UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY PUBLICATIONS

SPP Briefing Paper

Volume 12:17 June 2019

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

CYBERATTACK: WHAT GOES AROUND, COMES AROUND*

RISKS OF A CYBERATTACK STRATEGY

Ken Barker

SUMMARY

The Canadian government is now openly discussing the possibility of making cyberweapons part of its official national defence strategy. The new development was revealed in a recent government white paper, entitled "Strong, Secure, and Engaged" (SSE), which outlined defence policy across a wide range of activities. Specifically, the paper discusses working toward a "more assertive posture in the cyber domain by hardening our defences, and by conducting active cyber operations against potential adversaries in the context of government-authorized military missions" with an explicit commitment to developing cyberattack capabilities. This direction not only opens up new possibilities for Canadian defence, it could also represent significant new risks. Without good answers to the difficult questions this new direction could raise, the country could be headed down a very precarious path.

Cyberweapons do offer unique benefits. Since they tend to be far less costly to deploy than kinetic weapons — such as missiles, bombs and guns — they can level the playing field between richer, stronger states and weaker, poorer ones. Larger states may even be at further disadvantage by relying on larger, more sophisticated computer systems that could become a liability if successfully

* This research was financially supported by the Government of Canada via a partnership with Western Economic Diversification.

attacked. However, to date, countries have been reluctant to deploy cyberweapons in lieu of kinetic weapons. Furthermore, in those cases where cyberweapons appear to have been used by state actors, no state has accepted responsibility for using them. The Stuxnet virus used to cripple Iran's nuclear research equipment is a prime example: Israel and the U.S. remain the primary suspects, but both deny involvement.

Cyberweapons also possess risks of unintended consequences that can make the unintended consequences of kinetic weapons seem trivial. Notably, cyberweapons have a much greater potential to impact targets that were not intended by the attacker. For instance, when a virus-like computer weapon is unleashed on the Internet to exploit vulnerabilities in certain system software in a target country, there is a real possibility that the virus could also infect and damage computer systems inside the attacker's own country that use the same software, or even infect the software of allies who use the software. It is also possible that the weapon could have unintended consequences within the target country, by infecting other systems that were never meant to be targeted and causing more collateral damage than expected. Launching a cyberweapon to disable an enemy's supply-chain computer systems and accidentally infecting its nuclear systems, setting off a nuclear incident, is a terrifying scenario. It might even rise to the level of a war crime. It is worth noting, however, that there are no international treaties governing the use of cyberweapons. If Canada engages in cyberwarfare without one, there will be no formal limits on what actions are acceptable and what actions are not.

Indeed there are many discussions that still must be had within Canada and beyond to mitigate the risk of pursuing cyberweapons. The mere act of announcing someday that we are developing cyberweaponry (which, to be clear, Canada has not done) will already carry risk, suddenly making Canada suspect in future unattributed attacks, and perhaps enticing other countries to disguise their attacks by routing them through Canada. It is unclear even whether a prime minister or Parliament will be qualified to safely declare cyberwarfare, given its technical complexity. These are just some of the debates we need to have before Canada decides to embark on developing cyberwarfare capabilities. Now is a good time for those debates to start.

UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY PUBLICATIONS

SPP Briefing Paper

Volume 12:17 June 2019

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

CYBERATTAQUES : QUI SÈME LE VENT RÉCOLTE LA TEMPÊTE*

LES RISQUES D'UNE STRATÉGIE DE CYBERATTAQUE

Ken Barker

RÉSUMÉ

Le gouvernement canadien parle maintenant ouvertement de la possibilité d'intégrer les cyberarmes dans sa stratégie de défense nationale officielle. Ce nouveau développement est révélé dans un récent livre blanc du gouvernement, intitulé « Protection, sécurité, engagement » (PSE), qui décrit la politique de défense pour un large éventail d'activités. Plus précisément, le document aborde la question d'une « posture plus délibérée dans le cyberdomaine en renforçant nos défenses et en menant des cyberopérations actives contre d'éventuels adversaires dans le contexte de missions militaires autorisées par le gouvernement », avec l'engagement explicite de développer une capacité de cyberattaque. Cette idée ouvre non seulement de nouvelles possibilités pour la défense canadienne, mais elle pourrait également présenter de nouveaux risques importants. Sans réponses aux sérieuses questions que cette nouvelle idée peut soulever, le pays risque de s'engager sur une voie très précaire.

Les cyberarmes offrent des avantages uniques. Puisqu'elles sont en général moins coûteuses à déployer que les armes cinétiques – contrairement aux missiles, aux bombes et aux armes à feu –, elles pourraient permettre d'égaliser les règles du jeu entre les États plus riches et forts et les États plus faibles et

* Cette recherche a été soutenue financièrement en partie par le gouvernement du Canada via Diversification de l'économie de l'Ouest Canada.

http://dx.doi.org/10.11575/sppp.v12i0.56877 www.policyschool.ca

pauvres. Les plus grands États pourraient même se trouver encore plus désavantagés car ils s'appuient sur des systèmes informatiques plus grands et plus complexes, lesquels peuvent devenir un véritable problème s'ils sont attaqués. Cependant, à ce jour, les pays se sont montrés réticents à déployer des cyberarmes à la place des armes cinétiques. Qui plus est, dans les cas où des cyberarmes semblent avoir été utilisées par des acteurs étatiques, aucun État n'en a accepté la responsabilité. Le virus Stuxnet employé pour paralyser le matériel de recherche nucléaire iranien en est un excellent exemple : Israël et les États-Unis restent les principaux suspects, mais tous deux nient toute responsabilité.

Les cyberarmes présentent également un risque de conséquences non voulues, à côté desquelles les conséquences non voulues des armes cinétiques peuvent sembler dérisoires. Notamment, il y a beaucoup plus de risque avec les cyberarmes de toucher des cibles qui n'étaient pas prévues par l'attaquant. Par exemple, lorsqu'un virus informatique est lâché sur Internet pour exploiter la vulnérabilité de certains logiciels de base dans un pays cible, il y a une possibilité réelle que le virus puisse également infecter et endommager les systèmes informatiques du pays de l'attaquant qui utilisent le même logiciel, ou même infecter le logiciel d'alliés qui utilisent ledit logiciel. Il est également possible que l'arme ait des conséquences inattendues dans le pays cible, en infectant d'autres systèmes qui n'ont pas été visés et en causant plus de dommages collatéraux que prévu. Lancer une cyberarme pour désactiver les systèmes informatiques de la chaîne d'approvisionnement d'un pays ennemi et infecter par mégarde ses systèmes nucléaires, déclenchant un incident nucléaire, est un scénario terrifiant. Cela pourrait même être qualifié de crime de guerre. Il convient toutefois de noter qu'il n'existe pas de traités internationaux régissant l'utilisation des cyberarmes. Si le Canada s'engage dans une cyberguerre en l'absence de traité, il n'y aura pas de limites officielles pour déterminer si ses actions sont acceptables ou non.

En fait, de nombreuses discussions doivent avoir lieu au Canada et ailleurs pour atténuer le risque des cyberarmes. Le simple fait d'annoncer un jour que nous développons des cyberarmes (ce que, pour être clair, le Canada n'a pas fait) comporte déjà des risques, et rend soudainement le Canada suspect pour d'éventuelles attaques non attribuées. Cela incitera peut-être d'autres pays à dissimuler leurs attaques en les déployant par le biais du Canada. On ne sait même pas si le premier ministre ou le Parlement ont la compétence pour déclarer en toute sécurité une cyberguerre, en raison de la complexité technique. Ce ne sont là que quelques-uns des débats qui doivent avoir lieu avant que le Canada décide de se lancer dans le développement de cyberarmes. Le moment est venu de commencer le débat.

