



Ron Deibert, Rafal Rohozinski

## Cyber wars

While the role of technology in the political struggle in Iran and elsewhere should not be overstated, it should not be underestimated either. The "next generation" controls with which authorities aim to manage the Internet mark a shift from heavy-handed filtering to sophisticated multi-pronged methods. Ron Deibert and Rafal Rohozinski on the attempt to normalise the exercise of power in cyberspace.



At the end of 2009, a social movement mobilised once again around an Iranian political crisis — from the streets of Iran's cities spreading through networks of support to Europe, North America and beyond. In Toronto, where the [Citizen Lab](#) Internet research and development centre is located, a dynamic group of Iranian students banded together with activists across the world, raising awareness and building support. Together they have formed an identity unique to the twenty-first century: a cyber enabled, planetary resistance community.

The role of technology in events such as these is often overstated and the Iranian case is no exception. The battle is about much more than the most recent social networking tool, no matter what label is assigned to this latest revolution. But it should not be underestimated either. Cyberspace is the domain through which the battle of ideas takes place today, and it is a heavily contested domain.

It is widely known that demonstrations can achieve broader support and publicity through the use of the Internet and by the creative exploitation of mobile technologies such as SMS and video capture. But the Iranian authorities are taking active counter-measures aimed at controlling the spaces online for resistance and dissent. These measures include the well-known technique of filtering access to websites at key Internet chokepoints. But there are also more offensive operations that are subtle, flexible and insidious. These include tampering with Internet connections, mobile and other telecommunications services; monitoring social networking sites to identify key organisers, who are then subjected to threats and intimidation; pressurising services in Iran to remove "offensive" posts or blogs; and arresting prominent writers and dissidents.

As two of the principal investigators of the OpenNet Initiative, a project whose aim is to monitor Internet filtering and surveillance worldwide, these actions are increasingly familiar to us. What is happening now in Iran offers a clear example of "next generation" controls that are being exercised in cyberspace as the domain becomes more heavily contested and seen as a critical vector of the

exercise of power. Whereas in the past, freedom of expression activists and others concerned about human rights had to worry mostly about how to bypass Internet filters, they now have to worry about a much broader suite of restraints, risks and liabilities. Rather than first generation controls, as exemplified by China's great firewall, in which filtering technologies are employed in a constant manner at key Internet chokepoints, we are seeing instead the emergence of methods designed to go beyond denial to shape and contain the space for expression online. Since these controls tend to operate in the shadows, they are more difficult to monitor and thus present a challenge to rights organisations and monitoring groups like the OpenNet Initiative (ONI). They will require a new approach to research and advocacy in order to prevent the further encroachment of human rights online.

Burma 2007. Russia–Georgia 2008. China–Tibet 2008. Iran 2009. Xinjiang 2009. These recent events, although dissimilar in many ways, share several common threads. The struggles on the ground were accompanied and very much influenced by a related struggle in cyberspace, between activists on the one hand and entrenched authorities on the other. Not that long ago it would have been safe to assume the entrenched authorities were at a disadvantage, too inept to withstand digitally–enabled social movements. Today, that is no longer a safe assumption. The centre of gravity of techniques aimed at managing cyberspace has shifted from heavy–handed and often crudely implemented filtering to more sophisticated multi–pronged methods that seek to normalise control and the exercise of power in cyberspace. There are numerous examples of these next generation controls from widely different regional contexts, suggesting the emergence of a very troubling global norm. Countering all of them will require a new comprehensive approach.

## Legal measures

One of the fastest growing and effective next generation controls concerns the broad use of slander, libel and other laws to restrict permissible communications and to create a climate of fear, intimidation and ultimately self–censorship. In part, this reflects a natural maturation process as authorities seek to reign in cyberspace and bring it under regulatory oversight. But more nefariously, it also reflects a tactic of strangulation, whereby threats of legal action can do more to prevent strategically threatening information from seeing the light of day than do more passive controls implemented in a defensive manner. Although new laws are being drafted to deal with cyberspace security and regulation, sometimes old, obscure, or rarely enforced regulations are pointed to ex post facto to justify acts of Internet censorship.

