A MACDONALD-LAURIER INSTITUTE PUBLICATION

Commentary

TRUE NORTH IN CANADIAN PUBLIC POLICY

JUNE 2021

Everyone together now: Creating a resilient society in an age of cyber threats

Elisabeth Braw

Introduction

Cyber aggression has become a constant companion in modern life and is likely to increase as developed societies become even more dependent on digital technology, through the Internet of Things, for example. The aggression is also likely to continue to morph. In the past few years, for instance, ransomware attacks have grown extremely rapidly. While governments can protect their civil societies by taking defensive and offensive cyber actions, such protection can never be complete. As a result, businesses and citizens have a role to play in helping limit the effects of cyber aggression on themselves and the wider society.

Cyber aggression: The current situation

In early April this year, Swedish prosecutors announced they would drop an investigation into a string of cyber attacks against the Swedish Sports Confederation in 2017 and 2018. Thanks to the hacks, the attackers gained access to athletes' personal details, including medical records. These details subsequently found their way into the public domain. "The information has

been published openly and, based on these details, Swedish media have written articles which follow GRU's narrative of discrediting athletes and sports organisations in the West," says Mats Ljungqvist, the prosecutor in charge of the case, in an April 13 statement (Swedish Prosecution Authority 2021).

The hacks, in other words, had a real and detrimental effect on Swedish athletes. Swedish authorities quickly identified the perpetrators: several officers in Unit 26165 of Russia's military intelligence agency, the GRU. Although this was irrelevant for the prosecution, Russia also had reason to discredit foreign countries' athletes. Following the discovery of pervasive doping among Russia's top athletes, in December 2017 the International Olympic Committee (IOC) banned Russia from competing in the 2018 Summer Olympics (Chappell 2017). While a smaller group of athletes from Russia who had been proven clean were allowed to compete, they were only permitted to do so under a neutral IOC flag. Russia thus had reason to communicate to people in other countries that their athletes were not clean either.

Yet, despite the identification of the perpetrators and the availability of evidence, prosecutor Ljungqvist's office decided to drop the case. In his statement, Ljungqvist explains why: "Against the background of parties acting for a foreign power, in this case Russia, we have reached the conclusion that the necessary preconditions for taking legal proceedings abroad or extradition to Sweden are lacking. I have, therefore, today decided to discontinue the investigation" (Swedish Prosecution Authority 2021).

> *Losses from successful attacks have grown rapidly. The best aggressors can cause enormous damage.*

If a prosecutor cannot interview suspects or witnesses or gather evidence in a foreign country, the investigation will clearly be fatally flawed. And if the suspects will not be extradited in case of a trial or conviction, there is little point in pursuing even the most promising investigation. The case of the Swedish athlete hacks illustrates the reality of state-sponsored cyber aggression: any part of society can be targeted, and even when the perpetrator's identity can be established the affected country may not be able to respond.

Cyber aggression has afflicted countries, businesses, and citizens since the dawn of the Internet. For many years, though, the intrusions were primarily a criminal undertaking. Organized gangs and even individual criminals made life miserable for all by indiscriminately unleashing their cyber weapons and hoping that some of the ammunition would cause damage. Because many households and businesses lacked cyber protection, it often did. That threat has forced Internet users across the board to become more cyber literate. Most ordinary citizens know not to click on suspicious links, and many have

anti-virus software. Businesses have elaborate cyber defence and IT security experts all the way up to the now-common CISO (Chief Information Security Officer).

As the protection has evolved, so has the aggression. Each year the insurer Hiscox surveys how much cyber aggression has been directed against Western companies. In its 2020 *Cyber Readiness Report*, Hiscox found that in the past 12 months the share of companies affected by a cybersecurity event had fallen from 61 percent to 39 percent (Braw 2020a). This does not mean that cyber aggressors have simply lost interest, but that businesses have become better at protecting themselves and that less sophisticated aggressors have therefore given up trying. At the same time, however, losses from successful attacks have grown rapidly. The best aggressors can cause enormous damage, such as by stealing a considerable amount of intellectual property (IP) or stealing large sums of money, whatever their objective is.

