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.

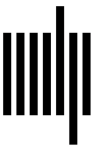
Access Contested

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