CANADIAN HACK-BACK?: A CONSIDERATION OF THE CANADIAN LEGAL FRAMEWORK FOR PRIVATE-SECTOR ACTIVE CYBER DEFENCE

KRISTINA GERKE*

In recent years, a debate has emerged over the extent to which victims of cyber security intrusions should be permitted to conduct activities in response — in particular, activities with effects in networks outside the victim's own. Such controversial efforts are often referred to as active cyber defence (ACD) or, more colloquially, as "hack-back." While multiple researchers have written about how private-actor ACD fits within the United States legal framework, this topic remains understudied from a Canadian perspective, raising the question of how Canadian legislation may address ACD. Currently, Canadian legislation implicitly prohibits most, if not all, ACD efforts, but international law likely leaves room for countries to legalize certain forms of ACD. Going forward, there may be a significant benefit to Canadian legalization of ACD if these efforts are limited to "intelligence gathering" and constrained by strict government oversight.

TABLE OF CONTENTS

* Master of Arts in International Affairs, Carleton University. Special thanks to Professor Stephanie Carvin for her encouragement, mentorship, and comments on this article. Thanks also to Jocelyn Gerke, *Alberta Law Review*'s anonymous reviewers, and the many others who provided input during earlier stages of this article.

I. INTRODUCTION

In 2019, a journalist for *MIT Technology Review* wrote an article on what he called "a recipe for cybersecurity chaos."[1] "Sometimes when tech policymakers try to solve a problem," he explained, "their proposed cure would only make matters much worse."[2] He was referring to active cyber defence (ACD) and more specifically, to the *Active Cyber Defense Certainty Act*, a bill introduced by United States Congressman Tom Graves.[3] ACD is based on the premise that current cyber security best practices have proven to be far from adequate to address the multitude of cyber threats that companies face. According to Graves and other proponents of ACD, more aggressive measures need to be legalized, in order to allow victims of cyber intrusions to defend themselves against malicious actors. With this in mind, the *ACDC Act* aimed to legalize certain cyber security practices or, at least, clarify their legality.[4]

ACD supporters suggest that the private sector's resources and willingness to address hacking efforts outweigh those of government but that firms cannot effectively channel those resources without increased authority.[5] Critics, on the other hand, allege that ACD is another name for "hack-back," an activity prohibited by the US *Computer Fraud and Abuse Act* on the grounds that it constitutes unauthorized access of a computer.[6] They suggest that legalizing hack-back could have disastrous effects, from violations of international law, to collateral damage to third party computers, to escalation of state-sponsored cyber intrusions. Rather than enhancing security, critics suggest, ACD has the potential to do just the opposite.[7]

Other countries are also grappling with the ACD question, albeit in different ways. France has stated its opposition to hack-back, while also acknowledging the need to clarify what actions private actors can take.[8] On the more permissive side, the Netherlands considered

---

1 Martin Giles, "Five Reasons 'Hacking Back' Is a Recipe for Cybersecurity Chaos," *MIT Technology Review* (21 June 2019), online: <www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/>.

2 *Ibid*.

3 US, Bill HR 3270, *Active Cyber Defense Certainty Act*, 116th Cong, 2019 [*ACDC Act*].

4 Herb Lin, "More on the Active Defense Certainty Act" (24 March 2017), online: <www.lawfareblog.com/more-active-defense-certainty-act>.

5 Michael Edmund O'Neill, "Old Crimes in New Bottles: Sanctioning Cybercrime" (2000) 9:2 Geo Mason L Rev 237 at 276–81; Jeremy Rabkin & Ariel Rabkin, "Hacking Back Without Cracking Up" (2016) Stanford University Hoover Institution Working Paper Series No 1606 at 5–6, online: <www.lawfareblog.com/hacking-back-without-cracking>.

6 See e.g. Nicholas Schmidle, "The Digital Vigilantes Who Hack Back," *The New Yorker* (30 April 2018), online: <www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back>. See also *Computer Fraud and Abuse Act*, 18 USC §1030(a)(2)(2012). Kosseff also states this point regarding "cyber vigilantism" in general (see Jeff Kosseff, "The Hazards of Cyber-Vigilantism," (2016) 32:4 Computer L & Security Rev 642 at 642–43).

7 See Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (New York: WW Norton & Company, 2018) at 203–204; Bruce P Smith, "Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help" (2005) 1:1 JL Economics & Policy 171 at 180–81.

8 France, Ministère de l'Europe et des Affaires Étrangères, *Stratégie international de la France pour le numérique* (December 2017), online: <www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf>; France, "France's response to Resolution 73/27 'Developments in the field of information and telecommunications in the context of international security' and Resolution 73/266 'Advancing responsible State behaviour in cyberspace in the context of international security'" at 11, online: <www.diplomatie.gouv.fr/IMG/pdf/190514-_french_reponse_un_resolutions_73-27_-_73-266_ang_cle4f5b5a-1.pdf>.

allowing law enforcement officials to take hack-back measures in 2012.[9] Meanwhile, Singapore has gone the furthest in exploring the possibility of ACD, amending legislation in 2003 to allow the government to issue a certificate to authorize private actors "to prevent or counter any [computer] threat."[10] While this provision was repealed in 2018, such innovations show that the US is not the only state considering the appropriate response to ACD.

To date, the ACD debate has centred on how the US government should address ACD and on how its computer legislation, specifically the *Computer Fraud and Abuse Act*, currently applies to ACD.[11] With this focus on the US context, relatively few academics have compared countries' relevant legislation[12] or explored questions of international law.[13] There are also few examinations of a particular country's approach toward ACD.[14] Meanwhile, among the few Canadian contributions to the literature,[15] no academic work has specifically considered ACD or hack-back through the lens of Canadian legislation or policy. This gap is worth filling for several reasons.

First, and most obviously, Canada's legislation is distinct from that of the United States and deserves its own treatment in the area of ACD. This is particularly true given that some areas of ACD fall within what one set of experts call "the gray zone" of US law.[16] For instance, Canada and the United States both have laws addressing computer hacking, but it is the details of those laws that matter when it comes to ACD. While it is fair to say that the majority of ACD activities are illegal in most jurisdictions,[17] the legality of certain forms appears less clear.

---

9 See Lucian Constantin, "Dutch Government Seeks to Let Law Enforcement Hack Foreign Computers," *Computerworld* (19 October 2012), online: <www.computerworld.com/article/2718950/dutch-government-seeks-to-let-law-enforcement-hack-foreign-computers.html>.

10 *Computer Misuse Act* (Ch 50A, 2003 Rev Ed Sing), s 15(A).

11 *Supra* note 6.

12 See e.g. Amanda N Craig, Scott J Shackelford & Janine S Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis" (2015) 52:4 Am Bus LJ 721; Scott J Shackelford et al, "Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking" (2019) 41:2 U Pa J Intl L 377.

13 Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures" (2014) 50:1 Stan J Intl L 103.

14 Some contributions outside the US include Robert S Dewar, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence" in Pascal Brangetto, Markus Maybaum & Jan Stinissen, eds, *6th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2014) at 7–21; Lennon YC Chang, Lena Y Zhong & Peter N Grabosky, "Citizen Co-Production of Cyber Security: Self-Help, Vigilantes, and Cybercrime" (2018) 12 Regulation & Governance 101; Dennis Broeders, "Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance," (2014), commissioned by Netherlands Defence Academy, Faculty of Military Sciences NLD MoD, Task Force Cyber at 41–44, online: <www.researchgate.net/publication/280522039_Investigating_the_Place_and_Role_of_the_Armed_Forces_in_Dutch_Cyber_Security_Governance>; Anže Mihelič & Simon Vrhovec, "Obligation to Defend the Critical Infrastructure?: Offensive Cybersecurity Measures" (2018) 24:5 J Universal Computer Science 646.

15 Canadians' main contributions in this area have been a work examining the concept of hack-back promoting equality in cyberspace and a work discussing hack-back in the context of ethical hacking. See Jennifer A Chandler, "Technological Self-Help and Equality in Cyberspace" (2010) 56:1 McGill LJ 39; Alana Maurushat, *Ethical Hacking* (Ottawa: University of Ottawa Press, 2019) at 237–52. Note that Maurushat's work is based on research done for Public Safety Canada over 2010–2011.

16 Center for Cyber and Homeland Security, The George Washington University, "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats" (Washington, DC: Center for Cyber and Homeland Security, October 2016) at 1–70, online (pdf): <wayback.archive-it.org/5184/20190102164841/https://cchs.gwu.edu/new-report-gray-zone-private-sector-and-active-defense-against-cyber-threats>.

17 Rosenzweig, *supra* note 13 at 114.

Second, the potential for the US to legalize ACD raises questions for Canada. Were the US to legalize ACD, US firms with a Canadian presence have an obvious interest in understanding how Canadian law would impact their efforts to employ ACD. Moreover, cyber intrusions do not respect political or geographical boundaries; US companies would almost inevitably conduct ACD that affected computers in Canada, as well as in other jurisdictions.[18] And even if the US passed legislation to legalize ACD, such a law would not provide immunity from Canadian laws if a US firm were to "hack back" a network located in Canada.[19] In this situation, Canada would be forced to clarify its own position on ACD.

Third, there are reports that ACD is already widely occurring, while going unprosecuted. A highly cited 2012 survey from Black Hat, one of the top two hacker conferences in the US, found that 36 percent of attendees admitted to engaging in retaliatory hacking — although it is unclear whether their responses referred to hacking back on their own behalf or on behalf of a firm.[20] Meanwhile, others have pointed to the use of automated software that conducts illegal retaliation[21] or to the possibility that cyber security firms are venturing into others' networks in order to produce attribution reports on hacking efforts.[22] Despite these reports, as of 2019, there had been no cases of prosecution of what could be construed as "self-defence" in cyberspace.[23] A particularly interesting case is that of Shawn Carpenter, a cyber security analyst who in 2003 traced a hack to a server in China and subsequently handed over this intelligence to the FBI. Not only did the FBI welcome his assistance, but when Carpenter's employer Sandia National Laboratories fired him on the grounds that he had broken the law, he sued for wrongful termination and won.[24] In fact, Rosenzweig suggests that "[i]t may well be that official disapproval with informal tolerance is a recurring model across the globe."[25] In such a context, it is important to clarify the state of Canadian law in regard to ACD — even if legislation in the US and other states does not become more permissive.