The Canadian government recently introduced a defence policy white paper entitled "Strong, Secure, and Engaged" (SSE) (Canada-SSE 2017) outlining Canada's defence policy across a wide range of activities. The document uses the term "cyber" precisely 86 times in its 113 pages — the vast majority of the references are to identify it as an area of importance and challenge — but the intended purpose appears to be defining this as an area of strategic importance. The definition of the "cyber domain" (Canada-SSE 2017, 56) sets the issues in the wider context and very briefly describes how it fits within the military setting from a defensive posture. The white paper further discusses the threat to military assets and identifies other agencies such as the Communications Security Establishment, Public Safety Canada, Global Affairs Canada and Shared Services Canada as partners in protecting Canadian cyber-infrastructure (Canada-SSE 2017, 72). The document also proposes some steps that should be taken to enhance our cyber capabilities, such as using reservists with specialized skills (Canada-SSE 2017, 69) and enhancing our cryptographic expertise (Canada-SSE 2017, 41), but remains largely silent on mechanisms. There is little doubt that these recommendations are necessary and this call to increase capacity in these areas is a step forward given modern threats in cyberspace.

One new factor in the SSE is the decision to assume a "more assertive posture in the cyber domain by hardening our defences, and *by conducting active cyber operations against potential adversaries in the context of government-authorized military missions*" (emphasis added) (Canada-SSE 2017, 15). Although these systems have likely been under development for many years within the Canadian military, the decision to openly develop active cyberattack capabilities and to openly signal that they could be potentially employed against adversaries is transformative.

This paper attempts to address questions around this transformative change by viewing them through a technological lens. Specifically, what are the intended and unintended consequences of a decision to publicly announce that Canada is condoning military-grade cyberweapons by developing them with the intention of using them against potential adversaries? This raises at least three separate questions that are addressed in this paper: (1) What are the consequences of deploying such weapons, for both the enemy and the state that deploys them? (2) What must be done to ensure that their use is in conformance with international law and the rules of engagement? (3) What are the consequences of condoning their development and by implication their deployment?

Unfortunately, we conclude the paper with a section entitled "Next Steps" because we do not have answers to all of these questions. Fortunately, the SSE document is a white paper and appears to be open for public discussion, so by taking some thoughtful next steps we may be able to avoid the most serious consequences of a decision to engage in cyberattacks.

Beyond the core elements of this paper, several overarching questions include defining under what circumstances cyberattacks should be permitted and what should be done to ensure they cannot subsequently be used against us or will not lead to harming

one of our allies. Canada's allies have already developed and deployed such weapons with some demonstrable success but with some unintended consequences. What can we learn from the available information about the safe use of cyberattacks and when is it reasonable to use such weapons? The nature of this technology is different than other forms of military aggression used in either peace or war time. What checks and balances need to be put in place to ensure that it is used only under appropriate government-authorized oversight? What protections can be put in place to ensure that the inadvertent release of a cyberattack cannot occur?

The decision to endorse the development a cyberattack capability introduces a difficult dichotomy. Cyberattack technology exploits discovered weaknesses in digital systems. In a regime that only permits cyberdefence activities, the discovery of weaknesses and deploying a repair for the discovered weakness is a consistent choice. However, if Canada is to incorporate a cyberattack strategy, the decision to repair the weakness must now be traded-off against exploiting the weakness against an enemy. These undiscovered weaknesses are known as *zero-day attacks* because a previously unknown vulnerability in a computer system (hardware or software) is exploited "on the same day" the vulnerability becomes known to the wider world.

This paper addresses several aspects of a decision to endorse cyberattacks in the SSE. Although this paper will consider the implications through a technical lens, it is not particularly technical, in that we consider what is possible rather than how it could be achieved. The scope that could be considered is exceptionally wide, so we begin by narrowing it to a more manageable one by defining the environment and terms (Section 1) and discuss/define the nature of cyberattacks (Section 2). We next consider the potential value of a cyberattack strategy in terms of the possible benefits and the utility in deploying these in a military context (Section 3), which is best considered as the intended consequences of such a strategy. The balance of the paper considers risks and consequences of a cyberattack-friendly policy both in terms of the technology itself and, to a lesser extent, the impact this will have on empowering adversaries to become more aggressive in their use of such weapons (Section 4), as well as other unintended consequences that may threaten our own infrastructure as a result of deploying such weapons (Section 5). We propose "next steps" that should be considered before, or in conjunction with, the decision to move forward with a cyberattack strategy such as that proposed in the SSE (Section 6).

1. ENVIRONMENT/TERMS (DEFINITIONS)

Security, privacy, attack, defence, war and any other physical activity occurring in the real world have specific definitions and implications based on the context where the term is used. The same is true in a *cyberworld*, but when a term is used within a military context, it is necessary to provide specific contextual definitions. Unfortunately, the connotations from both the physical and virtual worlds are often overlaid on the military context, so it is critical to provide specific definitions to avoid imprecision. We

assume that the definitions for these terms and their potential subtle connotations in the physical world vis-à-vis their military uses are not problematic, but we will provide more specificity when required.

The term cyberattack is used in several different ways in the literature. Most past work has focused on the protection of commercial and personal computers from what could be considered a high-tech form of crime using a computer. Thus, fraud, theft of data, theft of intellectual property, etc., using a computer or by attacking a computer is simply a modern version of criminal activity that has occurred throughout modern history. We do not consider "criminal" activity in this document except with respect to how it occurs in a military setting.

There are at least two potential kinds of participants in cyber-military activities. The first potential actor would be nation states (or states). Nation-state warfare has traditionally been waged between clearly identifiable states (or groups within a state in the case of civil war). The financial cost of waging war is extremely expensive, so historically the ability to go to war has been limited to known states with defined boundaries (or at least with claims to defined boundaries). Although undoubtedly occurring throughout history, the recent move to increased activities from non-state actors and the rise of international terrorism have expanded the scope of traditional nation-state warfare. The virtual world expands upon this recent trend where the combatants are not universally recognized state actors. ISIL, al-Qaida, and others (Denning 2011) do not exist as traditional states but are capable of engaging in warlike activities and with similar goals to those of nation states. The virtual world has expanded these groups' abilities significantly by allowing for fringe groups to engage in attacks on compute infrastructure. The potential for these virtual attacks becoming kinetic is an obvious consequence of the cyber aspects of these attacks. Although each group brings unique perspectives and challenges, the activities are similar and the potential consequences exist in both. However, as we will see, the non-state actors have much less at risk than traditional states if they engage in cyberattack activities because they have a relatively small set of assets that must be protected.

Cyberwarfare can be broadly defined as cyber-related activities, either defensive or offensive, undertaken by state or non-state actors intended to disrupt or influence normal operations undertaken by those being attacked (Theohary and Rollins 2015). This would include activities by *cybercriminals* and others, including a myriad of players that must ultimately be considered collectively. However, this document necessarily narrows the scope to consider the potential use of *cyberattack* by state-based military organizations. We do not limit our discussion solely to traditional military branches such as army, navy, air force and marines but rather consider a state's military activities more holistically, so espionage and military actions directed by a state intended to disrupt any target either military or civilian is within scope. Those who undertake these activities on behalf of a nation state are *cyberwarriors*, and these are distinct from other kinds of aggressive actors in cyberspace such as *cyberterrorists*, *cyberthieves*, *cyberactivists* (sometimes called *hacktivists*), or *cybercriminals* of various kinds (Theohary and Harrington 2015). *Cyberspies* may include non-state actors, such as in

the case of corporate espionage, but we will limit our use of this term to those activities undertaken on behalf of a state; but we could use the term cyberwarrior instead, given our more specific scope.

