values

In democratic governments that espouse participation and transparency, regulating people's comments and controlling information that is made public by a government's own services remains a delicate balance. In educational institutions, rules of access and use of the Internet are also just being developed. Likewise, corporations try to balance using these technologies to ensure efficiency and better communications with issues such as privacy and worker/citizen rights.

The space is being contested in various ways. In cases where there are system-level information systems, there is discretion on how Internet-use policies are automated. In some cases, content is actually filtered, not as a policy, but rather as a result of using preinstalled corporate software. While this eliminates discretionary action among managers, discretion actually still exists in how the systems programs are implemented. These decisions are made by programmers, IT managers, and systems administrators.[33]

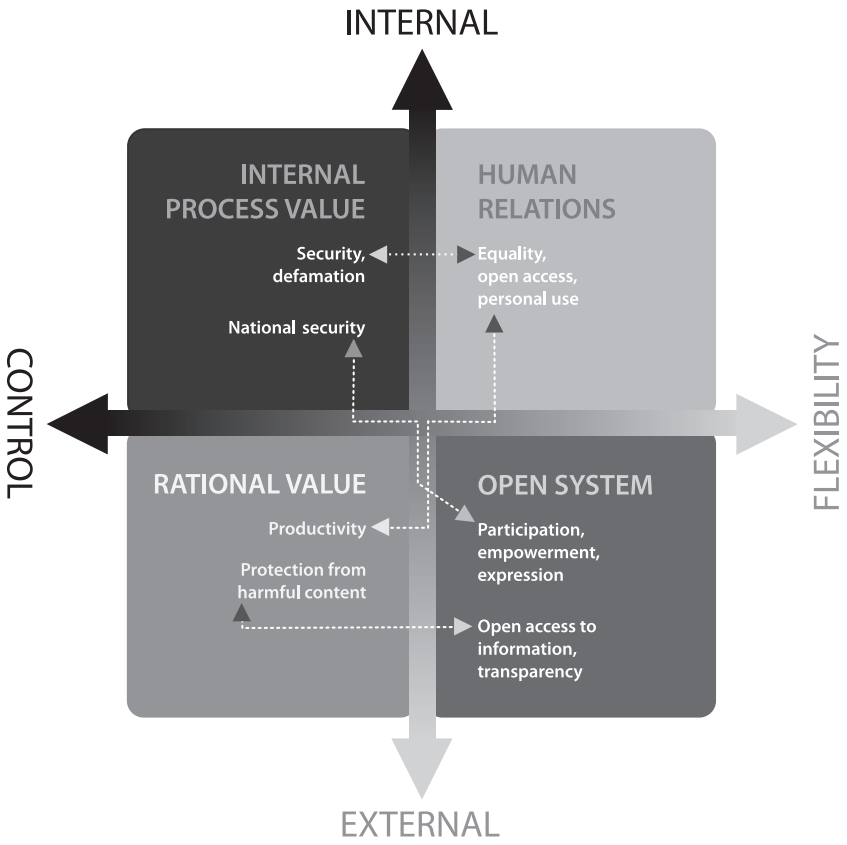

Figure 6.1
Competing values framework as applied to institutional Internet use.
Source: Figure adapted from Robert Quinn and John Rohrbaugh, "'A Spatial Model' of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis," *Management Science* 29 (1983): 363–377.

Even as formal rules and regulations are beginning to appear at the organizational level, legal avenues are also being used as a threat to control individual actions. Individual organizations are also becoming party to monitoring what happens online, especially for posts that may have an impact on their reputation, but also for internal posts that could have legal implications.

For individuals, the lesson here is that even as democratic societies offer space online, this access does not mean that an individual's online presence and actions are not monitored or unhindered. People who know that there is limited privacy in using the Internet within institutions are more careful of how they tread, what they view, and what they post. For the unwitting, what one does online may actually end up being a violation of their organization's rules and therefore subject to discipline, punishment, and dismissal. In some instances, behavior may be monitored by stakeholders outside the organization and can also be subject to prosecution.

As institutional policies begin to develop, organizations must consider the primary objective of providing access to the Internet. Do they want to promote participation and transparency in government? To encourage liberal ideas and access to knowledge in educational institutions? To ease communications, service improvement, and productivity in corporations? While organizations do have the right to develop their respective policies, they also have to make sure that the controls and regulations they impose do not end up curtailing their primary reason for providing Internet access in the first place.

To a certain extent, the tensions illustrated in the institutional-level cases mirror similar struggles to control the Internet at the national and global levels. For instance, institutions can be sensitive to, if not wary of, contrarian views to the point that they filter or censor online messages, file charges, or implement authorized-use policies to discourage such views. Likewise, network security is another concern mentioned among governments, schools, and corporations that want to monitor and limit access and use of Internet facilities. However, some of these practices are not based on well-thought-out or formally stated policies and are unknown to the employees themselves, so that these practices not only are selective in their implementation but also impinge on the privacy of employees. While policies in institutions cannot be prescriptive, the process of developing policies needs to involve management, administrators, users, and clients, just as with states and their citizens. Even then, however, contestations cannot be avoided, given the different priorities and competing values each side holds.

Notes

1. Victoria Buenger, Richard Daft, Edward Conlon, and Jeffrey Austin, "Competing Values in Organizations: Contextual Influences and Structural Consequences," *Organization Science* 7, no. 5 (September-October 1996): 557–576.

2. Robert Quinn and John Rohrbaugh, "'A Spatial Model' of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis," *Management Science* 29 (1983): 363–377.

3. Technical tests that the OpenNet Initiative conducted on Internet service providers in the Philippines from 2009 and 2010 found no evidence of Internet filtering.

4. Quinn and Rohrbaugh, "'A Spatial Model' of Effectiveness Criteria"; Buenger et al., "Competing Values in Organizations."

5. Amita Legaspi, "Lawmaker Seeks to Regulate Facebooking in Government Offices," GMANews .TV,http://www.gmanews.tv/story/198315/lawmaker-seeks-to-regulate-facebooking-in-govt-offices.

6. Jam Sisante, "Palace: No Need for Congress to Pass Law on Facebook Use," GMA News.TV, http://www.gmanews.tv/story/198401/palace-no-need-for-congress-to-pass-law-on-facebook-use.

7. Erwin Alampay and Ma. Regina Hechanova, "Monitoring Employee Use of the Internet in Philippine Organizations," *Electronic Journal of Information Systems in Developing Countries* 40 (2010): 10, http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/648.

8. At present, the Official Facebook page of the president is managed by a newly created new media team under the Presidential Communications Operations Office.

9. "Hong Kong Hostages Killed in Manila Bus Siege," BBC News, August 23, 2010, http://www .bbc.co.uk/news/world-asia-pacific-11055015.

10. One irony in the new administration's use of new media in this recent crisis was that even with cell phones, telephones, Facebook, and Twitter, at the height of the crisis Hong Kong's highest official could not get in touch with the president. In this case, the problem was not the technology, but rather unfamiliarity with protocols among the new administration and its counterpart in Hong Kong.

11. "Aquino Censors Facebook Page over Hostage Crisis Bashing," Inquirer, August 26, 2010, http://newsinfo.inquirer.net/breakingnews/infotech/view/20100826-288827/Aquino-censors -Facebook-page-over-hostage-crisis-bashing.

12. Malou Mangahas, "From Day 1, P-Noy Wanted to Save Lim, Puno, Verzosa," Philippine Center for Investigative Journalism, October 12, 2010, http://pcij.org/stories/from-day-1-p-noy -wanted-to-save-lim-puno-versoza/.

13. Marcell Machill, "Internet Responsibility at Schools: A Guideline for Teachers, Parents, and School Supervisory Bodies in Kids On-line," In *Promoting Responsible Use and a Safe Environment on the Net in Asia,* ed. Kavitha Shetty (Singapore: Asia Media Information and Communication Centre and SCI-NTU, 2002).

14. Shetty, *Promoting Responsible Use and a Safe Environment on the Net in Asia*.

15. Alampay and Hechanova, "Monitoring the Use of the Internet in Philippine Organizations."

16. In one of the universities in Malaysia for which the testing was performed, Ku Klux Klan Web sites were blocked, but similar Malay sites were not. This finding indicates that preselected

blocking was already part of the installed settings of commercial automated software some institutions use.

17. David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994).

18. Liane Pena Alampay and Ma. Emy Concepcion Liwag, "Growing Up Digital (in the Philippines)," Paper presented in the Living the Information Society 2.0 Conference, October 1–2, 2009, Ateneo de Manila, Quezon City, Philippines.

19. A Universal-McCann survey found Filipinos to be the top Internet video viewers in the world. "Filipinos are World's Top Internet Video Viewers," GMA News, August 27, 2010, http://www8.gmanews.tv/story/199588/filipinos-are-worlds-top-internet-video-viewers.

20. Machill, "Internet Responsibility at Schools."

21. Alampay and Hechanova, "Monitoring the Use of the Internet in Philippine Organizations."

22. Joselito Olpoc, Ma. Regina Hechanova, and Erwin Alampay, "Internet in the Workplace: Employees Perspective," paper presented to the seminar on Technology in the Workplace. Trendwatcher Series, November 6, 2009, at Rockwell, Makati City.

23. Ibid.

24. Nancy Flynn, *The e-Policy Handbook: Rules and Best Practices to Safely Manage Your Company's Email, Blogs, Social Networking and Other Electronic Communication Tools*, 2nd ed. (New York: AMACOM, 2009).

25. Alampay and Hechanova, "Monitoring the Use of the Internet in Philippine Organizations."

26. Ibid.

27. Ibid.

28. Ibid., 8.

29. Ed Lingao and Jaemark Tordecilla, "Blogs Targets of Libel Suits, Regulation," April 9, 2010, GMA News, http://www.gmanews.tv/story/188041/blogs-targets-of-libel-suits-regulation.

30. "CA Junks Yuchengco Libel vs. Parents Group," GMA News, April 10, 2009, http://www.gmanews.tv/story/173792/ca-junks-yuchengco-libel-vs-parents-group.

31. "Ex Adviser: Penalized Student Bloggers Not Notorious Kids," GMA News, January 16, 2009, http://www.gmanews.tv/story/144601/ex-adviser-penalized-student-bloggers-not-notorious-kids.

32. Aie See, "QCHS Principal to Be Transferred Amid Blog Controversy," February 3, 2009, GMA News, http://www.gmanews.tv/story/147191/qcshs-principal-to-be-transferred-amid-blog-controversy.

33. Mark Bovens and Stavros Zouridis, "From Street-Level to System-Level Bureaucracies: How Information and Communication Technology Is Transforming Administrative Discretion and Constitutional Control," *Public Administration Review* 62, no. 2 (March/April 2002): 174–184.

7 Interconnected Contests

Distributed Denial of Service Attacks and Other Digital Control Measures in Asia

Hal Roberts, Ethan Zuckerman, and John Palfrey

In early 2008 the Vietnamese government announced plans to mine bauxite, the mineral used to make aluminum, in the Central Highlands of Vietnam in cooperation with a Chinese company. These plans became the subject of increasing protest beginning in 2008 and continuing thereafter. Protesters have expressed environmental concerns about damage to mined areas and toxic by-products of bauxite mining. While some activists involved with the bauxite protests have been connected to banned prodemocracy movements, others have been protesting the Chinese-backed mine on grounds of environmental concern or national pride.[1]

In 2009 a group of activists distributed a petition and created a Web site named http://bauxitevietnam.info to protest the bauxite mining. According to reports from Vietnamese free-speech advocates, both the bauxitevietnam.info site and the larger bauxite protest movement have been under constant attack since 2009. The government has repeatedly detained and interrogated both the founders of bauxitevietnam.info and many of those who signed the petition. Forged e-mails, purportedly by the founders of the Web site, have been distributed online, falsely claiming that the leaders were quitting the protest. Activists report that the Vietnamese government broke into the site's servers to steal protester information and shut down the site.[2]

In January 2010 a flood of traffic from compromised computers overwhelmed bauxitevietnam.info, making it inaccessible not only in Vietnam but also throughout the entire Internet.[3] Political actors increasingly use this type of attack, known as a distributed denial of service (DDoS) attack, to control content on the Internet. Vietnam has routinely filtered Internet sites the government considers to be controversial, preventing users in Vietnam from accessing them without taking unusual steps. In contrast, a DDoS attack makes a Web site inaccessible to all online audiences by disabling a targeted Web server under a flood of traffic.

This particular DDoS attack used a botnet, an army of "zombie" computers that have been taken over, in the vast majority of cases, without their owners' knowledge. These zombie computers are generally used to commit some sort of fraud on the network. For example, some computers controlled by botnets are used to sign up for thousands of

free e-mail addresses and send spam. In this case, the zombie computers sent an extraordinary number of requests to http://bauxitevietnam.info, crashing the site.

Shortly after the DDoS attacks on the site began, Google announced that it would no longer censor its search results in China[4] because of attacks on its Gmail service, which it found had originated from within China. While investigating the source of those Gmail attacks, Google found evidence that the botnet attacking bauxitevietnam .info—though not involved in the Gmail attacks—consisted largely of computers that had been infected by a malicious program hidden by an attacker within a program called VPSKeys.[5]

Technicians at Google and at the antivirus firm McAfee then unraveled the story of the bauxitevietnam.info DDoS attacks. VPSKeys is the most popular Vietnamese keyboard input program. Distributed by the Vietnamese Professionals Society (VPS), it allows Vietnamese users to enter Vietnamese characters easily using Western keyboards. Some months before the attacks on bauxitevietnam.info, likely in late 2009, the Web site hosting the VPSKeys software had been compromised. The attacker replaced the VPSKeys program with a Trojan version designed to infect the host computer with botnet software. The attackers also alerted thousands of VPSKeys users by e-mail that a new (secretly infected) version of the software was available. Many Vietnamese users updated their software in response. It is likely that the attackers were able to obtain the mailing list used to send this e-mail through a separate attack—possibly intrusions that seized membership databases of popular Vietnamese discussion forum sites in 2009.

Tens of thousands of users downloaded the Trojan software, which infected the host computers and added them to a botnet before the Trojan software was discovered. The makers of VPSKeys replaced the infected software with a clean version, but not before the Trojan software had created the network of compromised computers. This botnet was used to mount the DDoS attack on bauxitevietnam.info and may have been used against additional targets.

Why did the attackers go through the effort of compromising computers and creating their own botnet? There is a thriving underworld business devoted to the sale of lists of infected computers, which in essence allows attackers to rent these computers for the purpose of a one-time attack like the one on bauxitevietnam.info.[6] A plausible explanation is that a botnet of computers based in Vietnam would be difficult for a site administrator to defeat through geographic filtering. If bauxitevietnam.info were attacked by thousands of computers located in South Korea, an administrator might respond by blocking all requests to the Web site from that country. But blocking requests from Vietnam would defeat the purpose of raising awareness within Vietnam itself. It is also possible that the botnet was an added benefit in a scheme that primarily sought to monitor the activity of Vietnamese-speaking users around the world. The botnet was certainly capable of spying on the owners of the infected computers,

possibly logging keystrokes and capturing passwords to online accounts, even possibly collecting the list of e-mail addresses used to encourage more people to download the Trojan software.

The administrators of bauxitevietnam.info defended the site from the DDoS attack by mirroring the site on multiple hosting providers. They created mirrors at http://bauxitevietnam.info, http://boxitvn.org, http://boxitvn.net, http://boxitvn.info, http://boxitvn.blogspot.com, and http://boxitvn.wordpress.com. The last two of these mirroring environments are especially important, because they are hosted by large blog-hosting services, Blogger (run by Google) and WordPress. These large-scale services offer highly DDoS-resistant services at no direct financial cost to the activists.

It is very rare that an observer can come to identify the owner of any botnet, as Nart Villeneuve and Masashi Crete-Nishihata also find in their fine-grained review of DDoS and defacement attacks in Burma in chapter 8 of this volume. It is the nature of a botnet to be distributed across a broad range of computers infected without the knowledge of their owners. Accordingly, no one (including Google and McAfee, two of a handful of actors most capable of diagnosing this sort of attack) has managed to determine who controlled the botnet during the course of the Bauxitevietnam attacks—or, for that matter, who controls it at the time of this writing. But there are indications that some DDoS attacks against Vietnamese sites have involved more than tacit approval of the Vietnamese government. Viet Tan, a Vietnamese prodemocracy dissident group, reports that their site is routinely subject to DDoS attacks and that many of the attacking computers are based in Vietnam.[7] Since http://viettan.org is generally blocked in Vietnam, these attacks require that authorities lift the blocks on attacked sites to permit attacks from zombie computers in Vietnam. It is difficult to verify this claim without access to Viet Tan's server logs documenting such an attack.

This example—by no means extraordinary, particularly in Asia—shows how DDoS attacks accompany a range of interventions that involve malware and related intrusions into the computers of ordinary Internet users. It demonstrates that governments and other political actors are using a broad array of intertwined methods to contest online (and offline) content that they find offensive. For example, the methods of attack in this case include the following:

- DDoS attacks
- Technical Internet filtering
- Surveillance
- Intrusion by means of malware
- Trojan software
- Online identity forgery
- Offline harassment

The difficulty of diagnosing (and defending against) these attacks is further complicated by the large set of actors, many of whose precise roles are unclear. For example, the attacks on http://bauxitevietnam.info may have involved the following:

- *Attackers* A set of attackers, which may or may not have included the Vietnamese and Chinese governments, whose precise identity is unknown and who are responsible for a number of DDoS attacks, intrusions, and forgeries; the hundreds or thousands of compromised computers used to attack http://bauxitevietnam.info, most likely without knowledge of their owners.
- *Defenders* The administrators of bauxitevietnam.info, and administrators of the hosting services and Internet service providers (ISPs) they use.
- *Affected third parties* The Vietnamese Professionals Society (which inadvertently distributed malware), McAfee (which detected the attack), and Google (responsible for both investigating the DDoS attack and defending against the attacks via Blogger).

The use of malware particularly complicates this type of analysis. Researchers usually consider malware the province of commercial actors who compromise computers to participate in schemes designed for financial gain. This type of example demonstrates how malware is now playing a major role in how political actors seek to constrain Internet users both within and beyond their borders.[8] These interconnected controls make diagnosing DDoS attacks an enormous challenge in many cases simply because it is difficult to understand the full array of methods used with the attacks as well as who is executing those methods. In this case, it is likely that some of the computers that attacked bauxitevietnam.info were owned by individuals who supported the goals of the organization. This possibility, in turn, made the attack even harder to block because distinguishing between legitimate and attack traffic was impossible to do on an IP basis.

Finally, this example demonstrates what relatively sophisticated activists can do to defend themselves from DDoS attacks. A common strategy is to diversify hosting and, especially, to flee to large blog hosts, often based in the United States, for cover. While simple to understand and implement, the strategy is extremely effective, allowing the activists behind bauxitevietnam.info to maintain an online presence in the face of a sustained attack without paying for a fee-based DDoS-protection service, the most effective of which start at thousands of dollars per month.

DDoS and Other Next-Generation Control Measures

This chapter is a deep dive into the growing phenomenon of DDoS attacks. We seek to describe the state of DDoS attacks in the context of the interconnected contests to control online content. Our central goal is to situate the phenomenon of DDoS attacks within the theoretical framework developed in OpenNet Initiative (ONI) research. In

particular, this in-depth review of the DDoS phenomenon builds on the observation that the types of control mechanisms that states and others may employ have evolved from the first-generation Internet control process of technical filtering to the second- and third-generation controls that we have observed emerging since the middle part of the 2000s.[9] As Ronald Deibert and Rafal Rohozinski say of these next-generation controls in the opening chapter of *Access Controlled*:

> Although there are several tactics that can be employed within this rubric—deliberate tampering with domain name servers, virus and Trojan horse insertion, and even brute physical attacks —the most common is the use of DDoS attacks. These attacks flood a server with illegitimate requests for information from multiple sources —usually from so-called ''zombie'' computers that are infected and employed as part of a ''botnet.'' The ONI has monitored an increasing number of just-in-time blocking incidences using DDoS attacks, going back to our first acquaintance during the Kyrgyzstan parliamentary elections of 2005.[10]

A group of ONI researchers have also tracked other early instances of DDoS attacks in the Belarus elections of 2005, the Russia-Estonia dispute in 2007, and the Russia-Georgia conflict of 2008.[11] In this chapter, we build upon these previous findings of our ONI partners in this broad-based review of DDoS attacks that were independent of particular sensitive political moments, as well as the detailed research on the 2008 Web defacement attacks in Burma in chapter 8.

Our research method in studying DDoS was multifaceted. We conducted an in-depth analysis of media reports on human-rights and independent media-connected DDoS attacks, surveyed independent media and human rights sites, conducted confidential interviews, and hosted a working meeting with participants from multiple related sectors in Cambridge, Massachusetts, in 2010. We shared our results with knowledgeable peers before disseminating them and discussed possible responses to the rising DDoS threat. Although our research was meant to cover DDoS broadly around the world, Asia proved to be one of two regions we focused on, along with the Commonwealth of Independent States (CIS). Our respondents in Asia came in particular from Burma, China, and Vietnam, and we focus on cases from those countries here.

We sent a survey on DDoS attacks to a sample of 317 independent media and human rights sites. We generated the sample by asking at least three local experts in each of the nine target countries for the most prominent independent media in their countries. We translated the survey into the primary Internet language of each surveyed country and also translated the recruitment e-mail to the primary language of each site. We received full responses from 45 sites, for a response rate of 14 percent.

These survey methods limited our findings in several ways. The sample involved was not large. Despite this limitation, we perceive that the 45 responses amount to a decent response rate for such a survey, given a series of special factors involved. These factors included the difficulty of reaching a key actor at each site, the inherent

sensitivity of the survey subject, and the early stage of research in this field. We used neutral language that did not explicitly refer to DDoS attacks when querying the experts for the list of sites, but some of the experts were familiar with our work and therefore likely to bias their lists of independent media toward sites known to suffer DDoS attacks. It is likely that the 14 percent of responding sites overrepresents sites that have suffered a DDoS attack, since a survey on DDoS attacks may seem more interesting—and worth responding to—to DDoS attack victims. These two factors make the results of the survey less useful for answering questions about overall prevalence of DDoS attacks. We cannot, for these reasons, answer questions about what percent of all independent media sites in our surveyed countries have suffered DDoS attacks. But we believe that the responses are useful for investigating the nature of attacks reported by the surveyed sites and the defenses used by those sites.

We conducted interviews in person, over Skype, and by e-mail with administrators of 12 sites that experienced DDoS attacks. We contacted every survey respondent who reported having been subject to a DDoS attack and requested a more in-depth interview. Six of the interview participants were recruited through this method. We found the rest of the interview participants through media analysis or through referrals from researchers and other contacts in the field. We interviewed administrators of sites based in Australia, Burma, China, Iran, Russia, and Vietnam. The interviews involved a series of questions and answers tailored to each interviewee exploring the technical details of attacks and the experiences of the administrators dealing with them. In a few cases, we obtained and analyzed logs of attacks. We cannot publish the interviews themselves for security reasons, but we include a number of findings, in aggregate form, from the interviews.

Additionally, we studied as many published reports of DDoS attacks as we could find by tracking accounts posted to the Web over the course of six months. Our sample set includes 329 reports of attacks against more than 800 sites going back to 1998. We also had the unexpected opportunity to study a DDoS attack that happened to occur during the course of our research. Our research home, the Berkman Center for Internet and Society at Harvard University, hosts the site of a sister research project, the Citizen Media Law Project, which happened to be attacked by a sustained denial of service attack. We were able to study that attack in progress, as it happened, for which we are grateful to the unknown attackers.