Finally, there is the strong possibility that Canadian firms may already be engaging in ACD to some extent, perhaps even unintentionally. For example, an innovative cyber security firm may develop new tools that have an effect outside its clients' networks, without understanding the legal implications. Or if a company is already supplying a government client (such as a military) with products or services for cyber defence, it may begin to provide similar products or services to private-sector clients. Certainly, Canada's cyber ecosystem holds the potential to enter into hack-back efforts. A 2019 report by the Canadian

---

18 *Ibid* at 113.

19 Alan Brill & Jason Smolanoff, "Hacking Back Against Cyberterrorists: Could You? Should You?" (2017) 9 Defence Against Terrorism Rev 35. The authors also point out that, due to the nature of information routing on the Internet, data packets cross multiple states' jurisdictions on their way to their destinations; in fact, a single message can be divided into multiple packets following different routes. They suggest that it may be not only the cybercrime laws of the origin country and the destination country that matter but also the laws of any countries through which the data travels.

20 "Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking," *Business Wire* (26 July 2012), online: <www.businesswire.com/news/home/20120726006045/en/Black-Hat-Survey-36-of-Information-Security-Professionals-Have-Engaged-in-Retaliatory-Hacking>.

21 Maurushat, *supra* note 15 at 244; Smith, *supra* note 7 at 176–79.

22 Rabkin & Rabkin, *supra* note 5 at 10.

23 Maurushat, *supra* note 15 at 249. Maurushat states, "There are no cases that deal with defending oneself against an online attack. There is likewise little literature on the topic in most jurisdictions other than the United States" (*ibid*).

24 Schmidle, *supra* note 6.

25 *Supra* note 13 at 115.

Association of Defence and Security Industries (CADSI) found 201 Canadian firms identifying as cyber security firms and 75 identifying as cyber defence firms.[26] Among cyber defence firms, capabilities include what CADSI classifies as "active" capabilities ("attack surface analysis, hunt and adversarial pursuit, red cells, counter-surveillance") and "reactive" capabilities ("internal defence measures, response actions").[27] In both categories, CADSI assesses that "Canadian firms have in-depth cyber defence knowledge, demonstrable capabilities, mature products/services and measurable successes in this area."[28] While these cyber defence firms work in partnership with government agencies, mostly Canadian allies,[29] there is obviously overlap between the expertise required for cyber security and cyber defence. Along the same lines, Canada's cyber and signals intelligence agency, the Communications Security Establishment (CSE), highlighted in its 2020 National Cyber Threat Assessment that "advanced cyber tools" are increasingly available in commercial markets.[30] These developments raise questions around what Canadian firms are allowed to do to support private-sector clients, as well as what kind of software they are allowed to provide — whether inside or outside Canada.

Given these factors, this article examines the relationship between ACD and Canada's legislative framework. It begins by defining ACD and hack-back. Next, it provides an overview of the relevant legislation, namely the *Criminal Code*[31] and Canada's anti-spam legislation.[32] Relevant international law will also be discussed. Three potential ACD scenarios are then considered, along with how legislation applies in these contexts. The article concludes with an analysis of ACD that examines the need for ACD in the current cyber security landscape, while also evaluating ACD's possible risks.

II. DEFINING ACD

Before exploring the subject of ACD, it is important to understand that there is no agreed-upon definition for ACD or hack-back, a gap that poses a challenge to the ACD debate. On one end of the spectrum, some consider ACD and hack-back to be directly equivalent. Schneier refers to ACD as a euphemism for hack-back, saying that the term "just serves to hide what it really is: server-to-server combat."[33] Similarly, much of the media discourse around the *ACDC Act* proposed in the US in 2019 referred to the bill as a "hack-back"

---

26 Canadian Association of Defence and Security Industries (CADSI), "From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence" (Ottawa: Canadian Association of Defence and Security Industries, 2019), online: <www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-24.pdf>.

27 *Ibid* at 15.

28 *Ibid*.

29 *Ibid* at 17.

30 Canadian Centre for Cyber Security, Communications Security Establishment, "National Cyber Threat Assessment 2020" (2020) at 13, online: <cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf>.

31 RSC 1985, c C-46.

32 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23, s 3 [*CASL*].

33 *Supra* note 7 at 203.

bill.[34]ACD has also been called "an intentionally ill-defined term" that is inclusive of both legal measures — inside one's own network — and illegal hacking back — inside an adversary's or a third party's network.[35]

Others suggest that ACD is a more nebulous concept, with hack-back being either an extreme version of ACD or something different altogether. Hoffman and Levite suggest that ACD is not an all-or-nothing proposition; the key question is not whether ACD in general should be legal but what kind of ACD is appropriate.[36] A report by the George Washington University's Center for Cyber and Homeland Security uses the term "active defense spectrum" to refer to the range of activities between passive defence (such as firewalls) and hack-back.[37] On this spectrum, some activities are widely accepted. For example, there is no controversy over whether threat hunting[38] is legal, though it is often considered to surpass mere "passive" security measures.[39] Other activities fall into what the report's authors term "the gray zone."[40] Similarly, Rosenzweig focuses less on a concrete definition for ACD and more on key definitional questions around a cyber response's location and effects — in other words, whether it takes place inside or outside the firm's own network and whether it involves observing the original hacker, accessing data, or disrupting or damaging the hacker's network.[41] These researchers would consider ACD to be a fairly broad category that may or may not encompass hack-back.

For the purposes of this article, ACD is defined as any non-governmental response to cyber threats or intrusions using technical means, when that response has effects outside the defender's own network. This definition includes private responses in cyberspace regardless of whether they are legal or illegal, proactive or reactive, automated or directed by a human. It also includes efforts to unobtrusively collect information about the intruder, as well as activities causing actual damage to an adversary's network. However, the definition excludes any actions taking place exclusively inside the defender's own network, such as honeypots (decoys set up inside a network to isolate and monitor hackers' efforts). In addition to the term "ACD," this article also sometimes uses the term "hack-back," either to refer to actions that clearly fall outside legal authorization, or when paraphrasing sources.

Note that this article typically uses the (admittedly broad) term "cyber intrusion" to refer to malicious actors gaining unauthorized access to a computer system. These terms are used

---

34 Shannon Vavra, "Congress to Take Another Stab at 'Hack Back' Legislation (13 June 2019), online: <www.cyberscoop.com/hack-back-bill-tom-graves-offensive-cybersecurity/>; Robert Chesney, "Hackback is Back: Assessing the Active Cyber Defense Certainty Act" (14 June 2019), online: <www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act>; Giles, *supra* note 1. Note that in the Center for Cyber and Homeland Security's report (*supra* note 16 at 39), Nuala O'Connor stands out as an exception in that she differentiates between hack-back and ACD, while also stressing that "unauthorized access to another's computer or network" is and should remain the difference between the two.

35 Schmidle, *supra* note 6.

36 Wyatt Hoffman & Ariel E Levite, "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?" (Washington, DC: Carnegie Endowment for International Peace, 2017) at 2, online: <carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf>.

37 *Supra* note 16 at 10.

38 Threat hunting involves searching one's own network for threats to observe and learn from hackers' behaviour, rather than the more aggressive response that constitutes hack-back.

39 Centre for Cyber and Homeland Security, *supra* note 16 at 10.

40 *Ibid*.

41 *Supra* note 13 at 107.

regardless of whether the malicious actor is a state, a criminal, or any other actor. While the term "cyber attack" is still commonly used, it is sometimes understood to refer only to attempts to disrupt the computer's functions, excluding attempts to collect data.[42] The term "cyber attack" is also less distinguishable from the term "armed attack" as defined in international law.

Finally, the word "defender" is used to indicate that ACD may include efforts by individuals as well as companies, although of course ACD could be legalized in such a way as to allow for only companies, or a subset of companies, to have the authority to conduct ACD.[43] That said, since companies are expected to be the primary users of ACD, I frequently refer to companies rather than "defenders" in this article.

III. CANADA'S LEGAL FRAMEWORK: LAWS IMPACTING ACD

While legal experts have explored the legal context for ACD in the United States, no similar discussion has taken place in Canada. Similarly to the US context,[44] however, the following discussion centres on the legal concepts of unauthorized computer use and defence of property in cyberspace. Several questions are relevant:

(1) How does the law define computer crime (for example, hacking)? Would some or all ACD efforts be considered an offence?

(2) Given that an exception exists in the *Criminal Code*[45] for the defence of property, does ACD qualify?

   i. Can the data that ACD (ostensibly) defends be considered a form of property?
   ii. If so, do ACD actions qualify as "defence" of that data?

This article explores the answers to these questions using an overview of applicable federal law.

---

42 Jay P Kesan & Carol M Hayes, "Thinking Through Active Defense in Cyberspace" in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010) 327 at 327–28.

43 ACD is generally discussed as a means for businesses, as opposed to individuals, to protect themselves, likely because sophisticated adversaries target businesses (and governments). For this reason, it is reasonable to assume that firms (particularly those with significant resources) would be the primary entities to possess both the resources and the motivation to conduct ACD. However, from the legislative perspective, several approaches are possible. ACD could be conducted by licensed IT professionals or licensed cyber security firms. It could also be limited to firms in particular sectors, such as those in critical infrastructure or, even more narrowly, the finance or technology sector. Note that, in previous legislative efforts, neither Singapore nor the US has distinguished between the ACD efforts of individuals and other entities in regard to ACD. See US, Bill HR 4036, *Active Cyber Defence Certainty Act*, 115th Cong, 2017, s 4(3)(A); *ACDC Act*, *supra* note 3, s 4(3)(A); *Computer Misuse Act*, *supra* note 10, s 15(A)(1).

44 See e.g. Zach West, "Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback" (2012) 63:1 Syracuse L Rev 119 at 138–39; Craig, Shackelford & Hiller, *supra* note 12 at 731–43. The latter article also explores laws around "unauthorized access" across the G8.

45 *Supra* note 31.