The *cyberweapons* used are constantly evolving, which makes it difficult to define precisely what tools are used to wage a cyberwar. An abstract definition for "(c)yber warfare … refers to conflicts that utilize cyberweapons or electronic weapons either offensively or defensively, or both" (Dycus 2010). Dycus is defining cyberwarfare in terms of the use of a particular kind of weapon, but this raises the question of what happens if the weapons change. Unfortunately, this requires an attempt to provide an exhaustive set of currently available tools that could include various kinds of malware, botnets, distributed denial-of-service attacks (Theohary and Harrington 2015), and any one of several other possible known attacks. If new, not-yet-enumerated weapons are developed, they would be precluded from the definition, so any consequences from that tool would, by definition, not be cyberwarfare. Thus, a definition of cyberweapon should mirror the definition of cyberwarfare in that it is a cyber artifact used either defensively or offensively by state or non-state[1] actors to disrupt or influence normal operations. The implications of this definition are that any defences used to protect state assets would be considered a part of the *cyberarsenal*, including firewalls, honeypots (Mairh et al. 2011), or any other tool associated with protecting critical cyber-infrastructure from SCADA (supervisory control and data acquisition) systems (Krutz 2006) to cloud services (Winkler 2011).

A key requirement to defining cyber-activities is to not limit its scope to impacts that are only felt in a cyber environment.[2] In short, we define cyber-activities as those that start and have an impact in the cyberworld and may impact on the physical world as well. A clear succinct definition that captures the essence of cyberattack is: "An act in cyber space that could reasonably be expected to cause harm" (Robinson, Jones, and Janicke 2015). Harm is defined beyond the virtual and includes any consequence that impacts on the object of the attack either directly or indirectly. A narrower definition that only considers the impact on computers or digital systems (software or hardware) is incomplete and does not truly reflect the potential for harms. However, a distinction is drawn between harms that only occur within a virtual world as distinct from those that also impact the physical world. These secondary consequences or harms are referred to here as *kinetic*. For example, an attack that only disables a computer system used for data analytics is not kinetic, although it may cause real harm; while an attack on the digital control systems of a nuclear plant that causes damage to the power generators is *kinetic* because it leads directly to physical harm.

---

1 Recall that we are not considering non-state attackers but they are included here to be consistent with the earlier definition of cyberwarfare and these actors would ultimately have to be considered in any holistic strategy.

2 "There is a difference between using information technology or cyber space as a domain to fight and fighting in the domain of cyber space." (Liles et al. 2012)

It is important to understand several other aspects of the cyber-theatre, including its unique mode of attack and the need to assess the intent behind the use of the weapon itself. As indicated above, cyberweapons can be deployed in two distinct ways. First, an attack can be direct with the goal of having an immediate effect. The hope is that the attacked infrastructure will be vulnerable when the weapon is deployed and the damage caused will be maximized, or at least most effective on its initial deployment. Alternatively, a cyberweapon can be planted into a victim's cyber-infrastructure with the hope of activating it at a later date when it will have the maximum effect. Kinetic weapons may also have both deployment modes in some limited circumstances, but planting a "bomb" stealthily is at best challenging, while embedding a latent piece of code within a large code-base is relatively simple and difficult to detect.

The definitions here are sufficient for our purposes but they would likely be debated by other commentators. With this caveat in mind, we now use this framework to consider the nature of cyberattacks and how they fit within the larger issue of cyberwarfare.

2. NATURE OF CYBERATTACKS

Truly kinetic weapons have a very specific life cycle in that they typically take many years to develop and a non-trivial amount of time to produce. During this time, thoughtful reflection can occur about their applicability and use, so by the time they become a viable weapon, the rules of engagement for their use has been carefully considered. Obviously, this cycle is shortened and the amount of thoughtful reflection undertaken during an active war is much less, but there is always a gap between a kinetic weapon's inception and its deployment in a theatre. The decision to deploy the weapon is also often carefully considered and the consequences of its use beyond its immediately apparent target can be evaluated both before and during its ongoing deployment. Finally, the consequences of using the weapon is almost always immediate and, once activated, those consequences are generally complete within a very short time frame. This life cycle also includes a careful consideration for how excess or unused weapons should be dismantled and disposed of in a safe way. Thus, a new missile will take years to design, develop and produce; it will remain a viable weapon for a protracted period and, when it is used, the consequences of its use will be fully executed almost immediately; finally, the decision to take it out of active use can occur immediately and a careful dismantling process can be undertaken to allow the remaining weapons to be safely disposed. Consequential issues, such as unexploded ordnance (e.g., landmines), are a part of the dismantling process, and although this may continue to have impact into the future, the scope remains limited and mitigation plans can significantly reduce this unintended consequence.

In contrast, the life cycle of a cyberweapon does not always include any of the long-term timeliness inherent in strictly kinetic weapons. The development of a cyberattack can occur in an exceptionally shortened period. Once developed, the cost and time required to replicate it or to "produce" it is negligible. The weapon is immediately viable but does require a strategy that allows it to be deployed. However, it is unclear

if this time frame is significantly different than the time required to deploy physical weapons into an active combat situation. The challenge in the virtual world is to find a suitable vulnerability at which to deploy the cyberattack, but once a weakness is identified, this can occur from any connected point on the web. Modern kinetic weapons can also be deployed through drones, but these still require the weapon be placed and deployed relatively close to its target. Cyberweapons can also be deployed well in advance of their use. Once developed, an attacker can wait for an opportunity at any time to place the cyberweapon into the opponent's cyber-infrastructure. Once placed, it can lay dormant until either an explicit command is issued from the attacker or when a set of conditions occurs that will signal the cyberweapon itself to activate. The latter case is analogous to placing bombs in an ally's command centre in case that state might become an enemy in the future. This would enable you to take out their command-and-control structure before the conflict even really begins. The effectiveness of the developed weapon can also be tailored or modified to allow for dynamic environments. Unlike a directly kinetic weapon that is essentially immutable after it has been produced, cyberweapons are often intrinsically modifiable. This allows them to be enhanced even after they are deployed and even modified while they are being deployed in the same way modern software is "upgraded" once installed on your computer system — although, in the case of a cyberweapon, permission from the owner would not be sought. A cyberweapon can also be altered to work on its target even if the underlying computer hardware is changed. Back-end compilers allow the attack functionality to be created independently of the actual hardware that it runs on. (Although some cyberweapons exploit vulnerabilities in specific hardware, many exploit software that is developed independently of its hardware platform.)

3. INTENDED CONSEQUENCES — POTENTIAL BENEFITS

Cyberweapons are developed for various reasons and each has an intended purpose. However, in all cases, the goals of these weapons can generally be defined based on the motivation of the developer and the potential benefits that might accrue as a result of their deployment. In the following, a number of potential benefits to the cyberattacker are considered, but there are undoubtedly many other hoped-for results. We continue to consider this from a nation-state perspective, but several of these motivations are also important to non-state actors.

1. Levels the field: Weaker states are less capable of launching kinetic attacks due to expense and logistics, but a cyberattack, although potentially costly to develop, is relatively inexpensive to deploy. Thus, a poorer state (or a non-state actor) can effectively engage in attacks on much larger more powerful and capable states.