Interconnected Methods of Contesting Information Online

A core finding from our survey and related methods is that DDoS attacks exist within a portfolio of different attacks suffered by these sites. We also found that the same site usually suffers from multiple types of attacks. During the past year, of the surveyed sites,

- 72 percent experienced national network filtering of their sites.
- 62 percent experienced DDoS attacks.
- 39 percent experienced an intrusion.
- 32 percent experienced a defacement.
- Of those experiencing a DDoS attack, 81 percent also experienced at least one of the following other content controls: Internet filtering, intrusion, or defacement.

These numbers provide strong evidence that DDoS attacks are not an isolated problem for independent media sites. Instead, DDoS attacks exist within a larger range of different kinds of attacks against the sites. In addition to the specific range of attacks reported, the surveyed sites reported a high level of unexplained downtime during the past year:

- 61 percent experienced unexplained downtime.
- Of those respondents who experienced unexplained downtime, 48 percent experienced seven or more days of unexplained downtime.

Unexplained downtime can be the result of factors other than attacks. Independent media sites often suffer from a lack of experienced system administrators, leading both to downtime and to the inability to diagnose the reasons for downtime. Still, the very high amount of unexplained downtime experienced by these sites suggests more, and possibly more complex, attacks than described by the answers to the preceding DDoS question.

Our finding that a significant number of sites have experienced 21 days or more of downtime suggests that there is a serious shortage of technical capacity available to respond to threats to independent media and human rights Web sites. Arbor Networks, a leading DDoS mitigation firm, surveys large ISPs annually about their experience with DDoS. Their survey of tier-one and -two ISPs suggests that most administrators of large ISPs respond to a typical DDoS attack within an hour.[12] The administrators we interviewed were unable to bring their sites back online in such a timely fashion.

Our in-depth interviews provided further support for the findings, in both our survey and media research, that DDoS attacks are often accompanied by intrusions, defacements, filtering, and offline attacks. One administrator of more than a dozen independent media sites reported DDoS attacks followed by offline extortion intended to force him to retract a story. (He refused.) That same administrator reported being subject not only to DDoS attacks but also to daily virus-laden e-mails targeting him personally and about topics of confidential interest to him; to weekly intrusion attacks based on guessed passwords; and weekly defacement and complete deletion of at least one of the sites under his control.

Another administrator had been subject to weeks-long, multigigabit DDoS attacks but reported that a greater problem was the harassment of participants in the publication's discussion forums: attackers broke into the discussion forum to steal and publish

the identities of its users and also posted inflammatory content to the forum to trigger governmental prosecution. Yet another administrator reported that intruders had repeatedly accessed internal databases to learn about stories before they were published. And another reported that attackers broke into his site to insert malicious code with the intent of triggering antivirus warnings for the site and thereby scaring users from accessing it. He also reported intrusions to his site that inserted code that slowed the Internet connections of his users by causing them to download large packages of Trojan horse software. In all cases, the DDoS attacks may have been the most visible manifestation that a site was under attack. But the attacks that accompanied the DDoS attacks were often of far more concern and import to the affected administrators.

DDoS attacks vary greatly in their nature and magnitude. In our interviews, we heard about a range of attacks, extending from multi-Gbps floods of traffic that overwhelmed the network connectivity of the affected sites to attacks that used as few as a few dozen requests per minute to cripple sites by exploiting holes in Web servers and other applications. Five of the interview participants reported attacks in the range of 500 Mbps to 4 Gbps. One participant, who was the administrator of a large service provider working for an independent media site, reported an attack of greater than 10 Gbps. Some of these attacks may have been bigger, since at greater than 1 Gbps, many local ISPs become saturated and drop any additional traffic. One interview subject, whose site experienced several DDoS attacks in the previous four years, reported an escalation of the size of attacks over time. His site had been successfully disrupted in 2007 with a 1 Gbps DDoS attack, and he moved to more robust, DDoS-resistant hosting provider. His contract with the provider specified that he would be protected from attacks up to 2 Gbps. When an attack in 2010 involved 4 Gbps of traffic, his host took his site offline, offering him the option of either increasing his monthly payments or remaining offline until the attack ended.

Three interview participants reported application attacks at low—even very low—bandwidths that caused significant downtime. One was taken down by fewer than 40,000 requests per day, another by less than ten machines hitting his search page. Two participants reported long-term success using mitigation strategies—caching and Web application optimization—which would be effective against only relatively low bandwidth attacks. We believe these attacks exploited known holes in application software, such as the Slowloris attack against Apache Web servers.[13]

It is likely that most or all network attacks that we encountered in our research involved the use of botnets to generate incoming traffic. Other indicators suggest that some of the attacks involved the use of rented botnets. Two interview subjects reported that attacks began and ended at the top of an hour, suggesting that a botnet had been rented for a specific duration. The DDoS attack against the Berkman Center's Citizen Media Law Project offered further evidence of rented botnet attacks. The DDoS attack was an application attack using HTTP GET requests originating from a shifting set of

exactly 500 IP addresses. The attack was highly effective, rendering the site inaccessible for 12 hours, despite steady work from the Berkman Center's highly experienced technical staff to keep the site online. That the attack came from a round number of attacking IPs and that the IP addresses in use shifted in real time in response to defenses suggests that the application attack came through a rented botnet.

We also saw a strong correlation between DDoS, filtering, defacement, and intrusion attacks in our media analysis. These techniques were often used in conjunction, and may have synergistic effects—making a site more DDoS resistant can make it more difficult to access using a Web proxy, for instance, which makes state-based filtering more effective. Independent media organizations participating in the working meeting repeated the same theme: sites suffer from multiple types of attacks, including DDoS, which in turn have complicated impacts on one another.

A key example of these impacts was the problems that a prominent Burmese independent Web site experienced from a combination of DDoS attacks and national filtering. The Web site has moved to a DDoS-resistant hosting provider to protect itself against high-bandwidth-traffic attacks. The site in question is routinely filtered by the Burmese government, so people within the country must use proxies to access the site. Burmese users gravitate toward a small set of proxies discovered through word of mouth. All the traffic from each of those proxies appears to come from the same IP address. One method the DDoS-resistant hosting provider uses to protect against attacks is to block IP addresses that are submitting too many requests. Since the proxies submit many more requests than other IP addresses, the hosting provider often bans them, to the end effect of blocking Burmese audiences from accessing the site. It is possible to address this problem by providing the hosting provider with a white-list of proxy servers, but that list is difficult to maintain because users in Burma keep seeking new proxies to stay one step ahead of government efforts to block them.

Non-DDoS attacks on a site are often more serious and less tractable than DDoS attacks. A common method for intrusions is to compromise the computer of someone who has administrator-level access to the target server. Access to the server is then used to delete sites; to discover the identities of dissidents, authors, and sources for further on- and offline harassment; to deface the target site; or to implant malware on the target site either to discredit the target site or to execute a DDoS attack on another site or both. Administrators of human-rights-related independent media consistently report being frequently subject to specifically targeted e-mail viruses, often connected to content tailored to be of interest to the administrator in question. These specifically targeted attacks are very difficult to defend against, requiring a high level of training and support for the victims. But many or most of the independent media organizations struggle to maintain even very simple client-side technology infrastructures.

For example, one participant—an administrator of a well-funded and prominent Asia-based nonprofit organization—reported that his organization shared two desktop computers among its staff of several dozen people. Many of these staff members had never touched a computer before working for the publication. Defending client computers that are so widely shared and used by such novice users, and that are specifically and aggressively targeted, is an enormously difficult problem to solve for even one organization, let alone for the field as a whole. We know of at least one organization focused on political rights in Asia that has a policy of reformatting the hard drive of laptop computers that have been removed from the office and used on other networks. Most organizations do not have nearly this level of concern or technical competence, even though most targeted organizations likely need to operate at this level of caution.

Two of the independent media site administrators we interviewed reported multiple types of attacks coming from multiple sources, as well as confusion about the source of the attacks. One participant was subject to a DDoS attack when he published a story about a prominent government actor, and then was approached separately both by the government actor with demands to take down the offending story and by the group of cybercriminals who were carrying out the attacks with demands for money. Another participant claimed that his site is sometimes attacked by the government when it is unhappy with a particular story and sometimes attacked by activists in opposition to the government when they are unhappy with a story (and sometimes the activists have taken credit for attacks that the participant thought were certainly coming from the government). Others we surveyed suggest that, in many cases, the effectiveness of DDoS attacks was a matter of gaining press coverage rather than success in taking and keeping a site down. In other words, even when DDoS is the only attack a site faces, the actors and their motivations may be complex and multilayered.

Site Administrators Worry about DDoS, among Other Attacks

Despite their prevalence, DDoS, intrusion, and defacement attacks are not the primary concern for most independent media sites. Asked to rank the impact of various issues, participants placed DDoS, intrusion, and defacement attacks squarely in the middle of the pack among other Internet content-control issues. The issues were ranked in the following order, with the most important issue listed first and with the average rank out of five noted (a higher number implies a lower priority):

- Blocking access to the publication's site by the government (2.47)
- Persecution of authors, publishers, or sources by the government (2.53)
- Intrusions, defacements, and denial of service attacks (2.89)
- Financial support for the publication (3.00)
- Technical issues other than defending against attacks (3.89)

While DDoS attacks are an increasingly prevalent form of Internet control, our respondents listed conventional government filtering as the most serious problem they face. Only 11 percent of respondents chose DDoS, intrusion, and defacement attacks as the most pressing issue, and only 32 percent chose these attacks as one of the two most pressing issues. These are particularly interesting findings given the bias of the study toward respondents facing such attacks. By comparison, 68 percent of respondents chose persecution of authors, publishers, or sources by the government as one of the two most pressing issues. Issues directly related to censorship and control (filtering, persecution, and DDoS and other attacks) all ranked higher than the two issues not directly related to censorship and control (finance and nonattack technical issues).

Effective Responses to DDoS Attacks Are Elusive

A common response to a DDoS attack is to turn to the hosting ISP during the time of the attack. The survey respondents had mixed luck getting their ISPs to defend them against attacks. Of those who experienced a DDoS attack in the past year,

- 55 percent had their site shut down by their ISPs in response to the attack.
- 36 percent report that their ISP successfully defended them against a DDoS attack.

The number shut down by their ISPs is surprisingly high, considering that an ISP will usually shut down an attacked site only when subject to a traffic-based attack (since other type of attacks generally do not directly affect the ISP's network or other customers). The fact that 55 percent of respondents suffering a DDoS attack had been shut down by their ISPs at least once indicates that at least 55 percent, and almost certainly more, of the sites had been subject to a traffic-based attack. This fact, along with the fact that only 36 percent of the respondents subject to DDoS attack had an ISP that defended them against attack, indicates that for many independent media, the local ISP is a weak point rather than a strong ally. We do not know whether the reason for this poor defense of sites by their ISPs is that independent media sites are customers of sites outside the core of ISPs able to respond to an attack in under an hour or whether the reason is that the independent media sites are customers of the core ISPs but are not able to pay for the DDoS protection that those ISPs generally sell as an add-on service.

In our survey, we also asked site administrators about the defenses they had tried when hit by a DDoS attack and how effective those defenses had been. Their responses can be read as a map of how independent media escalate defenses against DDoS attacks:

- 83 percent had fixed problems with their existing Web application software, with 80 percent reporting that this measure was "somewhat effective" or "effective."

- 75 percent had installed security software or hardware on their existing servers, with 92 percent reporting that this measure was "somewhat effective" or "effective."
- 62 percent had upgraded their Web server hardware, with 88 percent reporting that this measure was "somewhat effective" or "effective."
- 43 percent had downgraded the functionality on their existing sites, with 33 percent reporting that this measure was "somewhat effective" or "effective."
- 40 percent had subscribed to a denial-of-service-protection or other security service, with 100 percent reporting that this measure was "somewhat effective" or "effective."
- 38 percent had hosted content temporarily on a large hosting provider (Blogger, LiveJournal, etc.), with 67 percent finding that this measure was "somewhat effective" or "effective."
- 36 percent had changed their hosting providers, with 80 percent reporting that this measure was "somewhat effective" or "effective."
- 29 percent had changed their Web application software, with 75 percent reporting that the change was "somewhat effective" or "effective."

The vast majority of sites that experience DDoS attacks try to update the configurations of their local computers by fixing the existing Web application software, installing local security hardware or software, and installing upgraded local Web server hardware, or some combination of these three approaches. These basic strategies can all be taken by individual sites without help from core network providers, though in some cases core technical expertise may be needed to properly apply these upgrades. Each of these approaches rates as at least somewhat effective against DDoS attacks, insofar as these basic changes prove somewhat effective against further attacks.

A much smaller number of sites escalate their responses either by implementing more aggressive (and costly) defenses at the edge—downgrading functionality or changing Web application software—or by moving closer to the core of the network: subscribing to expensive protection services, hosting content on large providers, or changing hosting providers. The success of these defenses is more mixed than the simple edge-based fixes, perhaps because these are the defenses that are valid responses to network attacks, which are much more difficult to fend off than application attacks.

Our results indicate that the number of attacks against each site increased for a slight majority of participating sites:

- 16 percent reported many more attacks in 2010.
- 36 percent reported somewhat more attacks in 2010.
- 48 percent reported no change or fewer attacks in 2010.

ISPs—who are best positioned to defend sites against many types of DDoS—are often unable or unwilling to defend their customers. This finding leads us to speculate that many of the sites we surveyed are (or were, as many have been dropped by those

providers) tier-three providers, who may lack a fiscal incentive to protect their customers. Tier-three Web-hosting providers sell their services for a small margin over costs—the hours worth of system administration time necessary to fend off a DDoS attack is more costly than the annual profit for the average account. These providers evidently do not see a reputation risk in failing to fend off a DDoS, and they find it more profitable to end relationships with "troublesome" customers than to provide protection to them.

The apparent efficacy of upgrading servers and fixing Web server software strongly suggests that attacks are not all based on clogging network connectivity (where these defenses would be ineffective) and point to application-level vulnerabilities. These sorts of fixes are only really helpful for either very small traffic attacks or application attacks, both of which can be reasonably dealt with by individual publishers at the edge of the network.

Best Practices for Human Rights and Independent Media Sites Are Emerging for DDoS Response

According to experts with whom we consulted, the responses that a site might take to a DDoS attack include the following:

- Blackholing the IP address of the attacked site (i.e., taking the attacked site offline).
- Deploying additional network and server infrastructure for the attacked site.
- Downgrading the content and/or functionality of the attacked site to reduce resource consumption.
- Filtering out attack traffic.
- Using a service with a distributed architecture to scale and absorb attacks on demand.

These responses range from the simplest to implement (taking the site offline, which is essentially giving up in the face of an attack) to complicated and difficult to implement.

Blackholing the IP address of the attacked site fulfills the aims of the attacker by making the site unavailable. But this response also makes the attack traffic disappear entirely from the Internet. In so doing, it protects the network hosting the site. This is the approach taken by many ISPs that are faced with a large traffic-based attack that is either too big or too expensive for them to defend against.

An attacked site may deploy additional servers and bandwidth to protect itself. Our survey results show that this is indeed the most popular method of protection. But for all but the biggest sites, deploying additional infrastructure for a single site is cost effective for small, application-based attacks only, because the peak traffic of a large, traffic-based DDoS attack will be orders of magnitude larger than the peak legitimate traffic of a site.

An alternative to increasing the server resources is to reduce the resource consumption of each page, allowing the server to handle more traffic with the existing server and network. There are some methods for reducing resource consumption that are effective and have little cost, such as caching dynamic content to reduce database queries. As attack size increases, though, an attacked site has to make changes that have costly side effects, like disabling site functions that require expensive database queries, reducing or eliminating images and streaming media, or creating an entirely separate failover site with simpler and less-interactive content.

Another way to reduce resource consumption is to distinguish attacking traffic from legitimate user traffic and filter out the attacking IP address. This approach is frequently used, and several of our meeting and interview participants reported success with this method, but only when the number of attacking machines is small and relatively static. It is simple for a competent system administrator to find and block a hundred static IP addresses that are flooding a site with requests for a single page, but that job becomes much, much more difficult when there are tens of thousands of IP addresses that are rotating every couple of hours and actively trying to make their traffic look legitimate. In these cases, it is sometimes possible to filter attacking traffic based on a signature for the particular traffic, but this approach can be very difficult against a moderately skilled attacker even for a highly skilled defender. It is possible to defend against a range of common attacks by using ModSecurity, an open-source attack-filtering system. But this sort of filtering helps against generic attacks only, and it uses up machine resources for the process of filtering and can therefore make the site more vulnerable to traffic-based attacks.

Finally, a site can protect itself by paying for a hosting or DDoS protection service to serve the content of the Web site. There are many services capable of handling all but the biggest attacks, and a few capable of handling the biggest observed attacks, simply because they have sufficient bandwidth and server resources to accept and process the attack traffic. The advantage of using such a service is that these services have economies of scale both in learning how to defend against particular attacks and in the necessary bandwidth and servers. When using such a service, the attacked site needs to pay for the peak attack traffic only while the attack is happening, rather than paying for the entirety of the resources needed to handle peak attack traffic.

These services, however, can command a very high markup on those resources. Even without the high markup, simply paying for the bandwidth to handle the peak attack traffic can be prohibitively expensive, especially for an independent media site. An attacked site may be able to hire a provider capable of handling millions of requests per second but not be able to afford the resulting bandwidth charges. The economies of scale work best for these sites if a large proportion of the site is not likely to be attacked at the same time, which is important to keep in mind given the model we found in interviews of a single local expert managing many sites from a given area

(meaning that all or many of those are likely to be attacked at critical times for the country). As we noted previously, sometimes an attack will outstrip an administrator's ability to pay the associated bandwidth charges, and the site will be forced to go dark until the attack ceases.

Given the trade-offs of the various defense mechanisms, it is critical for sites that know they are likely to be attacked to weigh the various options before they are affected by DDoS. For instance, site administrators will need to know whether to pay the startup costs to hire a protection service, how much to pay a service to withstand a traffic-based attack, and at what point to accept that the cost of defending against a given attack is too high.

Hiding Their Tracks? Ample Suspicion, but No Hard Evidence, That States Are Involved in DDoS

Most sites participating in the interviews expressed a strong belief that the national government of the country their site reported on was ultimately responsible for the attacks. None, however, had clear evidence of state responsibility. One participant had reported a large, ongoing attack to the state's security service but got no help since "it is very difficult to look into this because it is very difficult to catch yourself." He asserted that the security service shut down its own attack only when other publications better connected to the government complained. One Vietnamese site pointed to a press report of a Vietnamese military official claiming responsibility for the attacks.[14] As mentioned previously, a Viet Tan administrator noted that his site was normally filtered from within Vietnam but that the filtering was taken down at precisely the time that a botnet from within Vietnam attacked the site. Most interview participants asserted the opinion that the national government was responsible for the attacks but did not claim any direct evidence for the responsibility. This inability to attribute direct responsibility for DDoS attacks is typical for the attacks. The distributed nature of the attacks makes it difficult to assign responsibility—it is certainly possible that either a government or progovernment individuals could attack a site critical of a specific regime, and our inability to trace the attack would not be an unusual circumstance. Our findings in these respects are consistent with the findings of Villeneuve and Crete-Nishihata in chapter 8.

As a related matter, we also found no obvious connection between the particular ideology of an attacker and the choice of DDoS as an attack method. We saw attacks from ostensibly right- and left-wing groups, attacks that targeted governments, and attacks that suggest government involvement. Neither is there an apparent geographic pattern to the DDoS attacks we saw in our media analysis. We found attacks reported in widely disparate corners of the world. Asian states were a common site for DDoS attacks, but certainly not the only region where they appear. While there is

speculation that some attacks are traceable to governments—for instance, the example of http://bauxitevietnam.info—it is unclear that this is an assumption with any merit. DDoS is a technique used by individuals, groups, and, perhaps, states. The accessibility of easy-to-use tools and the apparent success of single-user attacks on small Web sites, as well as the technique's visibility in the media, suggest that aggrieved individuals may look to DDoS as an easy way of making a political point or settling a score. We note, too, that the widely reported DDoS attacks in the context of the release of U.S. State Department cables by Wikileaks in the fall of 2010 involved attacks both on Wikileaks itself and on major banks and others in apparent retaliation. In an ironic and perhaps inevitable twist, 4chan—an online community that claimed responsibility for many retaliatory attacks—was taken down by a DDoS on December 28, 2010. As with other Internet control mechanisms, DDoS is an approach used by a variety of actors to accomplish a variety of ends.

Conclusion: Situating DDoS in the Context of "Next-Generation Controls" and Other Online Contests

In response to the growing usage of next-generation Internet controls, citizens may be banding together to fend off DDoS and related attacks, at least on a modest scale. In three of our interviews, we heard of local technical experts acting as hubs of technical expertise for their countries (in Vietnam, China, and Iran, specifically). The most productive and satisfied of these local experts was far along in the process of moving sites in his country to a common infrastructure well supported by a hosting provider that was well connected to the core of the Internet (in all senses of "core": community, expertise, and resources). He was able to exert a great deal of control over the structure of the moved sites, including imposing onerous security and posting restrictions on the sites' administrators. The most concerned and least content of these local experts was struggling daily with many poorly written sites on broken, incompatible code bases, often reinstalling a site from scratch following an intrusion and manually fighting off the simpler of the constant DDoS attacks. He told us that he had the desire, but not the resources, to fix the underlying problems with the supported sites, as well as gratitude for the help he has received from other individuals, but he was frustrated by his inability to fend off high-bandwidth traffic attacks.

The threat of DDoS attacks is inextricable from other security considerations, including human resources concerns, technical resources, and community connections. Ultimately, what human rights and independent media organizations face, in Asia and elsewhere around the world, is a combination of a shortage of skilled site-administration skills, the bandwidth needed to fend off large network attacks, and the community connections needed to ask core network operators for help to fend off attacks. The difficulty of responding effectively to DDoS attacks is a symptom of a

larger problem: most small, independent organizations simply do not have the talent, bandwidth, or connections to administer independent Web sites in the face of potential attack. The online environment not only offers new ways to reach a broad audience, inside a state and beyond, but also poses new challenges in keeping that online accessible in the face of the many types of attacks described in this book.

There is a final twist to the story. Citizens who wish to publish independent media sites but who do not have significant technical savvy are most likely to be able to resist DDoS and related attacks by signing up with a large, free hosting service. These services, such as Google's Blogger or WordPress, are often run by large, for-profit companies that are not based locally where the activists are situated. This approach was the strategy used by http://bauxitevietnam.info in the attacks described at the beginning of this chapter, which Google ultimately diagnosed and then defended the site by providing resistant hosting. The interconnected nature of these attacks, along with the possible responses, puts citizens in Asia and elsewhere in common cause with multinational companies based elsewhere, pitted together against an elusive opponent that may or may not include their own state. Rebecca MacKinnon takes up this topic in greater detail in chapter 10 of this volume.

Though increasingly unavoidable, this allegiance between human rights organizations and large corporations can be a tenuous and complicated one. In the fall of 2010, when Wikileaks was subject to a DDoS attack after releasing U.S. State Department cables, they turned to Amazon.com to serve their Web site.[15] A few days later, Amazon.com decided to stop hosting Wikileaks, which continued to be subject to DDoS attacks, just as the perceived allies of Wikileaks launched DDoS attacks against large banks and others perceived to have turned against Wikileaks.[16] While these independent media sites may have interests aligned with large corporate players to some extent, their allegiance may break down in the context of pressure from states or other powerful interests. It is important to note, however, that any ISP providing services to Wikileaks would likely have come under political pressure from the U.S. government. It is possible that other providers would have acquiesced under similar pressure.

The days of simple filtering of offensive Web sites, in the manner pioneered by Saudi Arabia and a few other states roughly a decade ago, are long past. The interplay of this range of public and private actors and next-generation mechanisms in cyberspace is becoming increasingly complicated and unpredictable. Independent media and human rights operations, especially in Asia, have a much harder job than ever before to keep their Web sites accessible in times of conflict.

