Rideau Institute
November 2017

The Cyber Domain and the Canadian Defence Policy Review

Amb. (ret'd) Paul Meyer

INSTITUT RIDEAU INSTITUTE

rideauinstitute.ca

The Cyber Domain and the Canadian Defence Policy Review

By Amb. (ret'd) Paul Meyer

Cyberspace is a term used to describe the global system of networked computers that provide for information and communication exchange, of which the Internet is the most prominent embodiment. It is a relatively recent, human-made environment on which global society has become increasingly dependent. How this unique environment is to be used and developed is a matter of current policy and practice.

Terminology is important, especially when one is seeking clarity about a new phenomenon or subject matter such as cyberspace that has only recently arisen. Considering what activities states and non-state actors might undertake within cyberspace were rightly an element for a defence policy review. The policy review decision to reference "the cyber domain" already suggests that this special environment is being considered a "domain" for military action alongside the traditional military domains of land, sea and air.[i] This is taken as a given rather than as a proposition to be debated and perhaps put to the public for consideration. Is it in the national interest to see an environment overwhelmingly owned and utilized by civilians accorded the status of a battleground? Could alternatives to inter-state cyber conflict be devised and championed by DND and the Government?

These are questions never apparently considered in the review process. We are told instead that our government, military and private sector are all vulnerable to "state-sponsored cyber espionage and disruptive cyber operations" and that this threat "can be expected to grow in the coming years".[ii] Of course, the planners are on solid ground with this forecast as the threat is certainly likely to grow if countries like Canada begin to engage in such actions. Indeed, developing the capabilities for just such disruptive external cyber action appears to be the chief policy advance proclaimed in the review.

DND having up to now spent its efforts primarily on cyber security defence, the review asserts (with no evident substantiation for the determination) that this "purely defensive cyber posture is no longer sufficient" [iii]. Capabilities to conduct "active cyber operations" against external threats to Canada will be developed in addition[iv]. The tendency to employ euphemisms in discussing cyber security action is in evidence here. The reader of the review might be puzzled by the exact nature of these "active cyber operations" except for a more candid reference later in the review to the development by the Canadian Forces of "offensive cyber operations capabilities able to target, exploit, influence and attack in support of military operations".[v] It seems clear that the intent of the Canadian Armed Forces is to develop a capacity to attack via cyber means. The "in support of military operations" suggests that offensive cyber actions would only be undertaken as part of wider conventional military operations, rather than standalone cyber attacks, but this apparent constraint on the employment of offensive cyber capabilities is unclear.

The review does offer up assurances that "cyber operations will be subject to all applicable domestic and international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments".[vi] This assurance might have greater weight if there were generally recognized international legal norms applicable to state conducted cyber operations, but this is currently something of a 'grey zone' with no universal standards in place. For example, what type of restraints might apply to offensive cyber operations in peacetime and what would govern such actions during armed conflict is a matter of international debate. This debate similarly extends to whether a damaging cyber attack can be equated with the "armed attack" that under the UN Charter can justify a state exercising its right to self-defence. Of course, the UN Charter also prohibits the threat or use of force without UN Security Council authorization (except in self-defence against an armed attack). Accordingly, there are also legal and political uncertainties as to whether a disruptive or damaging cyber operation would constitute a "use of force" and as such whether such an operation would be incompatible with UN Charter compliance. [vii] These are truly unchartered waters reflecting the fact that cyberspace is a novel environment that is largely without an internationally agreed governance framework.

If the claim that international law will apply to these new military cyber capabilities is less than compelling there is an assertion in the policy document that due national controls will be applied. The review states that the employment of an offensive cyber capability "will be approved by the Government on a mission-by-mission basis".[viii] While this may provide some reassurance that civil control of the military and relevant legal safeguards will be applied to cyber operations that go beyond defending one's own systems, it ignores the issue of whether engaging in offensive cyber action is really in the national interest or whether the costs of so doing actually outweigh the benefits. Unfortunately, this is an examination of options and a national debate that has not been held by politicians or public alike. The nature of existing and potential offensive cyber operations has been largely kept under wraps and hidden from public scrutiny. Part of the reason for this is the origin of much state-conducted cyber operations in intelligence agencies, an eternally shadowy realm not noted for its transparency.

The armed forces normally function in a somewhat more open fashion with the acquisition of new weapon systems and the establishment of new operational doctrines usually subject to consideration by both political leaders and citizen taxpayers. Regrettably the "militarization" of cyberspace has developed apace in recent years without the benefit of transparency and considered approval by democratic governing bodies. The military has found the mantle of secrecy surrounding action in this new environment as convenient as have the intelligence agencies which has enabled an almost "stealth" development of cyber activity as a distinct weapon of war and not simply an enabler of military operations. The billions of "netizens" who benefit from the relatively unimpeded operation of the Internet and other networked systems of cyberspace were never polled on whether they agree with turning this space into just another domain for "war-fighting". Given that the overwhelming ownership and utilization of cyberspace belongs to the private sector and civil society, one might have expected (at least in democratic states) that the government would consult with these stakeholders before taking steps that could gravely compromise the integrity of this environment.

