THE GLOBE AND MAIL

November 13, 2010

The Internet needs peacekeepers. Is Canada ready?

By Omar El Akkad
From Saturday's Globe and Mail

Crime, censorship and espionage have turned the digital world into a battlefield. What role should Canada play in saving the Web?

It is a crime in progress, a cyber-fraud network that moves with blistering efficiency between servers in England, criminals in Russia and victims around the globe. It is borderless, profitable and almost impossible to stop. It is the digital future of criminality.

From the basement office of the Citizen Lab at the University of Toronto's Munk School of Global Affairs, Nart Villeneuve allows one of his computers to become infected with the so-called Koobface malware - a piece of malicious code conceived by a group of hackers in St. Petersburg that essentially takes control of a computer and tricks users into inadvertently clicking on advertising links across the Web, generating revenue for the authors.

For more than a year, Mr. Villeneuve has been tracking the malware - the name given to code that is designed to illicitly control or otherwise compromise an unsuspecting user's computer. Until today, Mr. Villeneuve's work has largely been secret. Now, it is out in the open, in a report released Friday evening [http://www.infowar-monitor.net/2010/11/koobface] for the Information Warfare Monitor, a joint venture between the University of Toronto and the SecDev Group, an Ottawa-based security consultancy.

Between July of 2009 and July of 2010, Koobface netted its four known authors at least $2-million in profit. Koobface isn't spread through overly intrusive means, but rather, through messages and links sent via the world's most popular social network, Facebook.

Though Facebook Inc. is aware of the scam, and the FBI, the RCMP and other law enforcement agencies are investigating its authors, the malicious fraud network has proven exceptionally difficult to shut down. That's in large part because the network is so widespread, and each individual act of fraud so miniscule. In effect, Koobface causes the owners of infected computers to click on ads that then pay Koobface's authors a few pennies per click. Advertising networks are defrauded of a few cents at a time, and the individual users often have no idea their computers are being hijacked.

"In general, each law enforcement agency wants a domestic victim they can bring into court," says Mr. Villeneuve, who has spent much of his academic career tracking such criminal networks. "But given the nature of the operation, that's very difficult to do."

But perhaps the scariest aspect of these networks of compromised computers isn't their capacity to defraud users and Web sites. It is the fact that they are also the means by which much larger cyber-battles can be carried out - even between governments that are locked in a digital arms race.

At the birth of the Internet some 40 years ago, when the first bits of digital information flowed between two university computers in California, few could have envisioned what the communications network would one day become: the centre of the world's business, social and educational interaction and one of the most important inventions in human history.

But the Internet has also become a battlefield. From state-sponsored cyber-attacks in Russia and Eastern Europe to censorship in the Middle East and China, governments are increasingly building and militarizing borders in what was once considered a borderless medium. The very same techniques used in criminal networks such as Koobface are being utilized by authorities looking to wage digital war against their own citizens, or each other. When Estonia came under cyber-attack three years ago, some Estonian authorities alleged Russian government officials were behind the offensive, aided by individual hackers and criminal groups using networks of computers similar to those infected by Koobface.

But there is no global cybercop for the digital world. In fact, there exist few concrete mechanisms for stopping and prosecuting cybercrime networks, or mediating the virtual arms race.

It would seem a golden opportunity for Canada to take a leadership role, given the country's reputation as a neutral party, an honest broker in the world's most bitter political disputes. Some of the most talented cybercrime sleuths in the world operate out of Canada, and the country already wields significant influence within the groups charged with the Web's technical upkeep and maintenance.

But as countries such as the United States have built entire agencies to begin deal with the new realities of digital security, Canada has remained largely silent - unwilling to take any sort of position of leadership on the subject, and so far unable to even develop a comprehensive cybersecurity policy.

The rise of digital warfare and cybercrime creates several uncomfortable questions, the answers to which have the potential to reshape how every Canadian experiences the Web. So far, the Internet has succeeded because of its openness, its ability to transcend national borders and, to some degree, because of our ability to use it anonymously. But are those days numbered? Are we destined instead for a Chinese Internet, a Russian Internet, an American Internet - with each country playing by vastly different rules? What role should Canada play in attempting to save the Web as we know it?

EARLIER THIS YEAR, one of the biggest law firms in Canada came under attack. Staff members began receiving e-mails that appeared to be from one of the firm's partners, who was working on a major international M&A deal. The e-mail's author cited confidential details of the deal, and instructed recipients to open an attached file.