Notes

1. BauxiteVietnam Blog, http://boxitvn.wordpress.com/; Bauxite Vietnam Web site, http://bauxitevietnam.info; John Ruwitch, "Web Attacks Hit Vietnam Bauxite Activists: Google," Reuters, April 2, 2010, http://www.reuters.com/article/idUSTRE62U0TM20100402.

2. Ben Stocking, "2 Popular Web Sites Blocked in Vietnam," *Sydney Morning Herald*, February 27, 2011, http://news.smh.com.au/breaking-news-technology/2-popular-web-sites-blocked-in-vietnam-20100211-nupw.html.

3. Viet Tan, "Denial of Service: Cyberattacks by the Vietnamese Government," April 27, 2010, http://www.viettan.org/spip.php?article9749.

4. In January 2006, Google launched google.cn, a search engine hosted in China and censored to comply with Chinese law. In January 2010, Google shut down google.cn and redirected traffic to their unfiltered Google.com.hk site.

5. Neel Mehta, "The Chilling Effects of Malware," Google Online Security Blog, March 30, 2010, http://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html.

6. See the Shadowserver Foundation's resources on botnets and related activity at http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets for some of the most detailed analysis about the formation, growth, and application of botnets. One of the best of the white papers posted on the Shadowserver site, which addresses this question of rented botnets, is Krogoth, *Botnet Control, Construction, and Concealment: Looking into Current Technology and Analyzing Future Trends*, March, 2008 (special version for Shadowserver Web site), http://www.shadowserver.org/wiki/uploads/Information/thesis_botnet_krogoth_2008_final.pdf (see especially section 2.5, "Motivation and Usage"). See also *PC Magazine* Encyclopedia's entry on botnets: "Also called a 'zombie army,' a botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. The computer is compromised via a Trojan that often works by opening an Internet Relay Chat (IRC) channel that waits for commands from the person in control of the botnet. There is a thriving botnet business selling lists of compromised computers to hackers and spammers." Available at http://www.pcmag.com/encyclopedia_term/0,2542,t=botnet&i=38866,00.asp.

7. Viet Tan, "Denial of Service."

8. There have been an increasing number of reports of malware-related attacks on human rights organizations that may or may not have involved states. See, for instance, the path-breaking reports by our colleagues at the Information Warfare Monitor, available at http://www.infowar-monitor.net/research/.

9. For a description of first-generation Internet controls, see Robert Faris and Nart Villeneuve, "Measuring Global Internet Filtering," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008). For discussion of second- and third-generation controls, see Ronald Deibert and Rafal Rohozinksi, "Beyond Denial: Introducing Next-Generation Internet Controls," in *Access Controlled: The Shaping of Power Rights and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010).

10. Deibert and Rohozinksi, "Beyond Denial," 8.

11. Ibid.; OpenNet Initiative, "The Internet and Elections: The 2006 Belarus Presidential Election (and Its Implications)," OpenNet Initiative Internet Watch Report 001, April 2006, http://opennet.net/sites/opennet.net/files/2006%20Internet%20Watch%20Report%20Belarus.pdf.

12. Danny McPherson, Roland Dobbins, Michael Hollyman, et al., "Worldwide Infrastructure Security Report: Volume V, 2009 Report," Arbor Networks, January 19, 2010, http://staging.arbornetworks.com/dmdocuments/ISR2009_EN.pdf.

13. Christian Folini, "Apache Attacked by a 'Slow Loris,'" LWN.net, June 24, 2009, http://lwn.net/Articles/338407/.

14. Radio Free Asia, "Hackers in Vietnam: Do Not Confess Also That," May 19, 2010, http://www.rfa.org/vietnamese/programs/ReadingBlogs/%20VN-police-general-confesses-state-s-hacking-cb-s-web-and-blog-NHien-05192010161301.html.

15. Andrew R. Hickey, "Wikileaks Turns to Amazon Cloud to Dodge DDoS Onslaught," CRN, November 30, 2010, http://www.crn.com/news/cloud/228400232/wikileaks-turns-to-amazon-cloud-to-dodge-ddos-onslaught.htm.

16. Chloe Albanesius, "DDoS Attacks Continue to Plague Human Rights Sites," *PC Magazine*, December 22, 2010, http://www.pcmag.com/article2/0,2817,2374654,00.asp.

8 Control and Resistance

Attacks on Burmese Opposition Media

Nart Villeneuve and Masashi Crete-Nishihata

Burma is consistently identified by human rights organizations as one of the world's most repressive regimes. Human rights violations occur with regularity, especially in connection with the country's long-standing armed conflict. The ruling military junta, the State Peace and Development Council (SPDC), is best known for its political prisoners and its systematic denial of universal human rights such as freedom of expression.[1] The government's efforts to silence dissent pervade cyberspace and its system of Internet control is one of the most restrictive in Asia.

Despite the heavy hand that the regime wields over cyberspace, information communication technologies (ICTs) have provided Burmese opposition groups with the means to broadcast their message to the world and challenge the government. The ongoing battle between these two sides makes Burma a stark example of contested Asian cyberspace. The role of ICTs in this struggle can be framed by contrasting theories that view them either as "liberation technologies" that can empower grassroots political movements[2] or as tools that authoritarian governments can use to suppress these very same mobilizations.[3]

This contestation is dramatically illustrated by the series of protests that erupted across the country in 2007—in a movement popularly known as the "Saffron Revolution." During these protests, Burmese activists managed to bring the uprising to the world's attention by making images and videos of the demonstrations and subsequent government crackdown available on the Internet. Realizing the potential political impact of these images, the government severed Internet connectivity in the country for nearly two weeks.[4] This drastic action demonstrated that the regime had learned a significant lesson: although Burma's technical filtering system was successful in censoring access to information coming into the country from opposition media Web sites, it was unable to prevent information from flowing out of the country to these sites for global consumption.

As the one-year anniversary of the protests neared, the Web sites of the three main Burmese independent media organizations were attacked and effectively silenced. The Democratic Voice of Burma[5] and The Irrawaddy[6] were rendered inaccessible following

a distributed denial of service (DDoS) attack. While these attacks were under way, Mizzima News[7] was also compromised and its Web site was defaced.[8] Periodic attacks on Burmese opposition media sites continued through 2009 and 2010.[9] In late September 2010, around the third anniversary of the Saffron Revolution, Burmese opposition media were once again silenced by a series of DDoS attacks and Web site defacements.[10]

The timing of these attacks and the content of the messages in the Web site defacements indicate a political connection, and although the identity and capabilities of the attackers—as well as any relationships they may have with the government—remain unknown, it is widely believed that the government played a role in the attacks. This belief prevails because the Burmese government has consistently demonstrated an interest in controlling and censoring the communications environment in the country.

This chapter explores the complexities of information control and resistance in Burma based on an investigation conducted by the Information Warfare Monitor (IWM)[11] on the attacks launched against the Mizzima News Web site in 2008. Through technical evidence obtained from our investigation and field research conducted in Burma, we were able to uncover and analyze the characteristics and capabilities of the suspected attackers. We found that these attacks are consistent with government and military interest in information control and censorship of the Internet as well as a pattern of ongoing attacks against Burmese political opposition. However, they cannot be conclusively attributed to the military or government of Burma. Our investigation found that the attack on the Mizzima News Web site appeared to have been a result of a combination of two factors: political motivation and the availability of a target of opportunity. The attackers are certainly unfavorable toward the Burmese opposition media, but cannot be simplistically characterized as "progovernment" either. Their primary motivation appears to be nationalism and a belief that the opposition media demean the public image of their country. The timing of the attacks provided a strategic utility that would normally have been beyond the attackers' means. While Burma maintains a robust Internet censorship system that prevents its citizens from accessing alternative news media, these attacks effectively prevented global access to opposition media sites during a sensitive period.

We proceed by describing the spectrum of information controls in Burma that includes pervasive Internet filtering, repressive legal frameworks, and recurring cyber attacks. We then provide a detailed technical and contextual analysis of the Mizzima News defacement attacks and highlight the difficulty of determining the actors involved and motivations behind such attacks as well as questions surrounding state attribution. Finally, we situate the case study in the wider context of information controls in Burma and argue that gaining an understanding of threats to freedom of expression in cyberspace requires a holistic analysis that accounts for the unpredictable and contested nature of the domain.

Information Controls in Burma

The SPDC maintains tight authoritarian rule over all forms of media and communications in the country. All local television, radio stations, and daily newspapers are owned and controlled by the state.[12] Within the country there are 100 private publications, which are also heavily restrained and censored by state authorities.[13] The Printers and Publishers Registration Act, implemented in 1965, prohibits printed publications from being critical of the government and requires all printers and publishers to register with the government and submit materials for review.[14] The Video and Television Law applies similar regulations to television and film media.[15] Together, these restrictions have stifled what was once a vibrant free press.[16]

Amid this repression of traditional media the Internet has become an important source of information on Burma. Beginning in the early 1990s, Burmese expatriates and journalists living in exile set up news groups, mailing lists, and Web sites to disseminate information on the human rights and political situation in the country.[17] Today, the most popular independent Burmese Web sites operate outside of the country, with Mizzima News based in India, The Irrawaddy in Thailand, and the Democratic Voice of Burma in Norway. These Web sites receive reports from citizens within the country and provide an alternative to state-controlled media that often includes content critical of the regime. While these media organizations have become important outlets for international audiences to receive information on Burma, they are heavily censored within the country.

The regime aggressively denies, shapes, and controls online information in Burma. Internet penetration is very limited with an estimated online population of less than 1 percent.[18] OpenNet Initiative (ONI) testing has consistently found that the only two Internet service providers (ISPs), Yatanarpon Teleport (or Myanmar Teleport, formerly known as Bagan Cybertech) and Myanmar Posts and Telecom, extensively filter Internet content by targeting circumvention technologies, foreign e-mail providers, communications tools such as Skype and Gtalk, material related to human rights and the Burmese democratic movement, and independent news Web sites.[19] The Web sites of Mizzima News, the Democratic Voice of Burma, and The Irrawaddy have been filtered by the country's ISPs for years. Filtering is achieved through technology linked to U.S. companies Fortinet and Bluecoat despite an embargo that places limits on exports to Burma.[20] These technical restrictions are paired with hard legal enforcement, and bloggers and journalists in the country face a constant threat of prosecution for publishing dissenting material. The Reporters Without Borders's Press Freedom Index of 2010 ranked Burma 174 out of 178 countries, and in 2009 the Committee to Protect Journalists deemed Burma the worst country in the world to be a blogger.[21] These repressive controls create a climate of self-censorship in which citizens avoid publishing and seeking out banned content.

The Saffron Revolution was the scene of the most dramatic example of Internet controls and resistance in Burma. A small number of peaceful protests organized by Burmese social and political activists began on August 17, 2007, in reaction to a 500 percent increase in the retail price of fuel.[22] These initial demonstrations were quickly suppressed by the government, but peaceful protests spread throughout the country under the leadership of Buddhist monks. By mid-September the number of participants had swelled to 100,000, including 10,000 Buddhist monks.[23] The government reacted with a severe crackdown from September 26 to 29. During this time, a number of serious human rights violations occurred, including killings, mass beatings, and arrests.[24] Burmese independent media outlets, including Mizzima News, The Irrawaddy, and the Democratic Voice of Burma, along with numerous bloggers and citizen journalists, played a crucial role in disseminating reports of the crackdown to the international community. Despite the heavy restrictions enforced by the regime, activists and citizen journalists managed to upload images and videos of the protests and crackdown to the Internet. The dissemination of these images to the world did not go unnoticed by the SPDC, and on September 29, 2007, it employed a blunter tactic of information denial than its standard filtering practices.

Through its comprehensive control over Burma's international Internet gateways, the SPDC implemented a complete shutdown of Internet connectivity in the country that lasted for approximately two weeks.[25] Only two other states have taken such drastic measures. In February 2005, Nepal closed all international Internet connections following a declaration of martial law by the king.[26] On January 26, 2011, the Egyptian government ordered national ISPs to shut down in reaction to major protests in the country.[27] Severing national Internet connectivity in reaction to sensitive political events is an extreme example of *just-in-time-blocking*—a phenomenon in which access to information is denied exactly at times when the information may have the greatest potential impact, such as elections, protests, or anniversaries of social unrest.[28] The crude but effective means of information denial implemented by the SPDC shows the extent the junta is willing to go to restrict bidirectional flows of information in Burma. It also serves as an example of Internet control beyond filtering that is focused on denying information to international users rather than just blocking domestic access.

Silencing voices critical of the regime during key events is an ongoing occurrence in Burma, and there exists a long history of cyber attacks against Burmese activists and independent media organizations, which include a range of attack vectors from malware to DDoS attacks. In 2000, for instance, Burmese political activists received numerous e-mail messages containing viruses that many believe were part of an organized campaign perpetrated by state agents.[29] More recently, Burmese independent news organizations have confronted waves of attacks on their Web sites during the anniversaries of key political events in the country (table 8.1). As coverage of the one-year anniversary of the 2007 crackdown was emerging, the servers of The Irrawaddy

Table 8.1

TIMELINE OF MAJOR POLITICAL EVENTS AND RECENT CYBER ATTACKS AGAINST BURMESE OPPOSITION WEB SITES

Date	Event
August 8, 1988	Massive protests led by student activists in Burma known as the 8888 uprising
August–October 2007	Series of antigovernment protests led by Buddhist monks in Burma dubbed the "Saffron Revolution"
September 27, 2007	Military junta shutdown of access to the Internet within Burma
October 13, 2007	Internet access in Burma reconnected
September 2007	The Irrawaddy Web site infected with Trojan
July 2008	DDoS attack on Mizzima News Web site
July 2008	DDoS attack on Democratic Voice of Burma Web site
September 17, 2008	DDoS attack on Democratic Voice of Burma Web site
September 17, 2008	DDoS attack on New Era Journal Web site
September 17, 2008	DDoS attack on The Irrawaddy Web site
October 2008	Defacement attack on Mizzima News Web site
August 8, 2009	DDoS attack on Mizzima News Web site
September 2010	DDoS attack on Mizzima News Web site
September 2010	DDoS attack on Democratic Voice of Burma Web site
September 2010	DDoS attack on The Irrawaddy Web site

Sources: "Burmese Exiles' Leading Media Websites under Attack 20 July 2008," Burma New International, July 30, 2008, http://www.bnionline.net/media-alert/4590-burmese-exiles-leading-media-websites-under-attack-30-july-2008.html; "Press Release: DVB Web Site Hit by DDoS Attack," Democratic Voice of Burma, July 25, 2008, http://www.dvb.no/uncategorized/press-release-dvb-web-site-hit-by-ddos-attack/1256; "Websites of Three Burmese News Agencies in Exile under Attack," All Burma IT Students' Union, September 17, 2008, http://www.abitsu.org/?p=2502; Aung Zaw, "The Burmese Regime's Cyber Offensive," The Irrawaddy, September 18, 2008, http://www.irrawaddy.org/opinion_story.php?art_id=14280; Muchancho Enfermo, "Burma: Sri Lanka–Based Myanmar Media Website Attacked Again," Ashin Mettacara, March 17, 2009, http://www.ashinmettacara.org/2009/03/burma-sri-lanka-based-myanmar-media.html; http://www.ashinmettacara.org/2009/01/burma-myanmar-sri-lanka-based-burmese.html; "Fresh Attack on Mizzima Website," Mizzima News, August 8, 2009, http://www.mizzima.com/news/inside-burma/2599-fresh-attack-on-mizzima-website.html; Alex Ellgee, "Another Opposition Website Shut Down by Hackers," The Irrawaddy, June 19, 2010, http://www.irrawaddy.org/article.php?art_id=18759; Committee to Protect Journalists, "Burma's Exile Media Hit by Cyber-attacks," http://cpj.org/2010/09/burmas-exile-media-hit-by-cyber-attacks.php.

and the Democratic Voice of Burma were hit with DDoS attacks that overloaded the Web sites and rendered them inaccessible.[30] Similar attacks have occurred on subsequent anniversaries of the Saffron Revolution and the 1988 student protest known as the "8888 Uprising." The timing and coordination of these attacks suggest that the motivation behind them may be to censor the Web sites from commemorating the protests and possibly mobilizing new political actions.

It is unclear who was behind the attacks, although it is widely believed that the military or government played a role, since the regime maintains a strong interest in information control and actively seeks to silence opposition voices.[31] Opposition groups have come under persistent cyber attacks over the years and many believe such attacks are part of a wider campaign of state-sanctioned harassment.[32] However, positively determining attribution, motivations, and the extent of the attackers' abilities is a difficult task.

Mizzima News Defacement Attack

One example of the persistent attacks on Burmese independent media is the compromise and defacement of the Mizzima News Web site (http://www.mizzima.com) on October 1, 2008.[33] The original content of the site was replaced with a message from the attackers (figure 8.1):

Dear MIZZIMA Reader. . . . Listen please, Why Hack This Website? . . . Because We are Independence Hackers from Burma. We Born for Hack Those Fucking Media Website, Which are Ever Talk about Only Worse News For Our Country. We Very Sorry for Web Admin, You Need To More

Figure 8.1
A screen capture of the defacement of Mizzima.com.

Secure Your Website. New We Warn to All Media Webadmins That is "Prepare to more Secure your Work."

This case demonstrates how attackers mask their identity, thus making it difficult to determine those responsible for the attacks. The attackers who defaced Mizzima News—which is blocked by ISPs in Burma—used censorship-circumvention software to perpetrate the attack hosted on servers that had IP addresses allocated to the United States, France, and Germany in order to make it appear as if the attacks originated in those countries.[34] Mizzima News reported on October 1, 2008, that the attacker's IP address originated in the United States. On October 10, 2008, Mizzima News reported: "While it is still difficult to technically trace who is behind the hacking attempts, Mizzima's technical staff said the main attempt is found to have originated from Russia with cooperation from other hackers in Germany, France and India."[35] The incident highlights the difficulty in tracing the geographic location of the attacks, let alone determining the identity and intent of the attackers. In the absence of sufficient evidence to attribute attacks, analysts often turn to the political context to fill in the gaps. In view of the persistent efforts by the government and military to crack down on political dissent, it is clear that they have an interest in silencing critics such as Mizzima News. However, a careful examination of the technical evidence, as well as an exploration of alternative explanations, is critical to understand the characteristics of the attackers.

Investigating the Attack

Following the October 1, 2008, defacement of the Mizzima News Web site, the IWM offered to assist Mizzima News with an investigation of the attack, and the organization provided us with access to their Web server logs and sample copies of c99shell (a backdoor program that provides attackers with remote access to a victim's machine) that were found on the compromised Mizzima News Web server.[36] We processed these log files and isolated the IP addresses that connected to and issued commands on the c99shell backdoor program. We removed the IP addresses of the legitimate administrators who had later connected to test c99shell. We were left with a set of IP addresses that we identified as belonging to a censorship-circumvention proxy service. While some variation existed in the IP addresses, there were consistent browser user-agents[37] that (1) connected from the circumvention proxy service IP addresses and (2) connected to and executed commands on the c99shell backdoor. We collected and analyzed all log entries in which the identified IP addresses connected to and issued commands on instances of the c99shell backdoor.

We identified five attackers. The two primary attackers appeared to be working in tandem with one another. Although we believe that the remaining three attackers are

distinct individuals, there is the possibility that they are the two primary attackers using different browsers (and/or operating systems).

The log files indicate that in the days before and after the defacement, the attackers browsed the Mizzima News Web site from sites with Burma-related content such as http://komoethee.blogspot.com (September 10, 2008) and http://baganland.blogspot.com (September 30, 2008). They connected to Mizzima News from articles that referred to the ongoing DDoS attacks against The Irrawaddy and the Democratic Voice of Burma and were thus well aware of the scope of the attacks targeting opposition news media.[38] Just six hours before the defacement, the attackers visited Mizzima News from an article that detailed Burma's cyberwarfare capabilities and that claimed the attacks "may have been conducted by Myanmar military officers trained or undergoing training in Russia and China."[39] The attackers then accessed a variety of articles on the Mizzima News Web site. It is likely that at this stage they determined that the Mizzima News Web site was based on the Joomla! Customer Management System (CMS).[40]

Beginning on September 19, 2008, the attackers attempted to exploit a number of known vulnerabilities in the Joomla! CMS that the Mizzima News Web site was running on. After a series of unsuccessful attempts, Attacker 2 finally managed to exploit a password reset vulnerability in Joomla! and immediately logged in as the administrator. This "remote admin password change" exploit is very simple and can be conducted through any Web browser. The exploit was publicly available by August 12, 2008, about two months before it was used to compromise Mizzima News.[41]

After acquiring administrator privileges by exploiting the password reset vulnerability, Attacker 2 shared administrator access with Attacker 1. Both attackers attempted to download c99shell onto the compromised server, and within 20 minutes both attackers had set up the Trojan tool and began exploring the directories of the Mizzima News Web servers. Eventually, the attackers shared access with a third attacker and gained access to several My SQL databases. They deleted parts of the databases, and by 4:56 PM on September 30, 2008, they had defaced the Mizzima News Web site.

The attackers returned several times and installed more instances of c99shell as well as pBot, an Internet Relay Chat (IRC) bot with both Trojan and DDoS capabilities, while Mizzima's administrators attempted to delete the malicious files. The attackers also defaced the Mizzima News Web site repeatedly after Mizzima administrators tried to restore the original content. The attackers were finally locked out on October 4, 2008. They attempted—unsuccessfully—to return on October 5 and 6.

We approached the censorship-circumvention software provider that the attackers used with convincing evidence of the attacks and the use of their tool and asked if they could confirm that the attackers used the IPs we traced back to their services. The software provider confirmed that Attacker 1 and Attacker 2 logged in to the circumvention service from IP addresses assigned to Burma, which is interesting because the Mizzima News Web site is filtered by Burmese ISPs and inaccessible to Internet

users in Burma. Therefore, the attackers had to bypass this ISP-level filtering in order to attack the Web site. They also probably believed that using the service would shield their identities.

To summarize, the evidence suggests there were two primary attackers working in collaboration with one another other to exploit and "Trojan" the Mizzima News Web server. These attackers appear to have shared links to the Trojans that they had installed with additional attackers. In total, there appear to have been five attackers working together to maintain control over the Mizzima News Web server. The attackers deleted portions of Mizzima's database and defaced the Web site repeatedly. Over the course of seven days, they continued to attack Mizzima's server while the Mizzima administrators worked to delete the different backdoors that the attackers frequently installed. By the fifth day they were shut out of the system, although they continued to check for access on the sixth and seventh days but were denied. We further confirmed that the attacks originated from Burma and used the proxy service to bypass national-level filtering of Mizzima News.

Investigating the Attackers

We investigated the identities of the attackers by analyzing the versions of the backdoor program c99shell and the IRC bot pBot they used, the specific attackers who downloaded these files, and the location they retrieved the programs from. What follows is an analysis of the data trail we followed by analyzing and linking the information contained in these files.

The c99shell backdoor program is a widely available Trojan backdoor written in the PHP programming language.[42] The versions of c99shell that the attackers tried to download to the Mizzima News Web server were slightly modified to include text in the interface reading, "Hacked by doscoder—oGc Security Team—#cyberw0rm @ oGc" (figure 8.2).

Based on this information, we could infer that the tool had been modified by "doscoder"—who is a member of the "oGc Security Team" and IRC channel "#cyberw0rm" on an IRC network called "oGc." However, these data points do not necessarily

Figure 8.2
Screen shot of the modified interface for the c99shell backdoor program.

attribute the attacks to these aliases, since it is possible the attackers could be using someone else's tools.

Where the attackers downloaded the Trojan programs they used in the attack revealed further evidence. The attackers downloaded c99shell and pBot from two separate locations. The version of c99shell at both locations was identical. The pBot was functionally identical, but the connection information in the pBot configuration file was different. Attacker 1 and Attacker 3 both made attempts to download the same instance of c99shell from a compromised server. However, only Attacker 2 was able to successfully download c99shell from the Web site 0verkill.co.cc and upload it to the Mizzima Web server.

