Policy Brief

April 2024 Volume 9, Issue 2

Cyberwarfare:

The 'Pink Tax' of Hacking

Owen Wong
Graduate Researcher

Introduction

Cyber warfare is a threat to Canada's national security. As technology advances and the world becomes increasingly connected, Canadian defence practitioners must adapt to a changing strategic environment. Indeed, cyber-warfare presents a new domain through which Canada's adversaries can undermine Canadian sovereignty and weaken the sources of Canada's national power. This policy brief argues that Canada's cyber-security strategy must be sensitive to the gender-based dynamics of cyber threats. After providing a brief overview of how states engage in the cyber domain, I discuss how cyber-attacks can disproportionally affect women, over the next twenty years. I conclude with policy recommendations for the Department of National Defence and the Canadian Centre for Cyber Security.

State-sponsored and State-Facilitated Cyber Warfare

The cyber domain is a new strategic environment focused on exploitation rather than coercion. Scholars of cyber warfare consistently observe that cyber-attacks are an ineffective coercive tool (Fischerkeller et al. 2022). In other words, state-sponsored cyber-attacks, or the threat thereof, do not reliably 'force' a target to change their behaviour. Rather than coercive instruments, cyber-attacks must be understood as a tool of exploitation, whereby one state benefits at the other's expense. Acts of exploitation are persistent, and each act is limited in its aim, meaning that cyber-attacks occur below the threshold of conflict; the target state is either unwilling or unable to respond (Fischerkeller et al. 2022). Despite their small-scale nature, these attacks may have cumulative effects.

Small-scale persistent cyber-attacks have the potential to impact the balance of power. To illustrate, consider how North Korean hackers target cryptocurrency exchanges (Fischerkeller 2023). In the past two years, these hackers have stolen nearly three billion dollars in Bitcoin to fund North Korea's nuclear program. Over the last five years, their nuclear capabilities have developed to the point that it is unclear whether America's ground-based defence systems, established to defend against rogue pariah states like North Korea, would be able to defend against an attack from Pyongyang (Ward

Editor: Allison Brown

The Centre for International and Defence Policy

138 Union Street, Suite 403. Queen's University, Kingston, Ontario Canada K7L 3N6

cidp@queensu.ca

2023). In other words, North Korea's repeated small-scale cyber-attacks were able to alter the balance of power. Similarly, China has used cyber-attacks to maintain the balance of power. As its economy struggled in 2010, China feared it would lose its great power status. To bolster its economy, state-affiliated Chinese hackers began stealing intellectual property (IP) from American research institutions and firms (Fischerkeller 2023). The IP they stole contributed to China's subsequent economic growth, effectively maintaining the balance of power. As these examples illustrate, persistent small-scale cyber-attacks that occur below the threshold of armed conflict can have significant impacts in the international realm.

Understanding how the cyber domain is used as an instrument of hybrid warfare requires an accurate characterization of the actors working on behalf of 'aggressor' states. In the same way that the line between Russia's professional military and its private military corporation (PMC) Wagner is blurred, the distinction between state-sponsored and state-facilitated cyber-attacks is unclear. States like Russia may conduct cyber-attacks themselves or they may rely on cyber proxies, defined as intermediary groups that conduct cyber operations that benefit their state (Maurer 2018). For instance, Russian Federal Security Service (FSB) agents paid independent hackers to target Yahoo in 2016. Throughout Russia, these kinds of independent hacking groups are common because Russia values highly skilled and technically capable hackers. In fact, Russia allows quasi-professional hacking groups to conduct ransomware attacks against Western states to ensure that the 'free market of hacking' supplies Russia with a reliable stream of readily available hackers who can work to promote Russia's broader foreign policy goals. The evidence suggests that Iran and China likely operate in similar ways (Grimes 2016).