The file turned out to be a form of malware, giving the e-mail's real author access to the infected computers. When the law firm began investigating the incident, 20 computers were believed infected. The investigation eventually turned up 500 infected machines.

The law firm contacted a Toronto-based company called Digital Wyzdom, which specializes in investigating such attacks. Daniel Tobok, Digital Wyzdom's President, says his firm soon traced the attacks to an alarming source - the malicious e-mails originated from government servers in Asia. Indeed, the servers belonged to the government of the nation where the deal was taking place - and that government opposed the deal. (Mr. Tobok would not identify his client or the nature of the deal).

Two years ago, Mr. Tobok says such cases - in which a foreign government played a part, or appeared to play a part, in a cyber attack - made up about 1 to 5 per cent of Digital Wyzdom's business. Today, it makes up 10 to 15 per cent of cases.

"Governments are starting to realize that this is a vehicle for making things happen," Mr. Tobok says of such government-assisted cyber attacks.

"Honestly, unless criminal charges are pressed or our government gets involved through political channels, there's not much that can be done about it."

Malicious Web traffic is nothing new. What has been changing is the extent to which nations - rather than just individual criminals or groups - are utilizing what some analysts describe as the "dark web." The United States, for example, alleges that the Chinese military is behind a series of attempts to steal classified information from U.S. government computers dating back to 2003.

Perhaps the most famous example in recent years was the cyber attack on Estonia in April, 2007, which is alleged to have originated from Russia. The two nations were in the middle of a political dispute at the time, which appears to have spilled over into full-fledged cyber warfare. The attacks on Estonia infrastructure ranged from individual attackers employing fairly basic techniques, to massive networks of infected computers, similar to those infected by the Koobface malware, that were essentially rented out and temporarily repurposed as offensive weapons in a cyber war. The attacks appeared aimed at shutting down much of Estonia's critical infrastructure, from telecommunications networks to banks to broadcasters.

The Estonian incident was perhaps the highest-profile illustration not only of the disruptive geopolitical power of the Internet, but the growing overlap between the interests of petty cyber-criminals, organized crime and foreign governments.

"The next world war will likely happen in cyber space," says Hamadoun Touré, secretary general of the United Nations' International Telecommunications Union. "And we all know that the best way to win a war, any war, is to avoid it in the first place."

Mr Touré should know. The ITU is at the heart of a growing push to fundamentally change the way the Internet is governed - a push that would not only affect the influence countries such as Canada are able to exert in the digital world, but also the way every person on Earth experiences the Internet.

Today, the Internet is governed, in large part, by a private corporation. It's called the Internet Corporation for Assigned Names and Numbers, a California-based non-profit charged with handling tasks such as approving domain suffixes such as .ca for Canada, as well as myriad other technical and policy issues.

However, the next billion people to hop on the Internet will be from places such as Nairobi and Mumbai, not California. And increasingly, governments are pushing to replace ICANN - a group historically aligned with the U.S. Department of Commerce - with a UN-style body in which multiple nations have a direct say in how the Internet is run. A clear front-runner has emerged to serve that purpose: the ITU. [Read the op-ed [http://www.theglobeandmail.com/news/national/time-to-lead/internet/do-we-really-want-iran-or-china-in-charge-of-the-net/article1796415] by Canadian Internet Registration Authority President and CEO Byron Holland on the subject]

At the ITU's most recent conference, which wrapped up last month in Guadalajara, Mexico, Russian delegates proposed a motion that would see ICANN's government advisory council replaced with a UN-approved body. The move was seen as a first attempt to shift control away from ICANN and toward emerging powers such as Russia and China.

On the surface, the optics seem to favour the ITU over ICANN - that a multilateral, UN-style body, instead of a US-based private corporation, run the world's most important communications network. However the potential for such a shift has caused ripples of concern across the global digital community.

"Iran, Syria, Russia, China, Saudi Arabia, The United Arab Emirates - that's who will be starting to drive the bus on [Internet policy]," says Byron Holland, President & CEO of the Canadian Internet Registration Authority, the group responsible for managing Canadian domain names. "Most Canadians would be very concerned about those countries shaping and directing the Internet."

Mr. Holland's implication is clear: should countries such as the UAE - which recently threatened to block Research In Motion's BlackBerrys from the country unless the Canadian firm gave local authorities more ability to monitor communication on the devices - have a greater say in how the Internet is run, Canadians and other users who have become accustomed to a free and open Internet may see their Web experience diminish, as more authoritarian nations attempt to expand government's control over the communication medium.

