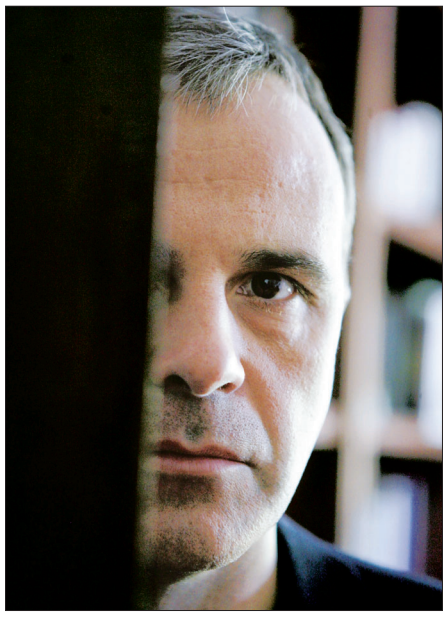
BREAKING UP DARK CLOUDS IN CYBERSPACE

Ron Deibert
Associate Professor of Political Science and Director of the Citizen Lab at the Munk School of Global Affairs



Rafal Rohozinski
CEO of the Ottawa-based SecDev Group

The Munk School's Citizen Lab made international news headlines in April with a report documenting a complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. Entitled Shadows in the Cloud: An Investigation into Cyber Espionage 2.0., *the report was published by the Citizen Lab, the SecDev Group, and the Shadowserver Foundation. Below is an essay by the authors on cyber espionage.*

Crime and espionage form a dark underworld of cyberspace. Whereas crime is usually the first to seek out new opportunities and methods, espionage usually follows in its wake, borrowing techniques and tradecraft. Our Shadows in the Cloud report illustrates the increasingly dangerous ecosystem of crime and espionage and its embeddedness in the fabric of global cyberspace.

As our everyday lives move online, criminals and spies have migrated to this domain. They leverage complex, adaptive attack techniques to take advantage of the fissures that have emerged in an era where "e" is everything. Every new software, social networking site, cloud-computing system, or web-hosting service represents opportunities for the predatory criminal ecosystem to subvert, adapt, and exploit.

Cat and mouse: Every new software site, cloud-computing system, or web-hosting service represents opportunities for the predatory criminal ecosystem.

This situation has also emerged because of poor security practices among individuals, businesses, and governments. The age of mass Internet access is less than 20 years old. Public institutions — particularly those in developing countries — have embraced these new technologies faster than procedures have been created to deal with the vulnerabilities they introduce. Today, data is transferred from laptops to USB sticks, over wireless networks at cafe hot spots, and stored across cloud-computing systems whose servers are located in far-off jurisdictions. The sheer complexity makes thinking about security in cyberspace mind-bogglingly difficult. Paradoxically, documents and personal information are probably safer in a file cabinet, under a bureaucrat's careful watch, than they are on today's networked PC.

"No country is secure in the global sea of information."

The ecosystem of crime and espionage is also emerging because of strategic calculus. Cyberspace is the great equalizer. Countries no longer need to spend billions of dollars to build globe-spanning satellites to pursue high-level intelligence gathering, when they can do so by harvesting information from government computers connected to the Internet.

Governments are engaged in a rapid race to militarize cyberspace, to develop tools and methods to fight and win wars in this domain. This arms race creates an opportunity structure ripe for crime and espionage to flourish. In the absence of norms, principles, and rules of mutual restraint, opportunists, criminals, spies, and others rush to fill the vacuum.

Against this context, the absence of Canadian policy for cyberspace is notable. For years, Canadian telcos have acted as the frontline against a surging tide of criminal botnets, malware, and other malicious online behaviour — largely in the absence of government policy. At least one Canadian institution was ensnared in the Shadow network we uncovered, but no doubt others have been that escaped our gaze.

Canada's cybersecurity strategy has been long promised, but a domestic cybersecurity plan is only a partial solution. In a networked world, you are only as secure as the weakest link — and that link can be anyone, including your allies and partners. Notably, our investigation discovered that Canadian visa applications submitted to Indian consulates in Afghanistan were stolen along with those of 12 other nationalities.

Improving cybersecurity requires a global effort, and one in which Canada's security and foreign policy must be attuned and synchronized to the unique needs of cyberspace. We should take the lead in pushing for a global convention that builds robust mechanisms of information sharing across borders and institutions, defines appropriate rules of the road for engagement in the cyberdomain, puts the onus on states to not tolerate or encourage malicious networks whose activities operate from within their jurisdictions.

At the same time, Canada should work to defend the openness of the global Internet commons — to ensure that policies and practices appropriate to security in the information age do not restrict, constrain, or threaten to roll back the gains in development, human rights, and democracy — values we as Canadians embrace — and which cyberspace has helped propel globally over the past 20 years.

Today, no country is secure in the global sea of information. Preserving cyberspace requires a strategy to address the dark side of the Internet. This requires urgent international co-operation, level-headed judgment, and a commitment to preserve our values of freedom of speech and access to information, so as to ensure that in our quest for online security we do not secure ourselves into a new dark age.

This essay first appeared in The Globe and Mail.