> *Hostile states do not direct cyber aggression against a vast number of random targets, but against specifically chosen ones.*

The potentially large payoff makes cyber aggression an attractive undertaking for the most sophisticated cyber gangs. However, it also makes cyber aggression an attractive undertaking for hostile states. Considering the considerable assets and expertise available to governments that might be attractive to thieves from foreign states, government-sponsored cyber aggression is an area of enormous concern. Unlike common cyber criminals, hostile states do not direct cyber aggression against a vast number of random targets, but against specifically chosen ones. Samu Konttinen, at the time CEO of the cybersecurity firm F-Secure, told me in the summer of 2020 for my upcoming book *The Defender's Dilemma* the difference between past attackers and those we confront today. In past years, "the sort of attackers who used to dominate, don't care who the target is. They just want the money." Today's attackers, by contrast, "are more like the armed forces. Armed forces are not opportunistic. They want to attack a particular country, not just any country. Cyber attackers becoming so sophisticated that you can't stop them." Konttinen adds that today it can take "100 days for a company to realize it has been attacked."[1]

That is precisely what happened to SolarWinds, the American IT infrastructure firm targeted in a phenomenally successful intrusion last year. (It is telling that although the intrusion was not yet known at the time of my interview with Konttinen, he warned of what subsequently turned out to have happened to SolarWinds.) SolarWinds was attacked in May or June 2020 in a so-called supply chain attack, where the perpetrator targets an entity that is part of an organization's supply chain, then gains access to the intended

target from there. But SolarWinds failed to notice the attack until December (Constanin 2020). By that time, the intrusion had reached 425 Fortune 500 companies, the top 10 US telecommunications enterprises, the top five US accounting firms, the State Department, the US Department of Defense, other government departments and agencies, and a large number of universities and foreign government agencies.

Microsoft's President Brad Smith has subsequently observed that "from a software engineering perspective, it's probably fair to say that this is the largest and most sophisticated attack the world has ever seen" (Reuters 2021). The fact that a target does not have to be targeted directly but can be attacked through its supply chain poses enormous risks to critical national infrastructure and other pillars of society.

Indeed, even though cyber attacks occur around the clock, the SolarWinds intrusion had enormous symbolic significance because it was so extensive and so painfully demonstrated the West's vulnerabilities. Yet despite their phenomenal penetration of US and other Western networks, the perpetrators opted not to cause destruction or to disrupt any operations, even though they could clearly have done so. The reason for this is likely that they were only interested in gathering intelligence, not causing disruption. Smith later estimates that "certainly more than a thousand" engineers must have been involved in the attack (Cerulus 2021).

> *A target does not have to be targeted directly but can be attacked through its supply chain.*

On April 15, 2021, the US government punished Russia by expelling 10 diplomats, imposing sanctions on six Russian companies, and banning US banks from buying Russian debt. At the same time, it formally attributed the hack to APT 29 (also known as The Dukes and CozyBear), a hacker group within Russia's foreign intelligence agency, the SVR (White House 2021). While the ban on Russian debt was an innovative form of punishment against grey-zone aggression, Biden's punishment cocktail was hardly a decisive blow – especially as it was also a response to Russian election meddling and bounties on US soldiers in Afghanistan.

Indeed, the Swedish prosecutor's decision and the Biden administration's punishment demonstrate the fundamental challenge in tackling today's highly sophisticated state-sponsored cyber aggression. Whom is the targeted country trying to tackle: the individual hacker or the sponsoring government? And what means can the targeted country use to effectively fight back?

The core of the issue is the status of cyber aggression under international law. Infuriatingly, there are no clear lines demarcating when the legal use of cyber ends and its illegal use begins.[2] This is, of course, a result of governments having failed to agree on binding rules in cyberspace. Today the cyber field is, as a result, a de facto Wild West, where actions are prevented only by the targeted side's resilience and threatened punishment. The US government acknowledges as much in its April 15 punishment of Russia, where it also outlined new steps to increase cyber defence: "We are also bolstering our efforts through the Marshall Center to provide training to foreign ministry lawyers and policymakers on the applicability of international law to state behavior in cyberspace and *the non-binding peacetime norms that were negotiated in the United Nations and endorsed by the UN General Assembly*" (emphasis added).

Failed deterrence, as we have seen, has enormous implications. The SolarWinds hack demonstrates that one act of aggression can undermine large parts of a country's government and private sector. The stakes will grow higher still as digitalization continues, especially in advanced economies. By 2030, the world is predicted to have some 50 billion digital devices (up from 22 billion as late as 2018 (Statista 2021)), which will be connecting not just smartphones and laptops but everyday devices from refrigerators to self-driving cars. While this trend towards ever-more digitalization makes daily life extraordinarily convenient for those with access to the digital services and IT-enabled devices, it also makes countries far more vulnerable to cyber aggression. I refer to this dilemma as the "convenience trap" (Braw 2020b).

> *There are no clear lines demarcating when the legal use of cyber ends and its illegal use begins.*

A massive attack in June 2017, which subsequently became known as NotPetya, demonstrates the convenience trap. The now-infamous attack began as a virus directed against Ukrainian critical national infrastructure and was so successful that it hit at least four hospitals, six power companies, two airports, about two dozen banks, ATMs and card payment systems, and most of the government. "One Ukrainian government official estimated that 10 percent of all computers in the country were wiped. The attack even shut down the computers used by scientists at the Chernobyl cleanup site," *Wired* subsequently reports (Greenberg 2018).