Attacker 2 made attempts to download an instance of c99shell as well as another file, an instance of pBot, from 0verkill.co.cc. 0verkill.co.cc was registered to "Charlie Root" with the e-mail address ir00t3r@gmail.com. It was registered from an IP address in Burma.[43]

The pBot that Attacker 1 attempted to download from 0verkill.co.cc was configured to connect to an IRC server, overkill.myanmarchat.org (with the prefix "vesali") to IRC channel "#jail." The pBot that Attackers 2 and 3 attempted to download from a compromised server, videovideo.it, was configured to connect to an IRC server at 64.18.129.9 with the prefix "soul" (figure 8.3).

To collect further information we attempted to connect to 64.18.129.9, but were unable to obtain access. We were able to briefly connect to the overkill.myanmarchat.org IRC server until we were kicked out and banned. The "overkill" subdomain was subsequently removed and failed to resolve. When connecting to the overkill.myanmarchat.org IRC server, the network names "irc.doscoder.org" and "irc.vesali.net" were displayed. Only one user was seen on the server:

[xer0] (~xero@overkill.name): xero
[xer0] @#jail
[xer0] irc.doscoder.org:Over Kill Over The WorlD
[xer0] is a Network Administrator
[xer0] is available for help.

The IRC server information indicated that there was some still-unknown relationship between "doscoder" and "0verkill." It is important to recall that modifications were made to c99shell by doscoder—a member of the "oGc Security Team" and the "#cyber-w0rm" channel on the oGc IRC network. Now, "doscoder" emerged as the host name for the overkill.myanmarchat.org IRC server. A Web search turned up a relationship between the file name and location path of the c99shell at now defunct locations on doscoder.t35.com. In addition, much of the code in the defacement page posted on the Mizzima News Web servers was similar to the code in another unrelated defacement by doscoder. However, no further information was found concerning the doscoder alias.

```
<?

set_time_limit(0);
error_reporting(0);
echo "ok!";
ini_set("max_execution_time",0);
class pBot
{
var $config = array("server"=>"overkill.myanmarchat.org",
                    "port"=>"443",
                    "pass"=>" ",
                    "prefix"=>"[]vesali[]",
                    "maxrand"=>"5",
                    "chan"=>"#jail",
                    "chan2"=>" ",
                    "key"=>" ",
                    "modes"=>"+p",
                    "password"=>"overkill",
                    "trigger"=>".",
                    "hostauth"=>"overkill.name"
                    );
var $users = array();
function start()
```

Figure 8.3
The configuration of Attacker 2's pBot.

Although the overkill.myanmarchat.org IRC server disappeared soon after we connected to it, we discovered another IRC server hosted on "irc.myanmarchat.org." This server is one of the IRC servers for the Olive Green Complex (oGc), an IRC network founded in 2004 by Burmese students studying at the Moscow Aviation Institute (MAI) in Russia, which provides advanced training in computer engineering and informatics[44] and is currently subject to a U.S. embargo for its alleged role in supplying nuclear weapons technology to Iran.[45] According to Aung Lin Htut, a former deputy ambassador to Washington, the attacks against the Burmese opposition Web sites were conducted by "Russian technicians" based in "Burma's West Point cyber city"—a reference to Myanmar's Academy of Defense Services in Pyin Oo Lwin, Mandalay Division, Myanmar.[46] Aung Lin Htut further stated that Burmese military officers are trained at the MAI.[47]

The oGc is described by members as being an IRC group for those interested in information technology and computer engineering.

oGc is a non-profit organization and it intends for all people who interest in Information Technology. We all are students and all of members are interesting in learning IT. The main of oGc Network is to give outs free psyBNC account, email and others free services to people in learning more about unix and linux features. We [would] be glad if you would find any useful information on oGc and trust that we will not have disappointed you with the fruits of our efforts. Finally, the oGc was born and we [would] like to thank to all people who [participated] and helped us get oGc off the ground. We dedicated to use Myanmar IRC gateway. We started it at November 2004.[48]

The students also operate an IRC server at irc.olivegreen.org that has the same IP address as irc.myanmarchat.org. The oGc IRC network is accessible by several domain names. According to registration information, some of these domains were registered by students at the MAI. The server is frequented by students studying in Burma, Russia, China, and Singapore. There is also a server, irc.mmustudent.org, for students of the Myanmar Maritime University, which has a computer science department.[49] The earliest domain name registrations indicated that oGc originated in Russia. However, the most recent activity on the server was traced to Burma.

In our observations of the oGc IRC network we found the group's members and frequent chatters were friendly and generally interested in information technology. There was the occasional discussion about an exploit or Web defacement, but that was not the focal point of the conversation. The oGc IRC network appears to be a legitimate IRC network as opposed to a specifically "hacker"-related network.

As our investigation progressed we provided the circumvention software provider with the aliases of several suspects from the oGc IRC network and asked to confirm if they had them in their system. We found that three of these nicknames were among some 20 account names on the circumvention software service utilized from the same installation as one of the attackers. Based on these correlations, we had substantial evidence that members of the oGc may have been involved in the attack.

On the oGc IRC network we found an operator identified as the administrator of oGc who, through our analysis, was revealed to be using multiple aliases associated with the alias found in the configuration of the pBot Trojan used in the attacks against Mizzima, as well as related accounts on the circumvention software service. We initiated IRC chats[50] with the oGc administrator and other oGc members and asked why they thought Mizzima News was defaced. Their general response was that the opposition highlights only the negative aspects of Burma and generally produces "nonsense." The oGc administrator suggested that there were "rules of every country" and implied that Mizzima News had broken those rules, noting "u should know, what kind of articles are written there." In general, the oGc administrator and other members of the group did not appear to be "progovernment" and acknowledged that issues of government corruption were legitimate. However, they were very proud of their

country and nationalistic, and they did not approve of the foreign media's portrayal of Burma. Although the oGc administrator denied being responsible for the defacement of Mizzima, he was often vague and implied that it may have been him. He was also aware of "doscoder" and "0verkill" but refused to discuss them.

Based on our correlative evidence, we directly accused the oGc administrator of defacing Mizzima in our IRC chat by linking his various aliases to the circumvention software used in the Mizzima attacks. The oGc administrator never directly accepted responsibility, but he used tongue-in-cheek responses that alluded to his involvement. For instance, although he said his involvement was "impossible," he added emoticon smiley faces to his replies. He also suggested that he was being framed and that a well-known hacker, Lynn Htun, was the person responsible for the attacks.

Lynn Htun, better known by his handle "Fluffi Bunni," defaced high-profile information-security-industry Web sites such as the SANS Institute with humorous, taunting text and images between 2000 and 2003. Lynn Htun was arrested in London on April 29, 2003, while attending the InfoSecurity computer security conference, for his failure to appear in court on (unrelated) forgery charges. He formerly worked in the U.K. offices of Siemens Communications.[51]

In response to a post on Myanmar IT Pros (http://myanmaritpros.com)—a popular forum for Burmese information technology professionals—Lynn Htun posted the following analysis of the oGc:

> Their server is called irc.olivegreen.org . . . they set up irc servers and rent them out to botnet owners, in return, they are allowed to use the botnet to ddos once a month or so. They didn't hacked the drones for the botnet, they are simply providing the server(s) for harvesting the botnet. So in other words, there's no real skills there. . . . You should contact their service provider and tell them to shutdown the botnet hub that is running on the following VPS. . . . All the above IPs are bound to a FreeBSD box running on a VPS. You wont find the bots on their server when you join because they are all in a secret channel with umode flags set to hide them from normal users.[52]

Lynn Htun's accusation that the oGc occasionally uses a botnet constructed by others for DDoS attacks as a form of payment infuriated the oGc administrator, who denied the claims vigorously when we mentioned them during our IRC chats with him. During one chat a strange coincidence occurred when an IRC user with the nickname "lynn" appeared in the oGc IRC channel, purporting to be Lynn Htun. The two times that "lynn" connected to the server, the following information was displayed:

```
lynn (~xero@bagan-3634EE84.childminder.co.uk)
Lynn (humm@bagan-888BA9F1.uk2net.com) has joined #Bagan
[Lynn] (humm@bagan-888BA9F1.uk2net.com): xero
```

Recall that the information seen when a user enters the overkill.myanmarchat.org server was "~xero overkill.name irc.doscoder.org xer0 H*:1 xero." It may be a coincidence but the "xero" is present in both. It is difficult to assess whether lynn was in fact Lynn Htun. In the chat, "lynn" appeared to backpeddle from the post made on Myanmaritpros.com, raising questions about whether the user was actually Lynn Htun.

Lynn Htun's profile on Myanmaritpros.com indicates that he works for Myanmar Online. The IRC group for Myanmar Online has an apparent rivalry with oGc, and if anyone creates a channel with a name associated with oGc, such as "ogc," he or she is kicked from the channel and given the following message: "You have been kicked from the chat room by ChanServ with the reason 'lamer channel' and cannot send further messages without rejoining."

In some of his posts on Myanmaritpros.com, Lynn Htun expresses views that appear unfavorable toward the Burmese political opposition but do not necessarily reflect a "progovernment" position either. His perspective appears to be nuanced and stems from what he refers to as the "excessive politicization of our daily lives"[53] as well as the "collateral damage" that emerges as a result of tying economics to political reform through the use of sanctions:

> Unfortunately our beloved politicians have [intertwined] the development of the country with political process. As such, as long as there are political deadlocks, our country's developments will be [hampered] and our IT industry will be stuck in a limbo forever more. I would like to show your posting to those who claim that sanctions are working and that they are essential for political transition. Insisting that economic and social development goes hand in hand with political progress is like saying prostrate cancer can be cure[d] with cough medicine. Yet, knowingly many insist that enforcing sanctions on Myanmar is a good thing because it serve[s] the greater cause and of course all the negative side effects are acceptable collateral damage.[54]

General discontent with opposition media is reflected in a thread on Myanmaritpros.com in which Lynn Htun and others expressed frustration over the coverage of a competition to develop a search engine sponsored by the Myanmar Computer Professional Association. After The Irrawaddy posted an article suggesting that the competition may have been "designed by the Burmese military junta in order to increase its Internet restriction technology and ability to control Web sites and blogs,"[55] Lynn Htun called them "democrazies" and suggested that The Irrawaddy was opposed to improving the state of information technologies in Burma: "I don't think that is on the agenda of the 'democrazies,' politicians and exiled media outlets. . . . Looks like they already cooked up some nasty accusations:-(."[56] This incident appears to illustrate a tension in the Burmese IT community that suggests how viewing the sociopolitical climate and its relation to technology in the country in black-and-white terms may overly simplify the situation.

Burmese Hacker Community

As part of our investigation, an IWM researcher traveled to Burma to gain insight into the local hacker community and assess their motivations. The hacker culture in Burma, as in many places around the world, appears to be oriented toward touting one's skills in order to improve business opportunities. One source within the information technology community indicated that the motives behind the attacks on Mizzima News may very well not have been political. Instead, they may have been motivated by a desire to demonstrate the hackers' skills online for personal gratification as well as to advance personal economic interests. He explained that by drawing attention to their expertise through such attacks, hackers may have hoped to attract demands for "protection" from network administrators. Essentially, they could have been creating a demand and, in turn, supplying the protection.

Hackers such as Fluffi Bunni have become respected members of Burma's information technology community and have commercialized their skills. While they do not support the political opposition, they are not necessarily hostile to it. Rather, they seem to believe that apolitical policies are better suited toward advancing both the economy and the ICT sector within Burma. As a result, they are critical of expatriate Burmese media that oppose the country's government and military.

In contrast, other sources within Burma indicated that political motivations were behind the attacks. They said that since very few people within Burma actually have an Internet connection, these attacks are likely the work of Russian-trained hackers. This view aligns with the charges made by Burmese opposition groups.

Ultimately, none of our sources could clarify whether those behind the attacks acted independently or alongside government interests. What we found in our field investigation is that there is a lively hacker community in Burma, but information regarding their relationship with the government and military is extremely scarce, and the information that is available is inconclusive.

The information obtained during the field investigation also provides context to the ongoing attacks against the Burmese opposition media. As we mentioned, the opposition Web sites are already blocked and inaccessible to Internet users in Burma. According to our sources in the country, the political opposition in Burma actually avoids using the Internet because they perceive communications over the Internet as being insecure, and using the Internet, as opposed to other forms of communication, makes them more vulnerable to government interception. In addition, computer literacy levels are very low, and few of those who use the Internet are familiar with security practices such as encryption. As a result, the opposition within Burma uses the Internet primarily for the dissemination of information through anonymous blogs and news reporting. The importance of sites like Mizzima News is not necessarily that they provide information to people within Burma, but rather that they provide

information about Burma to a global audience. This observation helps to explain why opposition media sites are routinely attacked despite the fact that they are inaccessible to Internet users within Burma.

Assessing Threat and Attribution

To assess the capabilities of computer network attackers, John Arquilla has defined three useful categories that indicate the skill and resources required to carry out various levels of attacks:

Simple-Unstructured The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
Advanced-Structured The capability to conduct more sophisticated attacks against multiple systems or networks and possibly to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
Complex-Coordinated The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organizational learning capability.[57]

Analyzing the attacks within this framework grounds political context in technical data in a way that provides a clearer picture of the identity and intent of the attackers.

Our analysis suggests that the attackers have significant knowledge of information technology, which enables them to launch attacks by leveraging basic, publicly available exploits and software tools. They may also have access to botnets capable of DDoS attacks, but they do not create or own the botnets themselves. In the attack against Mizzima News, the attackers employed basic means to mask their identities, but did not or were unable to escalate their user privileges to "root" administrator level on the server or successfully cover their digital tracks. They maintained a low level of operational security and left behind significant pieces of evidence. The evidence implicates members of the oGc in the attacks, and in particular the oGc's administrator. The relatively low sophistication of the attack and the capabilities of the attackers indicate that they are best placed within the "Simple-Unstructured" category of Arquilla's framework. However, the fortuitous timing of the attack provided the attackers with a "strategic utility" that would normally be beyond their means.

Despite the correlative evidence, there are several alternative explanations concerning attribution that we have to explore. The administrator of the oGc often suggested in our IRC chats that Lynn Htun was responsible for the attacks. Lynn Htun has a

history of prolific defacements and is critical of opposition media sites. An IRC user reporting to be Lynn Htun had xer0 in his connection information, which matched a user in a channel on "overkill.myanmarchat.org" that was used by the attackers. However, it is unclear if the user we spoke with was really Lynn Htun. In addition, oGc and Lynn Htun's Myanmar Online appear to be rival IRC networks, a fact that may explain why the oGc administrator implicated Lynn Htun in the attacks.

Another explanation concerns the use of the oGc's IRC infrastructure as a platform for the attackers. It is possible that the attackers used the oGc infrastructure through some arrangement with oGc or that the oGc simply tolerated their presence. This scenario is consistent with Lynn Htun's charge that the oGc provides hosting for botnets in return for the ability to occasionally use them for DDoS targets. Another consistent explanation is that the oGc could have also supplied access to censorship-circumvention proxies to their general membership. The administrator's accounts of oGc on the circumvention software network could have been shared across members of the oGc.

Based on the evidence we collected, we assessed that the suspected attackers in this case are not particularly favorable to the Burmese opposition but cannot be simplistically characterized as "progovernment" either. Their hostility toward the Burmese opposition appears to stem from feelings of nationalism and a belief that the opposition promotes a negative image of their country. Most appear to be concerned with gaining employment and improving the state of information and communications technology in Burma. Although they have both the skills and motivation to attack opposition Web sites, they may have attacked such Web sites without formal connections to the government. While our investigation provides indications of the possible identities of the attackers, it presents more questions than answers around state involvement in the ongoing cyber attacks against Burmese opposition groups.

The characteristics of the attackers and the opportunistic nature of the attacks may reflect a "swarming effect" in which private individuals, inspired by patriotic sentiments, voluntarily participate in cyber attacks during political events without clear approval or direction from state entities. This phenomenon has been observed in a number of recent conflicts and political events, including the 2008 Russia-Georgia war, the 2009 Gaza conflict, and the 2009 Iranian elections.[58] Our investigation shows that even a relatively simplistic attack can have significant effects if it is executed at a sensitive time. The attackers in this case were able to deface Mizzima News because it was running a version of Joomla! that was known to be vulnerable. In effect, this was a preventable attack—a known vulnerability that was exploited by opportunistic attackers. However, the timing of the attack coincided with ongoing DDoS attacks, and the addition of a visible threat (defacement) compounded the effect on the political opposition and their supporters. The involvement of private individuals in cyber attacks during political events demonstrates the chaotic nature of cyberspace and shows that

while it is possible that states may be instigating attacks, they cannot control outside participants from contributing to them, and such contributions can lead to unpredictable outcomes.[59]

Although we did not find evidence of state attribution in our investigation, it does not rule out the possibility that the SPDC is somehow involved in the recurring attacks against Burmese opposition groups. However, their involvement may be more subtle and indirect than speculations of elite military units leading cyber attacks on dissident Web sites convey. It is possible that the SPDC is engaged with individuals and groups in the Burmese hacker community and either subtly encourages them to participate in attacks against opposition groups or at least condones their actions. State-sanctioned patriotic hackers have been suspected in other cyber attacks originating from Russia, China, and Vietnam, but direct evidence is elusive.[60] The state may also be employing third-party actors to conduct cyber attacks through a crime-as-a-service model in which they hire criminal groups to perpetrate the attacks or rent necessary resources such as botnets from them.

The use of technical infrastructure related to criminal activities in seemingly politically motivated cyber attacks has been observed in high-profile cases such as attacks on Georgian government Web sites during the 2008 Russia-Georgia conflict.[61] This model of privateering is potentially attractive to nation-states because it permits them plausible deniability: actions take place in a criminal ecosystem that is removed from state entities and difficult—if not impossible—to trace back to them. Confirming these speculative scenarios in Burma is difficult, since much remains unknown about the attacks, the possible actors, and the motivations behind them. However, situating these events within the wider context of recent cyber attacks in other countries shows they are part of a troubling global trend that needs to be analyzed across both the technical and political complexities of cyberspace.[62]

Conclusion

Unlike Internet filtering at the ISP level that is limited to local control, cyber attacks conducted at strategically sensitive times have the ability to disrupt information flows to international audiences right when the content may have the most impact. States are obvious units of analysis when examining attribution and intent behind national filtering regimes. However, actors and their intentions are not as readily apparent in politically motivated cyber attacks. Despite the difficulties, due to the political nature of attacks against civil society organizations, many observers attribute these incidents to government and military entities. As a result, the attackers' capabilities are often overestimated, and their motivations are unknown. Although the issue of attribution is essential to analysis of such attacks, it remains the most difficult and ambiguous component of any investigation.

Our research illustrates the need to utilize a holistic approach that incorporates historical and political context into incident response and technical investigations, especially in cases where the attackers face little or no likelihood of being prosecuted. This analytical approach is especially applicable to civil society organizations that confront ongoing, politically motivated attacks originating from attackers who leverage geography, adversarial political relationships, and the lack of international cooperation to avoid prosecution. Careful technical analysis is required to properly assess the threat posed by attackers. However, if security incidents are treated as isolated cases focused solely on technical forensics, the bigger picture and broader implications of the attacks cannot be properly understood.

The struggle between information control and resistance in Burma takes place on a contested terrain that reveals unique characteristics of cyberspace that preclude simplistic explanations and frames. The opposition between state and citizen that is emphasized by images of military crackdowns on peaceful protesters can obfuscate the complexities of political power in cyberspace. The Burma case shows that even in a country with one of the world's most restrictive communications environments, an authoritarian state cannot maintain full control over the Internet without disconnecting from the global network all together. Conversely, the same dynamic properties of cyberspace that make it resistant to complete control are also what make vectors like denial of service attacks such effective and vexing threats against freedom of expression.

These attacks may be the product of users motivated by patriotism swarming in from the edges of the network to disrupt key information outlets, state-sanctioned military operations, or collusion between states and criminal groups operating in the shadows of the Internet. Any one or combination of these scenarios may be at work, making the study of these attacks all the more difficult.

Burma shows that Asian cyberspace cannot be simply classified as either a locus of control or resistance, but rather is better understood as the site of a constantly evolving and dynamic contest between a range of actors and agendas. Understanding how freedom of expression can be equally repressed and advocated in this environment requires studying it holistically and examining the subtle interrelations between the social, political, and technical facets of the network. Approaching the domain in this way presents significant practical and methodological difficulties for consortiums like the ONI, IWM, and the research and policy community at large, but confronting these challenges and peering into the subterranean depths of cyberspace are essential for revealing the contests being fought and the stakes involved in them.

Notes

1. Human Rights Watch, "Burma," 2009, http://www.hrw.org/en/world-report-2010/burma; Amnesty International, "Burma, Amnesty International Report 2009," http://report2009.amnesty.org/en/regions/asia-pacific/myanmar.

2. Larry Diamond, "Liberation Technology," *Journal of Democracy* 21, no. 3 (2010): 69–82.

3. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011).

4. Mirdul Chowdhury, "The Role of the Internet in Burma's Saffron Revolution," Berkman Center for Internet and Society, September 28, 2008, http://cyber.law.harvard.edu/publications/2008/Role_of_the_Internet_in_Burmas_Saffron_Revolution; OpenNet Initiative, "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," October 15, 2007, http://opennet.net/research/bulletins/013.

5. The Democratic Voice of Burma Web site is http://www.dvb.no.

6. The Irrawaddy Web site is http://www.irrawaddy.org.

7. The Mizzima News Web site is http://www.mizzima.com.

8. A Web site defacement is an attack in which the visual content of a page is altered.

9. For a listing of reported attacks on Burmese opposition groups, see the DoS Watch project, http://www.doswatch.org/search/label/burma.

10. Committee to Protect Journalists, "Burma's Exile Media Hit by Cyber-attacks," September 27, 2010, http://cpj.org/2010/09/burmas-exile-media-hit-by-cyber-attacks.php.

11. The Information Warfare Monitor is a sister project to the OpenNet Initiative that studies the emergence of cyberspace as a strategic domain and analyzes politically motivated cyber attacks and espionage. See Information Warfare Monitor, http://www.infowar-monitor.net.

12. Freedom House, "Burma (Myanmar) Country Report 2010," http://www.freedomhouse.org/template.cfm?page=22&year=2010&country=7792.

13. Roy Greenslade, "How Burma Quashes Press Freedom," Guardian Greenslade Blog, September 26, 2007, http://www.guardian.co.uk/media/greenslade/2007/sep/26/howburmaquashespressfreedom.

14. Printers and Publishers Registration Act (1962), http://www.burmalibrary.org/docs6/Printers_and_Publishers_Registation_Act.pdf.

15. Article 32, Television and Video Law (The State Law and Order Restoration Council Law No. 8/96), July 26, 1996, http://www.blc-burma.org/html/Myanmar%20Law/lr_e_ml96_08.html.

16. Chowdhury, "The Role of the Internet in Burma's Saffron Revolution."

17. Ibid.

18. International Telecommunications Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 figures. http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

19. See the Burma country profile in this volume; Reporters Without Borders, "Internet Enemies: Burma," 2010, http://www.rsf.org/en-ennemi26126-Burma.html.

20. Nart Villeneuve, "Fortinet for Who?" Nart Villeneuve: Malware Explorer, October 13, 2005, http://www.nartv.org/2005/10/13/fortinet-for-who/; United States Department of the Treasury, "Burma Sanctions," http://www.treasury.gov/resource-center/sanctions/Programs/pages/burma.aspx.

21. Reporters Without Borders, "Press Freedom Index 2010," 2010, http://en.rsf.org/press-freedom-index-2010,1034.html; Committee to Protect Journalists, "Ten Worst Countries to Be a Blogger," April 30, 2009, http://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php.