In effect, the balance of Web freedom will shift closer to the sensibilities of countries such as Iran, where censorship and eavesdropping is widespread, and away from countries such as Canada, Mr. Holland contends.

At the heart of the dispute is a pivotal question: should the countries responsible for the majority of the Internet's new citizens have a greater say in how the Internet is run?

Perhaps no nation is better positioned to play a vital role in resolving the issue than Canada. But until recently, Ottawa has largely viewed the Internet through the prism of business, rather than as a security or wider policy issue.

"Canada's response had been shaped by the fact that, until the very recent past, Canada's participation in global Internet governance was through Industry Canada ... which is fairly narrow in terms of focus," says Rafal Rohozinski, president of the SecDev Group. "You didn't have [Foreign Affairs] looking at the Internet commons as a policy issue, you didn't see and real kind of coordinated effort. I think that's starting to change."

For Canada, recreating its reputation as a geopolitical broker in the digital realm is far more than an altruistic policy goal. There are serious issues at stake, says Mr. Holland, such as freedom of information and limits on government's ability to collect information. Under the current system, Canada already has some say. For example, Heather Dryden, a Canadian representative, currently chairs ICANN's governmental advisory committee.

That's perhaps why Helen McDonald, an assistant deputy minister with Industry Canada and Canada's representative at the ITU's Guadalajara conference, issued what was seen as a relatively strong-worded objection to the Russian proposal.

"The Union must avoid the temptation to dilute its impact by seeking authority over issues that are being addressed appropriately by other organizations," Ms. McDonald said, according to a transcript.

What remains to be seen, however, is how steadfastly Canada is prepared to hold its position, as nations such as China and Russia push for greater control of the Internet.

Ultimately, what's at stake in battles such as those between ICANN and the ITU is what Mr. Rohozinski describes as the "Balkanization of the Internet." Should countries such as China not get their way when it comes to Internet governance - and, indeed, even if they do - Internet users in Canada and around the world face the prospect of the Internet being bordered up along real-world geographic lines.

The potential implications are profound: the introduction of tariffs for viewing content in certain jurisdictions; the imposition of strict rules for major technology companies wishing to operate in certain countries - something RIM recently experienced in India and the Middle East, and that Google has grappled with in China. For a country like Canada, which is built on a multicultural model that renders vital the ability of citizens around the world to communicate with one another, Mr. Rohozinski argues such an outcome would be disastrous.

"What Canada needs to recognize is that this country has benefited immensely from cyberspace," he says. "Our values are propagated through cyberspace."

IN LATE OCTOBER, Mr. Villeneuve of the Citizen Lab at the University of Toronto began trying to take down the Koobface network. [Read Ron Deibert and Rafal Rohozinski's op-ed [http://www.theglobeandmail.com/news/national/time-to-lead/internet/the-untouchable-hackers-of-st-petersburg/article1795650] on trying to crack the Koobface code]

It was slow and somewhat fruitless work. Without a robust mechanism in place for dealing with such networks - for example, a standard means of reporting criminal activity in cyberspace - Mr. Villeneuve was forced to contact individual Internet service providers and Web sites around the globe, informing each one about the malicious traffic that had been found on the networks. The list of Web sites that had at one time or another been compromised was vast and widespread - at one point, the Web site of the attorney general of Ontario had been compromised, among many, many others.

From his research, Mr. Villeneuve has collected an impressive amount of information about Koobface, including the cell phone numbers of its authors in Russia. However, he is not optimistic about the chances of shutting it down.

For one thing, the network is highly decentralized, and it would take the efforts of multiple companies and law enforcement agencies in at least three countries to shut down the main command and control infrastructure. Even then, short of arrest, there's nothing stopping the Koobface authors from simply setting up shop elsewhere in the world.

But perhaps the most frightening aspect of Koobface and other such networks is just how difficult it is to prove a crime has taken place. Police investigators usually need a victim to prove it, and in the case of Koobface, individual users were essentially being robbed of nothing, simply misdirected. If anything, the Koobface authors were robbing Internet advertising companies, but only to the tune of fractions of a penny per click. Even though the total amount collected was in the millions, the individual thefts were tiny.

It is those attributes - the ability to control computers around the globe, to reach across borders with ease, to operate in manner that makes prosecution extraordinarily difficult - that make networks such as Koobface the future of digital crime, corporate espionage and even state warfare. Indeed, Mr. Villeneuve is unsure Koobface will ever be fully shut down, or if the legislation and will exist to prosecute its authors.

"Is what's going on here unethical? Definitely," he says. But is it a crime that any current law can stop? "I'm not sure."