Then, however, the virus travelled on and hit a string of multinationals including Maersk (the world's largest container shipping company), the US snack giant Mondelez (which makes brands including Oreo, Cadbury, Halls, and Philadelphia cheese), the US pharmaceutical giant Merck, FedEx's Euro-

pean subsidiary TNT Express, the French construction leader Saint-Gobain, and the British hygienic-goods firm Reckitt (maker of Durex and Clearasil). All of them lost hundreds of millions of dollars. Half a year after the attack, Merck had sustained losses of $870 million as a result of the attack. Even more damaging, however, was the pharma firm's lost ability to manufacture vaccines. "NotPetya so crippled Merck's production facilities that it couldn't meet demand that year for Gardasil 9, the leading vaccine against the human papillomavirus, or HPV, which can cause cervical cancer. Merck had to borrow 1.8 million doses – the entire U.S. emergency supply – from the Pediatric National Stockpile," Bloomberg later reports (Voreacos, Chiglinsky, and Griffin 2019).

Fifty years ago, disabling vaccine manufacturing would have involved bombing the vaccine plant in question: a clear attack on a country's sovereignty. Now a virus can travel silently around the world and do the work. For Denmark, the implications of the NotPetya attack were even starker than for the United States: Maersk is not just the world's largest container shipping company but also Denmark's largest company. If a country's largest company were attacked with physical force and unable to operate for days, as was the case with Maersk, the affected country would retaliate. Because the NotPetya attack took place in cyberspace, and because identifying the cyber attacker's potential state sponsor took time, Denmark did not retaliate. It did not retaliate for another reason: much like in armed conflicts, retaliation in the grey-zone brings the risk of escalation. Denmark could clearly not risk the prospect of a cyber conflict with Russia that might spill over into other areas and even lead to a live, physical conflict.

> *NATO has to date only responded to cyber aggression by condemning it. That was also the case with the SolarWinds hack.*

While NATO considers cyber defence "part of NATO's core task of collective defence" and "has affirmed that international law applies in cyberspace" (NATO 2021a), it is unclear what response the alliance would muster in case of a serious cyber attack, and indeed against whom – countries or individuals – it would direct its retaliation. In fact, NATO has to date only responded to cyber aggression by condemning it. That was also the case with the SolarWinds hack. On the day the US government named the Russian government as the perpetrator and imposed the punishment described above, NATO announced that "Allies support and stand in solidarity with the United States, following its 15 April announcement of actions to respond to Russia's destabilising activities" (NATO 2021b). In reality, countries have to defend themselves against cyber aggression and punish successful perpetrators on their own. Indeed, considering that the targets of cyber attacks are often pri-

vate companies, countries are often wary of helping avenge cyber aggression against a private company based on an ally's territory because of the risk of escalation. As a result of such fears, Western governments have thus far never delivered a massive cyber blow in response to cyber aggression.

All of this makes resilience to cyber aggression extraordinarily important. While resilience alone cannot deter cyber aggression, it can absorb the blow of even the most sophisticated forms of aggression. Effective resilience requires cooperation between each country's government and private sector.

Cyber defence: Lessons from resilience efforts in Estonia, Latvia, and Lithuania

Estonia has the unenviable distinction of being the first advanced economy crippled by a cyber attack. The 2007 attack, thought to have been perpetrated by Russia, occurred the day after Estonian authorities had moved a World War II Soviet statue from the city centre of Tallinn to a cemetery. Government ministries went down, as did banks, news outlets, schools, and political parties. The country stalled for several weeks. For Estonia, which had made digitalization its calling card, such a policy also opened up an enormous vulnerability. Rather wisely, Estonia did not call on NATO for assistance during the attack, though it could have argued that Article 5 applied to such a major cyber attack. It is, however, likely that other NATO member states would not have agreed with this assessment and that some would have been unwilling to assist Estonia. An Estonian call for NATO assistance would thus have divided and weakened the alliance.

Because Estonia has dealt with the sort of cyber attack other countries desperately want to avoid, it is instructive to look at how the country has increased cyber security since 2007, even as it has grown ever-more digital. As a direct consequence of the cyber attack, in 2008 Estonia introduced a new cyber security strategy that included five strategic objectives:

- The development and large-scale implementation of a system of security measures;
- Increasing competence in cyber security;
- Improvement of the legal framework for supporting cyber security;
- Bolstering international cooperation; and
- Raising awareness on cyber security (Czosseck, Ottis, and Talihärm 2011).