22. Seth Mydans, "Steep Rise in Fuel Costs Prompts Rare Public Protest in Myanmar," *New York Times*, August 23, 2007, http://www.nytimes.com/2007/08/23/world/asia/23myanmar.html?_r=1&scp.

23. Ardeth Maung Thawnghmung and Maung Aung Myoe, "Myanmar in 2007," *Asian Survey* 48, no. 1 (2008): 13–19.

24. Ibid.

25. OpenNet Initiative, "Pulling the Plug."

26. OpenNet Initiative, "Nepal Country Profile," 2007, http://opennet.net/research/profiles/nepal.

27. James Cowie, "Egypt Leaves the Net," Renesys, January 27, 2011, http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

28. Ronald Deibert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet,'' in *Access Denied: The Practice and Policy of Global Internet Filtering,* ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 123–149.

29. Brian McCartan, "Myanmar on the Cyber-offensive," *Asia Times*, October 1, 2008, http://www.atimes.com/atimes/Southeast_Asia/JJ01Ae01.html.

30. Mizzima News also previously reported being the target of DDoS attacks on July 29, 2008. Saw Yan Nang, "The Irrawaddy Hopes to Defeat the Hackers Soon," The Irrawaddy, September 19, 2008, http://www.irrawaddy.org/article.php?art_id=14283; "Websites of Three Burmese News Agencies in Exile under Attack," Mizzima News, September 17, 2008, http://www.mizzima.com/news/regional/1052-websites-of-three-burmese-news-agencies-in-exile-under-attack.html; Connie Levett, "Burmese Dissident Websites Shut Down," *The Age*, September 20, 2008, http://www.theage.com.au/news/web/burmese-dissident-websites-shut-down/2008/09/19/1221935424916.html; and Kenneth Denby, "Dissident Websites Crippled by Burma on Anniversary of Revolt," *The Times*, September 22, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4799375.ece.

31. "Burma's IT Generation Combats Regime Repression," The Irrawaddy, October 7, 2008, http://www.irrawaddy.org/print_article.php?art_id=14399; "Mizzima Websites Hacked," Mizzima News, October 1, 2008, http://www.mizzima.com/news/inside-burma/1092-mizzima-websites-hacked.html; McCartan, "Myanmar on the Cyber-offensive."

32. McCartan, "Myanmar on the Cyber-offensive."

33. "Mizzima Websites Hacked," Mizzima News; Saw Yan Naing, "Burmese Exile Media Web Site Again under Attack," The Irrawaddy, October 1, 2008, http://www.irrawaddy.org/article.php?art_id=14348.

34. "Mizzima Websites Hacked," Mizzima News.

35. "Hack Attempts Suspend Mizzima Websites," Mizzima News, October 10, 2008, http://mizzima-english.blogspot.com/2008/10/hack-attempts-suspend-mizzima-websites.html.

36. "Backdoor programs" refer to malicious software designed to provide attackers with unauthorized remote access to computer systems. For a detailed technical description of the c99shell backdoor program, see "Backdoor.PHP.C99Shell.w," Secure List, July 15, 2008, http://www.securelist.com/en/descriptions/old188613.

37. The user-agent header is sent by your browser to the Web server you are connecting to. The user-agent header commonly identifies the operating system and browser that you are using.

38. In fact, they appeared to be monitoring news of attacks on opposition Web sites, with one user posting this article into the IRC chat Myanmar ISP, "Military Government Paralyses Internet," October 9, 2008, http://www.myanmarisp.com/20080816/ICTN/ictnews0101/, authored by Reporters Without Borders, which details the ongoing attacks and suggests that the military and government were behind the attacks.

39. "Myanmar on the Cyber-offensive," BaganLand, http://baganland.blogspot.com/2008/09/myanmar-on-cyber-offensive.html.

40. Joomla! is an open-source content management system. See, Joomla! http://www.joomla.org/.

41. The following instructions demonstrate the simplicity of this browser exploit:

1. Go to URL target.com/index.php?option=com_user&view=reset&layout=confirm.
2. Write into field "token" char ' and click OK.
3. Write new password for admin.
4. Go to url: target.com/administrator/.
5. Login as admin with new password.

42. "Backdoor.PHP.C99Shell.w," Secure List, July 15, 2008, http://www.securelist.com/en/descriptions/old188613.

43. See Co.cc lookup, https://www.co.cc/whois/whois.php?domain=0verkill.

44. Moscow Aviation Institute, "Faculty of Applied Mathematics and Physics," http://www.mai.ru/english/fac_8/computer_eng.htm; Moscow Aviation Institute, "Informatics and Mathematics," http://www.mai.ru/english/fac_8/informatics_eng.htm.

45. U.S. Department of Treasury OFAC, "Nonproliferation: What You Need to Know about Treasury Sanctions," April 7, 2009, http://www.treas.gov/offices/enforcement/ofac/programs/wmd/wmd.pdf; Federation of American Scientists, "A Sourcebook on Allegations of Cooperation between Myanmar (Burma) and North Korea on Nuclear Projects," February 14, 2011, http://

www.fas.org/man/eprint/burma.pdf; Charles G. Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," Institute for Security Technology Studies at Dartmouth College, December 2004, http://www.ists.dartmouth.edu/library/212.pdf.

46. Htet Aung Kyaw, "Burma's Generals Are Afraid of Telephones and the Internet," *The Nation*, March 24, 2009, http://www.nationmultimedia.com/2009/03/24/opinion/opinion_30098633.php.

47. Ibid.

48. See an archive of the oGc homepage at http://web.archive.org/web/20070227151313/http://www.globalogc.org.

49. Myanmar Marine University, http://www.mot.gov.mm/mmu/organization.html.

50. Before initiating conversations with members of the IRC group, we identified ourselves as researchers at the University of Toronto and explained that we were analyzing attacks against Burmese independent media Web sites.

51. Paul Roberts, "Alleged Fluffi Bunni Leader Worked for Siemens," *Computer World*, May 8, 2003, http://www.computerworld.com/s/article/81043/Alleged_Fluffi_Bunni_leader_worked_for_Siemens; Lain Tomson, "Infosec Hit by Arrest and Virus Attack," April 30, 2003, V3.co.uk, http://www.v3.co.uk/vnunet/news/2122174/infosec-hit-arrest-virus-attack; Drew Cullen, "Fluffi Bunni Nabbed at Infosec," The Register, April 3, 2003, http://www.theregister.co.uk/2003/04/30/fluffi_bunni_nabbed_at_infosec/; Gillian Law and Paul Roberts, "U.K. Police Nab Fluffi Bunni Hacker," *Computer World*, April 30, 2003, http://www.computerworld.com/s/article/80811/U.K._police_nab_Fluffi_Bunni_hacker?taxonomyId=017.

52. Myanmar IT Pros, October 23, 2008, http://www.myanmaritpro.com/forum/topics/1445004:Topic:79509?commentId=1445004%3AComment%3A79990.

53. Myanmar IT Pros, September 9, 2009, http://www.myanmaritpro.com/forum/topics/1445004:Topic:156949?commentId=1445004%3AComment%3A157606.

54. Myanmar IT Pros, August 10, 2009, http://www.myanmaritpro.com/forum/topics/1445004:Topic:148136?commentId=1445004%3AComment%3A149799.

55. Arkar Moe, "Burmese IT Contest to Aid Junta?" The Irrawaddy, August 25, 2009, http://www.irrawaddy.org/article.php?art_id=16633.

56. Myanmar IT Pros, August 26, 2009, http://www.myanmaritpro.com/forum/topics/1445004:Topic:152929?commentId=1445004%3AComment%3A153346.

57. Naval Post Graduate School, *Cyberterror Prospects and Implications*, October 1999, http://www.nps.edu/Academics/Centers/CTIW/files/Cyberterror%20Prospects%20and%20Implications.pdf.

58. Ronald Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 South Ossetia War," paper presented at 51st Annual

International Studies Association Convention, February 2010, New Orleans, LA; Jose Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009), 163–181.

59. Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace."

60. Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010); Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, March 29, 2009, http://tracking-ghost.net; Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: An Investigation into Cyber Espionage 2.0," April 6, 2010, http://shadows-in-the-cloud.net; Nart Villeneuve, "Vietnam and Aurora," Nart Villeneuve Malware Explorer, April 5, 2010, http://www.nartv.org/2010/04/05/vietnam-aurora.

61. Mike Johnson, "Georgian Websites under Attack—Don't Believe the Hype," Shadowserver Foundation, August 12, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080812.

62. For further analysis of the global prevalence and effect of DDoS attacks against civil society groups, see Hal Roberts, Ethan Zuckerman, and John Palfrey, "Interconnected Contests: Distributed Denial of Service Attacks and Other Digital Control Measures in Asia," chapter 7 in this volume.

9 China and Global Internet Governance

A Tiger by the Tail

Milton L. Mueller

As of June 2010 the Chinese government claimed the country's number of "netizens," or Internet users, had increased to 430 million.[1] That very large number is only 32 percent of China's total population.[2] Already one of the biggest presences on the Internet, and with a long way to go yet, China and the Internet enjoy a complex and seemingly paradoxical relationship. Many Westerners have trouble making sense of the way China's socialist market economy (SME) combines heavy restrictions with vibrant growth, and globalized networking with an insistence on territorial sovereignty. Western observers have long abandoned the notion that the Internet was inherently uncontrollable and that its use would automatically overthrow dictatorships. They are now replacing that simplistic notion with an equally coarse inversion: the image of China as the constructor of an impregnable "Great Firewall," a place of omnipotent surveillance, a population susceptible to well-organized propaganda campaigns, and a source of pervasive and insidious cyber attacks and cyber espionage. It is a new Internet version of the Cold War.

The Internet in the People's Republic of China (PRC) strains and challenges the capacity of the Chinese Communist Party (CCP) to maintain control. And the fact that China needs to be linked to the external world, through the Internet as well as through trade, provides a double challenge. The international environment of Internet governance is freer, is private-sector based, and is more capitalistic than China's rulers would prefer. And, it is subject to U.S. hegemony. If one combines an analysis of the global politics of Internet governance with an understanding of the long-term status of China's reform process, one can understand better which factors facilitate and which place constraints on the party's ability to regulate the Internet. One can even, perhaps, understand how the further development of digital communications might contribute to a transformation of Chinese society.

This chapter outlines a general framework for understanding Internet politics and locating China within it. It then analyzes China's attempt to move against the grain of the current Internet governance regime, promoting sovereignty and intergovernmental institutions in opposition to the new, transnational, and private-sector-based

Internet governance institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Regional Internet Registries (RIRs). The next section describes various interactions and spillover effects, both intended and unintended, between China's attempt to maintain its Great Firewall and the globalized operations that characterize the Internet, focusing in particular on the domain name system (DNS) and routing, and cyber espionage. A concluding section places these issues in a more general discussion of the tensions inherent in the Chinese "socialist market economy."

The Four Quadrants of Internet Politics and China's Place in Them

In another work I have described the politics of Internet governance using a space defined by two axes.[3] This conceptual scheme is predicated on recognizing that the Internet does indeed create a novel form of politics around communication and information policy. The novelty comes from the Internet's transnational scope, its massively increased scale of interaction, its distribution of control, its capacity to facilitate new forms of collective action, and the emergence of new, nonstate-based governance institutions native to the Internet.

The horizontal axis pertains to the status of the territorial nation-state in the governance of the Internet and communications technology generally. The vertical axis identifies the level of hierarchical control one is willing to countenance in the solution of Internet governance problems. Together, these axes form a four-quadrant space, which provides a useful schema for analyzing and classifying the various ideologies and policy systems related to the Internet.

In figure 9.1, the horizontal or nation-state axis locates one's view of the appropriate polity. Those on the right side of this axis prefer the traditional territorial nation-state as the institutional basis for governing the Internet. At the rightmost extreme stand those who would subordinate the Internet to national sovereignty completely—in effect, negating global networking altogether in favor of a bounded, analog telephone-network-like regime. At the left extreme, Internet governance decisions would be made by a globalized polity where national borders, national sovereignty, and national identity play almost no role.

The vertical or networking-hierarchy axis juxtaposes free association (at the top) with command and control (at the bottom). This reflects the degree to which one believes the problems associated with Internet governance should be solved using coercive and hierarchical mechanisms or left to the looser forms of association and disassociation among Internet users and suppliers. At the top of this axis, the shape of Internet governance would be defined by looser forms of *networked governance*; at the bottom, governance emerges from adherence to rules enforced by an authority. Of course, what makes Internet governance especially interesting is that there is no

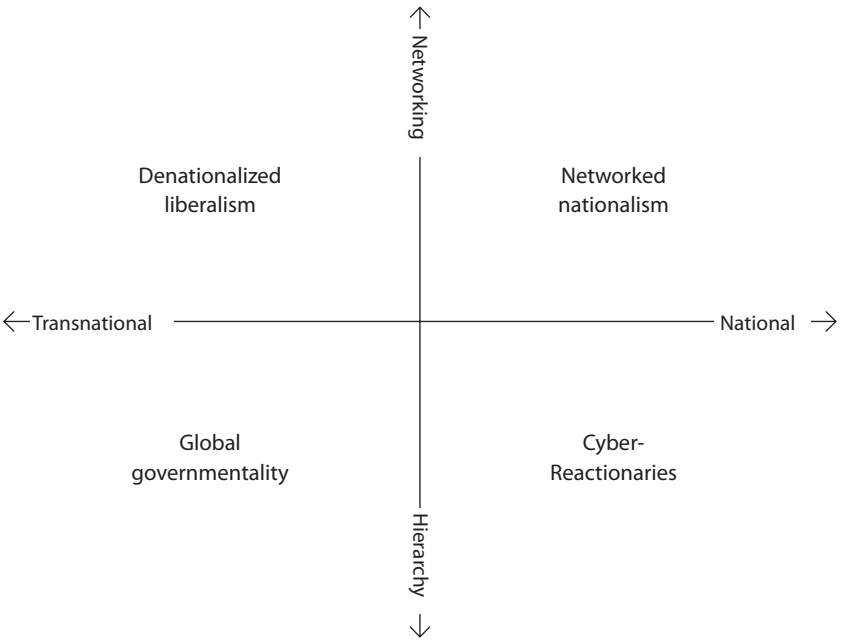

Figure 9.1
The quadrants of Internet politics.

universally recognized authority at the global level; therefore, advocates of hierarchy must also make choices regarding where they stand on the horizontal axis.

These two axes form a political space with four quadrants. In the lower-right quadrant, we have *cyber-conservatives* and outright *cyber-reactionaries*. In essence, these actors regret the rise of the Internet in most respects, and insofar as they tolerate its existence they strive to make it conform to the authority and parameters of the nation-state. Their intent is to realign control over the Internet's operational units and critical resources with the jurisdiction of the nation-state. Insofar as international policy is recognized as necessary, they believe that it should be handled by intergovernmental institutions and kept to the bare minimum required to protect or supplement domestic policy.

In the upper-right quadrant, which I call *networked nationalism*, the nation-state is still the dominant governance institution, but there is greater willingness to embrace the potential of networking and less of an attempt to impose territorial hierarchies on networked actors and network operations. National public policies and regulations are applied to actors within the territorial jurisdiction, but many loopholes and escape valves are left open because of transnational Internet access. States in this quadrant might cope with transnational problems through a mix of transgovernmental networks, delegation to private actors, or formal intergovernmental treaties, but international

institutions remain rooted in states, and any organically evolved Internet institutions would have to be recognized by and subordinated to states. This quadrant is characterized by an acute tension between the boundaries of the national polity and the (transnational) boundaries of networked activity.

The lower-left quadrant encompasses those who advocate *global governmentality*—namely, hierarchical control of the Internet by means of new institutions that transcend the nation-state. These new institutions are most likely to be private-sector based and created to advance business interests, though they could also be multistakeholder and public-private partnerships and even democratic for some version of democracy not rooted in 20th-century nations.

The upper-left quadrant, which I call *denationalized liberalism*, also supports a transnational institutional framework but is less hierarchical in its approach to the need for order. This quadrant combines economic and social liberalism; its adherents recognize individual network participants, not states or corporations, as the fundamental source of legitimate Internet governance and propose to create new institutions around them. Its adherents valorize freedom and propose to rely primarily on peer-production processes, networked governance, and competitive markets to handle the issues of Internet governance. Hierarchical interventions would be limited to the minimum required to secure basic protections against theft, fraud, and coercion.

Within this political space, China (along with Burma, Russia, and other postcommunist nations such as Vietnam) is unambiguously cyber-nationalist. It strives mightily to reorder the Internet by filtering content and by licensing and regulating the providers of Internet services in order to make them conform to national policy. Its philosophy is clear from its own 2010 White Paper:

> The Chinese government believes that the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security.[4]

Along with the emphasis on sovereignty, equally strong support for hierarchical control exists. Both the telecommunication infrastructure and the services that run on top of it are subject to strict licensing and entry restrictions, as well as outright censorship and repression:

> No organization or individual may produce, duplicate, announce or disseminate information having the following contents: being against the cardinal principles set forth in the Constitution; endangering state security, divulging state secrets, subverting state power and jeopardizing national unification; damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity; jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating

obscenity, pornography, gambling, violence, brutality and terror or abetting crime; humiliating or slandering others, trespassing on the lawful rights and interests of others; and other contents forbidden by laws and administrative regulations. These regulations are the legal basis for the protection of Internet information security within the territory of the People's Republic of China. All Chinese citizens, foreign citizens, legal persons and other organizations within the territory of China must obey these provisions.[5]

As a logical extension of its cyber-nationalism, China steadfastly supports a traditional, sovereignty-based communications governance regime in the international arena. It prefers an international regime organized around treaty-based intergovernmental organizations that rely on one-country, one-vote distributions of power. When China uses the word "democratic" in this context, it means one country, one vote. Its point of reference for "democracy" is not the rights and interests of the individual citizen, but is equality among sovereign states: "China believes that UN [United Nations] should be given full scope in international Internet administration and supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale. All countries have equal rights in participating in the administration of the fundamental international resources of the Internet."[6]

Both the domestic and international aspects of China's approach to the Internet underscore the inevitability of its attempt to create a bordered Internet subject to national policy. The Great Firewall of China (GFW) is but one aspect of this; more important than the filtering of external information are the licensing requirements, extensive state ownership, and entry controls that can be imposed upon domestic Internet intermediaries and service providers, as well as the growing identification and surveillance of users and potential for severe, arbitrary punishment that can be imposed on them domestically. This leads to extensive self-regulation and self-censorship.

All these points refer to the Chinese Communist Party's theory of how things *should* be—their preferred state of affairs. That preferred reality, however, is undercut by the realities of the Internet. As Wang Chen, the State Council's chief information officer, put it, "the Internet is a global open-information system." In a speech before the Chinese parliament, he recognized the fact that

as long as our country's Internet is linked to the global Internet, there will be channels and means for all sorts of harmful foreign information to appear on our domestic Internet. As long as our Internet is open to the public, there will be channels and means for netizens to express all sorts of speech on the Internet. Judging from our country's social development, our country is currently in a period of social transformation, rapid development, and conspicuous contradictions. Unavoidably, actual contradictions and problems in our society are reported on the Internet. Judging from our country's Internet management practices, we are still in the process of exploration and improvement. Many weak links still exist in our work. These problems have weakened our ability to manage the Internet scientifically and effectively.[7]

In addition to those limitations on control, China is constrained by the need for economic development and productive exchanges with the rest of the world. Thus, in its experimentation with combinations of restriction and openness and its sensitivity to its economic interdependence with the developed world, China's approach to the Internet mirrors its strategic approach to openness to foreign investment and trade generally. With its aspiration to become a global leader in high technology, China simply cannot afford to turn its back on the Internet.

China's Predictable Clash with (and Adjustment to) the Current Internet Governance Regime

The current Internet governance regime clashes with China's preferences in two distinct ways. First, the legacy of denationalized liberalism associated with the Internet's early development still powerfully shapes the Internet's operations and the social, economic, and political norms associated with its use. Instead of traditional, intergovernmental institutions there are private-sector-based, transnational forms of governance and a widespread ethic of self-regulation and civil society support for Internet freedom. Second, the privileged role of the United States in the current Internet governance regime, especially its control over ICANN, rankles the Chinese. Although in many respects denationalized liberalism and U.S. preeminence are at odds with each other, it is not surprising that China sees them as related and mutually reinforcing. In China's state-centric view, Internet freedom and the U.S. doctrine of the "free flow of information" are merely tools that a hegemonic America uses to penetrate and subvert other states with its own worldviews and values. China's accusations that Hillary Clinton's "Internet freedom" initiatives are part of a calculated "information imperialism" flow logically from this perspective.[8] The Chinese view is given some credence, since U.S. "Internet freedom" initiatives are in fact rather selectively targeted at U.S. geopolitical rivals China and Iran, as opposed to other equally censorious countries that are allies of the United States.[9]

China and ICANN

To the Chinese state (in common with other cyber-nationalist and cyber-reactionary nation-states), ICANN is highly objectionable for two reasons: first, because of its status as a nonstate actor that supplants or competes with states in the exercise of policy-making and governance responsibilities; and second, because of its unilateral establishment by the United States and its contracts that make it beholden to the U.S. Department of Commerce. Initially, the Chinese also objected to ICANN because, as a private corporation free from intergovernmental diplomacy, the corporation allowed representatives of the government of Taiwan to participate openly and freely in ICANN

activities and sit on its Governmental Advisory Commmittee (GAC). ICANN did not observe the protocols regarding the name affixed to Taiwan and used various other means of treating it as an independent state. Thus, after some early engagement with ICANN, China ceased sending representatives to its meetings in 2001.

During the World Summit on the Information Society (WSIS) from 2002 to 2005, China joined in the attack on ICANN. It made clear its support for a takeover of its functions by an intergovernmental institution such as the International Telecommunication Union (ITU). Adding to these tensions, members of the Chinese-language technical community (not all of whom lived in or were citizens of the PRC) were also frustrated with the slow development of new technical standards enabling the DNS to represent Chinese and other non-Roman scripts. Internationalized Domain Names (IDNs) represented not only a business and political opportunity for the Chinese, but a potential threat as well. U.S. companies such as VeriSign were licensing IDN technology and could use it to enter the Chinese market. The market for registration of Chinese-language domain names is potentially a very large one. If the Chinese government and its favored state enterprises were not in control of the standards for representing Chinese characters in the DNS and if they had no direct participation in the policy processes within ICANN for adding top-level domain names (TLDs) to the DNS root, this opportunity might be threatened.

During the ICANN-China freeze period, China mounted a challenge to ICANN that was less visible but far more radical and significant than the conference diplomacy of WSIS. It created what was, in effect, an alternate DNS root for Chinese-character domain names. China's national alternative to ICANN's global DNS root used the same technical approach pioneered by competing root operator New.Net to ensure that the new domains were globally compatible.[10] Chinese characters would appear as top-level domains inside China. If one of these Chinese-character domains was queried from outside China, the uniquely Chinese names would be rendered compatible with the global Internet by having the name servers add the globally recognized ICANN country code top-level domain, .cn, to the end of them. China created three new top-level domains in this fashion: Zhong guo, Gong si, and Wang luo. These additions were done some time in 2003 but were not widely publicized, and if inquiries were made, they were downplayed as "experimental" by the Chinese. In 2006, however, as ICANN began to develop new policies for the addition of top-level domains, the online version of *People's Daily* openly acknowledged the existence of these new domains and claimed that "[Chinese] Internet users don't have to surf the Web via the servers under the management of the Internet Corporation for Assigned Names and Numbers (ICANN) of the United States."[11]

Due to these preemptive moves, and because of China's realization after WSIS that ICANN was not going to go away, China and ICANN reached a mutual accommodation sometime in 2009. At the June 2009 ICANN meeting, the PRC officially returned

to the GAC, sending a divisional director of the Ministry of Industry and Information Technology (MIIT) to represent it. ICANN also made concessions, agreeing to rename Taiwan as "Chinese Taipei" and (more substantively) to create a "fast track" for the recognition and creation of new "country code top level domains" (ccTLDs) in non-Roman scripts.[12] Unlike ICANN's new generic top-level domain program for ordinary businesses and organizations, these new "ccTLDs" did not have to wait two or three additional years while stringent policies and regulations governing their award and use were developed; nor did they have to pay six-figure application fees or recurring annual fees based on the number of registrations. Indeed, the whole concept of a "country code TLD" was based on an ISO standard assigning two-letter codes using the Roman alphabet to specific geographic territories. Since no such standard existed for the rest of the world's writing scripts, the characterization of these new top-level domains as "country codes" provided political cover for a land grab by national ccTLD monopolies. By giving countries such as China, Russia, and India a privileged and accelerated right to get new top-level domains representing their country names in native scripts, ICANN and the U.S. government were giving the world's states an economically valuable and politically powerful gift in order to keep them happy with the ICANN regime.