Certain states have an identifiable cyber-attack signature, allowing for better tracing. For example, most Bitcoin thefts can typically be traced to North Korea. Similarly, most data breaches targeting IP can be linked to China. Denial of service (DoS) attacks that attempt to shut down a machine or computer network are often linked to Russia (Babb 2022). Although different states have different cyber-attack predilections, data breaches are the most common strategy used by states against their adversaries. Although it is unclear how attacks on cryptocurrency trading platforms and IP thefts have gendered impacts, the emerging evidence suggests that women and those who identify as non-binary may be disproportionately impacted by data breaches and DoS attacks over the next twenty years. The aforementioned vulnerable groups are alarming, given Russia's affinity for DoS attacks.

The Gendered Impact of Cyber-Attacks

There is limited gender-disaggregated data on how cyber-warfare impacts people with different gender identities. That being said, the existing evidence suggests that women and those who identify as non-binary will likely experience a disproportionate amount of harm as the frequency of cyber-attacks increases in the coming years. To illustrate this disparity, one must examine the existing evidence related to data breaches and DoS attacks.

Data Breaches and Computer Network Exploitation

Data breaches stem from Computer Network Exploitation (CNE) operations during which hackers infiltrate their target's computer networks to access, obtain, and extract confidential data. These attacks are common. In 2015, hackers linked to the Chinese Government

retrieved roughly 21.5 million personal records on American citizens that included names, addresses, and social insurance numbers (Nakashima 2015). The same year, state-sponsored hackers stole the addresses and names of 78 million customers and employees from U.S.-based Anthem Insurance (Reuters 2015). In 2023, Ontario's publicly funded birth registry BORN was hacked, compromising extant information, including the names and addresses of 3.4 million people who sought pregnancy care between 2010 and 2023 (Uday 2023). Although the perpetrator is unknown, the method the hackers used is linked to the Russian extortion group Clop, which has ties to the Kremlin. Evidently, without adequate cyber-security protections, both states and state-affiliated actors can not only obtain identifiable information about everyday citizens but also target certain identity groups.

Although state-sponsored hackers have yet to publicize their datasets of stolen personal information, there are no assurances that they will keep it to themselves. Although cyber-coercion is generally an ineffective tool to force another state to change its behaviour, Canada's adversaries may *try* to coerce the Canadian government by threatening to leak confidential information about citizens or government employees that may contain full names and addresses. Canada's foreign adversaries might also leak hacked information to demonstrate their cyber capabilities, disrupt their adversary's business operations, retaliate against their adversaries, or sway elections by leaking sensitive data. State-facilitated actors, or cyber proxies, may also leak information if the ransom they demand is not paid. In Canadian cases, roughly 11% of companies paid the ransom, providing enough capital to maintain these hacking operations (Griffiths 2024). However, in the remaining 89% of cases, sensitive information is often leaked. Indeed, once a data breach occurs, hacked data may be precariously stored by actors who have little interest in ensuring that the data remains private. The takeaway here is that sensitive information is available to hackers, posing a significant risk to civilian privacy and national security.

These hackers-for-hire are often able to maintain their operations through ransomware. Should these hackers publish datasets of identifiable information during ransomware attacks, it is unlikely Russia will prosecute their crimes, especially if they are aligned with state interests. States may also have an incentive to leak hacked data to coerce their foreign adversaries, demonstrate their cyber capabilities, disrupt the business operations of foreign companies, or retaliate against another state. Indeed, hacked data may be precariously stored by actors who may have little interest in ensuring the data remains private.

Leaked data that contains names and addresses will almost certainly lead to increased rates of gender-based violence against women. Consider the 2017 politically motivated WikiLeaks scandal that published the full names and addresses of roughly fifty million Turkish citizens (Brown and Pyltak 2020). Although the hackers were not trying to target women more than men, the attack had a disproportional effect on women. Every year, hundreds of Turkish women are killed by their partners, and thousands leave their homes to seek safety from domestic abuse. By publishing the names and addresses of Turkish citizens, the hackers put thousands of women in danger and contributed to well-documented incidents of offline gender-based violence; 'doxing', the process of publishing confidential personal information online, has led women to be the targets of offline stalking, sexual violence, death threats, and bomb scares (Brown and Pyltak 2020). Because women are more likely to be the victims of intimate partner violence, stalking, harassment, and sexual violence, cyber-attacks that

leak confidential data to the public can result in increased negative outcomes for women. Acknowledging how intersectional identities experience disinformation differently is a good step toward countering gendered disinformation.