2. Turns a strength into a weakness: Extremely powerful states typically have a large cyber-infrastructure supporting both their military and civilian organizations. By attacking these large-scale and diverse cyber-systems, a cyberattacker may be able to change a powerful state's apparent cyber-

advantage into a liability. It is well known that as there is an increase in the number of computing devices used so the likelihood of failures increases in proportion. Although the redundancy in larger systems affords some protection to ensure the key infrastructure remains available, a cyberattack exploiting specific vulnerabilities could lead to system-wide failure, thereby eliminating the anticipated benefits of redundancy to ensure availability.

3. Disrupt militaristic capacity-building activities: By engaging in cyberattack through various modalities, it is possible to disrupt or disable a potential enemy's ability to launch direct attacks (cyber or kinetic) in the future (Iasiello 2015). The 2010 Stuxnet attack on Iranian centrifuges is likely the best-known example, but other similar malware, more akin to cyberespionage, include Duqu, Flame, and Gauss (Bencsath et al. 2012).

4. Disrupt response capabilities at point of attack: Russia's military invasion of Georgia in 2008 occurred in conjunction (or at least concurrently) with distributed denial-of-service (DDoS) attacks on digital systems in the target country's public and private sectors, similar to cyberattacks against Estonia in the previous year. The goal of these attacks was to acquire control of the "information space" so the attacker could set the agenda and establish its voice as the only one providing information to those affected.[3]

5. Cyberweapon use during military actions: The potential benefit of cyberweapons in actual military conflict is currently only theoretical because it appears all governments are reluctant to choose or exploit this option if physical warfare is either underway or anticipated. Kaplan's work on the "secret" history of the U.S. military's use of cyberweapons provides several insights into the challenges of using cyberattack during direct military actions (Kaplan 2016), and also details the halting way the U.S. military and the wider U.S. government came to realize the potential of cyberattacks. Although there has been an increased interest in undertaking and using cyberactivities during non-war times, there appears to be a hesitation to exploit cyberactivities when things become kinetic. The military appears to prefer direct physical military actions to subtle and potentially (or at least perceived to be) less-effective cyberweapons. For example, in the 2011 Libya conflict, the U.S. considered using cyberattack to break down firewalls with the goal of disrupting military communications. However, U.S. commanders chose instead to use air strikes with conventional weapons to disable these installations kinetically. The U.S. is not alone in its reluctance to use cyberweapons when a kinetic option is available. For example, during the 2014 Ukraine-Russia crisis, Russia chose to use armed men

[3] Russia uses the term "information space" to describe what we are essentially calling "cyberspace" in this document. The distinction is primarily that "information space" emphasizes the desired goal of controlling "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure and the information itself" (Giles and II 2013). In any modern sense of the word, this is enabled, facilitated and implemented with what we are calling cyberspace and is built upon a cyber-infrastructure.

to physically cut and tamper with fibre-optic cables to disable telephone and internet communications. Given that the Russians had installed these systems and given their substantial knowledge of cyber-systems generally, it seems that an equally viable option would have been to use some form of cyberweapon to disable these communication channels without the need for direct physical military action.

In summary, the publicly documented examples of the use of cyberattack are all proven only by forensic analysis of the weapons themselves. Credible claims of state authorship for these weapons are rare if they exist at all. The major states, with the clear capability and/or interest to develop and exploit these weapons, all denied that they were involved once the weapon had been deployed. The U.S. and Israel publicly disavow any responsibility for Stuxnet; the Russian and Chinese provide similar denials whenever forensics indicate that they were involved in the development or deployment of cyberweapons; and even the North Koreans — generally considered to be the authors of the "wiper malware" aimed initially at South Korea's cyber-infrastructure — deny they were involved in any way. However, it is also clear from the above that the primary benefit for the cyberattacker is not necessarily directly supportive of physical war. In fact, no example could be found in the public record that indicates that a cyberattack was preferred to direct physical military operations. Thus, cyberweapons, with a willingness to undertake cyberattack, appear to be considered primarily to (1) level the playing field between countries, (2) attack countries that are more reliant on their cyber-infrastructure during non-war times, (3) disrupt an enemy's ability to build military infrastructure, or (4) to use it solely at the initial point of attack.

The potential benefits from the intended consequences appear to be sufficiently significant that pursuing a cyberattack strategy is potentially worthwhile. However, If we are reluctant or completely avoid the use of these cyberweapons during military activities, it is important to ask why are we really developing them? It appears that we are only using these, to date, to disrupt or monitor groups/states with whom we are not currently at war. Thus, to put our current activities in the most positive light, they are being developed for espionage or to undertake covert pre-war activities that would likely be considered a violation of international law if they became known or were being done in the physical world. The key question would change from "are we developing cyberweapons for military advantage?" to asking "are we developing these weapons for use in peace time or to undertake secret 'wars'?" If the latter is the case, then is the endorsement of cyberattack really an endorsement of non-sanctioned warlike activity on the part of those who have little public oversight? And, if so, is it even possible to provide appropriate checks and balances to ensure these activities do not lead us into unnecessary wars or cause us to lose important allies because we are using them against the very people we consider friends? With this in mind, we turn to potential risks and consequences.

4. RISKS AND CONSEQUENCES OF THE SSE'S CYBERATTACK-FRIENDLY POLICY

Before considering the cyberattack aspect of the SSE defence-policy white paper, it is helpful to set it within its wider context. SSE includes a longstanding and fundamental tenet that calls for the protection of "critical military networks and equipment from cyberattack by establishing a new Cyber Mission Assurance Program that will incorporate cybersecurity requirements into the procurement process" (Canada-SSE 2017, 73). The novelty in this statement is the explicit statement that cyber-related procurement should explicitly consider the threats from cyberattack, a requirement that is either long overdue or a codification of best practices aimed at defending our military's cyber-infrastructure, which may be going on already. However, this only explicitly speaks to new procurement, while the need to develop protection for existing cyber-assets should also produce an immediate call to action to assess all assets. Unfortunately, the document appears silent on the protection of legacy systems currently in place and the potential threat to them for a number of reasons.

Risks to current assets:

- Potential attack surfaces are already in place in the form of flaws in existing software and hardware assets currently deployed. Many of these systems are well beyond their anticipated lifetime and remain critical parts of our military's capacity. Cyberattacks on these systems should be carefully assessed and appropriate changes made either to the existing asset, or better, by replacing it with a current, state-of-the-art version.
- Maintenance of these legacy systems will likely require software alterations that may open new attack surfaces either embedded in the alterations themselves or because of unanticipated interactions between the original software and the update. Legacy heterogeneous systems are notoriously difficult to protect from unanticipated attacks because they may be vulnerable due to: the legacy software/hardware, the updates made to modernize the systems, or from the interaction of the old systems with the new ones.
- As legacy hardware becomes more difficult to procure or there emerges a desire to increase the functionality of deployed military assets, novel risks from the new technology will open up additional attack surfaces. For example, an IoT ("internet of things") device with enhanced communication ability will bring significant advantages to an asset, but may do so at the risk of making other, older elements in the asset vulnerable to cyberattacks that it would otherwise not be exposed to.

Thus, a critical risk raised in the SSE, but not addressed adequately by it, is the protection of currently deployed assets and how the impact of new technology that will be required to maintain its functionality can best be protected from cyberattack.

The real novelty in the SSE's policy goes further than the clearly mandatory need for cyberdefence on existing and new assets by explicitly calling for the development of "active cyber capabilities and (their) employ(ment) … against potential adversaries in

support of government-authorized military missions" (Canada-SSE 2017, 73). It is well known that some states have been developing cyberattack capabilities for many years and there is also clear evidence that these attacks have been deployed in the past. However, the decision to do so as a part of an endorsed strategy of a state is significant.