A. ACD AS COMPUTER CRIME?

The first question concerns whether ACD qualifies as computer crime. While Canadian law does not use the term "hacking" per se, the *Criminal Code*[46] contains two sections understood to address the illegal hacking of computers, and Canada's anti-spam legislation[47] similarly addresses the illegal installation of computer programs. The *Criminal Code* also contains a section relevant to the possession of devices used to commit computer crime.[48]

1. SECTION 430(1.1) OF THE *CRIMINAL CODE*: MISCHIEF IN RELATION TO COMPUTER DATA

First, section 430(1.1) of the *Criminal Code* establishes the offence of "mischief in relation to computer data" as follows:

> Everyone commits mischief who wilfully
>
> (a) destroys or alters computer data;
> (b) renders computer data meaningless, useless or ineffective;
> (c) obstructs, interrupts or interferes with the lawful use of computer data; or
> (d) obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it.[49]

Section 430(1.1)(a) and (b) speak to wilfully destroying data, altering it, or rendering it unusable. These charges likely apply to ACD efforts that destroy stolen data in an attempt to preserve its confidentiality. This is particularly true given how computer data is defined: "representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system."[50] Similarly, the term "wilfully" would also apply to any ACD efforts, given that the would-be victim knowingly caused the event to occur.[51]

This leaves section 430(1.1)(c) and (d), which refer to obstructing, interrupting, or interfering with the "lawful" use of computer data or a person lawfully using that data. The word "lawful" is key here: such a term would hardly apply to data illegally taken from a victim's network. For example, if a victim company conducts ACD that interferes with the hacker's efforts, (c) and (d) do not appear to apply given that the use of the data was not lawful in the first place. This would also be true in the case of a cyber security contractor hired by the victim company to act on its behalf.

---

46 *Ibid*.
47 *CASL*, *supra* note 32.
48 *Supra* note 31.
49 *Ibid*.
50 *Ibid*, s 342.1(2). (Note that section 430(8) advises that computer data is defined in this section as in section 342.1(2).)
51 *Ibid*, s 429(1), defines "wilfully causing event to occur" as follows:
> Every one who causes the occurrence of an event by doing an act or by omitting to do an act that it is his duty to do, knowing that the act or omission will probably cause the occurrence of the event and being reckless whether the event occurs or not, shall be deemed, for the purposes of this Part, wilfully to have caused the occurrence of the event.

2. SECTION 342.1(1) OF THE *CRIMINAL CODE*: UNAUTHORIZED USE OF COMPUTER

Another, broader offence concerns using a computer in an unauthorized manner. Section 342.1(1) states that anyone is guilty who, "fraudulently and without colour of right":

> (a) obtains, directly or indirectly, any computer service;
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or
> (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).[52]

Note that "computer service" is defined fairly broadly and includes "data processing and the storage or retrieval of computer data."[53]

This section appears to prohibit most, if not all, ACD efforts, on the grounds that any action taken outside the defender's network would likely qualify as obtaining and/or intercepting a computer service. For example, even if a "hack-backer" enters the network of either the hacker or a third party merely to perform surveillance, that individual could be considered to be intercepting computer functions. While section 430(1.1) speaks directly to the alteration of data, the "unauthorized use of computer" offence in section 342.1(1) is clearly more encompassing and would potentially apply to any and all ACD efforts.[54]

It is worth noting that section 342.1(1) applies only to those who act "fraudulently and without colour of right,"[55] terms left undefined in the *Criminal Code*. While the offence has never been tried by the Supreme Court of Canada, it has been considered by the Quebec Court of Appeal on two occasions, *R. c. Parent* and *Thibodeau. c. R*,[56] and most recently by the Alberta Court of Appeal in *R. v. McNish*.[57] All three cases involved a member of a police force using access to confidential databases to conduct searches for reasons other than professional purposes. In *McNish,* the Alberta Court of Appeal interpreted the word "fraudulently" consistently with previous interpretations of the way the word is used in other sections of the *Criminal Code*, such as section 332 (the misappropriation of funds) and section 322 (theft).[58] The Court concluded that, as in *Parent*, "a computer is used fraudulently within the meaning of s. 342.1(1) when it is used intentionally, without mistake, with subjective knowledge that the use is unauthorized."[59] The Court also agreed with *Parent* that it is not necessary for the accused to believe the act to be morally wrong.[60] Finally, the Court found that the accused acted "without colour of right,"[61] a term previously defined as

---

52 *Ibid*, s 342.1(1).
53 *Ibid,* s 342.1(2).
54 *Ibid*, ss 342.1(1), 430(1.1).
55 *Ibid*.
56 *R c Parent,* 2012 QCCA 1653 [*Parent*]; *Thibodeau c R*, 2018 QCCA 1476.
57 *R v McNish*, 2020 ABCA 249 [*McNish*].
58 *Ibid* at paras 58, 62.
59 *Ibid*; *Parent*, *supra* note 56 at para 50.
60 *McNish*, *ibid* at para 59. See also *Parent*, *ibid* at para 38.
61 *McNish*, *ibid* at paras 63–65.

"an honest belief in a state of facts which, [if true], would at law justify or excuse the act done."[62]

These cases are obviously quite different from ACD, involving the use of police resources for unauthorized purposes, rather than technical efforts conducted by a hacking victim. Nevertheless, they do imply that ACD would fall into the category of unauthorized computer use. First, as in *McNish*, anyone intercepting the services of another's computer could be said to be acting intentionally, knowing that use to be unauthorized.[63] Second, fraudulence need not involve an attempt at monetary gain, such as the theft of credit card data. It can involve the use of a database to collect information, even if, as in the case of *Parent,* that information is turned over to another person without monetary compensation.[64] This means that even an ACD user who gathers information about a threat and turns it over to the police could be said to be acting fraudulently. Finally, the question of whether an ACD user believes their actions to be morally right is irrelevant.[65]

3. SECTION 8 OF CANADA'S ANTI-SPAM LEGISLATION: INSTALLATION OF COMPUTER PROGRAM

Besides the *Criminal Code*,[66] a second law of significance to ACD is *CASL*, which, among other things, targets spyware.[67] *CASL* regulates "commercial conduct that discourages the use of electronic means to carry out commercial activities."[68] *CASL* specifies that an individual may not "in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system or, having so installed or caused to be installed a computer program, cause an electronic message to be sent from that computer system" unless the individual has either a court order or "express consent of the owner or an authorized user."[69]

This law is particularly relevant to "beacons." A beacon is one of several tools that can notify the owner if protected files leave the network, potentially even ascertaining the stolen files' new location.[70] In practice, this is a piece of computer code placed into an important file. It can either act as a "burglar alarm" to alert the file owner of an attempt to move the file outside the network, or, in more extreme cases, it can send "information about the internet addresses and network configurations of the computer systems that a stolen document is channeled through, ideally assisting with attribution and forensic evaluation of remote devices."[71] If a beacon causes the unauthorized installation of a computer program, it would

---

62 *R v Simpson*, 2015 SCC 40 at para 31, citing *R v DeMarco* (1973), 13 CCC (2d) 369 (Ont CA) at 372.
63 *McNish*, *supra* note 57 at paras 58, 62.
64 *Supra* note 56 at para 11. In *Parent*, a member of the Royal Canadian Mounted Police obtained information related to three vehicle registration numbers and then provided the information to a private investigator without remuneration.
65 *McNish*, *supra* note 57 at para 59.
66 *Supra* note 31.
67 *Supra* note 32.
68 *Ibid*, s 3.
69 *Ibid*, s 8(1).
70 Commission on the Theft of American Intellectual Property, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (USA, National Bureau of Asian Research, 2013) at 81, online: <www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf>.
71 Center for Cyber and Homeland Security, *supra* note 16 at 10.

qualify as an offence under section 8(1) of *CASL*.[72] This may not be the case for a beacon that simply notifies the owner that files have been copied to another network, but it is a potential concern if the beacon installs a program on the hacker's network, in order to send back information to the original data owner regarding its new location.[73]

4. SECTION 342.2(1) OF THE *CRIMINAL CODE*: POSSESSION OF DEVICE TO OBTAIN UNAUTHORIZED USE OF COMPUTER SYSTEM OR TO COMMIT MISCHIEF

Finally, while the legislation discussed so far applies to ACD itself, the *Criminal Code* also contains a prohibition relevant to companies that might market ACD tools, even if they do not themselves carry out ACD.[74] Section 342.2(1) declares anyone guilty who:

> without lawful excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available a device that is designed or adapted primarily to commit an offence under section 342.1 or 430, knowing that the device has been used or is intended to be used to commit such an offence.[75]

Notably, the definition of device includes computer programs,[76] which could, in turn, include ACD software. However, ACD software is often multipurpose software that can be used for legal as well as illegal means, depending merely on whether it is deployed inside or outside the defender's own network.[77] In other words, companies marketing ACD software could make the case that they designed and intended their software to be used only for legal purposes. This reasoning in itself might constitute "lawful excuse."

As things stand, then, ACD should in general be considered illegal under the *Criminal Code*, despite no offence having been prosecuted so far. This is due to the broad nature of the "unauthorized use of computer" offence in section 342.1(1) of the *Criminal Code,* which classifies any form of unauthorized interception of a computer service as an offence.[78] Other Canadian legislation is also relevant: section 430(1.1) prohibits tampering with data,[79] while *CASL* prohibits the unauthorized installation of computer programs.[80]

The next section will consider whether an exception may exist for ACD as the defence of property.

---

72 *Supra* note 32.

73 Note that CASL also prohibits altering "transmission data in an electronic message" to deliver it to another destination "in the course of a commercial activity" (*ibid*, s 7(1)). However, this provision would not generally apply to ACD, given that an electronic message is defined as "a message sent by any means of telecommunication, including a text, sound, voice or image message" (*ibid*, s 1(1)). While attribution data could certainly be transmitted back to the victim company in the form of a message, the data is unlikely to be a "message" in its initial state.

74 *Supra* note 31, s 342.2(1).

75 *Ibid*.

76 *Ibid*, s 342.2(4)(b).

77 Schmidle, *supra* note 6. This article refers to "MazeHunter," a product capable of being used inside or outside the defender's network.

78 *Supra* note 31.

79 *Ibid*.

80 *Supra* note 32.