Public reception to data breaches may interact with gendered social norms to influence elections. In 2014, a female Ukrainian politician lost her seat after Russian hackers leaked nude photos of her to the internet. Social understandings of gender could have led voters to sexualize and objectify Olga Lyulchak, victim blame her, or perceive that she is no longer a serious candidate (Neuendorf 2014). The release of thousands of Hillary Clinton's emails before the 2016 U.S. Presidential election further reveals how data breaches can interact with gender norms. After her emails were published on Wikileaks, media coverage portrayed Clinton as untrustworthy, incompetent, and unfit for leadership (Goss 2020). No state took credit for the leaked Clinton emails, but leaking candidates' is a strategy that Russia has recently used to influence elections (Ornstein 2017). Although it is unclear how significant the leaks were to the success of Lyulchak and Clinton's political campaigns, there is compelling evidence that in male-dominated environments, women often struggle to prove that they are strong, credible, and capable leaders (Born et al. 2018). The political scandals that women face can be catastrophic to their careers; when men face similar scandals, patriarchal gender norms often protect their reputation, credibility, and careers. In short, because women are often held to a higher standard than men, and because gender norms often change the public's perception of leaked information, female politicians are often disproportionately disadvantaged during data breaches.

Small-scale ransomware attacks can also interact with social norms to disproportionately impact the reputation and mental health of women. In 2022, the same Russian hacking group that triggered the U.S. National Emergency when they shut down the Colonial pipeline, leaked a dataset of Medibank customers entitled "Abortions.csv" after failing to receive a ransom payment (Taylor 2022). The dataset contained the names of 303 patients who had received abortions. It sorted patients into a "good" and "bad" list, based on the trimester during which they received their abortion. In 2023, Russian hackers published naked photos of female cancer patients obtained from hospitals in Pennsylvania after their ransom demands were refused (Stupp 2023). By leaking nude photos and abortion lists, hackers are explicitly targeting women because gender norms lead many people to view abortions and leaked photos as taboo and shameful. These are two examples of a broader phenomenon: Russian hackers 'train' for state-sponsored operations by conducting ransomware attacks against Western states, targeting victims based on how personally devastating their leaked data might be. The stigma associated with abortion and nude photos can facilitate women being disproportionately impacted by state-facilitated cyber-attacks.

DoS and Computer Network Attacks

Computer Network Attacks (CNAs) are the second main type of cyber threat. Once a threat actor has gained access to their target's computer network, they can initiate a set of harmful commands that can delete or modify data, cause physical harm to the computer network, or impede the proper functioning of services connected to the work. State-sponsored cyber-attacks on critical infrastructure frequently target power grids. In 2015 and 2016, state-

sponsored cyber-attacks used malware to target several power distribution companies in Ukraine, leading to prolonged outages that impacted roughly 250,000 civilians (CISA 2021) In 2023, pro-Russian hackers infiltrated Hydro-Quebec's computer network and shut down their websites to retaliate against Canada's support for Ukraine (Lapierre 2023). Although attacks in the US and Canada have yet to cause blackouts, their hacking activities are understood to be preparation for future attacks.

During prolonged power outages, hospitals must often triage the delivery of medical procedures to reduce their energy consumption. Although there is little gender-disaggregated data on the health outcomes of patients during power outages, there is compelling evidence that women's health suffers relative to their male counterparts. Blackouts lead fewer women to give birth in hospitals, contributing to higher mortality rates for women (Koroglu et al. 2019). The duration and frequency of power outages is also associated with "significantly lower odds of skilled birth attendance" which can negatively impact women's health (Koroglu et al. 2019, 1). Power outages also increase the risk of pregnancy complications such as threatened or early delivery and gestational diabetes mellitus (Xiao et al. 2021).