A perhaps more significant step, however, was the *Emergency Act* the country adopted in June 2009, which improved Estonia's national emergency preparedness and emergency management structure, including the responses

to cyber threats. As Christian Czosseck and his co-authors note, "the act foresees a system of measures which include preventing emergencies, preparing for emergencies, responding to emergencies and mitigating the consequences of emergencies.… It is the providers of public services and information infrastructure owners that are tasked with everyday emergency prevention and ensuring the stable level of service continuity. Providers of vital services are obliged, among other assignments, to prepare and present a continuous operation risk assessment… and an operation plan… to notify the citizens about events significantly disturbing service continuity as well as to provide the necessary information to supervisory bodies" (Czosseck, Ottis, and Talihärm 2011).

The law, in other words, obliges private companies to maintain high levels of cyber defence and also to have backup systems in place in case of successful cyber intrusion. Companies are required not just to have these resilience measures in place but are also to demonstrate this to the government and to notify the public of successful intrusions. By placing such significant responsibility on the private sector, the Estonian government has ensured that the government and the private sector form a united front in cyber resilience.

> *The Estonian government has ensured that the government and the private sector form a united front in cyber resilience.*

Most other countries lack such legislation and simply count on businesses to enhance cyber resilience because it is in businesses' interest to do so. Executives may, however, decide that the risk of serious cyber intrusion is too low to warrant extensive resilience measures. Indeed, they may argue that the cyber resilience measures that insurers require – for insurance payouts to be issued in case of successful intrusion – may be the only measurement that matters to their respective companies.

The 2007 attack acutely highlighted the need for volunteer cyber experts that the government could call on in a crisis. "During the cyber riots we decided that Estonia needed a unit that could get involved during a cyber emergency. We began a bit in 2008 and 2009 and were established in 2010," explains Andrus Padar, one of the unit's first participants.[3] In 2011 the government officially created the Cyber Defence Unit, which Padar now leads.

Now as in its earliest days, the Cyber Defence Unit operates within Estonia's auxiliary defence organization – the Estonian Defence League – and it has retained its original mandate: "to protect Estonia's high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defence" (Kaitseliit 2021). With its volunteer structure, which draws on the high level of IT expertise in Estonia's private sector, the unit is

a key part of the country's cyber resilience. As Estonia's Ministry of Defence explains, "the Cyber Unit includes specialists in key cyber security positions in national critical infrastructure, patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security (lawyers, economists etc.)" (Kaitseliit 2021).

Latvia and Lithuania, too, have established National Guard cyber units (Lithuania's national guard is known as the Riflemen's Union). In 2015 Lithuania also established a UK-style national cyber security centre (NKSC), which like the UK version is a one-stop shop for cyber defence, training, and cooperation with the private sector (Ministry of National Defence, Lithuania 2017).[4] In addition, as part of the European Union's Permanent Structured Cooperation (PESCO), Lithuania is leading the creation of so-called Cyber Rapid Response Teams (CRRTs), an initiative where participating EU member states will form six-month rotational rapid response teams that will assist any of the participating states that may need assistance (Ministry of National Defence, Lithuania 2019).

Lithuania's preparation appears to have limited the effect of a highly sophisticated cyber attack that took place in that country in December 2020 as a new government was taking office. According to Defence Minister Arvydas Anušauskas, the attack was one of the biggest and most complex in recent years and "was prepared in advance and with a goal in mind" (LRT 2020). According to the country's National Cyber Security Centre, the attackers tried to gain access to 22 websites administered by Lithuania's public sector, succeeding in some cases, then posting fake news about, for example, an alleged border incident and alleged NATO Baltic Air Policing corruption. Although the hack was quickly detected, Anušauskas notes that its relative success "shows huge gaps in cyber security of the public sector" (LRT 2020).

National Guard cyber units hold considerable promise in cyber resilience. Traditionally citizens have joined the Home Guard in the countries that have them in much the same way as people join the armed forces: joiners start at the bottom and work their way up the ranks by acquiring military skills.[5] In National/Home Guard/Defence League cyber units, civilian cyber experts can instead join on the basis of their particular civilian cyber expertise.

Involving private citizens – even citizens with expertise and no expectation of remuneration – is, however, more complicated than it may seem. Padar explains that "there's always a difference between our wishes and ideas, and the reality. Sometimes politicians think that volunteers are a free resource. They're not. They need to be trained to maintain their readiness. You can hope that their employers will keep training them but you can't count on it. Their employer may train them, but you can't count on it."[6]

There is also the thorny issue of public perception. If an issue does not appear urgent or critical, there is less public pressure to focus on it. Padar notes that "in the beginning when there was a lot of aggression, better-trained members

were happy to share their expertise. Now it's less. If the house isn't burning, people don't see the need for firemen."[7] That state of affairs makes it difficult to determine how many members a volunteer cyber defence unit should have and what the extent of their involvement should be. Estonia's Cyber Defence Unit has considered modelling what would be the optimal number of members and hours, but for now it operates with the membership that is already available. While it does not disclose the exact figures, it is in the range of several hundred.