Ironically, we experienced this very type of control ourselves while at the Internet Governance Forum (IGF) meeting last November in Sharm El Sheikh, Egypt, when UN officials asked us to remove a banner for the ONI's new book on the topic of next generation controls, *Access Controlled*. While the UN officials told us in person that the banner had to be removed because of references to China, they later justified the act publicly in reference to regulations prohibiting advertisements and banners in the halls of the IGF — regulations that seemed to many observers to be very unevenly enforced throughout the event. Although examples of similar measures can be seen in almost all countries of the world, the most compelling cases are found in the countries of the former Soviet Union. In Kazakhstan, for example, opposition websites or websites carrying material critical of the government are regularly deregistered from the national domain using a variety of vague laws and regulations as justification. In years to come, we expect to see more use of

legal levers such as these as a means to smother freedom of expression.

### **Informal requests**

While legal measures create the regulatory context for denial, informal requests and other pressures made by authorities to private companies can be employed for more immediate ends. Most often these informal requests come in the form of pressure on Internet service providers and online service providers to "take down" or remove offensive posts or information that threatens "national security" or "cultural sensitivities". Google's recent decision to reconsider its service offerings in China reflects, in part, that company's frustration with having to deal with such informal take-down requests from Chinese authorities on a regular basis. Such informal requests can go further, putting pressure on the companies that run the infrastructure to render services inoperative in order to prevent their exploitation by opposition groups or activists.

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

### **Outsourcing and downloading**

It is important to emphasise that cyberspace is owned and operated primarily by private companies. The decisions taken by those companies on content controls can be as important as those taken by governments. Often, private companies are compelled in some manner to do the job of censorship and surveillance in order to operate in a particular jurisdiction, as evidenced most prominently by the collusion of western search engines, such as Google (up until January 2010), Microsoft and Yahoo, in China's Internet censorship practices. In its most extreme forms, the outsourcing of these controls can take the form of illegal acts or acts that are contrary to publicly stated operating procedures and privacy protections. This was dramatically illustrated in the case of Tom-Skype, in which the Chinese partner of Skype put in place a covert surveillance system to track and monitor pro-democracy activists who were using the chat function as a form of outreach. The system was only discovered because of faulty security on the servers operated by Tom Online.

Presumably, many other such collusive acts of censorship and surveillance exist that are undiscovered. For governments in both the developed and developing worlds, offloading such controls to private companies allows them to place their controls on the "frontlines" of the networks and draw in the actors who manage the key access points and hosting platforms. If trends continue, we can expect more censorship and surveillance responsibilities to be exercised by private companies, carrier hotels, "cloud computing" (internet-based) networks, Internet exchanges and telecommunications companies. Such a shift in the locus of controls raises serious issues of public accountability and transparency for citizens of all countries. It is in this context

that Google's dramatic announcement to end censorship of its Chinese search engine should be considered a watershed moment. Whether other companies follow Google's lead, and how China, other countries, and the international community as a whole react, are key open questions that could help determine the shape of public accountability of private actors in this domain.

### **Just-in-time blocking**

Disabling or attacking critical information assets at key moments in time (for example during elections or public demonstrations) may be the most effective tool in terms of shaping outcomes in cyberspace. Today, computer network attacks, including the use of distributed denial of service attacks, can be easily marshalled 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 such attacks — called botnets — are now thriving like parasites in peer-to-peer architectures along the invisible underbelly of insecure servers, PCs, and social networking platforms. Botnets can be activated by anyone willing to pay a fee against any target of opportunity.

There are cruder methods of effecting just-in-time blocking as well, like shutting off power to the buildings where servers are located or tampering with domain name registration so that information is not routed properly to its destination. Such just-in-time blocking has been empirically documented by the ONI in Kyrgyzstan, Belarus and Tajikistan and reported in numerous other countries as well.

The attraction of just-in-time blocking is that information is only disabled at key intervals while kept accessible at other times, thus avoiding charges of Internet censorship and allowing for plausible denials of censorship by the perpetrators. In regions where Internet connectivity can be spotty, just-in-time blocking is easily reasoned away as just another technical glitch with the Internet. When such attacks are contracted out to criminal organisations, determining attribution of those responsible is nearly impossible.

### **Computer network attacks**

Just-in-time blocking can take the form of computer network attacks. But the latter can also be employed as a component of military action, low intensity conflict, or attacks on critical infrastructures — in other words, for strategic reasons separate from censorship. For years, such attacks have been speculated upon and it was thought that interdependence among states served as a strong deterrent on their execution. In recent years, however, there have been several high-profile incidences of computer network attacks, including those on Estonia in 2007 and during the Russia-Georgia war of 2008. In each of these cases, the circumstances surrounding the attacks were murky (see "Patriotic hacking" below), but the outcomes were not. In Estonia, key critical information resources, such as 911 systems and hospital networks, were debilitated, as were Georgia's official channels of government communication.