B. ACD AS THE DEFENCE OF PROPERTY?

While prohibiting mischief and unauthorized computer use, Canadian law does contain provisions in the *Criminal Code* allowing for the defence of property.[81] Such an allowance prompts the question of whether data is considered property and, if so, whether defence of property could be used as a legal defence for ACD. In fact, in one of the few instances of Canadian research on ACD, Chandler argues that the concept of "self-help" is about promoting "equality" when it comes to an attack.[82] If the defender's options for self-help are too limited, the attacker will always hold the advantage in cyberspace.[83]

Similarly, US proponents of ACD have argued that ACD is legal as a form of self-help, specifically defence of property. West states that US common law allows corporations to exercise "rights of defense of property."[84] He points to networks and intellectual property as forms of property that US companies might be entitled to protect.[85] While not in favour of unrestricted ACD, Kesan and Hayes also refer to US common law's provisions for self-defence and defence of property.[86] Although cautioning that lethal force is generally impermissible, they add that "mitigative counterstriking" (roughly equivalent to ACD) is likely to be considered non-lethal.[87] In fact, even if the defence of property harms a third party, the defender may not be guilty if they have made "reasonable efforts" to find the real intruder.[88]

Section 35(1) of the *Criminal Code* states that an individual is not guilty of an offence if they meet four criteria for the defence of property.[89] First, individuals must reasonably believe that they either own the property themselves or are acting under the owner's authority.[90] Second, they must reasonably believe that another person:

> (i) is about to enter, is entering or has entered the property without being entitled by law to do so,
>
> (ii) is about to take the property, is doing so or has just done so, or
>
> (iii) is about to damage or destroy the property, or make it inoperative, or is doing so.[91]

Third, the act of defence must be conducted to prevent the intruder from entering or to expel them from the property, or to prevent them from "taking, damaging or destroying the property or from making it inoperative, or retaking the property from that person."[92] Fourth,

---

81 *Supra* note 31.
82 *Supra* note 15.
83 *Ibid* at 39–76.
84 *Supra* note 44 at 130.
85 *Ibid*.
86 Jay P Kesan & Carol M Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace" (2012) 25:2 Harv JL & Tech 429.
87 *Ibid*.
88 *Ibid* at 521. Besides Kesan and Hayes, West is another example of a researcher who applies the term "self-defence" to hack-back efforts (*supra* note 44 at 130–38). While the *Criminal Code* has provisions for both self-defence and defence of property, I discuss only the defence of property here, as it is clearly more applicable to hack-back and is defined separately from self-defence in the *Criminal Code*. Self-defence only applies to situations when a person faces force or a threat of force "against them or another person" (*supra* note 31, s 34(1)).
89 *Criminal Code*, *ibid*.
90 *Ibid*, s 35(1)(a).
91 *Ibid*, s 35(1)(b).
92 *Ibid*, s 35(1)(c).

the defence must be "reasonable in the circumstances."[93] In summary, any defence must be undertaken under the authority of a property owner, acting to stop an intruder or would-be intruder from taking or harming property. The action taken must also essentially be for the purpose of mitigating damage and theft (for instance, as opposed to revenge), and that action must be reasonable.

Two issues would exist in using the exception for defence of property to justify ACD. The core issue is that data is not considered "property" under Canadian law. The *Criminal Code* differentiates between "mischief" committed in regard to property as opposed to computer data.[94] "Property" is defined as "real or personal corporeal property,"[95] while computer data is defined separately, as "representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system."[96] Similarly, in *R. v. Stewart*,[97] the Supreme Court of Canada ruled that confidential information was not considered to be property, as it could neither be "taken" nor converted. While not a case of cybercrime, the case concerned "the theft of confidential information *per se*," as opposed to a "tangible object containing confidential information."[98] Justice Lamer noted, "[i]f confidential information is considered as property for the purposes of the theft section, other sections of the *Criminal Code* relating to offences against property may also apply" to information, including defence of property.[99] Conversely, if confidential information is not considered as property for the purposes of the theft section, it seems reasonable to infer that information is also not property for the purposes of the section pertaining to defence of property.

Even if data were considered property, however, ACD would be unlikely to qualify as a defence of that property. For proactive measures like automated ACD, it would be difficult to claim that the would-be victim believed an intruder was "about to enter," let alone steal or compromise data. Automated ACD establishes steps to be followed before the intruder is even detected, so that "defence" becomes something more akin to a pre-set trap for any and all intruders. And if a proactive approach could not be taken, the alternative would be the use of ACD *following* the discovery of a breach. The difficulty here is that many breaches are not discovered until weeks or months after the fact. For this reason, security firms are not generally able to "strike down intruders."[100] ACD in this case becomes not a matter of immediate reaction, but prolonged intelligence gathering. In other words, the *Criminal*

---

93 *Ibid*, s 35(1)(d).
94 *Ibid*, ss 430(1), 430(1.1).
95 *Ibid*, s 428.
96 *Ibid*, s 430(8) advises that computer data is defined as in section 342.1(2), from which this definition is taken.
97 [1988] 1 SCR 963.
98 *Ibid* at 974 [emphasis in original]. Justice Lamer stated at 979–80:

> [P]roperty must be capable of being taken or converted in a manner that results in the deprivation of the victim.
>
> …
>
> The question is thus whether confidential information is of a nature such that it can be taken or converted. In my opinion, except in very rare and highly unusual circumstances, it is not. As we have seen, information *per se* cannot be the subject of a taking. As for conversion, it is defined as an act of interference with a chattel inconsistent with the right of another, whereby that other is deprived of the use and possession of it. Confidential information is not of a nature such that it can be converted because if one appropriates confidential information without taking a physical object...the alleged owner is not deprived of the use or possession thereof.

99 *Ibid* at 976–77.
100 Rabkin & Rabkin, *supra* note 5 at 11.

Code's provision for defence of property is likely insufficient to enable ACD in an effective way.[101]

IV. INTERNATIONAL LAW: IMPACTS ON ACD

Were Canada to contemplate the inclusion of an exception for ACD in its computer crime legislation, it would still be constrained by international law. The most relevant treaty is the 2001 Convention on Cybercrime, also known as the Budapest Convention, a treaty signed and ratified by Canada as well as its allies.[102] The Budapest Convention requires signatory countries to criminalize several acts that ACD would or could involve.[103]

First, Articles 2, 3, and 4 require the criminalization of illegal access, illegal interception, and data interference, respectively.[104] Illegal interception in Article 3 refers to "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system."[105] Meanwhile, data interference in Article 4 is "the damaging, deletion, deterioration, alteration, or suppression of computer data without right," although a state may require that interference to cause "serious harm."[106] Certainly, some forms of ACD would be at odds with these two articles. However, Article 2 is most problematic from an ACD perspective.[107] States must criminalize illegal access, defined as "access to the whole or any part of a computer system without right."[108] Article 2 thus poses the most definitive prohibition on allowing ACD. In other words, this article addresses not only more extreme forms of ACD that involve deleting data or damaging another network, but also any kind of surveillance outside one's own network.

Article 6 also addresses the "misuse of devices" for purposes of illegal access, illegal interception, data interference, or system interference.[109] States are required to criminalize "the production, sale, procurement for use, import, distribution or otherwise making available of" devices that are "designed or adapted primarily for the purpose of committing" one of the offences listed above, provided that it is "with intent" that they be used to commit one of the listed offences.[110] Included in the category of "devices" are computer programs,[111] and the fact that this definition would apply to ACD software means that states have agreed to prohibit companies from distributing such software "with intent." This article is of course reminiscent of section 342.2(1) of the *Criminal Code*.[112]

Despite these prohibitions, there are two qualifying factors to be considered. First, the articles pertaining to ACD itself (Articles 2–4) refer to actions conducted "without right."[113] The fact that this phrase is not defined in the Budapest Convention leaves some room for

---

101 *Supra* note 31.
102 *Convention on Cybercrime*, 23 November 2001, Eur TS 185 (entered into force 1 July 2004).
103 *Ibid*.
104 *Ibid*.
105 *Ibid*.
106 *Ibid*.
107 *Ibid*.
108 *Ibid*, art 2.
109 *Ibid*, art 6.
110 *Ibid*, art 6(1).
111 *Ibid*, art 6(1)(a)(i).
112 *Supra* note 31.
113 *Supra* note 102.

interpretation. Access "without right" could apply to any action a firm takes outside its network, assuming that a state has criminalized such an action. At the same time, it is possible that a state such as Canada could establish a right for firms (or individuals) to deploy ACD under certain conditions. In this event, users of ACD would be within their legal rights, and Canada would not be in violation of the Budapest Convention.

Second, Rosenzweig points out that the Budapest Convention's accompanying Explanatory Report[114] allows that would-be cybercrimes may be considered "legal or justified *not only in cases where classical legal defenses are applicable, like consent, self defence or necessity,* but where other principles or interests lead to the exclusion of criminal liability."[115] This wording suggests leeway for states to allow cyber self-defence as a legal defence in criminal law. Nevertheless, as previously highlighted in the context of Canadian domestic law, the characterization of ACD as either self-defence or the defence of property remains problematic. Rosenzweig himself states that the right to self-defence is a limited one and that, if the law of piracy is used as an analogy, only a state is entitled to take ACD measures — although he entertains the possibility that a state may issue "letters of marque" to authorize "cyber privateers."[116] Self-defence, then, could only justify ACD if companies are somehow authorized by the state as "privateers"; in order to apply to the private sector, self-defence would need to be conducted on behalf of a state.

Beyond international law, there is the separate but related question of international norms. Along with over 75 other states and hundreds of companies, Canada has signed the 2018 Paris Call for Trust and Security, condemning hack-back on the part of the private sector or other non-state actors.[117] Similarly, all G7 nations have domestic legislation forbidding unauthorized access, and as Shackelford et al. suggest, "If anything … the international community seems to be turning away from such a permissive regime [toward ACD] save, perhaps, for elements within the United States and Singapore."[118]

---

114 *Explanatory Report to the Convention on Cybercrime*, 23 November 2001, Eur TS 185.

115 *Supra* note 13 at 108–109 [emphasis in original], citing *ibid* at para 38.

116 Rosenzweig, *ibid* at 112–13. Note that the suggestion of "letters of marque" gives rise to yet another question, that of state sovereignty. Only a state is capable of violating another state's sovereignty. While a corporation that hacks back of its own initiative may violate another state's domestic laws, its actions do not violate that state's sovereignty. However, the situation changes if the defender's actions are attributable to a state — as they may be in a scenario involving "letters of marque." See Michael N Schmitt & Liis Vihul, eds, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed (Cambridge: Cambridge University Press, 2017) at 90–91. A separate but related consideration is the principle of due diligence. As stated in the *Tallinn Manual 2.0*, "a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States" (*ibid* at 30). Similarly, Graham suggests that a state's "imputed responsibility" to prevent cyber acts includes requirements such as criminal law against international cyber acts, investigation, prosecution, and co-operation with investigations conducted by victim states. David E Graham, "Cyber Threats and the Law of War," (2010) 4:1 J National Security L & Policy 87 at 93–94. At the same time, the *Tallinn Manual* remains essentially a legal opinion, and its characterization of the requirement for due diligence does not necessarily represent international consensus, let alone binding international law. As Efrony and Shany point out, it is not clear what due diligence would entail for issues such as whether host or intermediary states have a duty to stop potential cyber operations, or how to determine whether a state "should" be aware of a cyber operation launched from its territory. See Dan Efrony & Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice" (2018) 112:4 AJIL 583 at 592–93.

117 "Paris Call for Trust and Security in Cyberspace" (12 November 2018), online: <pariscall.international/en/call>.

