

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Cyber-Security at a Frantic Time: A Rational Plan

by Hugh Segal

July, 2017

POLICY UPDATE

Cyber-Security at a Frantic Time: A Rational Plan

by Hugh Segal

CGAI Fellow
July, 2017



CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1600, 530 – 8th Avenue S.W., Calgary, AB T2P 3S8
www.cgai.ca

©2017 Canadian Global Affairs Institute
ISBN: 978-1-988493-48-0

Cyber-attacks from foreign, state, state proxy or non-state actors present a difficult challenge in a democracy where the government has a measure of accountability, but security and intelligence officials have some duty to confidentiality in protecting the country and its people. The press doesn't make this challenge easier. On the pretext of alerting the public to danger or for the less admirable reason of a fascination with new and glittery things, the press has a tendency to overstate the importance of some cyber-attacks whose impact is rarely existential. Controversies surrounding recent American and French elections have also added to a general unease and anxiety.

The broadly held view that all of industry, the economy, government, the military and the very future of civilization itself are utterly dependent upon the digital octopus, does not help. Ubiquitous use of hand-held smart phones, which have more computing power than early space capsules, only adds to the mix of complacent reliance on these devices and sharp outbreaks of hysteria when some system is corrupted or hacked.

A number of factors contribute to a broad sense of angst and fear. These include recent developments, such as President Donald Trump's executive order to upgrade the U.S. government's cyber-defences, and assertions in Canada by private-sector U.S. cyber-defence branch plants that Canadian companies face exploding threats of cyber-attacks. Other factors include CSIS's statements in November 2016 that Russia and China are out to steal Canada's most important secrets, and a mandate letter for a new Minister of Democratic Reform to "lead the Government of Canada's efforts to defend the Canadian electoral process from cyber-threats".

In an era of the Phoenix payroll system failure, faith in the capacity of any Canadian government to get the defence of our cyber-networks right is less than robust. So too is the dither-path on fighter aircraft procurement or naval construction, and the frequent discussion of cyber-attacks having had variable, consequential impacts on diverse systems at the Canada Revenue Agency (CRA), the National Research Council (NRC) and elsewhere.

But the horizon is not totally dark. In corporate Canada, new definitions of cyber-literacy as part of the audit and risk management processes are very much in view. Governments, audit firms and business schools are engaging on the cyber-diligence and management file. Independent, peer reviewed, and deeply competent Canadian research organizations, like the Citizen Lab at The University of Toronto, produce and publish superb work on the hacking world and cyber attack organizations in places like Romania, Israel and elsewhere. These organizations sell their services to governments and non-state actors – not all of whom are friendly or respectful of rights to privacy and freedom.

Canada needs a rational measured approach that combines technical acuity, public education, some regulatory refinement, and a coherent and steady focus on defence, interdiction, prevention and enhanced awareness. In that context, recent developments should be kept in perspective.

It is now publicly asserted that Canada's NATO deployment to Latvia is aware of and preparing for the likely deployment by Russian cyber-forces of a series of cyber- and digital hacking schemes. Their goal is to disrupt digital communications between NATO forces and create false narratives and "disinformatia" – alleged news and social media stories seeking to portray Canadian and other NATO troops in the most disreputable way possible.

As part of the lead-up to substantive China/Canada trade talks, cyber security is on Canada's agenda just as it was when the US and the UK recently concluded "cyber non-aggression" pacts with China. In fact, Canada and China concluded a non aggression agreement re cyber attacks on commercial data in the last week of June, 2017. (It is one of the joys of modern diplomacy that the Chinese can conclude agreements not to continue doing what they have always denied doing in the first place.)

Canada has also announced and put into place a national cyber-security strategy that CSIS, Communications Security Establishment Canada (CSEC), and Public Safety Canada are advancing and deepening. By focusing on securing government systems, partnering with the private sector to secure Canadian cyber-systems outside of government, and promoting rational rules of the road for Canadians to be more secure online, the strategy seems grounded if not spectacular. Some in the private sector seek more government leadership and standard-setting, while others, reflecting perhaps legitimate angst about bureaucratic and political government layers, prefer less government involvement.

One of the challenges for government and the private sector in this area should be familiar to military and intelligence planners and practitioners. One needs to say enough to sustain one's own forces' confidence and deter the enemy. However, this must be done without actually revealing the precise mix of technologies, strategies, intelligence and security options available to deter or attack the putative predators – be they military, foreign power, private profit-seeking, terrorists or simply those interested in ransom-ware or political intimidation.

There is a short set of operating principles that, if adopted by Parliament and the government, would not only enhance public understanding of the genuine nature of the risk, but also increase the anticipatory, intelligence and preventive capacity of our private and public sectors in the cyber-combat world:

1. Perspective:

Beyond the actual damage cyber-attacks can do to critical military, civilian and information infrastructure, the enhanced impact of wildly overstated reports of the risks and damage done should not only be discouraged but quickly countervailed. As in the case of terrorist events, however tragic and horrible, they are rarely existential in threat or impact and the wild overstatement of their import can add to the damage to public confidence and trust.