CNAs can also impact public transit. In 2022, European Union Member states observed a 25% increase in the number of reported cyber-attacks affecting Toronto's transportation sector (ENISA 2022). In Canada, a high-profile 2021 attack on the Toronto Transit Commission's (TTC) infrastructure impacted the technology used to communicate between vehicle operators, reservation applications, and the TTC's internal email, indicating that Canada's transit systems are ill-prepared to defend against cyber-attacks (Auditor General 2022). In 2023, Russian hackers breached the D.C. Transit's computer network (Starks 2023). Over the next twenty years, artificial intelligence (AI) will play a greater role in the delivery of public transportation. Although AI can powerfully improve the speed and delivery of public transit systems through self-driving subway cars and computer-automated scheduling, the incorporation of AI into transit systems means that the frequency and severity of cyber-attacks will likely increase.

Because of traditional gender roles and social norms, women have the potential to be disproportionately impacted by DoS attacks against public transit systems because they are more likely to rely on public transit than men (Babbar et al. 2022). In Toronto, 57% of public transit riders are women. In Montreal, 35% of women rely on public transit compared to 24% of men. In Vancouver, 26% of women frequently took public transit, compared to 18% of men. Three reasons account for women's higher usage rates: women tend to be lower income than men, meaning they have fewer resources available to purchase a car; in single-care households, women tend to be lower in the car-use hierarchy; and finally, women tend to have lower driver's driver's license acquisition rates. Women are also more likely to take on unpaid caregiving responsibilities, either to relatives, elderly parents, or children. Because of these responsibilities, women in cities like Toronto, Vancouver, and Montreal make several short, multi-stop trips, on public transit (Babbar et al. 2022). Additionally, due to the unpaid nature of caregiving responsibilities commonly relegated to women based on traditional gender roles, women are often forced to take on less full-time employment. Owing to childbearing responsibilities, women then often take up part-time work which can be characterized by poor wages, furthering their need for reliable public

transit. In essence, when cyber-attacks disrupt public transit systems, women are more likely to be negatively affected.

Policy Recommendations

Canada is a target of cyberwarfare. States like Russia, China, Iran, and North Korea, as well as the cyber proxies operating within their borders, pose the greatest threat to Canada's national security. To best adapt and respond to the gendered effects of cyber warfare, the Department of National Defence and the Canadian Centre for Cyber Security should:

1. **Collect sex- and gender-disaggregated data:** As this policy brief has shown, over the next twenty years, cyber warfare will likely have a disproportionately negative impact on women. However, understanding the true impact of cyber-threats on people of different genders is difficult given the limited availability of gender- and sex-disaggregated data. Indeed, most analyses of cyber-attacks are gender-blind. The Government of Canada should collect gender- and sex-disaggregated data about the impact of cyber-attacks on civilians. When cyber-attacks disrupt the daily lives of Canadian citizens, routine impact assessments should be conducted with a gendered lens. For example, the impact assessment on the 2024 cyber-attack against Global Affairs Canada (GAC) should ask how people of different genders were affected. Changes in work-from-home policies following the cyber-attack might disproportionately impact women if they are no longer able to work remotely because traditional gender norms often place women in caretaking roles. It is also important to understand how intersectional identity can affect the way different identity groups experience cyber warfare. For this reason, the Government of Canada should not only be collecting data on gender and sex but also race, ability and religion, to effectively understand how intersecting identities both are targeted and portrayed.
2. **Encourage the meaningful participation of women and gendered perspectives in cyber-security and counter-cyberwarfare policymaking:** Canada should encourage women to participate in countering cyber warfare. When women are excluded from the policy-making processes, Canada leaves talent on the table. However, women should not be expected to contribute a unique perspective that accounts for the needs of *all* women simply because of their gender. Rather, Canada's cyber-security strategy and its annual cyber threat assessment should be informed by robust consultations with a diverse set of feminist civil society organizations so that policy can effectively respond to the unique needs of both men and women encompassing a multitude of identity groups.
3. **Establish Cyber Victim Support Units (CVSU):** Create specialized units within law enforcement agencies that focus on supporting victims of cybercrimes, with a particular emphasis on crimes that have a gendered component such as cyberstalking, harassment, and doxing. The purpose of these units would not only be to provide a unique understanding and support of gendered cyber-crimes but to raise awareness that women are at a higher risk.
4. **Create Positions for Gender Staff:** The Canadian Centre for Cyber Security should have a dedicated gender advisor responsible for ensuring that Canada's cyber-security strategy incorporates the unique needs of women. Teams within different divisions and