The issue of a state developing cyberattack capabilities and determining how or when to deploy them is multifaceted. The geopolitical lens is a critical one because it effectively, at least implicitly, justifies other states' efforts to develop such capabilities and acknowledges cyberattack as a legitimate form of warfare. On one hand, this is a potentially positive step because it brings cyberwarfare under the set of rules governing warfare in general, which implies that deploying a cyberattack would have to be framed as "war." This would discourage the use of cyberattack in the same way that physical attacks on another state must be consider in light of their potential consequences as it enters a war-footing. Recall that the use of these weapons currently appears to be done without the same implications of an equivalent physical attack on a state, but at the same time states are quick to deny any involvement in such activities. By engaging in legal warfare, states subscribe to certain kinds of behaviour, including not explicitly attacking non-combatants or committing war crimes, such as genocide. If cyberweapons were to be defined as weapons of war, then their use would at least implicitly force them to be used only under the rules of war.

Conversely, acknowledging this as a valid form of warfare and subjecting it to the "rules of war" implies that such a set of rules exists and have been generally accepted. This is not the current case and many states claim to either not participate in any cyberattack activities, except cyber-defensive ones, or are silent on the issue, so it is unlikely that a set of rules will be developed in the immediate future. Thus, before developing cyberattack as a weapon of war, the rules for its deployment should be carefully articulated and agreed to internationally. Furthermore, the implication of their use vis-à-vis an "act of war" should be defined and agreed to internationally.[4]

If this could be achieved, the question of enforceability of these rules would have to be addressed. The developer of current cyberweapons can often only be determined with complex forensics that are not yet perfected. Currently, the development of these weapons is likely undertaken by the same group that initially deploys them, but this will likely not be the case in the near future. Just as there are physical "arms developers" in the physical world, it would be much easier to create a cottage industry that develops cyberweapons and sells them to any purchaser willing to pay the price. Thus, the current methods used to identify the source of an attack by examining the fingerprints of the software itself will no longer work or will be unhelpful in identifying the group that actually deploys the weapon.

Enforcement will require that the group deploying the weapon be identified to either ensure justice is attained following inappropriate use or to confirm the group is in fact the one who delivered the weapon so subsequent military responses can be

[4] The challenges of accomplishing this a priori are discussed in Section 6.

legitimately undertaken. Cyberattacks, by their very nature, are often delivered from multiple sources and are deployed through complex and difficult-to-trace virtual modalities. A combination of network hops around the world and a co-ordinated cyberattack launch could be authorized in one part of the world but appear to come from anywhere in the world. Tracing the source of the attack may be impossible to verify with complete certainty, which might make it impossible to hold the real culprit to account. Current state-of-the-art forensics may be able to identify the author of malware, but it is exceedingly difficult to identify the precise deployment source. Thus, the technology necessary to definitively identify cyberweapon deployments does not exist and modern cyber-infrastructure does not provide sufficient traceability primitives to identify the source of cyberweapon use with sufficient certainty. In fact, this actually "encourages" the use of these weapons because their deployer would be difficult to detect. However, there is a substantial risk of other states launching cyberattacks by routing them through Canada to make it appear as if the attacks had originated from here. Thus, before adopting a cyberattack-capacity-building strategy such as the one proposed in the SSE, Canada should develop sufficient checks and balances on the use of cyberweapons to ensure that an attack by another state using Canadian infrastructure can be plausibly denied. This might require difficult changes to the current internet infrastructure or sufficient transparent overhead on the valid use of cyberweapons that are seen as very compelling to the rest of the world.

Although there are likely many other risks, the final issue raised here is related to the appropriate management of the development of cyberweapons. Unlike physical weapons, cyberweapons typically exploit an unknown vulnerability in existing hardware and software. Thus, the weapon developer must find the vulnerability, develop an exploit to take advantage of it, and identify an enemy to use the weapon against. Each of these three stages present unique weapon-management challenges that we consider next.

1. Identifying these vulnerabilities is a timely process and often involves a fair amount of luck, so they are more likely to be discovered with multiple people working on them. Once discovered, they must be kept secret or patches can be developed to disable the vulnerability (and as a result, the weapon itself) reasonably quickly. The ethics of not warning others about these vulnerabilities is beyond this document's scope, but at the very least it can lead to significant unintended consequences as discussed in Section 5. This means that the weapon's usefulness is limited by the vulnerability's life cycle; to be useful, the weapon must be deployed while the vulnerability is still unprotected. This might provide an inappropriate incentive to use the weapon too quickly and could even skew battlefield plans in unanticipated ways.

2. The challenge of developing an exploit to take advantage of an identified vulnerability may be fairly straightforward in some cases but it could also involve a significant amount of expertise and innovation to accomplish. This is clearly not something that can be readily "outsourced" to other states, and even if it was to be done by verified cyberweapon suppliers, the challenges of

managing this process should not be underestimated. If the approach is building capacity within military (or quasi-military) national centres, it will likely require a substantial investment in public dollars that would be difficult to justify given the clandestine nature of the activities and the possibility (ideally) that these cyberweapons would never be meaningfully deployed.

3. The final challenge of identifying an enemy to use the weapon against and to determine precisely when and how it should be used, given the two points above, is unclear. The hesitance to use cyberweapons at times of military conflict in preference to kinetic weapons suggests that they are unlikely to be the preferred choice once a military conflict has started. Using them beforehand is fraught with risk because their use, if they could be traced back to the originator, could lead to a war that might otherwise have been prevented. In the case of a large, powerful state using these weapons, this will likely be avoided because the weaker state is unable to respond in a meaningful way. Assuming that the U.S. was the originator and user of Stuxnet in the Iranian nuclear facilities, the fact that Iran did not respond in an overtly military way is likely because it could not. Thus, the most likely use of cyberweapons would be in some form of cyberespionage either passively (spying) or aggressively (disrupting another state's activities) with plausible deniability.

Overriding each of these potential risks is the need to have oversight on the development, use, and deployment of cyberweapons. Military activities can only be undertaken with the direct oversight of the prime minister, but they would likely involve a wider discussion for political reasons. Given the nature of these weapons and how they would need to be developed, this oversight would likely have to be done in a more secretive way. The ultimate deployment of cyberweapons might occur with the oversight of Parliament, but would those considering this have sufficient understanding of the implications and risks associated with cyberweapons, which could have many unintended consequences? This is the topic to which we turn next. If a more selective group were identified, how would the public be assured that this group was acting with sufficient oversight to ensure their activities did not lead to serious consequences that would not be endorsed by Parliament or the public at large?

5. UNINTENDED CONSEQUENCES

The unintended consequences arising from a cyberattack can be grouped into two categories: unintended consequences impacting on those being attacked; and ones impacting those undertaking the attack (or their allies).

Unintended consequences potentially impacting an enemy: Once weapons are deployed, the scope of their effect is difficult to anticipate. Ideally an attack would be highly targeted and very specific to a particular computer system or to the real-world resource it controls. There are unique identifiers in most hardware that would allow a cyberweapon to only impact a particular machine. However, the attacker would have to identify that machine in advance of developing and deploying the weapon, and the

cyberweapon would become useless if the victim simply changed or upgraded their hardware. Thus, there are very few incentives for a cyberattacker to produce a weapon with such a narrow target and it is unlikely that such a narrowly focused cyberweapon would be effectively deployed except in very limited circumstances (e.g., the Stuxnet attack on the Iranian nuclear systems).