Ubiquity in a free society often produces excess. From the sexual revolution of the 1960s, to the increased use of alcohol after Prohibition, to the broad take-up of tobacco decades ago, societies have had to cope with the negatives that emerged with greater freedoms and uses. A mix of access-limiting (especially for younger people) legislation, public education, enhanced medical diagnostics, civil litigation, regulations about inappropriate places for public consumption, varying tax regimes and engagement on illegal smuggling all conspired to get excess tobacco consumption down and cancer rates diminished.

Training for barkeeps, tough laws, public education on drinking and driving, clear statements about percentage of alcohol by volume in different drinks, rules on advertising aimed at young people and tougher enforcement regimes around zero tolerance all conspired to reduce impairment and the broad incidence of alcohol poisoning.

A strong focus on the challenges associated with sexually transmitted illness, the promotion of safe-sex practices and education aimed at teenagers also contributed to progress, as well as firm zero tolerance laws around sexual assault.

All of these initiatives that addressed the dangers of excess or impropriety contain hints that will help in shaping a rational and national cyber-defence capacity appropriate for a democratic non-police state country.

2. Capacity:

While Canadian government and private-sector cyber-capacities to defend, repel, adjust and engage are impressive, complacency is unconstructive. Partners like Israel in both the public and private sector, and the University of Toronto's Munk School of Global Affairs' Citizen Lab, all have depth, acuity, flexibility and talent banks that are truly impressive. While the former face existential threats in their neighbourhood that exceed ours, the latter is strictly independent and works for no government or corporation. Canadian government officials would do well to reflect on how best to ensure we have comparable or better analytical and instrumental capacity in the agencies tasked with civilian and strategic cyber-defence.

The new National Security Act (C-59) proposes powers that go a long way to ensuring that CSEC has the capacity and the statutory base for a robust engagement with the private sector in a defence/preventive context. It provides the authority to engage in active measures against those abroad who would seek to penetrate, harm, hack or destroy vital Canadian cyber-networks fundamental to health, governance, police, transportation, infrastructure, logistics, energy and telecommunications in the private and public sectors.

3. Flexibility:

A cyber-trained and security-cleared intelligence officer in a Canadian military role, seeking to take his or her skills to another government department with cyber-security or intelligence mission priorities, faces unconscionable delays as existing security clearances are started anew at great cost of resources and time. This not only diminishes cyber-security and intelligence, but discourages outstanding and experienced talent. Fluidity with security-cleared defence and government ranks, embracing the Armed Forces, Special Forces, CSIS, CSEC, RCMP, Canadian Border Services, CRA, Global Affairs Canada and Public Safety Canada, is vital to sustain real-time capacity, and to encourage the best and the brightest to join. The very advent of cyber-communications and connectivity is about getting around undue formality and bureaucratic barriers. No active defence in support of cyber-security can be effective if these barriers impede real-time and technologically adept engagement.

4. Democratic Oversight:

Cyber-attacks on Canada aim to dilute public confidence, steal corporate data and private research depth, and weaken the operational capacity of, or destroy, communications infrastructure. However, the net purpose is really the destruction of public confidence, trust and belief in the legitimacy and value of the very core data sets that underpin our democratic society and way of life. This is about weakening democracy. Our defences against these threats must not be anti-democratic themselves. That is why C-22's proposals are vital, but imperfect. C-22 was signed into law in June 2017 and is the present government's version of legitimate democratic oversight for security and national intelligence services, plans, activities, operations and strategies. Before this law, and alone among the main NATO countries, Canada had no such link between democracy and the forces mandated to its protection. Regular legislative oversight, in-camera or otherwise, would go a long way to ensuring a core accountability and broad support for those working hard on the cyber-security file in the military and public service frame, as well as greater understanding of what challenges they face. The powers that C-22 entrusts to a newly created National Security and Intelligence Committee of Parliamentarians (NISCOP) have never existed in Canada. To the credit of the government and both houses of Parliament, this is a great step forward.

The National Security and Intelligence Review Agency (NSIRA), announced by the government in its C-59 proposed legislation, further increases the analytical capacity to oversee all areas of government dealing with intelligence and national security, replacing more robustly the old role of the Security Intelligence Review Committee. SIRC has served honourably with limited resources for some time. As the NISCOP is stood up over the next few months, and as the law establishing NSIRA proceeds through parliamentary discussion, there is an opportunity to develop a special operating frame relative to the role of each on cyber-security.

That oversight frame, combined with the enhanced measures proposed on cyber-defence for CSEC, reflects an excellent new departure. It could significantly enrich Canada's proactive,

analytical and balancing capacity to defend our national and commercial cyber-security and protect the core democratic values of privacy, rule of law and presumption of innocence basic to the Canadian way of life.