the agency should have a gender focal point who can lead their unit's incorporation of gender perspectives.

5. **Communicate the gendered and non-gendered threat that cyberwarfare poses to civilians:** The Canadian Government already has tools to teach civilians about cyber-security. However, resources such as "Get Cyber Safe" do not signal the urgency or the importance of taking proper cyber precautions. Canadian civilians should learn that cyber-attacks often come from hostile foreign governments and that taking everyday cyber precautions can enhance Canada's national security. These cyber-security training programs should include workshops that teach women about their individual and disproportionate risks.
6. **Include a more robust gender analysis in Canada's National Cyber Threat Assessment:** Canada's current assessment is gender blind, meaning that the true impact of cyber threats on the Canadian public is unclear. Canada's future National Cyber Threat Assessment should include a section about the gendered impact of cyber-security, informed by sex- and gender-disaggregated data as well as consultations with civil society organizations.

Owen Wong *is a graduate researcher at the Centre for International and Defence Policy (CIDP) at Queen's University. With funding from the Department of National Defence, Owen works with Dr. Stéfanie von Hlatky, the Canada Research Chair on Gender, Security, and the Armed Forces, to study how international organizations implement the Women, Peace, and Security (WPS) agenda. Specifically, his research focuses on the European Union's WPS agenda, how gender-based disinformation can undermine international support for NATO's missions and operations, and how the Department of National Defence should best respond to the gendered impact of hybrid warfare. Owen has a master's degree in political studies and a bachelor's degree in political studies and economics from Queen's University. In addition to his work on WPS, Owen studies the macro-political regulation of ethnic conflict with Dr. John McGarry, the former Canada Research Chair in Nationalism and Democracy.*

Works Cited

Babb, Casey. 2022. "Digital Dictators: How Different Types of Authoritarian Regimes Use Cyber Attacks to Legitimize Their Rule." Carleton University.

Babbar, Priyanka, Joseph Peace, David Cooper, Geneviève Boisjoly, and Emily Grisé. 2022. "Understanding and responding to the transit needs of women in Canada."

Born, Andreas, Eva Ranehill, and Anna Sandberg. 2018. "A man´ s world?–The impact of a male dominated environment on female leadership."

Brown, Deborah, and Allison Pytlak. 2020. "Why gender matters in international cyber security." *Women's International League for Peace and Freedom and the Association for Progressive Communications*:2.

CISA. 2021. "Cyber-Attack Against Ukrainian Critical Infrastructure." https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

ENISA. 2023. "Understanding Cyber Threats in Transport." https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport.

Fischerkeller, Michael. 2023. "Cyber Persistence Theory with Michael Fischerkeller." S4.

Fischerkeller, Michael P, Emily O Goldman, and Richard J Harknett. 2022. *Cyber persistence theory: Redefining national security in cyberspace*: Oxford University Press.

Goss, Margaret. 2020. "Temporal News Frames and Judgment: The Hillary Clinton Email Scandal." Ph. D. Dissertation. Carnegie Mellon University.

Griffiths, Charles. 2024. "The Latest 2024 Ransomware Statistics." AAG. https://aag-it.com/the-latest-ransomware-statistics/#:~:text=90%25%20of%20ransomware%20attacks%20either,had%20their%20data%20leaked%20online.