118 *Supra* note 12 at 409. Note that the authors' remark refers to a bill viewed as enabling a limited form of ACD in Singapore, passed but no longer in effect.

In conclusion, international law and norms may discourage ACD, but this discouragement does not necessarily constitute outright prohibition. This leaves room for the possibility that Canada could amend the *Criminal Code*[119] to carve out an exception for ACD.

V. ACD IN PRACTICE: THREE SCENARIOS

As the above discussion highlights, Canadian law prohibits most, if not all, ACD efforts, while international law also potentially sets restrictions on what actions can be legalized. However, ACD can take several forms, depending on how it is conducted and the actors involved. With this in mind, the following sections explore three scenarios in which ACD may be used, along with illustrative aspects of each scenario and a summary of how the law relates.

A. SCENARIO 1: A COMPANY RESPONDS TO A CYBER INTRUSION WITH ACD

In the simplest form of ACD, a company responds to a cyber intrusion. Either the victim company acts on its own behalf, or a security firm carries out ACD on behalf of a client or clients.

An example of such an event may have taken place in 2009 to 2010, when Google became aware of a breach to its infrastructure. Tracing the intrusion, Google was able to "determine definitively" that the source was located in China,[120] and the company subsequently shared its intelligence with law enforcement, other affected companies, and the public as a whole.[121] While it is not clear how Google gained its intelligence, some speculated that Google had ventured outside its corporate network, using a Taiwanese server in the process of tracing the cyber intrusion.[122]

This incident demonstrates two main points about ACD. First, though the term "hack-back" may evoke warlike imagery of cyber offensives volleying between computers, the reality is quite different. What is called hack-back is frequently a matter of intelligence gathering, due to the challenges associated with stopping a real-time intrusion: an organization generally realizes an intrusion has taken place weeks or months afterward.[123] This precludes the possibility of "stopping" a threat before it takes hold. Rather, a security firm will examine the evidence in the aftermath of the intrusion and compare it with other information, such as that of other security firms.[124] In other words, ACD often becomes less about "striking" at an intruder, and more about collecting information in order to forestall future threats.

---

119 *Supra* note 31.

120 Kim Zetter, "Google to Stop Censoring Search Results in China After Hack Attack," *Wired* (12 January 2010), online: <www.wired.com/2010/01/google-censorship-china/>.

121 David Drummond, "A New Approach to China" (12 January 2010), online: <googleblog.blogspot.com/2010/01/new-approach-to-china.html>.

122 Center for Cyber and Homeland Security, *supra* note 16 at 40.

123 Indeed, a 2013 report by Mandiant on one threat actor, APT1, found that it held access to compromised networks for 356 days on average and almost five years in one case. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units" (2013) at 21, online: <www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

124 Rabkin & Rabkin, *supra* note 5 at 11.

Second, it is significant that Google was the firm that conducted this reconnaissance effort. Realistically, would-be users of ACD are a subset of the private sector, particularly those firms with significant resources or cyber expertise. Those companies are more likely to have the capacity to perform some measure of ACD — unlike small and medium enterprises, which may struggle to put even basic cyber security measures into place.[125] Additionally, large companies or those providing critical infrastructure[126] present a more tempting target for advanced persistent threats — sophisticated threats in the form of state actors or criminal groups. In contrast, the majority of companies have little incentive to use ACD because they face much less formidable threats; basic cyber security measures are generally adequate for their needs.[127]

In Canadian jurisdiction, such an intrusion would fairly clearly constitute a violation of section 342.1(1)(b) of the *Criminal Code,* assuming that the company "intercepted" a computer system's functions without any legal justification.[128] The same could be said generally of ACD efforts that follow a similar pattern, even if the "hack-backer" is charged only with unaggressive surveillance activities.[129]

B. SCENARIO 2: A COMPANY USES A BEACON

While the above scenario is fairly uncomplicated, a potentially grey area lies in efforts on the "passive" side of the ACD spectrum. This scenario focuses on the use of beacons given that this area has gained particular attention in the US context. Similar questions, however, could exist regarding any security measure that is put in place proactively, rather than as a reaction to an intrusion.

In a beaconing scenario, a company, or a security firm working on its behalf, embeds a beacon into a file proactively, before a hacker "steals" the file. The beacon then notifies the victim if the file is removed from the company's network. It has no detrimental effect on the

---

125 Joyce M Rosenberg, "Small Businesses Increasingly a Target for Cybercriminals," *Fifth Domain* (7 October 2019), online: <www.fifthdomain.com/industry/2019/10/07/small-businesses-increasingly-a-target-for-cybercriminals/>.

126 Public Safety Canada defines critical infrastructure as "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government." It lists ten critical infrastructure sectors: energy and utilities; finance; food; transportation; government; information and communication technology; health; water; safety; and manufacturing. Public Safety Canada, *National Strategy for Critical Infrastructure*, Catalogue No PS4-65/2009E-PDF (Ottawa: Public Safety Canada, 2009) at 4, online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>.

127 Richard A Clarke & Robert K Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin Press, 2019) at 43.

128 *Supra* note 31.

129 A slight variant of the above situation involves security firms venturing into others' networks solely for the purpose of gathering intelligence on cyber threats, possibly without being hired to do so by a corporate client. While such an action does not technically constitute "hack-back" given the lack of direct provocation, it similarly may take place outside a firm's own network. One example is that of a 74-page report released by the security firm Mandiant in 2013. The report includes detailed analysis of the techniques used by what it refers to as "APT1," presumed to be a unit of the People's Liberation Army. In the words of the authors, "We uncovered a substantial amount of APT1's attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures)" (*supra* note 123 at 2). As in the case of Google, reports such as this raise the question of exactly how the information was obtained. For example, Rabkin and Rabkin allege that Mandiant and another firm, Crowdstrike, are conducting what amounts to ACD, saying, "There are a number of episodes in which private security firms have traced hack attacks to their sources — that is, gone into computer networks, in the United States and abroad" (*supra* note 5 at 10).

hacker's network. As in the US context,[130] it is not obvious whether beacons can be used in Canada without violating the *Criminal Code*.[131] This instance of ACD does not seem to constitute "mischief in relation to computer data," as defined in section 430(1.1) of the *Criminal Code*, given that it does not destroy or otherwise alter data.[132] It is more debatable whether such an action violates section 342.1(1) on the unauthorized use of a computer.[133] A simple "burglar alarm" would probably not intercept another computer's functions, but a forensic beacon, sending back network configuration data, likely would.

Beacons may also violate *CASL*.[134] A person may not "install or cause to be installed a computer program on any other person's computer system or, having so installed or caused to be installed a computer program, cause an electronic message to be sent from that computer system" without either a court order or express consent of the owner.[135] However, in the case of a beacon, is it truly the victim (or its security firm) that "caused" the beacon to install and transmit data from the hacker's network? Or is it the hacker who "caused" the beacon's effect, meaning that no *CASL* violation took place?[136] While the hacker's actions triggered the beacon's functions, it was the victim who originally prepared the beacon, solely for the purpose of it later being activated. Considering that the victim had the intent for the beacon to be installed under certain circumstances, it is likely that the defender would be held responsible for this action.

In summary, any beacon that transmits attribution data is likely illegal under Canadian law. First, it may be considered to intercept a computer's functions, prohibited by section 342.1(1) of the *Criminal Code*.[137] Second, *CASL*'s prohibition on the installation of a computer program on another person's computer would likely limit the use of beacons as well.[138]

C. SCENARIO 3: A VENDOR SELLS SOFTWARE ENABLING ACD

In a final scenario, ACD may involve two distinct actors, in the form of a software vendor and a client. The software vendor sells ACD-enabling software to a company, which proceeds to conduct ACD. In all likelihood, these efforts would be conducted on an ongoing basis and possibly even automated to respond to threats.

Cyber security firm Symbiot produced an early example of such a software in 2005, in the form of its Intelligent Security Infrastructure Management System (iSIMS).[139] It advertised iSIMS as offering "graduated responses" to cyber threats, including the ability to conduct

---

130 Chesney, *supra* note 34; Christopher M Matthews, "Support Grows to Let Cybertheft Victims 'Hack Back,'" *The Wall Street Journal* (2 June 2013), online: <www.wsj.com/articles/SB10001424127887324682204578517374103394466>.

131 *Supra* note 31.

132 *Ibid*

133 *Ibid*.

134 *Supra* note 32.

135 *Ibid*, s 8(1).

136 *Ibid*.

137 *Supra* note 31.

138 *Supra* note 32.

139 Smith, *supra* note 7.

what it called "distributed denial of service counterstrikes."[140] The term "distributed denial of service" (DDoS) refers to an attacker disrupting the victim's web services by flooding them with service requests. While there are legitimate means of mitigating a DDoS attack, the term "counterstrike" certainly implied that Symbiot's product was in fact designed to interfere with other computer systems. And in fact, Symbiot went so far as to publish a set of "rules of engagement," essentially outlining a philosophy on counterstrikes.[141]

Maurushat suggests that similar counter-DDoS systems are in use today.[142] Such systems raise two legal questions.

First, are such systems illegal if they are pre-emptively put in place? The answer appears to be yes. As Maurushat states, "[t]here is an assumption that these systems are perfectly legal, when of course, they are not; the law does not allow for unauthorized access or modification of any system."[143] For instance, if a counter-DDoS deflected an attack but disrupted its attacker's system or any other intermediary systems, it would likely violate section 342.1(1) because it intercepted another computer system's functions.[144]

Second, is a vendor allowed to sell products that may or may not be used to conduct ACD? And can a vendor be held liable if such products cause harm — including harm to intermediary, third party computers that have been compromised and used to execute the original cyber intrusion? The answer to these questions may be less straightforward. The matter rests on whether the vendor is selling software that is "designed or adapted primarily to commit an offence," as articulated by section 342.2(1) of the *Criminal Code*.[145]

In some cases, such as automated counter-DDoS, the use of the tool seems obviously designed to be used for illegal purposes. In other cases, it may depend on how the tool is used. In general, a client can legally take any action they choose on their own network — such as collecting forensic information and then severing the intruder's server connection. The same actions, however, are not necessarily legal outside the client's network. In fact, in a 2018 interview, the vice-president of Cymmetria, a company that provides a tool for "legal hack-back," was asked whether its products could be used for illegal measures.[146] His reply was that "[i]t's up to the *client* to decide how to use them [Cymmetria's tools]…. Anything the bad guys can do, the clients can do. Not legally. There's a difference between 'can' and 'may.'"[147] In practical terms, then, the problem may lie less with cyber security firms themselves conducting ACD and more with firms selling products that enable their clients to conduct ACD on their own. This is a more difficult problem to address, because clients are less likely to educate themselves on the legal implications of their actions than firms whose core business is cyber security.