Most cyberweapons have a *virus-like* nature to them where they seek to infect as many systems as possible to maximize their impact. This alone would make it difficult to control the unintended consequences that might occur on an enemy. However, even if the cyberweapon does not contain a virus-like nature where it seeks all computer systems that have the vulnerability that allows it to perform its cyberattack, it is still extremely difficult to limit its effect to only the intended target. The unintended consequences on the enemy might be much wider than what has traditionally been considered acceptable in terms of collateral damage. For example, a cyberweapon aimed at disabling an enemy's supply-chain computer systems but which also infects the enemy's nuclear-weapons systems, causing them to deploy in situ, is unlikely to be considered a reasonable level of collateral damage and might even rise to the level of a war crime. Although these appear to be very different systems and are likely run on entirely different computer systems, the underlying operating systems and applications that enable them to function are often shared.[5]

Furthermore, best practices in the computer industry demand that systems are updated in a timely and regular way to ensure that the systems are current across an organization's entire scope.[6] Organizations (the military being no exception) seek to minimize high software/hardware maintenance costs by exploiting as much homogeneity as possible in their deployed systems because this simplifies and streamlines the updating process so is often a requirement in the procurement decision. However, this homogeneity also means that a cyberweapon meant to exploit a vulnerability found in one system can also attack other systems in the organization that have the same vulnerability. In short, a state's desire to minimize costs drives it toward homogenous solutions across its many sectors and this can be exploited by cyberweapons unintentionally. This widens the impact (a potential benefit from the attackers viewpoint), but also opens the possibility that the more narrow intended focus impacts other systems that were never intended to be touched. Thus, these unintended consequences are a likely occurrence given current efficient approaches to upgrading computer systems in most modern organizations, and they may be unavoidable.

---

5 This is less likely to be an issue for larger states with substantial capacity, because specific proprietary software and systems can be developed in-house. However, this is not universally true, as many states do not have sufficient capacity to develop their own unique operating systems for each aspect of their critical infrastructure. In fact, the cyberweapons most likely to be developed will rely on these states using a known suite of commercially available products.

6 It is unclear if the major military players in the world use a more tailored approach to system upgrades, but even if a few of the most advanced militaries do, it is a safe bet that most of them do this with efficiency rather than security in mind.

Unintended consequences potentially impacting the attacker: The nature of a cyberattack also introduces another potential threat. A kinetic weapon, once deployed, will either strike its target or be destroyed on its way. The same is true of cyberweapons, but this is where the analogy ends. A cyberweapon is generally victim-agnostic, so it is just as threatening to the attacker's cyber-systems as it is to the victim's. The question of how to deploy a cyberattack that cannot subsequently impact on your own systems is an open one. To consider how this might be addressed we consider a number of options:

1. Explicitly identify which machines will allow the cyberattack to be performed. The challenge is the same as described above when we considered limiting the scope of damage to an explicit subset of machines. It is extremely difficult to identify the victim's machine and to ensure that changes in hardware do not disable the efficacy of the attack. This "white list" approach, which specifies where a cyberattack is allowed to occur, is not feasible in a cyberwar scenario. The alternative is a "black list" that states where the cyberattack is not allowed to execute. This will only work if a complete list of all of the attacker's assets could be produced and could then be deployed with the cyberweapon to limit its functionality. Creating such a list might be possible, but it would be exceptionally long, and it would have to be constantly updated as new computers were purchased. Even if this were possible, the required access to the deployed cyberweapons would likely raise flags within the victim's IT group that would lead to its detection.

2. Protecting the attackers from their own weapons. This essentially requires an update to the attacker's vulnerability to the cyberweapon. This can be done in two ways:

    a) Use the appropriate vendor's update mechanism: The mechanism is likely to be the only truly universal way to update all of the potentially vulnerable systems within a state's critical infrastructure. However, the solution is, by definition, universal, so it would be nearly impossible to convince a vendor to selectively update specific systems to a particular vulnerability. In fact, this would likely lead to a very expensive lawsuit for the vendor if it knowingly left vulnerabilities in software that it sold to its customers, so there would be virtually no incentive for a vendor to do so.

    b) Secretly update all of the attackers' own systems' vulnerabilities: Since the attacker knows the vulnerability, developing a patch would likely be possible, if not straightforward, even if it required some reverse engineering of proprietary software. Assuming, for the moment, that this is possible, the question of how to distribute the patch to only a single organization in a confidential way is critical. If such a patch was to become known, any potential victims would likely immediately seek to determine how to protect their own systems. Even if they were not aware that a cyberweapon had been deployed on their system, the desire to patch their systems would

be extremely high and, once accomplished, it would disable the attacker's cyberweapon. Pragmatically, in a sufficiently complex organization, such as a large modern military (let alone all of its allies cyber-systems) with an uncountable number of suppliers, it would be effectively impossible to selectively update all potentially impacted systems with a vulnerability patch. Furthermore, many military suppliers provide goods and services to more than one country, which would increase the likelihood that potential victims might inadvertently receive the very patch necessary to protect themselves from such an attack.

c) Protecting the attacking state's non-military infrastructure: The cyberweapons are exploiting vulnerabilities that also exist in "everyone's" systems. All public and private organizations and their infrastructures have an important stake in the use of any cyberweapons. No state will want to deploy a cyberattack that quickly comes back and shuts down key national institutions, such as banking systems, financial markets, transportation and power systems, non-military communication systems, etc. Earlier, we touched briefly on the issue of the ethics of withholding knowledge about software/system vulnerabilities, but at this point it becomes a strategic issue as well as an ethical one. If a state has knowledge about a vulnerability but fails to notify its own organizations about the risk, and if we readily assume enemies are looking for these vulnerabilities as well, then we face two risks: attacks from our enemies, when we have a known solution; and attacks from ourselves when these weapons are deployed but come back to attack our own organizations.

Finally, consider the challenge of dismantling a cyberweapon. Several issues must be considered:

1. If a cyberweapon has been deployed but a decision is made to withdraw it, a key question is: Can these deployment sites be accessed again? It is unlikely that a cyberattacker would be willing to notify the victim about the latent weapons buried within its system, so the only way to remove it is to once again get access to it. One potential solution would be to send the victim a "friendly patch" that the attacker strongly encourages them to apply, but this will likely raise suspicion, at best, and could lead to the need to deploy the cyberweapon anyway because of a newly poisoned relationship! In short, once deployed, it would be difficult if not impossible to remove.

2. Most of these weapons have an ability to migrate either explicitly as a virus and/or physically by copying them across multiple devices (e.g., using an infected USB stick). Thus, even if we know where they were initially deployed, the question of how to ensure that the cyberweapon has not migrated to other machines without the attacker's knowledge is critical. Although it might be possible to leave a digital trail within the cyberweapon itself, so a forensic expert could attempt to follow its path, this would open the possibility that the trail

would be discovered by the potential victim, which would lead to the weapon's discovery and it being disabled while still in its active or operational phase.

3. Given that this software can travel through an enemy's system in difficult-to-track ways, the next concern is: What if this vulnerability shows up on an ally's systems? Several interesting question will likely be asked at this point, but the first one will be: Was it inadvertently migrated from within the attacker's system through normal operations, or is this an attack by the enemy on the ally's systems? If the cyberweapon was discovered by the enemy and the vulnerability was known to exist in one of the attacker's ally's systems, there is nothing to stop the victim from patching its own systems and using the weapon itself. Furthermore, if this is discovered by the ally and reported to the attacker, how can this be disabled without revealing the danger to which the attacker has exposed the ally? It is likely, especially if this is a cyberweapon used for espionage, that the ally will become suspicious about whether this was placed on its systems accidentally by the attacker, intentionally by the attacker, or intentionally by the victim using it itself. Clearly different kinds of responses would be called for depending on each case.

