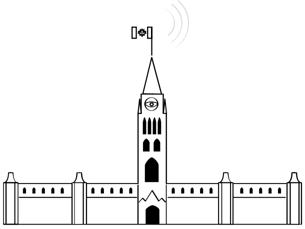
SECURING  CYBERSPACE

Canada needs to set an example for global Internet security

By Ron Deibert

Another day, another announcement of hacker exploits. Only this time, the perpetrator is not Anonymous or LulzSec, or any of their hacker sympathizers. A group calling itself the Syrian Electronic Army (SEA) posted email credentials, including usernames and passwords, of Al Jazeera journalists, as well as a series of emails that pertained to bias in reports of the revolution in Syria. The SEA boasted about it on their Arabic Facebook page, and went so far as to publish on Internet forums what they claim are the private correspondences of a Syrian Al Jazeera anchorwoman complaining of the apparent biased coverage she was pressured to adopt at the network.

Encountering episodes such as these is unfortunately all too common in the day-to-day routine of the Citizen Lab, an advanced research and development laboratory working at the intersection of digital security and human rights at the University of Toronto. Although based in Canada, the Citizen Lab monitors global cyberspace using a combination of technical and in-country field research methods. Working with groups in Asia, the Middle East, Africa and Latin America, we document targeted cyber attacks on human rights groups, and monitor censorship and surveillance practices and technologies, all with an eye towards protecting and preserving cyberspace as a medium for free expression, association and access to information.

Canadians may find the SEA's invasion of private email correspondences between Al Jazeera reporters distant from their daily lives. How is an obscure hacking attack amidst a far-away civil war in the Arab world connected to Canada? In fact, the connections are not so remote. What we do here in Canada can have important consequences for what goes on abroad. Canadian approaches to cyber security help set standards that other countries follow. When we raise the bar, it puts a spotlight on those who fall below it. Alternatively, when we set low standards at home, we legitimize actions that work at cross-purposes to our core values.

The SEA is a curious hybrid, and a model of the new type of "active defense" that is emerging among autocratic regimes. Not formally linked to the government of Syria, but receiving its tacit support, the SEA undertakes information operations in support of the regime—but does so at an arm's-length, so as to provide the government with a degree of plausible deniability. Its methods are not technically complex by any measure; indeed, they are among the run-of-the-mill techniques widely employed in the world of cyber crime. The SEA defaces and spams websites of adversaries of Assad, but also targets groups that appear to have dubious relevance to Syria, and look more like convenient targets of opportunity. For example, the SEA once defaced the website of an obscure town council in the United Kingdom.

But Syrian active defense in cyberspace is evolving: the regime's methods are showing signs of climbing up the ladder of sophistication. Recently, CNN profiled a malicious software program that was hidden in images that had circulated among Syrian diaspora and pro-democracy activities. Researchers who analyzed the malware determined that the Trojan horse, which connected back to command and control computers based in Syria, was an open-source remote access tool that the Syrians had commandeered for their purposes. Those infected by the Trojan horse would have their computers fully exposed to the attackers, who would then be able to remotely monitor every communication and map their social networks through email and other contacts. Whereas prior defacement and spam attacks had the imprecision of a sledgehammer, the Trojan horse attack is more like a carefully calibrated set of pliers. Targeted attacks such as these are especially dangerous because they could expose dissidents' private correspondences, and even location, leading to arrest, assault or murder.

Around the world, pro-regime hacking attacks on opposition groups are becoming widespread and a growing menace. China's adversaries have been the most frequently targeted for the longest period of time. They are the most well-known, in part because so many other high profile targets—including major corporations and U.S. government agencies—have fallen victim to Chinese-based cyber espionage attacks. The research our group helped to undertake in the *Tracking Ghostnet* and *Shadows in the Cloud* reports, which began with evaluations of targeted threats against the offices of the Dalai Lama and Tibetan Government-in-exile, revealed dozens of government ministries, foreign affairs departments and international organizations that had also been victimized by the same perpetrators. It is noteworthy that in both of our reports we could make no direct connection to the Chinese government itself—there was no "smoking gun." Many observers believe China tacitly condones the vast cyber criminal underworld as a kind of convenient malaise from which it strategically benefits.