China and the Internet Governance Forum

When WSIS failed to bring about a major change in ICANN's status, China acceded to the creation of the Internet Governance Forum (IGF). The IGF is yet another new institution associated with the Internet that fails to conform to cyber-nationalist norms. Although nominally created under UN auspices, it is a multistakeholder environment that mixes governments, civil society, the Internet technical community, and business actors in nonbinding dialogue about Internet issues. All actors are afforded equal status. Within the IGF, China initially took a low profile. Its main accomplishment was to insist that the IGF directly grapple with the issue of U.S. unilateral control over critical Internet resources. On several occasions it has expressed sharp (and valid) criticism of efforts by the United States and its allies in the private sector to avoid confronting those issues in IGF meetings. At one point a frustrated China publicly expressed opposition to the renewal of the IGF after its initial five-year mandate expired because of its avoidance of the WSIS-related issues. That position was later moderated, and now seems to have been replaced with reliance on a longer-term war of attrition that attempts to make the IGF gradually become more intergovernmental and a standard part of the UN bureaucracy.

This war of attrition attained tangible success in late 2010. In the early days of the IGF, no one at the UN headquarters was paying much attention to the IGF or even to

the Internet. This situation has changed. China has taken the lead in shaping the institutional environment for the IGF at the UN. Chinese diplomat Sha Zukang, who represented China during WSIS, became the United Nations' undersecretary-general for economic and social affairs on July 1, 2007. From that platform he has made a series of moves designed to bring the IGF more under the control of the UN system and make it more intergovernmental in character. China has the support of many Arab states and the BRICs in this regard. (Brazil, Russia, India, and China make up the BRICs.) While business interests and the United States thought they were minimizing damage by making the Committee on Science and Technology for Development (CSTD), a near-dormant entity within the UN Economic and Social Council (ECOSOC), responsible for WSIS follow-up, they were later outmaneuvered. The UN resolution renewing IGF was conditioned on a review and "improvement" process that made it more intergovernmental. In setting the parameters of the improvement process, Undersecretary Sha, with the support of other cyber-nationalist states, minimized the role of civil society and business. He also reinstituted the old way of excluding non-state actors from speaking during parts of the public consultations.

These moves actually do more to exclude the United Nations from the broader currents of Internet governance than to assert UN control over Internet governance. Without full and equal-status participation of Internet businesses and users, the United Nations is unlikely to have much influence and the IGF will not be much of a forum. But the changes bring a halt to the multistakeholder innovations and reforms that came from WSIS.

China and the Regional Internet Registries

The Regional Internet Registries (RIRs) manage and set policy for Internet Protocol (IP) address resources. Like ICANN, the RIRs are private, nonprofit corporations that have transnational governance responsibilities. Although they are not under the direct contractual authority of the U.S. Commerce Department, they do rely on ICANN for the initial allocations of large address blocks, which they subdelegate to Internet service providers (ISPs) and organizations in their regions. China has consistently attempted to make IP addresses conform to the governmental, sovereigntist model. Led by the Chinese director of the ITU's Telecommunication Standardization Bureau, Houlin Zhao, it has backed efforts by the ITU to compete with the RIRs.[13] It also supported a more recent attempt by the ITU to propose a parallel system of IPv6 address allocation based on country Internet registries.[14] Within its region, it has acquired addresses through its own National Internet Registry (NIR) rather than allowing ISPs and companies to go directly to the IP addressing authority for its region, the Asia Pacific Network Information Centre (APNIC). The cyber-nationalist pattern is consistent here, too.

International Incidents

The Chinese Communist Party has more direct authority over the domestic institutional environment than it does over the international regime. It has used this authority to create a comprehensive system of blocking/censorship, public-opinion management, and intermediary responsibility that has come to be known colloquially as the Great Firewall of China. Even so, its attempt to maintain and enforce cybernationalism is challenged domestically by four tendencies: the need for Internet operations to be globally coordinated and compatible; the ability of domestic actors to grasp the communicative opportunities of the Internet; the greater transparency fostered by Internet communications; and China's need to maintain trade relationships with the rest of the world.

The China country profile in this volume covers the domestic situation in more detail. This chapter focuses instead on the way China's attempt to maintain cybernationalism has interacted or conflicted with the globalized nature of Internet operations and governance. It describes the way the Chinese state's attempt to tamper with the domain name system to support censorship "spilled out" into the rest of the world. It looks next at a routing misconfiguration incident that created a minipanic in the United States. Then it shows how cyber espionage efforts traced to China are also shaping global attitudes toward Internet governance.

Exporting the Great Firewall?

DNS root servers tell Internet users where to find the information needed to connect to other domains. In March 2010, Internet users outside China found that their access to popular Web sites such as Facebook, YouTube, and Twitter was impaired. The problem, which was known to affect users in Chile and California, was eventually traced to their use of root servers located in China.[15]

The origins of this story go back to the early days of ICANN, when U.S. control of the DNS was becoming a global political issue. Root servers are the starting point for the hierarchical resolution process that makes domain names globally unique and matches IP addresses to domains. Because of the Internet's U.S. origins, all but three of the world's 13 root servers were located in the United States; a few were run by the U.S. military. Many national leaders (assuming they were aware of the problem) viewed this as an unacceptable kind of dependency on a foreign power. Although many of the people who were concerned about this had no idea what a DNS root server actually does, they were quite sure that they wanted one in their country. And there were, in fact, legitimate technical reasons supporting a greater geographical diversification of the root server infrastructure, such as greater resiliency in the face of outages and reduced latency in response times.

A zero-sum solution to this problem would have required taking root servers away from the United States and moving them to other countries. Aside from being a non-starter politically, given U.S. power and the lack of any institutionalized process for designating and removing root server operators, such a measure had the potential to create adjustment and compatibility issues. Therefore, leading DNS experts developed and implemented a technical modification that allowed existing root servers to multiply themselves with "instances" elsewhere in the world.[16] This was a positive-sum solution that used some aspects of the "anycast" service to make an authoritative name-server operator provide access to a single-named server in multiple locations.

China was one of the first countries to set up "mirrored" or "anycasted" root servers. There are now instances of three different root servers located in Beijing. And due to routing agreements among ISPs, it is possible that root-level domain name queries coming from sources outside China might make use of those root server instances in China.

What makes this interdependency interesting is that China relies heavily on domain name blocking to implement the GFW. As a result, its name servers will modify or tamper with responses to queries about where to find the blocked domains. If someone lives outside China and, because of network topography, happens to query a root name server hosted in China, that person's queries will pass through the Great Firewall, potentially subjecting the person to the same censorship imposed on Chinese citizens. Apparently, China's version of the "I" root was not visible to the rest of the world. In early March 2010, however, it seems to have become visible.[17] As a result, Chinese censorship "spilled out" and affected a number of users outside of China. Despite some countermeasures taken by the main root server operators, the problem happened again in June. Like the incident described in the next section, the Chinese impact on the rest of the world's Internet was almost certainly unintentional.

The BGP "Hijack"

U.S.–China Internet relations were inflamed again in November 2010, when the U.S.–China Economic and Security Review Commission (USCESRC) issued its report to Congress.[18] Discussing what was probably an unintentional routing-prefix configuration error that took place in April, the USCESRC stated that "a state-owned Chinese telecommunications firm 'hijacked' massive volumes of Internet traffic. For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers."[19]

In technical jargon, this is a problem in the border gateway protocol (BGP) routing protocol, sometimes called "BGP hijacks" or more frequently known as "BGP leaks," in which an ISP announces a route it is not authorized to service and the route

announcement is propagated to other ISPs and begins to affect routing patterns around the world. Inaccurate or unauthorized BGP route announcements happen frequently and are a well-known problem. While the USCESRC report did not explicitly assert that the prefix leak was intentional, the report framed the event as an "interception of Internet traffic" rather than as a routing configuration error. Those hostile overtones were picked up and amplified by the U.S. mass media, which publicized the idea that China had diverted "15 percent of the Internet" to its own country. The "15 percent of the Internet" claim confused Internet traffic volume with Internet route announcements—a completely false equation. Internet technical experts quickly weighed in to correct the understanding of the situation. According to Arbor Networks' Craig Labovitz, "This hijack had limited impact on the Internet routing infrastructure—most of the Internet ignored the hijack for various technical reasons."[20] Labovitz wrote that far from diverting "massive amounts of the Internet's traffic," there was "no statistically significant increase for either [of the two Chinese Internet service providers]. While we did observe modest changes in traffic volumes for carriers within China, the BGP hijack had limited impact on traffic volumes to or from the rest of the world."[21]

Both the incident and the reaction to it underscore the global interdependencies created by the Internet and the dangerous tendency for interstate rivalries to inflame mundane operational problems into military and political tensions. Correctly interpreted, the April 2010 Chinese routing hijack had little if anything to do with China and its geopolitical rivalry with the United States, but instead should be viewed as a spur for instituting more secure routing protocols on the Internet. Greater routing security is something that would benefit both China and the United States—and proper implementation of such a goal would require cooperation between the United States and China especially.

Cyber Espionage and the Blurring Line between State and Nonstate Actors

As China becomes a powerful state on the global scene it will—like other powerful states before it—engage in power and spying games with its rivals. Just as traditional, "meatspace" (i.e., physical) forms of spying and infiltration provide governments with ways to disrupt their enemies' plans or obtain valuable information, so does Internet-based espionage. Evidence in the West suggests that China has been especially active and effective at using cybercrime tactics to monitor and disrupt its enemies.

In early 2009 the Information Warfare Monitor (IWM) released one of the first unclassified reports detailing the activities of a cyber espionage effort.[22] The network, dubbed GhostNet, appeared to have been controlled from commercial Internet accounts located on the island of Hainan, China. A year later, another report from the IWM and the Shadowserver Foundation uncovered more extensive evidence of a China-based computer espionage network targeting India: its diplomatic missions,

government departments, national security and defense groups, Indian academics, and journalists focused on China. The Office of the Tibetan Dalai Lama was also targeted.[23] Leaked State Department cables show that U.S. and German government agencies were becoming concerned about Chinese cyber espionage as early as 2006.[24]

The Google-China incident (covered in more detail in the China country profile in this volume) can be seen as a straightforward clash between China's domestic policy and Internet freedom in that it involved a transnational business founded on the free and indiscriminate dissemination of information demanded by users. It was that, but it was something more as well. Google's sudden questioning of its presence in China was triggered not by ongoing Chinese censorship but by a break-in to its corporate network that Google believed could be attributed to Chinese state-sponsored or state-directed actors. This break-in not only involved the theft of proprietary information but also seemed to target the e-mail accounts of human rights activists.

State Department cables released by Wikileaks provide support for the conclusion not only that China's government was involved in the break-ins, but also that China's government views the Internet in general and Google in particular as state-directed pieces that are being played in its geopolitical power competition with the United States:

> A well-placed contact claims that the Chinese government coordinated the recent intrusions of Google systems. According to our contact, the closely held operations were directed at the Politburo Standing Committee level. . . . Chinese concerns over the recent Google threat to take down the company's Chinese-language search engine google.cn over censorship and hacking allegations were focused on the service's growing popularity among Chinese Internet users and a perception that the USG and Google were working in concert.[25]

Ties between China's leadership and Google rival Baidu are also asserted in the cables. The current dialogue over Chinese cyber espionage may be overlooking the extent to which China is subject to the same tactics from other countries, especially the United States. The State Department cables, for example, warn darkly of "potential linkages of China's top companies with the PRC [state]" and claim that such links "illustrate the government's use of its 'private sector' in support of information warfare objectives."[26] Coming from the United States, it sounds very much like the policeman at Rick's casino in the movie *Casablanca* proclaiming that he is "shocked, shocked to discover that gambling is going on here." The massive U.S. military-industrial complex and the deep, long-term ties between Internet technical experts, cyber security firms, and Defense Department and the Department of Homeland Security's research funding are almost exactly the same as those described in threatening terms in the State Department cables.

An inherent feature of the nation-state system of governance is that concepts of order and security apply first and foremost in the domestic sovereign's jurisdiction. Different, negotiable standards apply to outsiders. Because China believes that it is

both necessary and justified to "manage" the information environment and control political activity, it makes sense that it would use cyber espionage to its fullest capacity to survey its international and domestic environment.

Ongoing Tensions between China's Sovereigntism and the Internet

To decode the paradox of the Chinese Internet we need to return to the dialogue within the international communist movement about the future of socialism. By the 1950s it was clear that true, thoroughgoing socialism—an economy devoid of private property, a price system, or markets—had failed economically and was simply unworkable. Leftist intellectuals contemplated two ways forward, one known as reform and the other as transformation. Reform did not mean, as many Westerners assume it does, a liberalization of economy and society that leads to convergence with the West. The communists referred to that path as *transformation*—the abandonment of communism and a move toward liberal democracy. A *reformed* communism would make socialism economically viable by permitting the existence of enough market forces and trade to deliver growth, while retaining the Leninist approach to centralized political control associated with classical communism. This is clearly the path that China has chosen. The whole point of China's reform process is to benefit from Western technology and from trade with the global market economy *without* converging into the West's liberal democratic governance model. Its opening and reform process was and is intended to deliver continued economic development without fundamental political change. Continued economic growth, they believe, makes political transformation unnecessary.

At least since the early 1990s, China's approach to information and communication technology has played a significant role in facilitating the achievement of these reform objectives. An early discourse among Chinese intellectuals about "informatization" set the stage for this. The CCP viewed information technology as the best way to scale up the control capabilities of the state to keep pace with its growth and greater wealth. In a typically pragmatic Chinese style, which has been described as "touching the stones to cross the river," the Chinese Communist Party has gone through repeated cycles of loosening control to foster development and growth, and then tightening restrictions to ensure that the party stays in control. The first step releases suppressed economic energy and generates growth; the second phase prunes the development so that it conforms to the parameters of the SME and does not threaten the stability and security of the political system.

An observation by the former Beijing bureau chief of the *Financial Times* dispels any notion that the economic development based on these reforms is inherently incompatible with party control:

> If you benchmark the Chinese Communist Party against a definitional checklist authored by Robert Service, the veteran historian of the Soviet Union, the similarities are remarkable. As with

communism in its heyday elsewhere, the party in China has eradicated or emasculated political rivals, eliminated the autonomy of the courts and media, restricted religion and civil society, denigrated rival versions of nationhood, centralized political power, established extensive networks of security police, and dispatched dissidents to labor camps. There is a good reason why the Chinese system is often described as "market-Leninism."[27]

Unfortunately, in the West there is a persistent refusal or inability to grasp and accept the meaning of the SME. Westerners, and especially American politicians and businesses, are constantly mistaking China's *reform* with *transformation*. As a result, they are repeatedly disappointed and angry with China's suppression of individual rights and its limited and fitful openings to foreign investment and free trade. United States policies that attempt to change China are usually based on the premise that the country's leaders are making false steps on the road to embracing liberal democratic norms and models. They are not. Zhao Ziyang and a few other Chinese leaders from the mid-1980s may have flirted with or embraced transformation, but the Tiananmen Square incident settled that issue decisively within China's party.[28] Since then, the CCP mainstream has reaffirmed the notion of the SME and has explicitly rejected convergence. One need not approve of this approach to accept its reality and form one's expectations based on it.

It would make sense, then, that the Chinese state's approach to information and communications technologies (ICTs) in general and the Internet in particular is neither to completely suppress it in order to preserve a brittle and unpopular regime, nor to provide the Internet-based economy and society free rein. It is a constant, iterative attempt to release productive forces and then corral them into supporting the continued control and dominance of the CCP. Rebecca MacKinnon has called this "networked authoritarianism,"[29] although I am not sure it is the best label. The term may attribute too much intentionality to China's approach. What is really going on is an improvised response to the contradictions of the socialist market economy. On one hand, the market economy part of the package thrives on open exchanges with foreigners and robust circulation of information, both of which deliver the economic development and growth needed for the CCP to maintain its legitimacy; the continued political grip of the CCP, on the other hand, requires limiting entry into the market for information services, constant monitoring and surveillance of communications, propaganda activities, repressive capabilities, and accurate targeting of political and social threats.

Note that the attempt to subject the Internet to hierarchical control relies in many respects on the unique capabilities of networked computers, whether it is the use of DNS blocking and deep packet inspection to filter Web and search-engine queries, the mobilization of armies of freelance propagandists to search for and intervene in public discourses critical of the government, the surreptitious use of cyber espionage, or the "identification and record-keeping" activities invoked by Wang Chen. In an information age, the label "networked authoritarianism" is practically redundant—if there is

to be authoritarianism on this scale, how can it *not* be networked? Still, China's online economy and innovative capacity is certainly stunted by these self-limiting applications of ICTs. While China's huge domestic economy makes the growth of major Internet companies inevitable, it is hard to imagine major service innovations or globally competitive online service providers emerging from this environment.

The oscillation between progress and control appears regularly across a number of different economic sectors, including China's approach to telecommunications sector reform.[30] In sum, the experience of China and the Internet is the latest episode in the familiar tale of Chinese reform, which recalls the parable of the man who caught a tiger by the tail. As the tiger gallops and struggles along, the man finds it more and more demanding to maintain his grip. But if he lets go, the tiger will surely turn and destroy him. Unlike the man in the parable, the CCP is, to some extent, strengthened by the tiger's energy—but the tiger keeps getting bigger and bigger. How long this cycle can go on is difficult to know. For those who seek transformation of communist China the trick is to conceptualize how this self-reinforcing cycle works and how it might break down. One thing seems certain: for other governments, especially the United States, neither external intervention nor subversion directed from outside is likely to work. The CCP thrives on exploitation of nationalism and by positioning itself as the people's defender against the humiliations and dominations of foreigners. If anything can make the tiger and the man hanging onto its tail work together in harmony it would be that process.

Notes

1. China Network Information Center, "Internet Fundamental Data," June 30, 2010, http://www.cnnic.cn/en/index/0O/index.htm, accessed January 5, 2011.

2. Ibid.; U.S. CIA, *The World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html.

3. Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010).

4. Information Office of the State Council of the People's Republic of China, chapter 5, "The Internet in China," June 8, 2010, http://www.gov.cn/english/2010-06/08/content_1622956.htm.

5. Ibid.

6. Information Office of the State Council of the People's Republic of China, chapter 6, "The Internet in China."

7. Wang Chen, "Development and Administration of Our Country's Internet," delivered on April 29, 2010, before the Standing Committee of the National People's Congress. Unofficial English translation is available at http://www.hrichina.org/public/contents/article?revision%5fid=175119&item%5fid=175084.

8. Christopher Bodeen, "China Slams Clinton's Internet Speech: 'Information Imperialism,'" Associated Press, January 22, 2010, http://www.huffingtonpost.com/2010/01/22/china-slams-clintons-inte_n_432691.html.

9. Sami ben Gharbia, "The Internet Freedom Fallacy and the Arab Digital Activism," Samibengharbia.com, September 17, 2010, http://samibengharbia.com/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism.

10. For a good discussion of this, see the comments appended to Rebecca MacKinnon, "China's New Domain Names: Lost in Translation," CircleID, February 28, 2006, http://www.circleid.com/posts/chinas_new_domain_names_lost_in_translation/#1905. The blog itself understates the significance of the situation, but the comments on the post and the tests reported there clarify the situation.

11. "China Adds Top-Level Domain Names," *People's Daily* Online, February 28, 2006, http://english.people.com.cn/200602/28/eng20060228_246712.html.

12. A country code is a top-level domain based on the ISO-3166 standard of two-letter codes, such as .cn for China, .fr for France, or .br for Brazil. They were created in the mid-1980s as alternatives to the so-called generic top-level domains (.com, .net, .org, .mil) at the insistence of some non-U.S. Internet developers. Not wanting to put himself in the position of deciding who or what qualified as a "country," Internet pioneer Jon Postel found an existing ISO standard, originally developed for postal uses, which assigned unique two-letter codes to each territory. Most of these territories correspond to nations, but many (e.g., .io for Indian Ocean) did not.

13. Houlin Zhao, "ITU and Internet Governance," input to the seventh meeting of the ITU Council Working Group on WSIS, December 12–14, 2004, Geneva, 30 November 2004. In this WSIS contribution Zhao wrote, "in addition to the current arrangements for allocation of IPv6 address by the RIRs, one could reserve a portion of the large IPv6 space for country-based assignments, that is, assign a block to a country at no cost, and let the country itself manage this kind of address in IPv6."

14. Sureswaran Ramadass, *A Study on the IPv6 Address Allocation and Distribution Methods* (Geneva: International Telecommunication Union, 2009).

15. Earl Zmijewski, "Accidentally Importing Censorship," Renesys Blog, March 30, 2010, http://www.renesys.com/blog/2010/03/fouling-the-global-nest.shtml.

16. Tim Hardie, "Distributing Authoritative Name Servers via Shared Unicast Addresses," RFC 3258, April 2002.

17. Zmijewski, "Accidentally Importing Censorship."

18. U.S.–China Economic and Security Review Commission (USCESRC), *2010 Report to Congress of the U.S.–China Economic and Security Review Commission* at the 11th Congress, Second Session, November 2010.

19. U.S.–China Economic and Security Review Commission, Section 2, *2010 Report to Congress of the U.S.–China Economic and Security Review Commission*, November 2010, http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf.

20. Craig Labovitz, "China Hijacks 15% of Internet Traffic?" Arbor Networks Security to the Core Blog, November 19, 2010, http://asert.arbornetworks.com/2010/11/china-hijacks-15-of-internet-traffic.

21. Craig Labovitz, "Additional Discussion of the April China BGP Hijack Incident," Arbor Networks Security to the Core Blog, November 22, 2010, http://asert.arbornetworks.com/2010/11/additional-discussion-of-the-april-china-bgp-hijack-incident.

22. Information Warfare Monitor, *Tracking Ghostnet: Investigating a Cyber-espionage Network*, March 29, 2009, http://www.tracking-ghost.net.

23. Information Warfare Monitor and the Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, April 6, 2010, http://shadows-in-the-cloud.net.

24. The German Federal Office for the Protection of the Constitution (BfV) delivered a briefing on its analysis of the cyber threat posed by the People's Republic of China (PRC), which appears to mirror conclusions drawn by the U.S. intelligence community. The BfV surmises that the intention of PRC actors is espionage, and the primary attack vector used in their malicious activity is socially engineered e-mail messages containing malware attachments and/or embedded links to hostile Web sites. From October 2006 to October 2007, 500 such e-mail operations were conducted against a wide range of German organizations, and the attacks appear to be increasing in scope and sophistication. See Wikileaks cable at "A Selection from the Cache of Diplomatic Dispatches," *New York Times*, November 28, 2010, http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/. Once on the site, click on "China" to get to the cable.

25. "US Embassy Cables: Google Hacking 'Directed by Chinese Politburo Itself,'" Latest China (The Guardian online China News), December 4, 2010, http://latestchina.com/article/?rid=24361.

26. "WikiLeaks Cables Reveal Fears over Chinese Cyber Warfare," Latest China (The Guardian online China News), December 4, 2010, http://latestchina.com/article/?rid=24367.