---

140 *Ibid* at 176–78.
141 *Ibid* at 178, citing Paco Nathan & Mike Erwin, "On the Rules of Engagement for Information Warfare," 4 March 2004.
142 *Supra* note 15 at 244–45.
143 *Ibid* at 245.
144 *Supra* note 31.
145 *Ibid*, s 342.2(1).
146 Schmidle, *supra* note 6.
147 *Ibid.*

Additionally, some have suggested that cyber security vendors in certain countries (such as the United States and Israel) may be taking a more aggressive stance in cyberspace than their counterparts elsewhere.[148] For Canada, there is not only the question of whether any form of ACD is legal but also whether Canadian firms may sell software that is easily, and perhaps commonly, used for illegal purposes. And as articulated by the Budapest Convention, international law is very specific when it comes to the use of such software, stating that "the production, sale, procurement for use, import, distribution or otherwise making available of" such software should be established as a criminal offence under countries' domestic law.[149] Again, however, it is possible to make the case that software used for ACD has not been designed to facilitate committing an offence, but is simply a multi-purpose tool that can be misused — similar to a knife or a firearm.

D. INSIGHTS FROM THE THREE SCENARIOS

As these scenarios demonstrate, most forms of ACD are illegal under Canadian law. If a hacking victim enters another network in response to a hack, that action likely violates the *Criminal Code*, even if the victim is only collecting information about the intruder.[150] Legality becomes less certain when it comes to the use of beacons. It may be that beacons are legal but only to issue an alert that a file has been removed, rather than to transmit attribution information back to the victim. The latter function likely constitutes a violation of the *Criminal Code* and *CASL*.[151] This lack of clarity is of concern, given that some companies openly offer beaconing services to their clients.

Canada may also need to confront the question of whether it will allow vendors to sell products that facilitate conducting ACD. Some products may be obviously designed for ACD purposes, but others may be tools that could be used either inside the network (legally) or outside it (illegally). Indeed, international law may require Canada to take a more active stance against such tools in the future.

VI. EXPLORING THE NEED FOR ACD

As demonstrated by both the legal analysis and the three scenarios, Canada's legal environment is generally prohibitive of ACD, with beaconing being the main possible exception. This section explores several reasons to consider the legalization of ACD. Beginning with a brief overview of the current cyber threat environment, it then discusses cyber security practices, including measures undertaken by companies themselves, internet service providers (ISPs), or the government.

A. THE CYBER THREAT LANDSCAPE

A number of high-profile cybercrimes have affected Canadians over the last decade, with targets that included critical infrastructure. One recent example is the 2019 hack of Canadian medical testing company LifeLabs, recorded as the largest data breach in Canada to date,

---

148 Center for Cyber and Homeland Security, *supra* note 16 at 24; see also Broeders, *supra* note 14 at 43.
149 *Convention on Cybercrime*, *supra* note 102, art 6.
150 *Supra* note 31.
151 *Ibid*; *supra* note 32.

which resulted in the exposure of the personal information of 15 million Canadians — close to half of Canada's population.[152] Moreover, a 2020 report by IBM found Canadian data breaches to have an average data breach cost of USD $4.5 million, the third highest average cost for data breaches among the 17 countries and regions surveyed. In Canada, 42 percent of data breaches were attributed to malicious attack.[153]

Nor are cybercriminals the only kind of cyber actor threatening Canadian organizations. A threat actor known as "Cozy Bear," assessed to be part of a Russian intelligence service, has targeted multiple organizations working toward COVID-19 vaccine development in Canada, the United States, and the United Kingdom.[154] Moreover, in 2020, Canada's main cyber security agency judged state-sponsored actors as "very likely attempting to develop" capabilities allowing them to disrupt the Canadian electricity industry.[155] In fact, it was reported in 2019 that a hacker group associated with Russia had already probed the networks of electric systems in North America.[156] And while the perpetrators of such infrastructure intrusions may include cybercriminals and state actors alike, their victims are typically the private sector.[157]

In this environment, there is reason to believe that there is demand for ACD. According to one cyber security firm's vice-president of operations, most cyber security firms "dance at the limits of computer trespassing every single day of the week."[158] In a Dutch study commissioned by the Netherlands Ministry of Defence, interviews with stakeholders in the private cyber security sector revealed that all interviewees reported "frequent requests from their clients to 'take down the server' that commands an attack, including when it is likely to be located abroad."[159] All of them also reported awareness of firms "operating on the Dutch market" that would obey such a request.[160] Similarly, a former senior litigator for the US Justice Department stated in 2013 that companies "routinely" sought (and were denied) "tacit approval" for ACD activities during her time at the department.[161]

B. ACD IN THE CONTEXT OF OTHER CYBER SECURITY MEASURES

Given these challenges, the question is whether companies are adequately equipped to respond to threats using current security measures. It is important to note that for most companies, traditional cyber security measures, such as firewalls or anti-virus software, are

---

152 Scott Ikeda, "Lifelabs Data Breach, the Largest Ever in Canada, May Cost the Company Over $1 Billion in Class-Action Lawsuit," *CPO Magazine* (8 January 2020), online: <www.cpomagazine.com/cyber-security/lifelabs-data-breach-the-largest-ever-in-canada-may-cost-the-company-over-1-billion-in-class-action-lawsuit/>.

153 The report studied 524 organizations across 17 countries and regions, all of which experienced a data breach between August 2019 to April 2020: IBM Security, "Cost of a Data Breach Report 2020" (2020) at 23, 33, online: <www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf>.

154 UK, National Cyber Security Centre, *Advisory: APT29 Targets COVID-19 Vaccine Development* (16 July 2020), online: <www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development>.

155 Canadian Centre for Cyber Security, *supra* note 30 at 21.

156 *Ibid*. See also Andy Greenberg, "The Highly Dangerous 'Triton' Hackers Have Probed the US Grid," *Wired* (14 June 2019), online: <www.wired.com/story/triton-hackers-scan-us-power-grid/>.

157 O'Neill, *supra* note 5 at 276.

158 Schmidle, *supra* note 6.

159 Broeders, *supra* note 14 at 43 [emphasis in original].

160 *Ibid*.

161 Matthews, *supra* note 130.

in fact adequate. However, this is not true for all companies. The difference lies in opportunistic versus targeted hacking. The average company faces an opportunistic hacker, who probes for vulnerabilities and seeks to take advantage of them. If unable to discover a vulnerability, the hacker moves on to a new potential victim. For opportunistic hacking, vulnerability mitigation in the form of firewalls and patches can be effective because the hacker moves on to easier targets when resistance is encountered.[162]

These measures are not effective, however, against targeted hacking, which features an adversary seeking to obtain specific information or achieve certain effects in a particular network. For example, this was true in the Google scenario discussed above; one of the hackers' goals was to obtain access to Chinese human rights activists' Gmail accounts.[163] Such an intruder is often considered an "advanced persistent threat" and may be a state actor or sophisticated criminal group with significant resources, seeking to obtain information in what may amount to a multi-year campaign.[164] In this case, passive network defence measures prove insufficient, because they can never achieve perfect defence against a determined adversary. If only passive measures are in place, breaches become inevitable because the adversary outlasts the defender.[165] Given this reality, the defender must take an approach that focuses not only on the defender's own vulnerabilities but on the threat itself.[166] ACD has the potential to become one means of addressing the threat after it has penetrated the network, rather than seeking to block off threats entirely from the network's perimeter.

In this context, it may be most helpful to consider ACD as an extension of current threat-based cyber security practices. A prime example is threat intelligence. Threat intelligence focuses on the threat, rather than controls and vulnerabilities; in this way, it allows the defender to address threats with an understanding of the adversary's techniques, rather than fixating on incident response.[167] Similarly, threat hunting involves seeking out the threat on the victim's network following a breach. Fundamental to threat hunting is the idea of deception — tricking the adversary by limiting access to real information and instead allowing the would-be victim to watch as the hacker displays their tools and techniques. This practice not only provides the defender with an understanding of how the hacker operates, but it also frustrates the hacker by wasting their time.[168]

Another alternative lies in leveraging ISPs for cyber security. For example, one Microsoft security executive asserts that the ideal way to thwart an intruder is simply to determine the

---

162 Commission on the Theft of American Intellectual Property, *supra* note 70 at 79–80.

163 Drummond, *supra* note 121.

164 One definition of advanced persistent threats is "well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information": Eric M Hutchins, Michael J Cloppert & Rohan M Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," (2010) at 1, online: <www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>.

165 West, *supra* note 44 at 128.

166 Commission on the Theft of American Intellectual Property, *supra* note 70 at 79–80.

167 Michael Muckin & Scott C Fitch, "A Threat-Driven Approach to Cyber Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization," (2019), online: <www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf>. For an understanding of sample techniques, see MITRE, "Enterprise Techniques," online: <attack.mitre.org/techniques/enterprise/>.

168 Clarke & Knake, *supra* note 127 at 55–58.

IP addresses for the "immediate" source of the intrusion, rather than its origin.[169] At that point, one can call the hosting service to ask for the account using the relevant IP addresses to be shut down.[170] Similarly, Canada's telecommunications regulator, the Canadian Radio-television and Telecommunications Commission, is considering the development of a framework to better harness ISPs' capabilities in cyber security. The framework would require ISPs to use new strategies to block botnet activity.[171] ISPs already play a significant role in cyber security, and that role holds the potential to expand in the future.

Undoubtedly, passive security, threat-based security, and ISP involvement are all invaluable to cyber security, and ACD would by no means replace these practices. Nevertheless, this fact does not necessarily negate the need for ACD. ACD may never be the primary means of collecting threat intelligence, but it does have the potential to expand a company's cyber security toolkit by allowing further reach to its intelligence collection activities. And indeed, there is reason to believe there is demand for cyber security efforts that reach outside the victim's own network. As the next section will explore, one of the most convincing arguments for ACD comes from an unlikely source: the Canadian government itself.

C. ACD IN THE CONTEXT OF GOVERNMENT INVOLVEMENT

In recent years, countries have ramped up their development of offensive cyber capabilities,[172] and Canada is no exception. In 2017, Canada announced the development of active cyber capabilities in its defence policy,[173] while in 2019 the *Communications Security Establishment Act*[174] expanded the mandate of the CSE[175] to allow for defensive cyber operations and active cyber operations.[176] The *CSE Act* hints at the intention for the government to protect not only government infrastructure but also critical infrastructure owned and operated by the private sector. Under the *CSE Act*, the CSE is responsible to "carry out activities on or through the global information infrastructure to help protect" not

---

169 Sydney J Freedberg Jr, "Don't Hack Back: Call the FBI & They'll Call NSA," *Breaking Defense* (6 September 2019), online: <breakingdefense.com/2019/09/dont-hack-back-call-the-fbi-theyll-call-nsa/>.