5. Collaborative Public Education:

In the same way as various industries, governments and civic organizations have launched constructive engagements with respect to important behavioural and information challenges, (financial literacy, drinking responsibly, disease prevention, smoking cessation, symptom recognition, consumer awareness, road safety, fire prevention and the rest), government should work with the high-technology industries to do the same. This would include hardware manufacturers, software creators and service providers, artificial intelligence designers and promoters, and key cyber-consumer industries such as banking, insurance, telecommunications, logistics, transportation, online merchants, energy, etc. The idea would be to shape constructive and engaged public education programs on what all Canadians can and should do to increase their own cyber-security awareness, protection and informed personal practices. This is not a new or radical departure.

The Y2K transition made it necessary to ensure the sustainability of a myriad of vital cyber-systems facing the risk of malfunction as a result of the millennial digital change from a one to a two in the year date. The private and public sectors invested massively at all levels to make the changes necessary to avert serious systemic interruptions that carried the full potential of harm. Establishing alternative server farms as back-up, and the entire notion of vital excess capacity that emerged as a strategic redundancy, contributed to the ability of most global cyber-systems in the financial world to survive the mass system and hardware destruction created by the 9/11 attack on the World Trade Center in New York City.

The proposed C-59 creates new powers with respect to cyber-defence while active measures contemplate government's ability to declare any private entity's cyber-networks to be of national interest, with the associated regulatory and other implications. The incentives for co-operation and collaboration on a host of fronts, including public education, are both reality-inspired and very much in the broad national, local, private and industry-wide interest.

Another creative option for a government that wished to advance public awareness and education on cyber-security would be the appointment of a minister of state for privacy and cyber-security within either the portfolio of the Minister of Public Safety, or the Privy Council Office. This new minister could lead, encourage, advocate and engage publicly on this society-wide challenge. This would be an opportunity for a younger and perhaps more cyber-savvy member of Parliament with constructive analytical and communications skills. Recent efforts by the Minister of Democratic Reform, along with the head of CSEC, relative to protective measures and practices being encouraged for the 2019 federal election, are a step in the right direction, but not sufficient by themselves.

Conclusion

Cyber-security is a societal risk in large measure because of the ubiquity of cyber-use by a large majority of Canadians, along with the corporate, police, institutional, commercial, government, educational and related organizations of all sizes and scope. The vast majority of these, even if targeted by malevolent artificial intelligence or cyber-predators, do not present a meaningful national security risk. However, many do. A federal strategy is not a simple single-faceted undertaking. It must keep pace with the changing and dynamic nature of that risk, and protect the required secrecy of some systems and the privacy exigencies of others, but with sufficient scope, depth, technical acuity, apprehensive intelligence and public support. If done properly, it will require the kind of co-ordinated large brushstroke strategy, multi-department and interprovincial co-ordination and broad socially collaborative outreach and posture reflective of the risk's true nature, with all its incumbent variations. It will also require a deeply determined breakdown of inter-departmental barriers and stovepipes that often slow the federal government's capacity to engage as effectively as its civil service and political leadership would wish.

When the enemy or putative predator is a foreign power, the relative low cost to them of cyber-attacks launched on Canada provides an asymmetric capacity to do genuine harm. This is true especially when the source country is unburdened by democracy, statutory accountability or any measure of domestic public debate produced by the work of a free press. Certainly, Russia, China, North Korea, Iran or Syria have reasons to de-stabilize and infiltrate Canadian cyber-systems for geopolitical or commercial gain. Non-state actors for commercial intelligence reasons, proxies for state actors and those seeking criminal or commercial gain have reasons as well.

The open nature of Canadian society and the wide availability of small, powerful devices that broaden the interconnections and vulnerabilities of the networks to which they are connected directly or through derivative linkages, are strategic targets of opportunity for those with criminal, subversive or exploitative intent, whether political, strategic or commercial. The kind of careful context and horizon analysis which fully sorts through the mix of intent and capacity relative to any prospective predator is important here, and a valid purpose for our intelligence services. The attributes associated with tolerant, pluralist and democratic societies present us with disadvantages when we engage with totalitarian governments and their proxies. However, our advantages remain compelling in dealing with key actors who are unaccountable to the rule of law, independent courts or the public, and who survive through the use of force, imprisonment and censorship.

The net benefits that freedom, open markets and the accompanying enhanced prosperity and opportunity create need not be sacrificed in the execution of a rational and effective cyber-defence. Non-democratic or terrorist foreign forces are seeking to catch up with or destroy what we have, however imperfect it may be. This is all the more reason to build our engagement and defence on the very values and attributes that define our way of life. In fact, to do otherwise would be a serious misstep.

About the Author

Hugh Segal is Master of Massey College, a Senior Fellow of the Canadian Global Affairs Institute and a senior advisor at Aird & Berlis, LLP. He is a former chair of the Senate committees on Foreign Affairs and Anti-Terrorism.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to the Institute.