27. Richard McGregor, "Five Myths about the Chinese Communist Party—Market-Leninism Lives," *Foreign Policy* (online), January/February 2011, http://www.foreignpolicy.com/articles/2011/01/02/5_myths_about_the_chinese_communist_party.

28. Willy Wo-Lap Lam, *The Era of Zhao Ziyang: Power Struggle in China, 1986–88* (Hong Kong: A.B. Books and Stationery, 1989).

29. Rebecca MacKinnon, "China's Internet White Paper: Networked Authoritarianism in Action," RConversation Blog, June 15, 2010, http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html.

30. Milton Mueller and Zixiang Tan, *China in the Information Age: Telecommunications and the Dilemmas of Reform* (Westport, CT: Praeger, 1996); and Irene S. Wu, *From Iron Fist to Invisible Hand: The Uneven Path of Telecommunications Reform in China* (Stanford, CA: Stanford University Press, 2009).

10 Corporate Accountability in Networked Asia

Rebecca MacKinnon

In 2010, Google's defiance of Chinese government censorship demands, followed by its decision to remove its Chinese search operations from mainland China, grabbed front-page headlines around the world. Human rights groups and socially responsible investors praised the global Internet giant for standing up to the Chinese government's censorship policies. China's sophisticated system of Internet censorship and control depends on the compliance of domestic and foreign corporate intermediaries, which are required by Chinese law to help authorities track user activity and to remove or prevent publication and transmission of politically sensitive content on or through their services.

Yet China is by no means the only Asian country where companies face government pressure to reveal user data or remove content in ways that violate internationally recognized human rights principles. Local and international human rights groups point to Vietnam, Burma, Thailand, and the Philippines as countries where "Chinese-style" Internet controls are increasingly deployed to silence or monitor dissent, often implemented by means of private-sector information and communication technologies (ICTs) service providers, carriers, and platforms.[1] Reporters Without Borders includes Thailand, Sri Lanka, Malaysia, Australia, and South Korea on its watch list of countries with surveillance trends heading in the wrong direction.[2]

Recent studies of global surveillance and censorship by the OpenNet Initiative (ONI) and others are showing that private-sector Internet and telecommunications companies play an increasingly important role in government efforts to control what citizens can or cannot do in cyberspace.[3] Even in Asia's most vibrant democracies such as South Korea and India, companies—domestic and foreign—face government demands for censorship and user-data handover in ways that violate Internet users' rights to free expression and privacy.

The idea that upholding free expression and privacy rights should be a component of "corporate social responsibility" (CSR)—alongside other corporate responsibilities including labor standards, environmental protection, and sustainability—is a new concept for nongovernmental organizations (NGOs), investors, companies, and

governments in the industrialized West, let alone anywhere else.[4] In the first ONI volume, *Access Denied*, Jonathan Zittrain and John Palfrey called for an industry code of conduct.[5] In 2008 came the launch of the Global Network Initiative (GNI), a multi-stakeholder initiative through which companies not only make a commitment to core principles of free expression and privacy, but also agree to be evaluated independently on the extent to which they actually adhere to these principles.[6] In the second ONI volume, *Access Controlled,* Colin Maclay examined the challenges facing this newly formed organization, a core challenge being the recruitment of members.[7] As of this writing, only three companies, Google, Microsoft, and Yahoo!, have agreed to be held publicly accountable for the way in which they handle government demands for censorship and surveillance around the world. No other North American companies have made this public commitment, and no companies from any other continents or regions have yet been willing to make a similar public commitment to free expression and privacy as a core component of responsible business practice.

Yet other forms of CSR—including environmental, labor, and sustainability standards—are by no means foreign to Asian businesses, even in China.[8] Might public expectations for corporate accountability in the area of free speech and privacy also rise in Asia in the coming years—particularly if these expectations are fed by increased civil society activism, pushing for greater accountability and transparency by ICT companies around their interactions with governments? In this chapter I compare government censorship and surveillance demands faced by companies in authoritarian China alongside the challenges faced by companies in two neighboring democracies that also have robust ICT industries and markets: South Korea and India. I argue that efforts to hold companies other than Google, Yahoo!, and Microsoft accountable for free speech and privacy in authoritarian countries like China will face an uphill battle unless companies in Asia's democracies are pushed by domestic civil society actors to defend and protect user rights in a more robust manner than is currently the case.

China: "Networked Authoritarianism" and the Private Sector[9]

As ONI research over the past decade has shown, China has the world's most sophisticated system of Internet filtering, which blocks access to vast numbers of Web sites and online content hosted by companies and on computer servers located mainly outside China.[10] But filtering is only the top layer of the country's elaborate system of Internet censorship. For Web sites run by individuals or companies located inside China, the government has direct jurisdiction—and thus more powerful instruments of control. Why merely filter a Web page when you can get it removed from the Internet completely or prevent its publication or dissemination in the first place? Over the past decade as Internet penetration grew rapidly in China, government regulators

have created strong negative incentives—including Web site registration requirements, the threat of jail sentences for individuals, and the cancellation of business licenses for companies—in order to keep certain kinds of content off the Internet.[11] Ronald Deibert and Rafal Rohozinski classify this approach to censorship as "second-generation Internet controls."[12] The Chinese government calls the system corporate "self-discipline," and hands out an annual award to companies that have done the best job of keeping their Web sites "harmonious" and free of sensitive content—ranging from the pornographic to the political.[13]

In Anglo-European legal parlance, the legal mechanism used to implement such a "self-discipline" system is a form of "intermediary liability."[14] It is the legal mechanism through which Google's Chinese search engine, Google.cn, was required to censor itself until Google redirected its simplified Chinese search engine offshore to Hong Kong.[15] All Internet companies operating within Chinese jurisdiction—domestic or foreign—are held liable for everything appearing on their search engines, blogging platforms, and social-networking services. They are also legally responsible for everything their users discuss or organize through chat clients and messaging services. In this way, much of the censorship and surveillance work is delegated and outsourced by the government to the private sector. If private companies fail to censor and monitor their users to the government's satisfaction, they will lose their business licenses and be forced to shut down.[16] All large Internet companies operating in China have entire departments of employees with hundreds of people whose sole job is to police users and censor content around the clock.[17]

Companies are also expected to play a role in the surveillance of Internet and mobile users. In a country like China where "crime" is defined broadly to include political dissent, companies with in-country operations and user data stored locally can easily find themselves complicit in the surveillance and jailing of political dissidents. The most notorious example of law enforcement compliance gone very wrong was when Yahoo!'s local Beijing staff gave to the Chinese police e-mail and user-account information of journalist Shi Tao, activist Wang Xiaoning, and at least two others engaged in political dissent.[18] There are other examples of how law enforcement compliance by foreign companies has compromised activists. In 2006, Skype partnered with a Chinese company to provide a localized version of its service, then found itself being used by Chinese authorities to track and log politically sensitive chat sessions by users inside China. This happened because Skype delegated law enforcement compliance to its local partner without sufficient attention to how the compliance was being carried out. The local partner, in turn, was merely following standard industry practice that is commonplace for domestic Chinese Internet companies.[19]

In this way, the private sector in China plays a key role in a political innovation that I call "networked authoritarianism."[20] Compared to classic 20th-century authoritarianism, this new form of Internet-age authoritarianism embraces the reality that

even when extensive filtering regimes are put in place, people cannot be prevented from accessing and creating a broad range of Internet content and holding all kinds of conversations, including those related to politics and policy. Networked authoritarianism thus accepts and allows a lot more give and take between government and citizens than in a pre-Internet authoritarian state. The regime uses the Internet not only to extend its control but also to enhance its legitimacy. While one party remains in control, a wide range of conversations about the country's problems rage on Web sites and social-networking services. The government follows online chatter and sometimes people are able to use the Internet to call attention to social problems or injustices, and even manage to have an impact on government policies. As a result, the average person with Internet or mobile access has a much greater sense of freedom—and may even feel like he or she has the ability to speak and be heard—in ways that were not possible under classic authoritarianism. It also makes most people a lot less likely to join a movement calling for radical political change. Meanwhile, the government exercises targeted censorship focused on activities and conversations that pose the greatest threat to the regime's power, and also devotes considerable resources to proactively seeding and manipulating the nation's online discourse about domestic and international events.[21]

Thus, while over 500 million Chinese people are finding their lives greatly enhanced by the Internet, Communist Party control over the bureaucracy and courts has strengthened, and the regime's institutional commitments to protect the universal rights and freedoms of all its citizens have weakened.[22] According to a recent report by the Dui Hua Foundation, in 2008 arrests and indictments on charges of "endangering state security"—the most common charge used in cases of political, religious, or ethnic dissent—more than doubled for the second time in three years.[23] Meanwhile, the Chinese government has made clear in its 2010 Internet White Paper that the rapid nationwide expansion of Internet and mobile penetration is a strategic priority. The development of a vibrant indigenous Internet and telecommunications sector is critical for China's long-term global economic competitiveness.[24] At the same time, Chinese companies are fully expected to support and reinforce domestic political stability, and to ensure that ICTs will not be used in a manner that threatens Communist Party rule.[25]

The China case demonstrates how companies can be used as an opaque extension of state power, helping authoritarian regimes to control and manipulate citizens with a lighter hand than was possible in the pre-Internet age while still maintaining power and preventing viable opposition movements from emerging. But what about democracies? In democratic societies, can ICT companies be used as an opaque tool for incumbent leaders, ruling political parties, and other powerful groups to manipulate public discourse and marginalize critics? Trends in South Korea and India suggest that such a situation is possible and may already be happening to different degrees. To

prevent creeping networked authoritarian tendencies in democratic societies, stronger strategic alliances between civil society and industry will be needed to push back against abuse of government power by means of digital networks and platforms.

South Korea: From Dictatorship to E-Democracy to "Free-Floating Control"[26]

After decades of dictatorship, South Korea underwent a successful transition to democracy in the 1990s. At the same time, thanks to a strong government emphasis on ICT investment over the past two decades, by 2009 more than 80 percent of South Koreans had become Internet users, with Internet access reaching more than 95 percent of households.[27] Upon his inauguration in 2003, late President Roh Moo-hyun was hailed in the international media as the world's first "Internet president" of the world's most advanced "Internet democracy."[28] His narrow election victory was widely credited to viral mobilization by his online supporters via citizen-media Web sites like OhmyNews.[29] Yet by 2009 domestic and international human rights groups were sounding the alarm about mounting and blatant violations of Korean citizens' right to free expression and privacy on the Internet.

In March 2010, Reporters Without Borders placed South Korea on its watch list, citing "a liberticidal legislative arsenal that is inducing netizens to practice self-censorship—all that in the name of the fight against dissemination of 'false information.'"[30] After visiting South Korea in May 2010 and meeting with local human rights organizations as well as government officials, the United Nations special rapporteur on freedom of expression, Frank La Rue, concluded, "I am concerned that in recent years, there has been a shrinking space for freedom of expression in the Republic of Korea." Online expression, he wrote in a press statement, was being squeezed by "arbitrary procedures for the deletion of information on the Internet" as a result of the broadening of regulatory requirements placed on Internet service providers (ISPs) and other content-hosting services.[31] He also cited South Korea's real-name identification requirement for Internet portals, which he concluded "has the potential to undermine individuals' right to express opinions, particularly criticisms of the Government, as well as the right to privacy."[32]

Laws requiring real-name registration tied to the National ID system for all users of Internet portals and services over a certain size, as well as other laws targeting "spread of rumors," defamation, and "campaigning" during an election period, were first enacted during the Roh administration.[33] The reasons for their enactment are familiar to many democratic societies in the Internet age: protecting innocent people against cyber harassment, cyber bullying, and cyber attack. By the middle of the first decade of the 21st century, cyber bullying had become a serious social problem in Korea: vicious cyber mobs had caused the suicide of several celebrities and turned ordinary citizens into national pariahs for being caught on cell-phone cameras

engaging in offensive yet relatively common behavior.[34] South Korean government, industry, and society at large were by 2003 already beginning to feel the cost of sophisticated cyber attacks.[35] A 2006 poll revealed that 85 percent of South Korean high school students were under stress from cyber bullying.[36] Real-ID requirements on Internet platforms and enhanced surveillance capabilities were touted by policymakers as a solution to social problems and crimes that the Internet had enabled, amplified, and exacerbated.

However, South Korean human rights activists argue that since the current president, Lee Myung-bak, took office in 2008, government measures have had an increasingly adverse impact on free expression and privacy. The ruling party, they say, has used media and communications laws to maximize its own political advantage, resulting in a marked "chilling effect" on political speech.[37] Measures include deletion or "temporary blocking" of Internet postings that criticize the government and powerful individuals, and prosecutions of individuals for dissemination of information characterized as "false communication using electronic communication facilities for the purpose of derogating public interest."[38] Laws against dissemination of false information, combined with the real-name registration requirement for all Internet services with more than 100,000 visitors per day, have resulted in the identification and prosecution of a number of Internet users for speech that is supposed to be protected under international human rights norms. Examples include the arrest of a teenager who proposed a student strike on a popular forum, and the arrest of the influential economic commentator known as "Minerva" for posting articles critical of the government's currency policy.[39] The man who wrote pseudonymously as "Minerva," Park Dae-sung, was identified by government investigators because the Internet portal Daum was required by law to hand over records of the account holder's real identity and National ID number. He was eventually acquitted, but only after spending five months in jail. Human rights groups argued that his experience has had a chilling effect on other citizens who might otherwise be motivated to post critiques of government policies online.[40] In December 2010, South Korea's Constitutional Court ruled that the telecommunications law banning the spread of false information was unconstitutional, citing unclear definitions in the law of terms such as "false" and "public interest."[41] While this ruling was hailed by digital rights groups as a major victory, other laws, including the real-ID requirements, remain in force.

While the Internet initially had a politically disruptive and democratizing effect on South Korean politics, enabling a political insurgent to win election in 2002 by circumventing political narratives promoted by mainstream broadcast and print media, the Internet has been used by the current regime as part of its efforts to chill dissent and marginalize critics.[42] Scholar Kwang-Suk Lee describes this process as an evolution from a dictatorship reliant on centralized, hierarchical control to a democracy whose political establishment seeks, through laws passed by a democratically elected

legislature, to develop a new "distributed and ubiquitous network model" of governance and manipulation of the public discourse, enabled by "positive technologies for free floating control" which "can hide under an ethical patina the real intention of control directed at establishing the new digital rule of cybersociety."[43]

In 2009, Google decided that it would not contribute to this trend. In April of that year the company announced that the local Korean section of its video-sharing service, YouTube, would disable users from uploading videos or posting comments because allowing them to do so without registering their real names and ID numbers was a violation of local law. The company cited a concern for South Korean Internet users' right to freedom of expression, stating on its official blog, "We believe that it is important for free expression that people have the right to remain anonymous, if they choose."[44]

Unnamed executives quoted in the press at the time indicated that South Korean companies resent being used as agents for the chilling of free expression in their country, but find themselves in a weaker position to resist given that their main customer base—and in many cases sole market—is domestic. In the wake of Google's announcement, The Hankyoreh news Web site quoted an unnamed executive at one of South Korea's major Internet portals who said, "When I saw Google's decision, I was jealous and at the same time deeply distressed. . . . South Korean businesses will have to endure criticism from users while following unwanted regulations."[45] The *Korea Times* quoted a similarly frustrated official from Daum, the country's second-largest Web portal: "The increasing government regulations can't help Korean Web portals if Internet users feel they're on a short leash. Korea is one of the few countries where local companies introduced enough quality services to stay ahead of global Internet giants in the market, but now it seems we may be losing some of our competitive edge."[46]

In China, where there is little hope of a fair hearing in the courts, no free media coverage, and no recourse to oppositional politics, executives can ill afford to stand up to the government. However, South Korean companies, operating in a democracy, are in a much stronger position to advocate on behalf of the rights of their users, challenge government orders in cases that are arguably unconstitutional or even illegal, and push for changes in law so that they will not be compelled to act as de facto opaque extensions of the ruling political power in a way that taints their own relationship with users and customers.

It appears that at least some attempts are being made in this direction. In April 2009, the *Korea Times* reported that K-Internet, an industry lobby of 150 Internet companies, protested against a controversial bill proposed in parliament by members of the ruling Grand National Party that would grant intelligence authorities greater powers to intercept user communications on mobile telephone networks and Internet services, requiring all ICT companies to maintain comprehensive logs of user and

customer communications. K-Internet argued that the bill "seems to be focused excessively on improving the 'efficiency' of investigations and less on protecting communication freedoms and limiting threats to privacy, posing a serious threat to the fundamental rights of citizens, limiting the business of communications operators and needlessly increasing social costs." An "industry insider" was further quoted as saying, "There is no fun in joking about Pakistan and China anymore, when our own government seems to have a similar approach to Internet users."[47] Korean ICT companies clearly see a link between protecting users' and customers' rights and their long-term brand reputation and commercial success. It is less clear whether civil liberties groups and Korean businesses are seeking or finding ways to work together effectively, not only to prevent further incursion but also to regain lost ground.

India: Systematizing Surveillance[48]

In contrast to South Korea's 82 percent Internet penetration as of 2009, India's Internet penetration hovered around 5 percent. While small in percentage terms, that still translates into nearly 60 million Internet users—larger than South Korea's roughly 40 million.[49] More broadly, India's telecommunications market is the fastest growing in the world, with industry executives predicting that the number of Indian mobile phone users could surpass one billion by 2015.[50] While India has a lively blogosphere and large communities on Orkut, Facebook, and Twitter, Indian citizens also expect their government to protect them from the spread of online crime, shield youth from pornography in a country where traditional values remain important, and take measures to prevent ethnic and religious violence in a country with a highly complex and volatile mix of religions and ethnicities. Internet and mobile technologies were used to coordinate the 2008 Mumbai terrorist attacks.[51] Cyber attacks launched from China, uncovered in 2009, exposed the need for improved cyber security.[52] Although these are all serious concerns for any democracy in the Internet age, the Indian government's approach to addressing these problems has raised concerns from civil liberties groups and industry.

The Information Technology Act of 2000 established the legal framework for filtering and regulating India's Internet, as well as the procedures by which ISPs and other Internet content and service companies can be compelled to censor online material or share information with government authorities.[53] Several incidents took place in the early 21st century in which the government ordered ISPs to block specific blogs and groups hosted on international services like Orkut, Yahoo Groups, and Blogger. These filtering efforts proved counterproductive because ISPs lacked the technical capacity to block individual subdomains, resulting in the blanket blocking of Blogger, Yahoo Groups, and Orkut at different points in time. This in turn prompted widespread public outcry and ridicule in the Indian media and blogosphere. It also sparked

grassroots efforts to spread knowledge among Indian Internet users about circumvention technologies so that most people who really wanted to access the offending content could still manage to do so.[54]

By the end of the decade the Indian government had changed its strategy for dealing with problematic content posted on, or transmitted through, the services of Internet companies. Ham-fisted and overbroad ISP-level filtering gave way to direct demands to the companies themselves to hand over user data and delete content.[55] The Information Technology (Amendment) Act of 2008 facilitated this transition by empowering the state to direct any ICT service to block, intercept, monitor, or decrypt any information through any computer resource.[56] The act also requires companies to have a designated point of contact for content-blocking, removal, and data requests. Company officials who fail to comply with government requests can face fines and up to seven years in jail.[57] Analysts point out that the new act has made ISP-level filtering more difficult, while strengthening and systematizing surveillance processes.[58] While most critics acknowledge the legitimate role of law enforcement, they have called for more comprehensive rules and procedures to supervise the process by which government demands are made, in order to prevent privacy violations, foul play, and political abuse.[59]

It was against this backdrop in early August 2010 that the Indian government demanded that Research in Motion (RIM), maker of Blackberry smart phones, grant Indian security agencies access to all corporate e-mail and instant-messenger communications transmitted within or through Indian borders. Failure to comply by the end of the month would result in blockage of all encrypted Blackberry traffic on Indian networks.[60] Gaining access to Blackberry's consumer services sold locally over domestic mobile carriers was one thing, and RIM expressed willingness to help the Indian government in this regard.[61] However, given that even RIM itself cannot access user data on Blackberry Enterprise Services—it is transmitted in highly encrypted form and retained on the corporate customers' servers—full compliance with the government's order in its original form is difficult if not impossible.[62] The company reportedly offered Indian authorities manual access to its messenger service with a pledge of real-time automated access by early 2011 and gained a reprieve from punishment until that time.[63]

Indian authorities claim to have begun conversations with other global companies, including Google and Skype, neither of which would comment publicly because they say they had not yet received any formal government requests or orders. Meanwhile, by late 2010 concerns were mounting in the Indian business community about the economic implications of their government's threats.[64] "We need a more balanced approach for lawful interception," wrote S. Ramadorai, vice chairman of Tata Consultancy Services Limited. "Bans and calls for bans aren't a solution. They'll disconnect India from the rest of the world. We can't allow that to happen, because then terrorists will win without even firing a bullet."[65]

Google has demonstrated that while companies are not in a position to commit civil disobedience if they want to stay in a market, they may be able to contribute to greater accountability by releasing more information about the demands that government authorities are making and whether they have been complied with. In September 2010, Google released a transparency report showing that from January through June, the Indian government made 30 content-removal requests (totaling 125 items), 53.3 percent of which Google claims to have "fully or partially complied with." Fourteen hundred and thirty Indian government requests to Google for user data ranked India the third highest in the world (behind 2,435 by Brazil and 4,287 by the United States)—not counting China.[66] The number of requests made by the Indian government to other foreign or domestic operators is unknown.

The Google Transparency Report has brought up some interesting questions. What if other multinational companies operating in India, along with Indian companies, all released similar data? Would that provide concerned citizens with at least some of the ammunition they need to hold their government accountable and ensure that censorship and surveillance in a democracy are restricted to the absolute minimum needed to protect innocent citizens' lives when they are clearly endangered by specific online activities by specific individuals, and that these tactics are not being abused for broader political purposes? Should India's vibrant activist community mount a campaign demanding that all companies operating in India must release similar transparency reports? Might they even lobby for the passage of a law requiring it? Might that at least be a first step toward necessary accountability?