What is most ominous about computer network attacks is that many governments are now openly considering their use as part of standard military doctrine. President Obama's cyber security review, completed in May 2009, may have unwittingly set off a security dilemma spiral in this respect with its official acknowledgment that the United States has such capabilities at its disposal — a decision that may come back to haunt the information dependent

country when other actors follow suit.

### **Patriotic hacking**

One of the characteristics of cyberspace is that individuals can engage in creative acts that have system-wide effects. This is no less true in cases of individuals taking action against those they consider threats to their own state's national interests. Citizens may bristle at outside interference in their country's internal affairs and can take offence at criticism directed at their own governments, however illegitimate they may appear to outsiders. Some with the technical skills take it upon themselves to attack adversarial sources of information, often leaving provocative messages and warnings in their wake. Such actions make it difficult to determine attribution behind the attacks — is it the government or the citizens acting alone? Or is it perhaps some combination of the two? Muddying the waters further, some government security services informally encourage or tacitly approve of the actions of patriotic groups.

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

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

The growth in this sector can be attributed, in part, to the unintentional practices of civil society and human rights organisations themselves. As our colleagues Nart Villeneuve and Greg Walton have shown, many civil society organisations lack simple training and resources, leaving them vulnerable to even the most basic of Internet attacks. Moreover, because such organisations tend to thrive on awareness raising and advocacy through social networking and email lists, they are often unwittingly compromised as vectors of attacks even by those whose motivations are not political per se. In one particularly egregious example cited by Villeneuve and Walton, the advocacy group Reporters Without Borders unknowingly propagated a link to a malicious website posing as a Facebook petition to release the Tibetan activist Dhondup Wangchen. As with computer network attacks, targeted espionage and social malware attacks are being developed not just by criminal groups and rogue

actors, but also at the highest government levels. The US director of national intelligence, Dennis Blair, recently remarked that the United States must be "aggressive" in the cyber domain in terms of "both protecting our own secrets and stealing those of others".

Together, these next generation controls present major challenges for monitoring groups, rights organisations, and all of those who care about the future of openness and human rights online. Our own OpenNet Initiative, for example, developed an elaborate methodology primarily oriented towards technically monitoring "first generation" filtering at key Internet chokepoints using network interrogation tools within countries under investigation. While this mission is still essential and important, its methods are ill equipped to identify the range of next generation controls. To remain relevant, the ONI needs to adjust, perhaps even undertake a paradigm shift, and develop new techniques to monitor more offensive means of blocking. Next generation controls require next generation monitoring.

For rights organisations, darker clouds are looming on the horizon. The context around free expression has become much more ominous and militarised than it was in the past as the norms around next generation controls spread and mature. There is an arms race in cyberspace, with state militaries, extremists, non-state actors and other organisations engaged in increasingly aggressive interventions. Meanwhile, the private actors who control the infrastructure of cyberspace are also becoming more important players in determining the scope for free expression online. Together these present major new challenges and an entirely more hostile context that is becoming the norm. Arms control in cyberspace is now an urgent matter. Lastly, citizens around the world need to be made aware of the threats to the openness of cyberspace that this new generation of controls presents. There is a degradation of valuable global communications occurring as ominous as the degradation of the natural environment. For generations, philosophers have long speculated about a global communications platform through which citizens could communicate, share ideas and develop common solutions to problems in an unmediated fashion. Writing in 1937, HG Wells presented the outlines of such a possibility in his essay entitled "World Brain":

The whole human memory can be, and probably in a short time will be, made accessible to every individual [...] It need not be concentrated in any one single place. It need not be vulnerable as a human head or a human heart is vulnerable. It can be reproduced exactly and fully, in Peru, China, Iceland, Central Africa, or wherever else seems to afford an insurance against danger and interruption. It can have at once the concentration of a craniate animal and the diffused vitality of an amoeba.

No doubt Wells would shudder if he could see now that having come so close to achieving this very possibility, citizens of the world would allow it to implode in a spiral of weaponisation, militarisation and censorship. A planetary social movement is required today that mobilises us all to protect the net as a forum for free expression, access to information and open communication.

First published in Index on Censorship 1/2010  
© Ron Deibert / Rafal Rohozinski  
© Index on Censorship  
© Eurozine