Even though there are undeniable hurdles in organizing unpaid volunteers, the need for armed forces to tap into reservists' civilian expertise is becoming increasingly clear far beyond cyber issues. In the UK, the Ministry of Defence's Reserve Forces 2030 study was conducted partly with the ambition of better using reservists' civilian skills, and indeed of recruiting reservists with particular skills into the reserves. If National/Home Guards can become a destination for cyber experts wanting to contribute to keeping their countries safe, it could become a phenomenally important part of cyber resilience.

> *National Guard cyber units hold considerable promise in cyber resilience.*

Estonia in particular has for years also focused heavily on cyber education for children. Back in the 1990s, the Estonian government made significant investments in IT infrastructure across the country, and by the end of the decade all Estonian schools were online. The early 2000s brought with them further steps in the efforts to digitize the country, when leading companies launched the Look@World Foundation. As UNESCO subsequently reports, "supported by telecom and banking interests, the project raised digital awareness and popularized the use of the internet and Information and Communication Technologies (ICT), particularly in education, science and culture. The initiative's first project aimed to bridge the country's 'digital divide' by providing free computer training to 102,697 participants, or 10% of the adult population" (Roonemaa 2017).

This digitalization drive appears to have motivated Moscow to launch the crippling cyber attack in 2007. But when in 2012 schools began teaching programming and robotics to pre-school students, aided by the government-funded ProgeTiger curriculum for teachers (HITSA 2017), they were also able to add cyber resilience skills to the curriculum.

Strengthening the resilience of liberal democracies against cyber aggression

It seems obvious: societal resilience must involve all parts of society. Until very recently, however, governments have been reluctant to ask the population to contribute to resilience, adopting instead a whole-of-government approach to all manner of national crises. Now the Nordic and Baltic countries, which have been the standard-bearers of the whole-of-society approach, are getting company from other countries. A highly noteworthy development has taken place in Britain. In its Integrated Review published in March 2021, the UK government resolutely embraced the whole-of-society approach, explaining that it will "establish a 'whole-of-society' approach to resilience, so that individuals, businesses and organisations all play a part in building resilience across the UK" (HM Government 2021). As part of that approach, the UK will, for example, "explore options for a wider civilian reserve" (HM Government 2021, 99).

The civilian reserve is a highly innovative initiative, the civilian equivalent of the long-standing military reserves that many countries have. Although the government has not yet provided any details regarding the civilian reserve, the fact that it is planning to create such a force reflects the changing nature of national security threats: the so-called grey-zone aggression between war and peace (which includes cyber aggression) is increasing, and the national security tools traditionally used by governments – government actions, including use of armed forces – are insufficient to withstand such aggression. Indeed, the armed forces are of little use against most forms of grey-zone aggression, which includes coercion of companies and disruption of supply chains.[8]

The Czech Republic, too, is pioneering new forms of societal resilience. As with the UK, its new focus demonstrates how society-wide resilience is becoming a priority as grey-zone aggression increases. The Czech government has rapidly implemented the new concept of joint military-industry grey-zone exercises that I first proposed in September 2020. The exercises, which are of a purely defensive nature and involve the armed forces and invited companies, allow both the government and the private sector to better handle forms of grey-zone aggression that may be directed against them. "We see industrial policy as part of not only economic welfare, but geopolitics and also defence and security," Deputy Defence Minister Tomáš Kopečný, who leads the initiative, told the *Financial Times* in February 2021. "This exercise is basically about creating [a] nexus between the military and civilian, between the government and private side" (Warrell 2021).

In April 2021, following the discovery that a 2014 explosion that killed two people was likely carried out by Russian operatives, the Czech Republic expelled 18 Russian diplomats, whereupon Russia responded by expelling 20 Czech diplomats, crippling the Czech embassy in Moscow. Prague, in turn, responded by expelling 60 Russian diplomats, crippling Russia's diplomatic

presence in the Czech Republic (Mortkowitz 2021), which means that the Czech Republic now has to assume Russia will retaliate in the grey-zone, perhaps by harming Czech companies. While the Czech Republic clearly cannot predict what precisely Russia might to, thanks to the grey-zone exercises a key segment of its private sector is prepared.