170 *Ibid*.

171 Canadian Radio-television and Telecommunications Commission, *Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9*, Public Record: 11011-NOC2012-0009 (Gatineau: CRTC, 13 January 2021), online: <crtc.gc.ca/eng/archive/2021/2021-9.htm>.

172 In 2017, Richard Ledgett, the former director of the National Security Agency, estimated that over 100 countries possessed the capability to launch offensive cyber operations: Mike Levine, "Russia Tops List of 100 Countries That Could Launch Cyberattacks on US," *ABC News* (18 May 2017), online: <abcnews.go.com/US/russia-tops-list%20-100-countries-launch-cyberattacks-us/story?id=47487188>.

173 Canada, National Defence, *Strong, Secure, Engaged: Canada's Defence Policy*, Catalogue No D2-386/2017E (Ottawa: National Defence, 2017) at 111, online: <www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf>.

174 SC 2019, c 13, s 76 [*CSE Act*].

175 The CSE describes itself as "Canada's national lead for foreign signals intelligence and cyber operations, and the technical authority for cybersecurity" (Public Safety Canada, *Cyber Security in the Canadian Federal Government*, online: <www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx>). The CSE's mandate includes collecting foreign intelligence, defending Canada's cyber systems, conducting defensive and active foreign cyber operations, and assisting federal law enforcement and security agencies, as well as the Canadian Forces and the Department of National Defence (Canada, Communication Security Establishment, *Mandate*, online: <www.cse-cst.gc.ca/en/corporate-information/mandate>). Notably, the CSE is a civilian agency.

176 Both the defence policy and the *CSE Act* use the term "active" cyber operations, rather than "offensive" cyber operations. Based on the context, however, the meaning appears to be the same. For example, the defence policy articulates the need to use active cyber operations in military missions (*ibid*; *CSE Act*, *supra* note 174).

only federal institutions' information and infrastructure, but also any "electronic information" or "information infrastructures" that the Minister of National Defence designates as important to the Government of Canada.[177] For example, the CSE could hypothetically be called upon to respond to a cyber threat against the financial sector with its own cyber operation.

While the *CSE Act* differentiates between defensive and active cyber operations, both forms of operations are to be conducted outside Canadian networks. Active cyber operations are intended to interfere with "capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[178] Defensive cyber operations are intended to "help protect" Canadian information and infrastructure.[179] However, neither form of cyber operations may be "directed at any portion of the global information infrastructure that is in Canada."[180] While defensive operations are defined somewhat vaguely as "protecting" Canadian infrastructure, the fact that such operations cannot be "directed" toward Canadian infrastructure suggests that, by definition, they will have effects outside either private-sector or government-owned networks. In other words, defensive cyber operations can be viewed as the rough equivalent of ACD but conducted by the CSE rather than the private sector.

The implication is significant: such powers are deemed necessary to protect Canada's information and infrastructure. The government seems to have accepted the rationale of deterrence, that protection of information infrastructure could necessitate cyber operations.[181] The provision of such powers in the *CSE Act* begs the question of whether, if such powers are considered necessary for the Government of Canada, they are also necessary for the private sector that the government is charged with protecting.

One potential argument is that granting this authority to the CSE negates the need for companies to conduct ACD for themselves. A closer look, however, calls into question whether such a responsibility is feasible for a government agency. Some degree of partnership with the private sector will in fact be necessary for Canada to take advantage of these newly granted authorities. It is hard to imagine how these cyber operations could be conducted without some level of co-operation from the private sector.

This is due to what one researcher calls the "sovereignty gap" in cyber defence.[182] As things stand, the federal government holds the authority to defend national security and consequently to conduct any aggressive defence efforts in cyberspace. On the other hand, it is the private sector, along with provincial, territorial, and municipal governments, that own

---

177 *CSE Act*, *ibid*, s 18.
178 *Ibid*, s 19.
179 *Ibid*, s 18.
180 *Ibid*, s 22(2)(a).
181 This point was made explicitly by Paul Nakasone, US Cyber Command chief and director of the National Security Agency, and Michael Sulmeyer, now Senior Director for CyberCommand with the National Security Council: "We learned that defending our military networks requires executing operations outside our military networks. The threat evolved, and we evolved to meet it" (Paul M Nakasone & Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs* (25 August 2020), online: <www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>).
182 Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017) at 229–46.

the majority of critical infrastructure.[183] Obviously, private firms would be wary of providing government bodies with access to their networks given concerns around the government having overly broad access to communications.[184] In the case of the financial sector, for example, it is not obvious how the CSE could conduct cyber operations without extensive assistance from firms that hold highly sensitive personal information. As Bendiek points out, "[a] clear separation between private and public sector can hardly be upheld in this area [the fight against cybercrime], because the companies that have been attacked are frequently the only bodies that have the means of resolving cyber attacks."[185] The CSE's intention to conduct cyber operations, then, does not preclude the private sector from being involved in cyber operations. If anything, it may necessitate private-sector involvement.

Indeed, there are other reasons why the private sector is uniquely suited for cyber operations or ACD. Companies often boast greater technical expertise than their public-sector counterparts,[186] partly due to the challenges associated with a government attracting and retaining cyber security personnel.[187] And in general, the private sector's resources and willingness to address hacking efforts outweigh those of government.[188] Canada has only to consider the United States' experience to understand the implications of this imbalance. As Clarke and Knake point out, "the buck does not actually stop in Washington," despite the government's reluctance to say so.[189] One "former White House official" offered a telling anecdote when Google was hacked in 2010: "After Google got hacked, they called the N.S.A in and said, 'You were supposed to protect us from this!' The N.S.A. guys just about fell out of their chairs. They could not believe how naïve the Google guys had been."[190]

The government does not have the means to protect all public and private infrastructure, and if this is true in the United States, it is even truer in Canada, a country with significantly fewer cyber resources.[191] Given the reality that even the United States finds itself unable to defend its critical infrastructure, smaller countries like Canada face significant challenges in terms of adequately protecting critical infrastructure from cyber threats.[192] There is a

---

183 Office of the Auditor General of Canada, *2012 Fall Report of the Auditor General of Canada*, online: <www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html>.

184 Kello, *supra* note 182 at 238. Even information sharing between the public and private sectors has historically proven less than successful due to companies' reluctance to allow the government access to private information. See also Kesan & Hayes, *supra* note 86 at 463; Kristan Stoddart, "Live Free or Die Hard: U.S.-UK Cybersecurity Policies" (2016) 131:4 Political Science Q 815.

185 Annegret Bendiek, "Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy" translated by Tom Genrich (2016) German Institute for International and Security Affairs, SWP-Studie 3/2016 at 25.

186 O'Neill, *supra* note 5 at 276.

187 Broeders, *supra* note 14 at 38–40. Broeders suggests that it is challenging to recruit "hackers" to law-and-order organizations for reasons such as a competitive labour market and the reluctance of the typical hacker (described as an "anarchic freethinker") to work for government authorities.

188 *Ibid* at 42–44; Rabkin and Rabkin, *supra* note 5 at 5–6.

189 Clarke & Knake, *supra* note 127 at 90.

190 Michael Joseph Gross, "Enter the Cyber-Dragon," *Vanity Fair* (2 August 2011), online: <www.vanity fair.com/news/2011/09/chinese-hacking-201109> [emphasis in original].

191 Moens, Cushing, and Dowd identify six states with "superior capabilities" that would enable them to launch an advanced persistent threat in cyberspace: the United States, the United Kingdom, Russia, China, Israel, and France. By their classification, Canada falls among states in the next tier of cyber power, those that "possess some capability but have not reached the same level of sophistication" (Alexander Moens, Seychelle Cushing & Alan W Dowd, *Cybersecurity Challenges for Canada and the United States* (Vancouver: Fraser Institute, 2015) at 16).

192 Greg Austin, "Middle Powers and Cyber-Enabled War: The Imperative of Collective Security," in Cherian Samuel & Munish Sharma, eds, *Securing Cyberspace: International and Asian Perspectives* (New Delhi: Pentagon Press, 2016) at 40.

significant gap between the cyber resources needed to protect the private sector versus the government resources that are available, and it is becoming clear that it is not feasible for governments to own the responsibility of defending the private sector.

VII. MITIGATING THE RISKS OF ACD

Of course, even if ACD is deemed effective in deterring hackers, its benefits must also be weighed against its risks. These risks appear on two levels. First, incorrect attribution and abuse of ACD may lead to collateral effects for other organizations and the rest of society. Consequences may also have international scale, if ACD escalates international cyber conflict or erodes Canada's credibility around cyber norms. This section discusses these risks in greater detail, as well as the extent to which they can be mitigated.

A. THE RISK TO SOCIETY

One of the key challenges of ACD is to attribute a cyber intrusion to the original hacker's computer. This is particularly true given that the hacker often launches the initial intrusion from a third party computer under their control, known as a "bot" or a "zombie."[193] A cyber threat can travel through a whole network of third party computers, obscuring its origins; in fact, the hacker may deliberately cover their tracks by routing activities through other machines and countries.[194] This means that if a hack-back effort damages a computer, that computer could easily be a third party bot. In other words, it is the bot owner who will suffer the damage to their device, despite being an innocent party who is almost certainly unaware that the device is infected.[195]

A second, less commonly raised objection to ACD is that a company could abuse the right to ACD and use it as justification to attack a competitor. For example, a company could frame a competitor by staging what appears to be a network intrusion or by planting certain files in the competitor's network.[196] Google and Microsoft raised a similar objection regarding a cyber security bill introduced in the US state of Georgia, arguing that hack-back could be used for anticompetitive purposes.[197]

While these risks are real, they can also be mitigated through placing three main conditions on ACD.

---

193 Smith, *supra* note 7 at 180–81.

194 Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace" (2018) 31 Philosophy & Technology 339 at 344.