Indian digital rights activists worry that India's vibrant nongovernmental sector has failed to mobilize on issues of digital free expression and privacy. In 2003, Supreme Court advocate Pavan Duggal wrote, "There is a need to change people's mindset [where most] view IT in isolation to democracy."[67] The problem does not seem to have improved over the decade. In 2007 lawyer Raman Jit Singh Chima lamented an "apparent lack of interest amongst traditional Indian civil liberties organizations in anything to do with the Internet or digital civil liberties in general."[68] In a 2009 report summarizing the state of Internet rights in India, activists Gurumurthy Kasinathan and Parminder Jeet Singh concluded that "unfortunately, in India, while different groups engage with some of the issues . . . in a piecemeal manner, there is little recognition of how they connect and reinforce each other in the building of a new social paradigm—euphemistically called an *information society*—that may require a set of coordinated civil society responses."[69]

Even in China, business leaders have expressed concern in private and semipublic forums that excessive burdens imposed on companies by governments can adversely impact innovation, which ultimately hurts national competitiveness.[70] The nature of China's legal and political system, however, makes it nearly impossible for Chinese companies to challenge government demands in the courts, take the debate to the

court of public opinion through the media, or make common cause with civil liberties activists. Their position is made even weaker, unfortunately, when neighboring democracies like India and South Korea—and many other democracies around the world—set legal, technical, and regulatory precedents for government-directed censorship and surveillance to be built within privately operated digital networks without sufficient public oversight, transparency, and accountability. Chinese media frequently cite South Korean examples in particular when arguing that China's Internet controls are in line with international practice.[71]

Corporate Social Responsibility

While it may be easier said than done, the idea of CSR—the notion that long-term corporate success requires the inclusion of environmental, sustainability, and human rights concerns in companies' core technologies, management, and business practices—is being embraced by publics around the world.[72] John Ruggie, special representative of the secretary-general of the United Nations on business and human rights, in examining how companies can and should be expected to contribute to human rights around the globe, concluded that while human rights are primarily the responsibility of the nation-state, companies must also respect, protect, and uphold internationally recognized human rights norms in the spheres of human life and activity over which their business exerts influence or on which it has an impact.[73] The problem is that most companies do not have systems or procedures in place to identify when they are doing harm, let alone processes to anticipate harm done by new business activities and technologies. The core work of genuine corporate social responsibility involves building such systems and mechanisms. Doing so generally requires working with outside stakeholders including environmental, labor, and human rights activists, socially responsible investors, industry groups, and governments.[74]

Concepts of CSR and "sustainable business" are taking root around Asia, albeit in different forms and guises in different Asian countries, given the region's tremendous variation in cultural, political, and economic contexts.[75] More Asian countries are shifting from a focus on labor-intensive manufacturing and export-oriented growth strategies. Governments around the region are placing growing emphasis on innovation in services, technology, and knowledge sectors as the key to economic growth and national competitiveness. The "knowledge-based corporation" is critical to South Korea's continued economic success and is considered by the Chinese and Indian governments to be an important driver of their nations' economic futures. Such companies have few tangible assets and rely heavily on intellectual property, innovative processes, and public reputation. Experts in business management point out that "reputational capital" is difficult to build and easy to lose, making it all the more

important that such companies anticipate and seek to avoid problems that could damage their reputation and lead to loss of "legitimacy" with their target users and customers.[76]

In India, the idea that business has a duty to serve the greater social good has deep roots in Gandhi's "trusteeship" model.[77] The Tata Group, which owns a number of ICT-related businesses, proudly quotes its founder Jamshetji Nusserwanji Tata (1839–1904): "In a free enterprise, the community is not just another stakeholder in business, but is in fact the very purpose of its existence."[78] While Indian companies have traditionally equated "corporate social responsibility" with charitable donation, a growing number—pushed by a broad range of civil society groups from national and international NGOs to local grassroots movements—are recognizing the need to engage with a broad range of "stakeholders" affected by their business, including India's many vibrant NGOs and grassroots activist groups, representing the interests of affected communities and groups.[79] As Indian multinationals expand around the world and seek to sharpen their competitiveness, more of them are adopting international standards for corporate social responsibility in order to improve their reputational capital in foreign markets.[80]

In South Korea, research shows that consumers tend to reward companies with reputations for being "good" to their communities and to their workers, while being less inclined to base purchasing decisions on companies' environmental practices.[81] Yet the South Korean environmental movement, which blossomed after the political system democratized in the early 1990s, achieved substantial change through public campaigns, media tactics, and political strategy. Most importantly, over the course of two decades the South Korean environmental movement—with the support of a broader global movement—was successful in reframing national priorities and values away from an earlier "developmentalist" narrative, promoted by government and industry, that economic development should be achieved at all costs.[82] Over time, thanks to democratization and greater media freedoms, the public and policymakers alike came to embrace the notion that clean soil, air, and water and conservation of national resources were not only essential for people's health and well-being, but were ultimately necessary for the nation's continued economic success. This shift in values has been crucial to bringing about change in government policy and business practice.[83]

South Korean society—like all modern industrialized consumption-driven economies—struggles with the problem of how to truly walk the talk. But the critical first step was to reframe prevailing narratives of what national "success" should look like. Globally, the mounting public pressure on companies to act responsibly is due to a dramatic shift in public expectations. That, in turn, is thanks to civil society's success in reframing the public discourse. Again, implementation remains a constant struggle. But once the concept was firmly planted in the public consciousness, it took root and has continued to grow.

In China, corporate social responsibility has been driven primarily by government fiat, based on the urgent recognition that environmentally sustainable business practices are imperative for the nation's long-term competitiveness as well as its people's physical survival. In January 2008, China's State-Owned Assets Supervision and Administration Commission decreed that "Corporate Social Responsibility has become a key criterion worldwide when people assess the value of a company."[84] Chinese companies were ordered to adopt global best practices so that their value for investors would rise. The number of Chinese companies producing sustainability reports shot up—from a handful in 2006 to more than 600 by 2009. By 2010 more than 600 companies were also participating in the United Nations Global Compact.[85] An ICT company—China Mobile—became the first mainland Chinese company to meaningfully disclose its carbon dioxide emissions, and it was also the first to be listed on the Dow Jones Sustainability Index.[86] While it would be difficult to imagine China Mobile signing on to the Global Network Initiative principles of free expression and privacy in China's current political climate, it is significant that Chinese companies—and Chinese policymakers—now view adherence to global CSR standards and expectations as an important part of Chinese companies' investment value. Such changes point to some reason for hope in the event that free expression and privacy become a more mainstream and established component of CSR for corporations, socially responsible investors, and civil society groups in the world's industrialized democracies.

Conclusion

Asia's governments—like all governments around the world—are grappling with many difficult challenges that the Internet has created for law enforcement and national security. Meanwhile, not only do civil society groups face new issues in terms of learning and deploying all the latest digital technologies for advocacy and discourse, but activists also have to keep developing new strategies, new knowledge, and new capacities in the fight to preserve civil liberties in the digital realm.

There are many questions to which nobody yet has answers. How can free expression and privacy be integrated into public definitions and expectations of responsible business behavior? What will it take for a critical mass of ICT companies operating in Asia to become more assertive in defending users' rights to free expression and privacy? What will it take to compel more multinational companies beyond the three GNI members, Google, Yahoo!, and Microsoft, to stand up for their users' rights to free expression and privacy not only because it is the right thing to do but also because they understand that in the long run this is the most successful business strategy?

In *Big Business, Big Responsibilities: From Villains to Visionaries: How Companies Are Tackling the World's Greatest Challenges,* authors Andy Wales, Matthew Gorman, and

Dunstan Hope point out that the issues of free expression and privacy involve relationships between citizens, companies, governments, and laws that are different from "traditional" CSR issues. In the case of environmental and labor practices, for instance, citizens often work with governments to force companies to stop polluting or improve treatment of workers, through the passage and enforcement of laws. However when it comes to government-driven incursions on free expression and privacy by means of censorship and surveillance, the problem lies with domestic laws, regulations, or law enforcement practices that are not in line with international human rights norms. Thus a "common cause" between citizens and companies is necessary in order to achieve the desired goal of protecting citizens' rights from the potential abuse of government power. "What we are witnessing," they observe, "is an intriguing alliance between the user and the company in defense of human rights."[87]

Environmental-protection and labor rights groups in countries such as South Korea and India have historically had good reason to view corporations as adversaries whose pursuit of profit has resulted in environmental degradation and human exploitation. Democratically elected government is won over by civil society as an ally in imposing standards and rules on the private sector. When it comes to Internet surveillance and censorship, however, interests are aligned in a different way so that citizens need corporate-owned digital intermediaries to help shield them from abuses of government power. Companies can do this by challenging—or at the very least publicly exposing—government demands for censorship and surveillance, which, if not arguably unconstitutional or illegal according to domestic law, clearly infringe on rights enshrined in the Universal Declaration of Human Rights and other international covenants.

Finding common cause *with* the private sector *against* government abuse of citizen rights does not come naturally to many civil society activists in Asia's democracies, many of which have only recently emerged either from corporatist-authoritarian pasts or from centralized systems of economic planning. As digital rights activists quoted earlier in this chapter pointed out, joining forces with the business community is not consistent with the anticapitalist culture of many Indian civil society groups. Similarly, South Korean civil society groups came of age in a culture of often-violent labor protest against corporate *chaebols* with close ties to the regime. Corporate managers have equally large cultural and mental barriers preventing them from tapping the moral force of civil society groups, who can potentially be powerful allies in helping companies stave off government interference of the sort that is likely to hamper their ability to innovate and compete on a global scale.

Achieving common cause between civil society and business thus requires new thinking, new attitudes, and new strategies on all sides. While these innovations will not be accomplished easily, in countries where civil society and business succeed in

working together to promote transparent and accountable governance of digital networks, the result could be a win-win for citizens' rights *as well as* high-tech competitiveness. Multinational companies from India and South Korea might even gain a competitive and reputational edge with global customers by joining the Global Network Initiative—even ahead of many of their European and North American competitors.

Studies of CSR practices in Asia show that even in democracies, managers and investors prefer to avoid terms like "human rights" and "social justice," which tend to be culturally associated with Western-style moralism. Instead, proponents and practitioners of CSR in Asia tend to emphasize concepts like "sustainability," with a strong emphasis on why environmental and labor standards contribute positively to social stability as well as companies' long-term value.[88] Such arguments have proven economically compelling even to corporations and regulators in authoritarian regimes such as China. If civil society and businesses in Asia's democracies can successfully make the economic value case for upholding global standards for free expression and privacy in the governance of digital networks, and if ICT companies from those nations gain a competitive boost as a result, there may well be reason to be optimistic that something similar may even happen in China someday.

Notes

1. Ben Doherty, "Silence of the Dissenters: How South-east Asia Keeps Web Users in Line," *The Guardian,* October 21, 2010, http://www.guardian.co.uk/technology/2010/oct/21/internet-web-censorship-asia.

2. Reporters Without Borders, "Web 2.0 Versus Control 2.0," March 18, 2010, http://en.rsf.org/web-2-0-versus-control-2-0-18-03-2010,36697.

3. Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy* 21, no. 4 (October 2010): 43–57.

4. "New Responsibilities in the Networked Age," in Andy Wales, Matthew Gorman, and Dunstan Hope, *Big Business, Big Responsibilities: From Villains to Visionaries: How Companies Are Tackling the World's Greatest Challenges* (New York: Palgrave Macmillan, 2010), 87–102.

5. Jonathan Zittrain and John Palfrey, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 103–122.

6. Global Network Initiative, http://globalnetworkinitiative.org.

7. Colin M. Maclay, "Protecting Privacy and Expression Online," in *Access Controlled: The Shaping of Power, Rights, and Rules in Cyberspace,* ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 87–108.

8. "The Government of Big Business," in Wales et al., *Big Business, Big Responsibilities*, 119–124.

9. This section borrows heavily from Rebecca MacKinnon, "Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom," a paper presented at Liberation Technology in Authoritarian Regimes Conference, sponsored by the Hoover Institution and the Center on Democracy, Development, and the Rule of Law (CDDRL), Stanford University, October 11–12, 2010, http://rconversation.blogs.com/MacKinnon_Libtech.pdf.

10. OpenNet Initiative, "China: Country Profile," in *Access Controlled,* 449–487.

11. Rebecca MacKinnon, "Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China," *Public Choice* 134, nos. 1–2 (January 2008): 31–46.

12. Ronald Deibert and Rafal Rohozinski, "Beyond Denial: Introducing the Next Generation of Internet Controls," in *Access Controlled,* 3–13.

13. Rebecca MacKinnon, "Are China's Demands for Internet 'Self Discipline' Spreading to the West?" McClatchy Newspapers syndicated service, January 18, 2010, http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html.

14. Ethan Zuckerman, "Intermediary Censorship," in *Access Controlled,* 71–84.

15. Miguel Helft and David Barboza, "Google Shuts China Site in Dispute Over Censorship," *New York Times*, March 22, 2010, http://www.nytimes.com/2010/03/23/technology/23google.html?_r=1.

16. Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday* (February 2006), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

17. Wen Yunchao, "The Art of Censorship," *Index on Censorship* 39, no. 1 (2010): 53–57.

18. For detailed analysis of the Yahoo! China case, see Rebecca MacKinnon, "Shi Tao, Yahoo!, and the Lessons for Corporate Social Responsibility," working paper presented December 2007 at the International Conference on Information Technology and Social Responsibility, Chinese University, Hong Kong, http://rconversation.blogs.com/YahooShiTaoLessons.pdf.

19. Nart Villeneuve, *Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform*, Information Warfare Monitor and ONI Asia Joint Report (October 2008), http://www.nartv.org/mirror/breachingtrust.pdf.

20. MacKinnon, "Networked Authoritarianism in China and Beyond."

21. Kathrin Hille, "How China Polices the Internet," *Financial Times*, July 17, 2009, http://www.ft.com/cms/s/2/e716cfc6-71a1-11de-a821-00144feabdc0.html; David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review*, July 2008, http://feer.wsj.com/essays/2008/august/chinas-guerrilla-war-for-the-web.

22. Congressional-Executive Commission on China, *2009 Annual Report*, http://www.cecc.gov/pages/annualRpt/annualRpt09/CECCannRpt2009.pdf.

23. "Chinese State Security Arrests, Indictments Doubled in 2008," *Dui Hua Human Rights Journal*, March 25, 2009, http://www.duihua.org/hrjournal/2009/03/chinese-state-security-arrests.html.

24. Information Office of the State Council of the People's Republic of China, *The Internet in China,* June 8, 2010, http://china.org.cn/government/whitepaper/node_7093508.htm.

25. David Talbot, "China: Our Internet Is Free Enough," *MIT Technology Review,* June 16, 2010, http://www.technologyreview.com/web/25592/page1/.

26. Please refer to the South Korea country profile in this volume for a comprehensive overview of South Korean laws and regulations aimed at controlling online speech.

27. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 figures, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

28. Jonathan Watts, "World's First Internet President Logs On," *The Guardian*, February 24, 2003, http://www.guardian.co.uk/technology/2003/feb/24/newmedia.koreanews.

29. Elizabeth Woyke, "OhmyNews Chooses Influence over Income," *Forbes*, April 3, 2009, http://www.forbes.com/2009/04/02/internet-media-video-technology-korea-09-media.html.

30. Reporters Without Borders, "Enemies of the Internet, Countries under Surveillance," March 12, 2010, http://en.rsf.org/IMG/pdf/Internet_enemies.pdf.

31. Frank La Rue, "Full Text of the Press Statement Delivered by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Frank La Rue, after the Conclusion of His Visit to the Republic of Korea," May 17, 2010, http://www2.ohchr.org/english/issues/opinion/docs/ROK-Pressstatement17052010.pdf.

32. Ibid.

33. Eric Fish, "Is Internet Censorship Compatible with Democracy? Legal Restrictions of Online Speech in South Korea," *Asia-Pacific Journal on Human Rights and the Law* 10, no. 2 (2009): 43–96.

34. Jonathan Krim, "Subway Fracas Escalates into Test of the Internet's Power to Shame," *Washington Post,* July 7, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html.

35. "Korean Companies Still Open to Cyber Attacks," *Asia Times Online,* November 21, 2003, http://www.atimes.com/atimes/Korea/EK21Dg02.html.

36. "Cyber Bullying Campaign against Korean Singer Dies Down," Agence France-Presse, October 13, 2010, http://www.google.com/hostednews/afp/article/ALeqM5ig4StQI4mbvccWeFCGC5uuihUyAg?docId=CNG.9dd1a1176881e712993720a765eec626.1d1.

37. Joint Korean NGOs for the Official Visit of the Special Rapporteur to the Republic of Korea, *NGO Report on the Situation of Freedom of Opinion and Expression in the Republic of Korea since 2008*, April 2010, http://kctu.org/7978.

38. Byongil Oh, "Republic of Korea," *Global Information Society Watch 2009,* Association for Progressive Communications and Humanist Institute for Cooperation with Developing Countries, 150–152, www.apc.org/system/files/GISW2009Web_EN.pdf.

39. Ibid.

40. Matthias Schwartz, "The Troubles of Korea's Influential Economic Pundit," *Wired Magazine,* October 19, 2009, http://www.wired.com/magazine/2009/10/mf_minerva.

41. Song Jung-a, "S. Korean Court Rules on Internet Law," *Financial Times,* December 28, 2010, http://www.ft.com/cms/s/0/38b354a4-126d-11e0-b4c8-00144feabdc0.html.

42. Fish, "Is Internet Censorship Compatible with Democracy?"

43. Lee, Kwang-Suk, "Surveillant Institutional Eyes in Korea: From Discipline to a Digital Grid of Control," *The Information Society* 23, no. 2 (2007): 119–124.

44. Stephen Shankland, "YouTube Korea Squelches Uploads, Comments," *CNET,* April 13, 2009, http://news.cnet.com/8301-1023_3-10218419-93.html.

45. *The Hankyoreh*, "S. Korea May Clash with Google over Internet Regulation Differences," April 21, 2009, http://english.hani.co.kr/arti/english_edition/e_international/350252.html.

46. Kim Tong-hyung, "Google Avoids Regulations, Korean Portals Not So Lucky," *Korea Times,* April 27, 2009, http://www.koreatimes.co.kr/www/news/tech/tech_view.asp?newsIdx=43939&categoryCode=129.

47. Kim Tong-hyung, "Is Korea Turning into an Internet Police State?" *Korea Times*, April 9, 2009, http://www.koreatimes.co.kr/www/news/tech/2010/05/133_42877.html.

48. Please refer to the India country profile in this volume for a comprehensive overview of Indian laws and regulations aimed at controlling online speech.

49. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers."

50. "India to Have 'Billion Plus' Mobile Users by 2015: Executive," *Economic Times,* November 18, 2009, http://economictimes.indiatimes.com/News/Economy/Finance/India-to-have-billion-plus-mobile-users-by-2015-executive/articleshow/5242284.cms; Shilpa Kannan, "India's 3G Licence Bidders Bank on Big Change," BBC News, April 7, 2010, http://news.bbc.co.uk/2/hi/business/8607866.stm.

51. Noah Schachtman, "How Gadgets Helped Mumbai Attackers," *Wired Magazine*, December 1, 2008, http://www.wired.com/dangerroom/2008/12/the-gagdets-of/.

52. Mehul Srivastava and James Rupert, "China-Linked Hackers Attacked India, Researchers Say," *Bloomberg Business Week*, April 6, 2010, http://www.businessweek.com/news/2010-04-06/researchers-find-china-linked-cyber-spy-ring-targeting-india.html; Information Warfare Monitor and the Shadowserver Foundation, *Shadows in the Cloud: An Investigation into Cyber Espionage 2.0*, April 6, 2010, http://www.shadows-in-the-cloud.net.

53. See the India country profile in this volume.

54. Nishant Shah, "Subject to Technology: Internet Pornography, Cyber-terrorism and the Indian State," *Inter-Asia Cultural Studies* 8, no. 3 (2007): 349–366.

55. Amol Sharma and Jessica Vascellaro, "Google and India Test the Limits of Liberty," *Wall Street Journal,* January 4, 2010, http://online.wsj.com/article/SB126239086161213013.html.

56. An annotated copy of the full text can be found at: http://cyberlaws.net/itamendments/IT%20ACT%20AMENDMENTS.PDF.

57. Sharma and Vascellaro, "Google and India Test the Limits."

58. "Govt Can't Ban Porn Websites for Obscenity," *Economic Times,* February 11, 2010, http://economictimes.indiatimes.com/infotech/internet/Govt-cant-ban-porn-websites-for-obscenity/articleshow/5558340.cms.

59. Sevanti Ninan, "In the Name of National Security," *The Hindu,* June 7, 2009, http://www.hindu.com/mag/2009/06/07/stories/2009060750090300.htm.

60. Vikas Bajaj, "India Warns It Will Block BlackBerry Traffic That It Can't Monitor," *New York Times,* August 12, 2010, http://www.nytimes.com/2010/08/13/technology/13rim.html.

61. Phred Dvorak, Amol Sharma, and Margaret Coker, "RIM Offered Security Fixes," *Wall Street Journal,* August 14, 2010, http://online.wsj.com/article/SB10001424052748703960004575427312899373090.html.

62. Andrew Vanacore, "BlackBerry CEO Suggests Route to Eavesdropping," *Associated Press*, September 27, 2010, http://www.msnbc.msn.com/id/39387290/ns/technology_and_science-security/.

63. "India Extends BlackBerry Access Deadline," Agence France-Presse, October 12, 2010, http://www.google.com/hostednews/afp/article/ALeqM5h9tMlmC3AyuCjurj2tA4rPZj0alg?docId=CNG.3af003c84a71aeca2db44ba857bb01cc.401.

64. Vikas Bajaj and Ian Austen, "India's Surveillance Plan Said to Deter Business," *New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/28/business/global/28secure.html.

65. S. Ramadoral, "Don't Disconnect India," *Hindustan Times*, September 21, 2010, http://www.hindustantimes.com/News-Feed/columns/Don-t-disconnect-India/Article1-603075.aspx.

66. Google, "Google Transparency Report: Government Requests," http://www.google.com/transparencyreport/governmentrequests/.

67. Pavan Duggal, "Internet and Democracy in India: A Report," in *Rhetoric and Reality: The Internet Challenge for Democracy in Asia,* ed. Indrajit Banerjee (Singapore: Times Media Academic Publishing, 2003), 61–98.

68. Raman Jit Singh Chima, "The Regulation of the Internet with Relation to Speech and Expression by the Indian State," Social Science Research Network, April 25, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1237262.

69. Gurumurthy Kasinathan and Parminder Jeet Singh, "India," Global Information Society Watch 2009, Association for Progressive Communications and Humanist Institute for Cooperation with Developing Countries, 127–130, www.apc.org/system/files/GISW2009Web_EN.pdf.

70. "Edward Tian: Google Is China's Best Tool for Understanding the West," *China Digital Times,* April 15, 2010, http://chinadigitaltimes.net/2010/04/edward-tian-google-is-chinas-best-tool-for-understanding-the-west/.

71. See, for example, "China Not Alone in Internet Regulation," *China Daily*, December 3, 2009, http://www.chinadaily.com.cn/opinion/2009-12/03/content_9111690.htm.

72. Aron Cramer and Zachary Karabel, *Sustainable Excellence: The Future of Business in a Fast-Changing World* (New York: Rodale, 2010).

73. United Nations Human Rights Council, *Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development—Protect, Respect and Remedy: A Framework for Business and Human Rights*, April 7, 2008, http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf.

74. Ibid.

75. Aron Cramer and Jeremy Prepscius, "Corporate Social Responsibility in Asia," *Global Asia* 2, no. 3 (Winter 2007), http://globalasia.org/new/l.php?c=e113.

76. Marc Newsona and Craig Deegan, "Global Expectations and Their Association with Corporate Social Disclosure Practices in Australia, Singapore, and South Korea," *International Journal of Accounting* 37 (2002): 183–213.

77. Subratesh Ghosh, "Trusteeship in Industry: Gandhiji's Dream and Contemporary Reality," *Indian Journal of Industrial Relations* 25, no. 1 (July 1989): 35–44.

78. Tata company, "About" page, http://www.tata.com/aboutus/articles/inside.aspx?artid=1U2QamAhqtA=.

79. Mahabir Narwal and Tejinder Sharma, "Perceptions of Corporate Social Responsibility in India: An Empirical Study," *Journal of Knowledge Globalization* 1, no. 1 (2008): 61–79.

80. Ibid.

81. Ki-Hoon Lee and Dongyoung Shin, "Consumers' Responses to CSR Activities: The Linkage between Increased Awareness and Purchase Intention," *Public Relations Review* 36, no. 2 (June 2010): 193–195.

82. Moon Chung-in and Lim Sung-hack, "Weaving through Paradoxes: Democratization, Globalization, and Environment Politics in South Korea," *East Asian Review* 15, no. 2 (Summer 2003): 43–70.

83. Ibid.

84. Cramer and Karabell, *Sustainable Excellence*, 82–83.

85. Ibid.

86. Wales et al., *Big Business, Big Responsibilities,* 119–124.

87. "New Responsibilities in the Networked Age," in Wales et al., *Big Business, Big Responsibilities*.

88. Cramer and Prepscius, "Corporate Social Responsibility in Asia"; Simon Powell and Jonathan Galligan, *Ethical Asia: Corporate Good Guys? It's All about Labour and Environment,* CLSA Asia-Pacific Markets, November 1, 2010, https://www.clsa.com/assets/files/reports/CLSA-Ethical-Asia.pdf.