While the UK's planned civil reserve and the Czech Republic's military-industry grey-zone exercises are not limited to the cyber domain, they demonstrate the potential for societal resilience. Indeed, countries across the Western alliance can build on longstanding efforts by the Baltic states and on the more recent British and Czech ones to involve both businesses and citizens in cyber resilience. National/Home Guards could, for example, launch cyber units. While no country has polled its private-sector IT professionals to measure their interest in helping keep their country safe, it stands to reason that given the disruption a cyber attack could cause to a country, many IT professionals would happily volunteer as cyber defenders. (Today the United States has a Cyber Command, the UK has a National Cyber Force, and a few countries including Sweden have small conscripted cyber units (SVT 2019), but Estonia's Cyber Unit and some US states' National Guards remains the benchmark for how to involve private-sector cyber specialists in the country's defence.) Delaware's National Guard, for example, is considered a cyber defence leader and has, among other things, helped protect the 2020 US elections (Delaware.gov 2020).

> *A cyber expert is, of course, of most use to the government as a cyber expert, not as a sentry.*

As Estonia's Cyber Unit does, National/Home Guard cyber units should allow private-sector cyber experts to volunteer their time without participating in other National/Home Guard activities. Unlike many other aspects of national defence, cyber defence does not require any physically strenuous activities; indeed, requirements for physical activities would likely deter many experts from joining a cyber unit. A cyber expert is, of course, of most use to the government as a cyber expert, not as a sentry. Indeed, since many IT professionals may feel uneasy in the formal structures of the armed forces (including uniforms), National/Home Guard cyber units could operate without the armed forces' standard formalities (and without uniforms), though a chain of command would clearly remain essential.

Countries could also build on the Czech Republic's grey-zone exercises, which demonstrate the enormous potential of government cooperation with the private sector in grey-zone defence. Precisely because the exercises cover whichever grey-zone threat are the most relevant or urgent at any given time, the government can adjust the scenarios to reflect current or predicted develop-

ments, including in the cyber domain. Two months after the Czech Republic had launched its exercises, its security services established that two Russian agents had caused a 2014 arms depot explosion that killed two people. When the Czech Republic punished Russia for the deed by expelling 18 Russian diplomats (Janicek 2021), it was at least able to do so in the knowledge that a core group of companies would be prepared for grey-zone aggression Russia was likely to direct against them.

Countries could also build on the example Estonia has set by focusing on children. While Estonia's priority has been to teach schoolchildren programming and coding, cybersecurity is clearly part of any such curriculum. Indeed, even countries not wishing to teach primary-school children coding could include cyber security in their curriculums. Indeed, many countries have done this for the past decade or so, with a focus on online predators. Such efforts have succeeded in raising awareness of online predators among children, but there has not been a similar effort in the area of cyber resilience. Considering that the vast majority of teenagers (so-called Gen Z) in industrialized countries today own smartphones and laptops (in the UK, for example, 85 percent of 5-to-16-year-olds own a computer (vom Orde and Durner, eds. 2020)) and that their digital use will only continue to increase, it stands to reason that countries can significantly enhance their security by teaching Gen Z and the next-younger generation cyber resilience.

Conclusion

Precisely because it is impossible to deter all cyber aggression by promising that retaliation will follow such acts of aggression, the need for cyber resilience will continue to grow as digitalization increases. Resilience is vital because it absorbs the blow of cyber aggression, thus both limiting the harm and signalling that cyber aggression is not a worthwhile undertaking. Such resilience cannot be created by governments alone, and as this report has highlighted, there are numerous opportunities to involve society. Most of the involvement can take place on a voluntary basis; indeed, considering businesses' and citizens' extreme dependence on digital connectivity, it is in their interest to help limit the harm caused by cyber aggression.

About the author

Elisabeth Braw is a resident fellow at the American Enterprise Institute (AEI), where she focuses on defense against emerging national security challenges, such as hybrid and grayzone threats. Concurrently, she is a columnist with Foreign Policy, where she writes on national security and the globalized economy, and a member of the National Preparedness Commission (UK).

Before joining AEI, Ms. Braw was a senior research fellow at the Royal United Services Institute for Defence and Security Studies in London, where she founded its modern deterrence project. She has also been an associate fellow at the European Leadership Network, a senior fellow at the Atlantic Council, and a senior consultant at Control Risks, a global risk consultancy.

Ms. Braw started her career as a journalist working for Swedish newspapers and has reported on Europe for The Christian Science Monitor and Newsweek, among others. She is often published in a wide range of publications, including *The Economist*, *Foreign Affairs*, *The Times* (of London), and *The Wall Street Journa*l. She is also the author of *God's Spies: The Stasi's Cold War Espionage Campaign Inside the Church* (Eerdmans, 2019).

A frequent speaker at European and NATO conferences, Ms. Braw often appears on BBC Radio 4 and other international media.

Ms. Braw attended the University of Hagen in Germany, graduating with an MA in political science and German literature. She has a BA from Friedrich Schiller University Jena, Germany.