195 Smith, *supra* note 7 at 180–81. In 2016, the botnet Mirai became the first "large-scale IoT botnet," prompting the vigilante hacker "Janit0r" to release a permanent-denial-of-service attack known as BrickerBot. BrickerBot pre-emptively damaged almost 2 million devices that were highly vulnerable to becoming part of the botnet. The justification lay in the idea that these faulty devices would damage other computers if allowed to become part of a botnet (KK e Silva, "Vigilantism and Cooperative Criminal Justice: Is There a Place for Cybersecurity Vigilantes in Cybercrime Fighting?" (2018) 32:1 Intl Rev L Comp & Tech 21 at 26). Strictly speaking, this action was not hack-back but third party vigilantism; nevertheless, it demonstrates how cyber retaliation may create a new set of victims.

196 Schneier, *supra* note 7 at 203.

197 Zaid Zhoorbajee, "Google and Microsoft Ask Georgia Governor to Veto 'Hack Back' Bill," *CyberScoop* (27 April 2018), online: <www.cyberscoop.com/georgia-sb-315-hack-back-google-microsoft/>. While the representatives of Google and Microsoft did not elaborate on what was meant by "anticompetitive" purposes, they were likely espousing a viewpoint similar to that of Schneier (*ibid*).

First, as discussed in the context of the three scenarios, ACD can take various forms, and not all forms of ACD imply damage to computer systems or deletion of data. Any legalization of ACD should therefore allow only for low-risk forms of ACD, that is, ACD conducted purely for the purposes of intelligence gathering. Intelligence gathering could include the use of beacons or other proactive ACD measures used to gather information in the event of a prospective intrusion. It could also include investigations conducted after an intrusion has already taken place. Intelligence gathering may not be completely risk-free, but it is obviously less problematic to collect attribution data from a bot than it is to alter data without the bot owner's permission.

Second, the government can retain some level of control over private-sector ACD in order to mitigate its risks. For example, a fairly conservative, non-disruptive form of ACD could see federal agencies authorizing a cyber security firm to perform a cyber investigation in the aftermath of a cybercrime.[198] ACD would be allowed only through a contracted or partnering arrangement with the federal government, perhaps channeled through the CSE. An alternative model could see security firms issued with licenses to conduct cyber investigations. Victims would hire such a firm similar to the way that one might hire a private investigator.[199] A third model could see any firm theoretically allowed to use ACD but only after first notifying the government. The "hack-backer" would need to supply both justification for the action and a plan for how to mitigate risks to third party computers.[200] The government would then be able to verify that the company's justification and plan are sufficient — that the action is not an abuse of power and that the company will take reasonable action to verify attribution of the hack to the source. While these three models range in the level of freedom that would be afforded to "hack-backers," one or a combination of these models could be used as a means to harness ACD, without introducing unnecessary risk. The rationale is to allow the government to oversee ACD, while private companies supply the funding for these efforts and the technical expertise.

A final risk mitigation is to hold companies liable for any damage inflicted on intermediary computers, or for that matter, on the original hacker's network. The prospect of liability would, presumably, give companies an incentive to act responsibly.[201] More specifically, the threat of legal liability should incentivize companies to avoid damaging any computer that they "enter," as well as that computer's data.

B. THE RISK TO THE INTERNATIONAL ORDER

When it comes to the international order, the principal objection to ACD is that it has the potential to escalate the cyber conflict. Detractors of ACD argue that if a firm retaliates against a hacker, it is unlikely that the instigator would back down. For example, in 2006,

---

198 Rabkin & Rabkin, *supra* note 5 at 15.

199 Michael Chertoff, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (New York: Atlantic Monthly Press, 2018) at 188–94; Stevan D Mitchell & Elizabeth A Banker, "Private Intrusion Response" (1998) 11:3 Harv JL & Tech 699 at 716-718; *ibid* at 5–10; West, *supra* note 44 at 139–41.

200 This is a model similar to that proposed in the *ACDC Act*, which would have required firms or those acting on their behalf to notify the FBI beforehand. Notification would include detailed situational information, including a plan for how to preserve criminal evidence and how to avoid harming any "intermediary computers" not owned by the instigator (*ACDC Act*, *supra* note 3, s 5).

201 Smith, *supra* note 7 at 190–94.

an Israeli anti-spam firm, Blue Security, responded to spammers by facilitating what was essentially a DDoS attack on the spammers' websites. The spammers countered by not only conducting a denial-of-service attack on Blue Security but also attacking organizations associated with the company.[202] While not a case of hack-back per se, this incident does demonstrate the danger of escalation when dealing with a cyber threat.

This risk becomes more acute if the original hacker is from another country or even sponsored by another government; in many cases, cyber threats do not come from private actors but from state-sponsored hackers.[203] It is one thing to envision a company "at war" with a hacker, but such a situation quickly becomes more serious if the recipient of a hack-back is government-sponsored. Lin points out that compared to governments, companies (or individuals) do not have the same capacity to judge how a cyber adversary will respond to a hack-back.[204] Nor is it necessarily possible to avoid the recipient of a hack-back misinterpreting that hack-back as also being state-sponsored.[205] For this reason, Lin evokes the image of hack-back as "the opening volleys of a cyberwar, which could escalate into a physical or kinetic war."[206]

Another potential concern is that legalized ACD would lessen Canada's ability to influence other countries' governments. It will be difficult for Canada to criticize other countries' use of cyber mercenaries or to negotiate for other countries' law enforcement against hackers, if Canada is viewed as promoting what many see as the cyber equivalent of vigilantism.[207] This is particularly true given that the 2018 Paris Call for Trust and Security in Cyberspace, as mentioned earlier, takes a stand against hack-back.[208] While by no means a binding treaty, the Paris Call for Trust and Security in Cyberspace may indicate the development of norms opposing hack-back or ACD more generally.[209]

However, there is reason to believe that these risks are overstated. First, an obvious counter-argument to the threat of international escalation is that hack-back is already (and perhaps inevitably) occurring, without having so far provoked any major international crises or otherwise destabilizing international relations.[210] Second, the risk of international escalation becomes much less severe if ACD is limited to intelligence gathering, especially with government oversight. As Rabkin and Rabkin point out, in the early 2010s, the NSA did contract companies for intelligence purposes.[211] They add, "[t]he practice of authorizing private companies to gather intelligence is hardly new [and allowing limited ACD] merely

---

202 Brian Krebs, "In the Fight Against Spam E-Mail, Goliath Wins Again," *The Washington Post* (17 May 2006), online: <www.washingtonpost.com/archive/politics/2006/05/17/in-the-fight-against-spam-e-mail-goliath-wins-again/8461271c-eb03-4cb6-adc5-7f1d69dfba9c/>; John Leyden, "Blue Security Calls it Quits after Attack by Renegade Spammer," *The Register* (17 May 2006), online: <www.theregister.com/2006/05/17/blue_security_folds/>.

203 Schneier, *supra* note 7 at 203.

204 Patrick Lin, "Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies," online: <ethics.calpoly.edu/hackingback.pdf>.

205 *Ibid*.

206 *Ibid* at 15.

207 Kosseff, *supra* note 6 at 646. Note that Kosseff is speaking of vigilantism in a broad sense, including any hacktivist efforts.

208 *Supra* note 117.

209 *Ibid*.

210 Lin, *supra* note 204 at 17–18.

211 *Supra* note 5.

extends the scope of what is already a prevalent practice."[212] While it is possible that some forms of ACD could lead to international escalation, this event is unlikely if strict limitations are set in place, as discussed in the section above.

Finally, regarding international norms, it is worth questioning whether norms surrounding ACD can truly be said to exist at this point. Two major Canadian allies, the United States and Israel, refrained from signing the Paris Call for Trust and Security in Cyberspace, as did Russia, China, and Iran.[213] While their reasons were not publicized, this fact nevertheless suggests that the Paris Call for Trust and Security in Cyberspace may not necessarily reflect the international consensus. Even more significantly, there is no unanimity regarding whether or not beacons are legal under the US's current cybercrime legislation, the *Computer Fraud and Abuse Act*.[214] Given these ongoing questions, it is unlikely that Canada would face a loss of credibility for legalizing a low-risk form of ACD with government oversight in place.

VIII. CONCLUSION

As this article's legal analysis has articulated, ACD is generally illegal under Canadian legislation, with the possible exception of beacons. This criminalization falls in line with international law, in the form of the Budapest Convention, which calls for the criminalization of ACD-related activities such as access, interception, and data interference without right.[215] That said, it may be possible for states to satisfy the Budapest Convention's requirements by one of two means: either by establishing a right of ACD limited to their own jurisdictions, or by associating the government with ACD efforts to the extent that ACD could be considered a form of self-defence by the state.

With these things in mind, there is a case to be made for the legalization of ACD in some form. Many critics of ACD and hack-back have framed the debate in binary terms: ACD is either legal or illegal, either an opportunity for more secure cyberspace or a threat to the international order. What is needed going forward is recognition of the several forms that ACD can take, ranging from destruction of data, to automated systems, to intelligence gathering.

This article has argued that ACD has the potential to augment current means of cyber security. Certainly, security measures such as "passive" cyber measures, threat-based measures, and ISP involvement have their role in cyber security. Without downplaying this role, the fact that governments are increasingly shifting to defensive and offensive cyber operations is telling. Indeed, Canada itself has passed the *CSE Act*,[216] legislation implying the need for Canadian information and information infrastructure to be protected by cyber operations taking place outside those networks themselves. While the *CSE Act*[217] assigns this responsibility to the CSE, a civilian government agency, there is reason to doubt that this situation is entirely feasible. The private sector is the most common target for hacking

---

212 *Ibid* at 10.
213 *Supra* note 117.
214 Chesney, *supra* note 34; Matthews, *supra* note 130; *Computer Fraud and Abuse Act*, *supra* note 6.
215 *Convention on Cybercrime*, *supra* note 102, arts 2–4.
216 *Supra* note 174.
217 *Ibid*.

operations, raising the issue of whether the government will encounter issues around privacy when requiring access to non-governmental networks. Additionally, the private sector tends to have cyber security resources and expertise that the government does not. For these reasons, the private sector should be empowered to take a greater role in cyber security — including activities with scope outside a company's own network. In such a scenario, the government would still hold an indispensable role in providing oversight for ACD.

To date, Canada has not specifically contended with cases of ACD, nor has it explicitly stated its stance on the issue, apart from its assent to the Paris Call for Trust and Security in Cyberspace's general denunciation of hack-back.[218] Going forward, what Canada requires is a conversation on the possibilities of ACD — a conversation focused on the appropriate division of responsibility for cyber security between the government and the private sector. While the *CSE Act*[219] perhaps serves as the start of this conversation, by no means does it represent its conclusion. Further work is needed to identify how Canada's government can support the private sector's urgent need for improved cyber security.

[218] *Supra* note 117.
[219] *Supra* note 174.