6. NEXT STEPS

Drawing conclusions at this point would be premature. This paper has attempted to raise certain issues based primarily on what cyberwarfare technology is capable of at this point in time. We have raised many issues in the paper about the consequences (both intended and unintended) of developing cyberweapons and it is clear that there are more questions than answers surrounding many of them. To move forward at this point to implement or even formally endorse a strategy of cyberattack would be risky and premature. There are challenging technical controls that must be put in place as well as a critical international discussions on how cyberweaponry fits within the rules of war. Countries appear to be moving forward with cyberattack strategies but subsequently deny any such participation. This approach has the potential for serious consequences, and the need for better oversight (from non-military sectors) is critical to a safe coherent strategy for any nation. Furthermore, the management of deployed cyberweapons and their subsequent removal has not yet been addressed from either a technical or social-engineering perspective. The many technological issues identified above should be sufficient to cause at least a pause in the current SSE proposal to endorse cyberattack and the debate must become broader than the viewpoint of military proponents. It should be opened to the public for thoughtful fulsome discussions that include various technical, political, legal, and geopolitical/ regulatory perspectives.

We now turn to identifying what Canada's next steps should be to fully explore and consider the many questions developed above. Although there are likely many different directions open, the following seem to be the most key and self-evident initial steps.

1. **Canada must define the goals of a cyberattack strategy**

    a) Who are potential opponents that could be subject to an attack?

    b) What are acceptable reasons to use cyberweapons?

    c) How do we define successful attacks and distinguish them from failed attempts?

2. **Rules of engagement must be clearly defined**

    a) When should cyberweapons be allowed to be used?

    b) When should they be used: before, after or in conjunction with direct kinetic military actions?

    c) Should their use be reported upon openly and honestly to the Canadian public?

3. **Who has the authority to use cyberweapons either in peace or wartime?**

    a) Who should be allowed to authorize their use?

    b) Once authorized, who should be allowed to deploy them and under what circumstances?

    c) Who has oversight after their use in terms of assessing their effectiveness, their appropriateness, and evaluating any unintended consequences or collateral damage.

4. **Rules of war need to be defined for cyberweapons.**
    Canada must work with other nation states to formally codify the rules under which states can engage in cyberattack and cyberespionage. These might mirror existing kinetic-warfare rules, but they will require articulation through a technological lens. These issues need to be developed because it is unclear if Ongstad's claim is in fact true that "… cyberattacks alone are unlikely to cause an escalation towards kinetic or conventional warfare" (Ongstad). Garrie argues that "(c)yber-warfare occurs when one country perpetrates a cyberattack against another country that would to the reasonable person constitute a state act of war" (Garrie 2012). If we do not have clear rules about the use of these cyberweapons as a nation state, then we run the risk of stumbling into a kinetic war! Thus, a critical next step is undertaking the difficult task of coming to international agreements about the use of these weapons, their production, and their implications. Although this may be considered by some to be naïve and currently unachievable, why should it not be required for cyberweapons as it is for every other weapon? Historically, new weapons are developed, deployed

and the consequences measured retrospectively. This is precisely why we have prohibitions against nuclear, biological and chemical weapons but only after observing their severe consequences during wartime. Do we need to wait until society suffers these consequences again before putting in place rules about their use?

5. **Partnership with cybersecurity stakeholders.**
   The issues of cybersecurity are much broader than their application to cyber-military either for offensive or defensive purposes. The question of whether a partnership could be forged between the military and public/private cybersecurity organizations is a valid one to consider. As a representative example, the government of Canada established the "Canadian Centre for Cyber Security" (CCCS) in 2018 to inform, protect, develop and share, and defend cyberdefence technologies where the mandate is to engage in cyber-related security issues in both the private and public sectors. Although there is substantial overlap with the military use of cyberweapons and the defence against potential attacks, it is important to make a distinction between the two. Covert cyberespionage or cyberattacks could seriously impact on the systems that the CCCS was established to address, but the mandate for the centre is to protect existing cyber-infrastructure, which contradicts the largely clandestine uses proposed in cyberwarfare. An obvious approach would be that the military works in partnership with the CCCS so that, if an attack were to be initiated, the CCCS could quickly disseminate the necessary patch to protect allies' cyber-systems. Unfortunately, this would directly contradict the CCCS's primary mandate of protecting Canadian cyber-infrastructure and expose the CCCS to serious, legitimate criticism.

   Imagine a very plausible scenario: The CCCS is asked to withhold a patch of a known vulnerability by the military to allow its use as a cyberweapon. While waiting for this opportunity, the vulnerability is exploited to attack Canadian systems. This would undoubtedly lead to significant criticism because an agency, specifically funded to protect Canada, has acted as an arm of the military and exposed the country's systems to cyberattack. Thus, the mandate of the CCCS directly contradicts the SSE's goal of developing cyberattack capabilities, so it hard to envision a partnership that would ultimately be mutually beneficial. If this kind of partnership is not viable, then how can the military meaningfully engage with non-military stakeholders to ensure the utility of any weaponry produced and the safety to Canada and its allies?

REFERENCES

Bencsath, Boldizsar, Gabor Pek, Levente Buttyan, and Mark Felegyhazi. 2012. "The Cousins of Stuxnet: Duqu, Flame, and Gauss." *Future Internet* 4:971 - 1003. doi: 10.3390/fi4040971.

Canada-SSE, Department of National Defence. 2017. Strong, Secure, Engaged: Canada's Defence Policy. Available at: dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy- report.pdf: Department of National Defence and Canadian Armed Forces.

Denning, D.E. 2011. "Cyber Conflict as an Emergent Social Phenomenon." In *Corporate Hacking and Technology-Driven Crime: Soical Dynamics and Implications*, edited by T. Hold and B. Schell, 169 - 186. IGI Global.

Dycus, Stephan. 2010. "Congress's Role in Cyber Security." *Journal of National Security Law & Policy* 4 (1):155 - 171.

Garrie, Daniel B. 2012. "Cyber Warfare, What are the Rules?" *Journal of Law & Cyber Warfare* 1 (1):2 - 7.

Giles, Keir, and William Hagestad II. 2013. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, June 4 - 7, 2013.

Iasiello, Emilio. 2015. "Are Cyber Weapons Effective Military Tools?" *Military and Strategic Affairs* 7 (1):23 - 40.

Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster Paperbacks.

Krutz, Ronald L. 2006. *Securing SCADA Systems*. Indianapolis, USA: Wiley.

Liles, S., J. E. Dietz, M. Rogers, and D. Larson. 2012. "Applying traditional military principles to cyber warfare." 2012 4th International Conference on Cyber Conflict (CYCON 2012), 5-8 June 2012.

Mairh, A., D. Barik, K. Verma, and D. Jena. 2011. "Honeypot in network security: A Survey." International Conference on Communication Computing and Security (ICCCS'11), Rourkela, Odisha, India, February 12 - 14, 2011.

Ongstad, Michael. "Cyber-warfare: Offensive Versus Defensive Balance." SecurityZap. https://securityzap.com/cyber-warfare-bounded-chaos/.

Robinson, Michael, Kevin Jones, and Helge Janicke. 2015. *Cyber warfare: Issues and challenges*. Vol. 49.

Theohary, Catherine A., and Anne I. Harrington. 2015. Cyber Operations in DOD Policy and Plans: Issues for Congress. In *Congressional Research Service Report*. Washington D.C.: Goverment of the United States.

Theohary, Catherine A., and John W. Rollins. 2015. Cyberwarefare and Cyberterrorism: In Brief. In *Congressional Research Service Report*. Washington D.C.: Goverment of the United States.