References

Braw, Elisabeth. 2020a. "Cyberattacks Are on the Decline." *Foreign Policy* (December16). Available at https://foreignpolicy.com/2020/12/16/cyberattacks-are-on-the-decline/.

Braw, Elisabeth. 2020b. *The Case for Joint Military–Industry Greyzone Exercises*. Royal United Services Institute for Defence and Security Studies Briefing Paper. Available at https://rusi.org/sites/default/files/20200928_braw_greyzone_exercises_web.pdf.

Braw, Elisabeth. 2021a. *The Defender's Dilemma: Defining, Identifying, and Deterring Gray-Zone Aggression*. American Enterprise Institute (February 8). https://www.aei.org/research-products/report/the-defenders-dilemma-defining-identifying-and-deterring-gray-zone-aggression/.

Braw, Elisabeth. 2021b. *Building a Wall of Denial against Gray-Zone Aggression*. American Enterprise Institute (April 12). Available at https://www.aei.org/research-products/report/building-a-wall-of-denial-against-gray-zone-aggression/.

Cerulus, Laurens. 2021. "SolarWinds is 'Largest' Cyberattack Ever, Microsoft President Says." *Politico* (February 15). Available at https://www.politico.eu/article/solarwinds-largest-cyberattack-ever-microsoft-president-brad-smith/.

Chappell, Bill. 2017. "Russia is Banned from 2018 Olympics; Athletes Told to Compete under Olympic Flag." *NPR* (December 5). Available at https://www.npr.org/sections/thetorch/2017/12/05/568585759/russia-is-banned-from-2018-olympics-athletes-told-to-compete-under-olympic-flag.

Constanin, Lucian. 2020. "SolarWinds Attack Explained: And Why It Was So Hard to Detect." *CSO Online* (December 15). Available at https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. 2011. E*stonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security Cooperative*. Proceedings of the European Conference on Information Warfare & Security.

Delaware.gov. 2020. "Governor Carney Authorizes Delaware National Guard Cybersecurity Squadron to Support 2020 Election."October 16. Available at https://news.delaware.gov/2020/10/16/governor-carney-authorizes-delaware-national-guard-cybersecurity-squadron-to-support-2020-election/.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired* (August 22). Available at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [paywall].

HM Government. 2021. *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*. Report number CP 403 (March). Government of the United Kingdom. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

Information Technology Foundation for Education [HITSA]. 2017. ProgeTiger Programme. Education Estonia. Available at https://www.hitsa.ee/it-education/educational-programmes/progetiger.

Janicek, Karel. 2021. "Czechs Expel 18 Russians over Huge Depot Explosion in 2014." *AP* (April 17). Available at https://apnews.com/article/czech-republic-russia-andrej-babis-c593f724a16622eb6d0a19bae3d710be.

Kaitseliit. 2021. Estonian Defence League's Cyber Unit. Kaitseliit. Available at https://www.kaitseliit.ee/en/cyber-unit.

LRT. 2020. "Lithuania Came under Biggest Cyber Attack in Years, Says Defence Minister." *LRT* (December 16). Available at https://www.lrt.lt/en/news-in-english/19/1300455/lithuania-came-under-biggest-cyber-attack-in-years-says-defence-minister.

Ministry of National Defence, Lithuania. 2017. *Lithuanian Defence System: Facts and Trends*. Republic of Lithuania. Available at http://urm.lt/uploads/nato/documents/nato.pdf.

Ministry of National Defence, Lithuania. 2019. "Further Formation and Development of the Cyber Rapid Response Teams Discussed in Vilnius." News Release (October 10). Available at https://kam.lt/en/news_1098/current_issues/further_formation_and_development_of_the_cyber_rapid_response_teams_discussed_in_vilnius.

Ministry of National Defence, Lithuania. 2020. "President Familiarised with Kaunas Unit of the National Cyber Security Centre." News Release (January 7). Ministry of National Defence, Republic of Lithuania. Available at https://kam.lt/en/news_1098/current_issues/president_familiarised_with_kaunas_unit_of_the_national_cyber_security_centre.

Mortkowitz, Siegfried. 2021. "Czechs Expel More Russian Embassy Staff over Bombing Claims." Politico (April 22). Available at https://www.politico.eu/article/czech-republic-russia-embassy-staff-bombing-claims/.

North Atlantic Treaty Organization [NATO] 2021a. *Cyber Defence*. NATO (April 12). Available at https://www.nato.int/cps/en/natohq/topics_78170.htm.

North Atlantic Treaty Organization [NATO]. 2021b. "North Atlantic Council Statement Following the Announcement by the United States of Actions with Regard to Russia." Statement (April 15). Available at https://www.nato.int/cps/en/natohq/official_texts_183168.htm.