Grimes, Roger. 2016. "Why it's so hard to prosecute cyber criminals." CSO. https://www.csoonline.com/article/559099/why-its-so-hard-to-prosecute-cyber-criminals.html.

Joyce, Miriam. 2012. *Bahrain From the Twentieth Century to the Arab Spring*.

Koroglu, Mustafa, Bridget R Irwin, and Karen A Grépin. 2019. "Effect of power outages on the use of maternal health services: evidence from Maharashtra, India." *BMJ global health* 4 (3).

Lapierre, Matthew. 2023. "Pro-Russian group claims responsibility for cyberattack against Hydro-Québec." *CBC News*. https://www.cbc.ca/news/canada/montreal/hydro-quebec-website-cyberattack-1.6808947.

Maurer, Tim. 2018. "Why the Russian government turns a blind eye to cybercriminals." *Slate,(February 2, 2018), retrieved from https://slate. com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals. html*.

Nakashima, Ellen. 2015. "Chinese breach data of 4 million federal workers." *The Washington Post*. https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

Neuendorf, Henri. 2014. "Politician Compares Leaked Nudes to Van Gogh Painting." *artnet*. https://news.artnet.com/art-world/politician-compares-leaked-nudes-to-van-gogh-painting-113554.

Orenstein, Mitchell A. 2019. *The lands in between: Russia vs. the West and the new politics of hybrid war*: Oxford University Press.

Rana, UIday. 2023. "Ontario's BORN birth registry breach sees data 'taken' from 3.4 million." *Global News*. https://globalnews.ca/news/9983285/ontario-birth-registry-data-breach-born/.

Reuters. 2015. "Massive Anthem health insurance hack exposes millions of customers' details." https://www.theguardian.com/us-news/2015/feb/05/millions-of-customers-health-insurance-details-stolen-in-anthem-hack-attack.

Starks, Tim. 2023. "A cyber scare for public transit." *The Washington Post*. https://www.washingtonpost.com/politics/2023/05/19/cyber-scare-public-transit/.

Stupp, Catherine. 2023. "Patient Seeks to Force Hospital Network to Pay Hackers Ransom to Remove Naked Photos Online." *The Wall Street Journal*. https://www.wsj.com/articles/patient-seeks-to-force-hospital-network-to-pay-hackers-ransom-to-remove-naked-photos-online-46ee754.

Taylor, Josh. 2022. "Abortion data from Medibank hack posted on dark web as Clare O'Neil pledges to pursue 'scumbags'." *The Guardian*. https://www.theguardian.com/australia-news/2022/nov/10/abortion-data-from-medibank-hack-posted-on-dark-web-as-clare-oneil-pledges-to-pursue-scumbags#:~:text=Sensitive%20health%20data%20from%20Medibank,%E2%80%9Cscumbags%E2%80%9D%20behind%20the%20hack.

Toronto Auditor General. 2022. "Toronto Transit Commission Cybersecurity Audit Phase 1: Critical IT Assets and User Access Management." https://www.torontoauditor.ca/report/toronto-transit-commission-cybersecurity-audit-phase-1-critical-it-assets-and-user-access-management/.

Ward, Alexander. 2023. "North Korea displays enough ICBMs to overwhelm U.S. defense system against them." *Politico*. https://www.politico.com/news/2023/02/08/north-korea-missile-capability-icbms-00081993#:~:text=The%20U.S.%20only%20has%2044,U.S.%20than%20America%20has%20interceptors.

Xiao, Jianpeng, Wangjian Zhang, Miaoling Huang, Yi Lu, Wayne R Lawrence, Ziqiang Lin, Michael Primeau, Guanghui Dong, Tao Liu, and Weihong Tan. 2021. "Increased risk of multiple pregnancy complications following large-scale power outages during Hurricane Sandy in New York State." *Science of the Total Environment* 770:145359.