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.

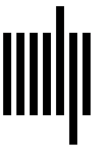
Access Contested

Security, Identity, and Resistance in Asian Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Contested: Security, Identity, and Resistance in Asian Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/9780262016780.001.0001
ISBN (electronic): 9780262298919
Publisher: The MIT Press
Published: 2011



The MIT Press

The online edition of this work is available from IDRC and at http://www.access-contested.net.

International Development Research Centre
PO Box 8500, Ottawa, ON K1G 3H9, Canada
info@idrc.ca / www.idrc.ca <http://www.idrc.ca>
ISBN 978-1-55250-507-6 (IDRC e-book)

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access contested : security, identity, and resistance in Asian cyberspace / edited by Ronald Deibert . . . [et al.].
p. cm. — (Information revolution and global politics)
Includes bibliographical references and index.
ISBN 978-0-262-01678-0 (hardcover : alk. paper) — ISBN 978-0-262-51680-8 (pbk. : alk. paper)
1. Cyberspace—Government policy—Asia. 2. Computer security—Asia. 3. Computers—Access control—Asia. 4. Internet—Government policy—Asia. 5. Internet—Censorship—Asia. I. Deibert, Ronald.
HM851.A253 2011
303.48′33095—dc23

2011031273

10 9 8 7 6 5 4 3 2 1