This “militarization” of cyberspace and the subtle, if insidious move from a former focus on cyber defence to the acknowledgment and then trumpeting of offensive capabilities has largely been the work of states other than Canada. This cyber realm is all too vulnerable to irresponsible acts on the part of states and non-state actors alike. No state may have claimed responsibility for the “Stuxnet” cyber payload that destroyed centrifuges at an Iranian uranium enrichment facility, but this act constituted a “weaponization” of the underlying technology for information exchange and hence created a dangerous precedent for similar state action in future. It is chilling to recognize that just as this “Stuxnet” payload, as sophisticated as it was, managed to escape its controllers and spread globally, so has the more recent, state sponsored cyber attack against Ukrainian entities wreaked havoc far afield from its putative target. If the leading cyber powers can’t seem to restrict their cyber weapons to targeted military objectives, how much more successful will be the second and third tier armed forces as they begin to exercise “active cyber operations” abroad. [ix]

The Canadian Armed Forces are understandably responding to trends being set by bigger powers in investing in the cyber security realm, but do they need to mirror problematic steps simply because “Big Brother” has done so? No one will contest that providing for a high degree of cyber security to protect your systems from external intrusion is warranted. By reducing your vulnerability to exploitation through strong cyber defences you are denying an intruder the potential gains (in intelligence or disruption) of a clandestine cyber operation. In this regard, the indications in the review document that DND and the Canadian Forces will enhance their cyber defences are to be welcomed. References to establishing a “Cyber Mission Assurance Program” that will ensure cyber security considerations are incorporated into the procurement process would be a prudent step to take as would the development of internal cyber situational awareness and threat identification capabilities.[x]

Cyber security requires knowledgeable and skilled staff and it is only appropriate that DND would be addressing how best to acquire and sustain such individuals through recruitment and personnel policies. The designation of a “Canadian Armed Forces Cyber Operator” occupation category may be a necessary step if a viable career stream is to be developed for this special field of expertise. Drawing on relevant skill-sets available in the Reserves is another logical measure to build-up cyber security capabilities within the military. These steps would be useful without making the transition from a posture of cyber defence to one of cyber offense. The probable consequences of a focus on offensive cyber operations, intended or unintended, are likely to be more damaging to Canada’s national security broadly understood than they would be beneficial. Exacerbating the damage that state conducted cyber operations can cause to the peaceful use of cyberspace is not an appropriate aim for Canada’s foreign or security policy. There are far better ways for our financial and human resources to be employed.

However attractive it may appear to some in the military establishment to emulate certain major cyber powers in the development of offensive cyber capabilities, we are on firmer ground in seeing to our defences while promoting responsible state conduct in this crucial if vulnerable sphere on which our global well-being is increasingly dependent. It is striking that

the cyber section of the defence review has no equivalent to the commitment set out in the outer space section: "We actively support Global Affairs Canada's participation in international diplomatic efforts to ensure that space does not become an arena of conflict".[xi] Surely cyberspace is equally deserving of diplomatic efforts (with active DND support) at conflict prevention and the promotion of international cooperation.

Canada should be an advocate of developing norms and arrangements to preserve the peaceful nature of cyberspace rather than "piling on" with those states ramping up offensive cyber capabilities. Canada should be part of the solution to the challenge of conflict prevention in cyberspace rather than contributing to the problem. The language of the review at times suggests a certain confusion as to the strategic implications of crossing the threshold of offensive cyber actions. The review proclaims that Canada "will assume a more assertive posture in the cyber domain…by conducting active cyber operations against potential adversaries…". [xii] The reader can't but wonder if the military recognizes that the surest way of turning "potential adversaries" into real ones is to subject them to cyber assault. The Canadian Government and military would be better advised to stick to a focus on enhancing cyber defence capabilities and the exercise of restraint in this new realm until a clearer international governance regime emerges, one that recognizes the overriding interest of humanity in preserving cyberspace for peaceful use.[xiii]

---

[i] *Strong, Secure, Engaged: Canada's Defence Policy* DND June 2017 pg 56
[ii] Ibid pg 56
[iii] Ibid pg 72
[iv] Ibid pg 72
[v] Ibid pg 41
[vi] Ibid pg 72
[vii] For a good examination of the legal issues surrounding cyber attacks see Ido Kilovaty, "Virtual Violence-Disruptive Cyberspace Operations as 'Attacks' under International Humanitarian Law" *Michigan Telecommunication and Technology Law Review* Vol 23 Issue 1, 2016
[viii] *Canada's Defence Policy* pg 72
[ix] For an excellent history of the development of offensive cyber operations in the United States see Fred Kaplan, *Dark Territory: the Secret History of Cyber War,* 2016.
[x] *Canada's Defence Policy* pg 73
[xi] Ibid pg 71
[xii] Ibid pg 15
[xiii] For an alternative vision of cyber peace see the author's "Cooperative Measures for International Cybersecurity" in *Reintroducing Disarmament and Cooperative Security to The Toolbox of 21st Century Leaders,* D.Plesch, K. Miletic and T.Rauf (eds) 2017,www.sipri.org