China is not alone in this respect. Over the years, our research has documented denial of service and hacking attacks, information operations and other computer network exploitation against human rights and opposition groups originating from shadowy underground groups whose operations coincidentally benefit entrenched authorities in places like Russia, Kyrgyzstan, Belarus and Burma. Perhaps the most aggressive of these is associated with Iran. In the wake of the 2009 "Green Movement" that sprouted in and around Iran, a group calling itself the Iranian Cyber Army emerged and began menacing Green Movement sympathizers at home and abroad. As with the SEA, the Iranian Cyber Army defaces websites and anonymously spams forums with threatening messages, creating a climate of fear and suspicion within the Green Movement. Recently, quite sophisticated attacks on the certificate authority systems that secure Internet traffic were undertaken by an individual claiming to be connected to the Iranian Cyber Army. As with other governments of its ilk, the Iranian regime has tacitly condoned the activities of the Iranian Cyber Army, even going so far as to applaud its efforts, while also keeping one step removed from formal endorsement and incorporation.

Quasi-national cyber armies like these are spreading for at least two reasons. First, the tools to engage in cyber attacks and exploitation have become widely available and increasingly easy to use as the ecosystem of cyber crime diversifies and expands worldwide without check. Today, botnets (a large number of compromised computers) that can be used to bring down virtually any website with a denial of service attack can be rented from open websites—and some even offer real-time customer service support. Trojan horses and other so-called "Zero Day" exploits can be purchased from underground forums. We have entered the age of do-it-yourself information operations. As recent actions by Anonymous have shown, just about anyone with a grievance can marshal an attack on nearly any target of their choosing. With enough crowd support, these can be devastating and effective.

A second factor, which reinforces and builds upon the first, is the growing pressures on governments and their armed forces to develop cyber warfare capabilities. While cyber warfare threats are often exaggerated to justify massive defense contracts, there is an undeniable arms race occurring and a process of militarization unfolding. Governments around the world now see cyber security as an urgent priority, and their armed forces are stepping up to the challenge. However, not all of them will follow the same playbook. While the United States and other western countries build official "cyber commands," employing uniformed personnel with clearly defined missions, the world's corrupt, autocratic and authoritarian regimes will likely continue to exploit the cyber criminal underground. These regimes will also target a different adversary, reflecting their own unique perception of what constitutes a threat to regime stability: opposition groups, independent media, bloggers and journalists, and the vast networks of civil society groups pressing for openness, democracy and accountability.

For many years, global civil society networks saw the Internet and other new media only as powerful fuel for their cause. They have gradually come to learn that these media can be controlled in ways that limit access to information and freedom of speech for citizens living behind national firewalls. Now there is another, more ominous, cause for concern: cyberspace is becoming a dangerously weaponized and insecure environment within which to operate. It is now a domain through which global civil society networks can be entrapped, harassed and exploited, as much as they can be empowered.

Reversing these trends will not be easy, and will require a multi-pronged strategy among civil society networks, the private sector and liberal democratic governments. Distributed research and monitoring networks that lift the lid on cyberspace and track and analyze the growing threats to rights and openness are critical, as are information sharing coalitions that point to best practices and secure technologies. For liberal democratic governments, the growing militarization of cyberspace has to be seen in more than the narrow terms of the threat to national security, but also as a disease that is gradually undermining the gains that have been made in rights and networking over the past decade. These risks underscore the importance of building global coalitions of governments to protect and preserve cyberspace as an open commons governed by multiple stakeholders at an international level, and also the importance of creating a regulatory environment and a system of incentives to encourage responsible private sector behaviour, particularly when it comes to market opportunities that violate human rights.

Viewed from this broad perspective, the counterproductive impacts of short-sighted domestic policies are put in stark relief: Who are we in western liberal democratic countries to criticize the Iranian Revolutionary Guard for compelling mobile operators to share private conversations of dissidents and activists, when we are about to pass a law that authorizes massive electronic surveillance without judicial oversight? On what basis can we condemn the Syrian Electronic Army or other quasi-state hacker groups for infiltrating the computers of opposition groups when Canadian companies openly market offensive computer network attack products and services in Las Vegas-style trade shows? Protecting and preserving cyberspace as a secure and open commons has to begin at home.

Ron Deibert is director of the Citizen Lab and Canada Centre for Global Security Studies at the Munk School of Global Affairs, University of Toronto.