We need a Minister of Everything… Cyber

BY

TIMOTHY GRAYSON

Cyber is an enormous economic opportunity. It is also an existential threat to our way of life. That confluence practically *begs* for a holistic response. Our federal government, recognizing these facts and having the power to structure an optimal national response, is pursuing a segregated approach. One that experience assures us will underwhelm.

Several departments have cybersecurity on their to-do lists (aka, PM's mandate letters), the only apparent connection being "cybersecurity" and the PM's expectations. In this circumstance especially, compartmentalized attacks will lead to cross purposes, excess spending, and a disappointing outcome. It is not sane.

Each department tasked to do *something* about cybersecurity will spend public money doing its own thing. Public Safety will explore fording defenses against cyberthreat. Science, Innovation and Economic Development will pursue cybersecurity as an economic sector to lift GDP. Since cyberthreat in the age of mobility, Cloud computing, and the Internet of Things means a threat to *everything*, all functions and departments of every government is affected. And all departments, never mind the provinces, will pursue their own policies and protections substantially independent of the others. Yet none will be sufficiently concerned about how its actions could be amplified by the others or *vice versa* (particularly Economic Development and Public Safety) to act holistically. They are hostage to departmental structure, budget, and politics.

But cybersecurity begs for the holistic approach that C.D. Howe ("the Minister of Everything") brought to Ottawa in the 1940s and 50s, particularly in guiding Canadian industry through and after World War II. Those were extraordinary times. Cybersecurity is an extraordinary circumstance too.

It is equally extraordinary because cyberthreat affects everyone: every individual or organization that uses mobility or the Internet in any way is a potential victim. The persistent rapid change means protecting oneself and the important structures (financial, critical, commercial systems and individual home networks/devices) is not yet normalized. So we can't anticipate and defend ourselves like we can from common, understandable threats. And, because the digital foundation is so pervasive, any tear in its fabric can destabilize our social and economic world.

On the other side of the coin, like revving up wartime production, the cybersecurity economy is exploding to counteract the evolving threat. Because it tracks the threat and expansions of the underlying technology, this industry has a hundred-year global growth path. Canadians have been ahead of the curve in critical areas like (quantum) encryption, and are poised to own the podium unlike any industry outside of natural resources.

The confluence of such great challenges: safety on the one hand and opportunity on the other… attributable to the same thing… is atypical. It calls for atypical measures.

Compartmentalize threat from opportunity and both will suffer because there is only so much money to go around. Risk of loss weighs heavier than opportunity for gain (justifiably in this situation), so a large but insufficient "cyber" budget will be targeted toward public safety. The amount left to pursue economic opportunity will be anemic because other priorities need support too. It will all be mediocre.

In short, we will not be safe and once again a "Canadian Century" of economic opportunity—to dominate cybersecurity globally—will fizzle, letting us get back to hewing wood and drawing water.

Institute X recently responded to the Public Safety Cyber Security Consultation. Rather than repeat data and air self-serving suggestions, our recommendations included the following. The government should:

- Set "unreasonably" high cybersecurity standards;
- Prefer procurement from Canadian firms, for national security sake;
- Help direct *collective* growth of the national cyber-security industry;
- Assign an independent, nationally focused body (like the National Institutes of Health Research: the *National Institutes of CyberSecurity*) to develop, implement, and manage a holistic national strategy.

We have one more recommendation for the Prime Minister and industry. Mr. Prime Minister: we need a C.D. Howe, "Minister of Everything Cyber." Industry: consider how valuable to Canadian cybersecurity development and to your own firm a strategy of having some of your best and brightest business people be 21st-century dollar-a-year (wo)men to make the Canadian industry globally dominant before splitting the spoils.

XXX

Institute X's submission paper is available here: http://bit.ly/2elxTbs

Institute X is a (technology) transformation consultancy and think tank. Timothy Grayson writes and lives near Ottawa, Canada. Find him at tim@institute-x.org @graysonicles