Reuters. 2021. "SolarWinds Hack was 'Largest and Most Sophisticated Attack' Ever: Microsoft President." *Reuters* (February 14). Available at https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R.

Roonemaa, Mari. 2017. "Global Lessons from Estonia's Tech-Savvy Government." *UNESCO Courier* (April-June). Available at https://en.unesco.org/courier/2017-april-june/global-lessons-estonia-s-tech-savvy-government.

Statista. 2021. "Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030." Infographic. Statista (January 22). Available at https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.

SVT. 2019. "Försvarsmakten kallar in it-soldater till värnplikt." SVT (January 15). Available at https://www.svt.se/nyheter/inrikes/forsvarsmakten-kallar-in-it-soldater-till-varnplikt.

Swedish Prosecution Authority. 2021. "Investigation into Serious Breach of Data Secrecy by Russian Intelligence Agency Discontinued." Press release (April 13). Swedish Prosecution Authority. Available at https://www.aklagare.se/en/media/press-releases/2021/april/1/january/investigation-into-serious-breach-of-data-secrecy-by-russian-intelligence-agency-discontinued/.

vom Orde, Heike, and Alexandra Durner (eds.). 2020. *International Data on Youth and Media 2020*. International Central Institute for Youth and Educational Television (IZI). Available at https://www.br-online.de/jugend/izi/english/International%20Data%20on%20Youth%20and%20Media.pdf.

Voreacos, David, Katherine Chiglinsky, and Riley Griffin. 2019. "Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?" *Bloomberg* (December 3). Available at https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war.

Warrell, Helen. 2021. "Czech Republic Turns to War-Games to Build Cyber Defences." *Financial Times* (February 17). Available at https://www.ft.com/content/8c018644-3866-4f69-9105-d3c0e68ca491 [paywall].

The White House. 2021. "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government." Briefing Room Release (April15). The White House. Available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

Endnotes

1 Personal interview with Samu Konttinen, summer 2020.

2 I discuss this in *The Defender's Dilemma* (Braw 2021a).

3 Interview with the author.

4 See also Ministry of National Defence, Lithuania (2020).

5 It is worth noting that the national guards in the Nordic and Baltic countries – known as the Home Guard in Denmark, Norway, and Sweden and the Defence League in Estonia – are rather different from the US National Guard. They are less heavily equipped, and importantly, do not carry out policing duties or crowd control in the same way the US National Guard does. Indeed, to a much larger extent than the US National Guard they are seen as citizens in uniform; locals doing service in their community.

6 Interview with the author.

7 Interview with the author.

8 For further background, see Braw (2021a) and Braw (2021b).

constructive important forward-thinking excellent insightful high-quality active

Ideas change the world

WHAT PEOPLE ARE SAYING ABOUT **MLI**

The Right Honourable
Paul Martin

I want to congratulate the **Macdonald-Laurier Institute** for 10 years of excellent service to Canada. The Institute's commitment to public policy innovation has put them on the cutting edge of many of the country's most pressing policy debates. The Institute works in a persistent and constructive way to present new and insightful ideas about how to best achieve Canada's potential and to produce a better and more just country. Canada is better for the forward-thinking, research-based perspectives that the **Macdonald-Laurier Institute** brings to our most critical issues.

The Honourable
Jody Wilson-Raybould

The **Macdonald-Laurier Institute** has been active in the field of Indigenous public policy, building a fine tradition of working with Indigenous organizations, promoting Indigenous thinkers and encouraging innovative, Indigenous-led solutions to the challenges of 21st century Canada. I congratulate **MLI** on its 10 productive and constructive years and look forward to continuing to learn more about the Institute's fine work in the field.

The Honourable
Irwin Cotler

May I congratulate **MLI** for a decade of exemplary leadership on national and international issues. Through high-quality research and analysis, **MLI** has made a significant contribution to Canadian public discourse and policy development. With the global resurgence of authoritarianism and illiberal populism, such work is as timely as it is important. I wish you continued success in the years to come.

The Honourable
Pierre Poilievre

The **Macdonald-Laurier Institute** has produced countless works of scholarship that solve today's problems with the wisdom of our political ancestors. If we listen to the **Institute**'s advice, we can fulfill Laurier's dream of a country where freedom is its nationality.

MACDONALD-LAURIER INSTITUTE

TRUE NORTH IN CANADIAN PUBLIC POLICY

323 Chapel Street, Suite 300,
Ottawa, Ontario K1N 7Z2
613-482-8327 • info@macdonaldlaurier.ca

@MLInstitute
facebook.com/MacdonaldLaurierInstitute
youtube.com/MLInstitute
linkedin.com/company/macdonald-laurier-institute