Winkler, Vic (J.R.). 2011. *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Edited by Bill Meine. Waltham, Mass, USA: Syngress: an imprint of Elsevier.

About the Author

Ken Barker is a professor of computer science at the University of Calgary. He holds a PhD in computing science from the University of Alberta (1990) and has many years of experience working with industrial computer systems. He has interest in system integration, distributed systems and the privacy and security of data repositories. He has served as the dean of the faculty of science and as head of computer science at the University of Calgary. He is the director of the University of Calgary's Institute for Security, Privacy and Information Assurance and the president of the Alberta body of the Canadian Information Processing Society (CIPS Alberta). He is a past president of the Canadian Association of Computer Science (CACS/AIC) and has served on the Computer Science Accreditation Council. As the director of research laboratories at the University of Calgary and University of Manitoba he has supervised over 60 graduate students, in addition to several post-doctorates and research assistants. Dr. Barker has published over 200 peer-reviewed publications.

ABOUT THE SCHOOL OF PUBLIC POLICY

The School of Public Policy has become the flagship school of its kind in Canada by providing a practical, global and focused perspective on public policy analysis and practice in areas of energy and environmental policy, international policy and economic and social policy that is unique in Canada.

The mission of The School of Public Policy is to strengthen Canada's public service, institutions and economic performance for the betterment of our families, communities and country. We do this by:

- *Building capacity in Government* through the formal training of public servants in degree and non-degree programs, giving the people charged with making public policy work for Canada the hands-on expertise to represent our vital interests both here and abroad;
- *Improving Public Policy Discourse outside Government* through executive and strategic assessment programs, building a stronger understanding of what makes public policy work for those outside of the public sector and helps everyday Canadians make informed decisions on the politics that will shape their futures;
- *Providing a Global Perspective on Public Policy Research* through international collaborations, education, and community outreach programs, bringing global best practices to bear on Canadian public policy, resulting in decisions that benefit all people for the long term, not a few people for the short term.

The School of Public Policy relies on industry experts and practitioners, as well as academics, to conduct research in their areas of expertise. Using experts and practitioners is what makes our research especially relevant and applicable. Authors may produce research in an area which they have a personal or professional stake. That is why The School subjects all Research Papers to a double anonymous peer review. Then, once reviewers comments have been reflected, the work is reviewed again by one of our Scientific Directors to ensure the accuracy and validity of analysis and data.

The School of Public Policy
University of Calgary, Downtown Campus
906 8th Avenue S.W., 5th Floor
Calgary, Alberta T2P 1H9
Phone: 403 210 3802

DISTRIBUTION
Our publications are available online at www.policyschool.ca.

DISCLAIMER
The opinions expressed in these publications are the authors' alone and therefore do not necessarily reflect the opinions of the supporters, staff, or boards of The School of Public Policy.

ISSN
ISSN 2560-8312 The School of Public Policy Publications (Print)
ISSN 2560-8320 The School of Public Policy Publications (Online)

DATE OF ISSUE
June 2019

MEDIA INQUIRIES AND INFORMATION
For media inquiries, please contact Morten Paulsen at 403-220-2540. Our web site, www.policyschool.ca, contains more information about The School's events, publications, and staff.

DEVELOPMENT
For information about contributing to The School of Public Policy, please contact Catherine Scheers by telephone at 403-210-6213 or by e-mail at catherine.scheers@ucalgary.ca.

RECENT PUBLICATIONS BY THE SCHOOL OF PUBLIC POLICY

TOWARDS SOCIAL SERVICES SYSTEM INTEGRATION: A REPORT FROM ALBERTA'S ELDER CARE SUPPORT PROVISION COMMUNITY
https://www.policyschool.ca/wp-content/uploads/2019/05/Social-Services-Walsh-Khayatzadeh-Mahani-Leslie-final.pdf
Connor Martin Walsh, Akram Khayatzadeh-Mahani and Myles Leslie | May 2019

FISCAL POLICY TRENDS: BALANCING ALBERTA'S BUDGET BY 2022 IS ONLY PART OF ALBERTA'S LONG-RUN FISCAL CHALLENGE
https://www.policyschool.ca/wp-content/uploads/2019/04/Tombe-AB-Fiscal-Future-SPP-Trends-May-2019.pdf
Trevor Tombe | May 2019

AN ALBERTA GUARANTEED BASIC INCOME: ISSUES AND OPTIONS
https://www.policyschool.ca/wp-content/uploads/2019/04/AB-Income-Simpson-Stevens-final-USE-THIS-VERSION.pdf
Wayne Simpson and Harvey Stevens | April 2019

TWO DIFFERENT CONFLICTS IN FEDERAL SYSTEMS: AN APPLICATION TO CANADA
https://www.policyschool.ca/wp-content/uploads/2019/04/Conflicts-in-Federal-Systems-Mintz.pdf
Jack Mintz | April 2019

SOCIAL POLICY TRENDS: AGE-SPECIFIC FERTILITY RATES BY PROVINCE AND TERRITORY, 2000 AND 2017
https://www.policyschool.ca/wp-content/uploads/2019/04/SPT-Birth-Rates-Final.pdf
Ronald Kneebone | April 2019

PING-PONG ASYLUM: RENEGOTIATING THE SAFE THIRD COUNTRY AGREEMENT
https://www.policyschool.ca/wp-content/uploads/2019/04/Ping-Pong-Asylum-Falconer.pdf
Robert Falconer | April 2019

A PACE PROGRAM IN ALBERTA: AN ANALYSIS OF THE ISSUES
https://www.policyschool.ca/wp-content/uploads/2019/04/PACE-Program-Khanal.pdf
Mukesh Khanal | April 2019

SOCIAL POLICY TRENDS: THE DEPTH AND PREVALENCE OF POVERTY
https://www.policyschool.ca/wp-content/uploads/2019/03/Social-Policy-Trends-Poverty-Depth-and-Prevalence-March-2019-USE.pdf
Ronald Kneebone | March 2019

UPDATING AN ODA POLICY IN CANADA: THE ROLE OF GLOBAL REMITTANCES IN DEVELOPMENT
https://www.policyschool.ca/wp-content/uploads/2019/03/ODA-Policy-Bansak-Simpson.pdf
Nicole Simpson and Cynthia Bansak | March 2019

PROVINCIAL PUBLIC INFRASTRUCTURE SPENDING AND FINANCING IN ALBERTA: SEARCHING FOR A BETTER COURSE
https://www.policyschool.ca/wp-content/uploads/2019/03/Searching-for-a-Better-Course-McMillan.pdf
Melville McMillan | March 2019

TRADE POLICY TRENDS: CHINESE PROTECTIONISM: RESTRICTION ON CANOLA IMPORTS FROM CANADA
https://www.policyschool.ca/wp-content/uploads/2019/03/Trade-Policy-Trends-Canola-Imports-Beaulieu-Klemen.pdf
Eugene Beaulieu and Dylan Klemen | March 2019

UNBLOCKING THE BOTTLENECKS AND MAKING THE GLOBAL SUPPLY CHAIN TRANSPARENT: HOW BLOCKCHAIN TECHNOLOGY CAN UPDATE GLOBAL TRADE
https://www.policyschool.ca/wp-content/uploads/2019/03/Global-Supply-Chain-Norberg-final.pdf
Hanna C. Norberg | March 2019

WHICH POLICY ISSUES MATTER IN CANADIAN MUNICIPALITIES? A SURVEY OF MUNICIPAL POLITICIANS
https://www.policyschool.ca/wp-content/uploads/2019/03/Canadian-Municipalities-Lucas-Smith.pdf
Jack Lucas and Alison Smith | March 2019