Politically motivated cyber attacks have made global headlines in recent months. At pivotal moments in the run-up to the United States’ presidential election, Democratic candidate Hillary Clinton’s campaign was knocked off message when the private communications of her campaign manager John Podesta, the Democratic National Committee, and other targets were made public in a series of leaks. Several media reports suggested the accounts were likely hacked by actors supported by the Russian government.

Before the U.S. elections on Nov. 8, the government had been exploring options for a response to attempts by foreign actors to digitally disrupt elections, which some see as an act of hybrid warfare. Since the election of Republican candidate Donald Trump, there are now fears of an American slide into a repressive surveillance state, and the impact a Trump presidency may have on Canada’s national security policies. At the same time, police in Quebec confirmed this month that they had been tracking the cellphones of six journalists, and CSIS was found to be illegally storing Canadians’ metadata. In the UK, the controversial Investigatory Powers Bill, nicknamed the “Snoopers’ Charter,” was passed this week, allowing for unprecedented hacking powers.

These threats point to a global problem: states and conflict actors now routinely use digital technologies to spy on, hack, disrupt and silence their political opponents. Sometimes these digital threats remain within state borders, and sometimes they target opponents around the world. This is yet another way in which war — and repression — are just a click away.

Policymakers have given a great deal of attention to the cyber security of governments, critical infrastructure, military targets and commercial enterprises. But civil society groups are also under threat, including human rights defenders, environmental activists, political watchdogs, and other groups promoting the rule of law and democracy.

What can be done about these digital threats to civil society around the world?

To answer that question, we consulted 15 experts on the issue. They include one of the world’s lead investigators into digital attacks on civil society (John Scott-Railton of the Citizen Lab) at the University of Toronto, the director of an advocacy organization for civil society actors facing...

In questioning these and other experts, we wanted to see if there is consensus about who is most responsible for digital threats to civil society, and how the Canadian government and other actors might respond to these threats. This article summarizes what we heard.

**Civil society under digital threat**

Around the world, civil society actors face digital threats to their security and their activities. What kinds of threats? States use mass surveillance systems that allow them to know where, when and for how long people communicate with each other, and in some cases they monitor the content of telephone and internet conversations. Human rights activists and political reformers frequently have their devices infected (https://www.johnscottrailton.com/security-for-the-high-risk-user/) with malware that allows attackers to monitor their keystrokes, read their data, access their cameras and microphones, and track their movements. Denial of service attacks (https://equalit.ie/portfolio/deflect/) are used to shut down the websites of activists and independent media outlets at key moments, such as during elections.

These assaults on the digital security of civil society occur throughout the world, though they may play out somewhat differently depending on the region in which they occur.

In conflict zones, the consequences of surveillance and digital attacks can be dire. For instance in Syria, non-violent civil society groups face continual monitoring of their phone and internet communication by the Assad regime, as well as phishing attacks aimed to install malware on their phones and computers. People in areas controlled by the regime or ISIS are routinely stopped and forced to turn over their devices and divulge their passwords. Security forces may use that information to detain, torture or murder people in their networks.

Many repressive governments use digital means to monitor and silence human rights defenders and political activists. For instance, Human Rights Watch recently documented the cases of 140 individuals in Gulf states who have been targeted (https://features.hrw.org/features/HRW_2016_reports/140_Characters/index.html) by their governments for surveillance and repression. As HRW Middle East director Sarah Leah Whitson says (https://www.hrw.org/news/2016/11/01/arab-gulf-states-attempts-silence-140-characters): “The Gulf states have engaged in a systematic and well-funded assault on free speech to subvert the potentially transformative impact of social media and Internet technology.”


Even countries with a strong rule of law, like Canada, often target civil society groups within their borders. The United Kingdom’s intelligence agency was found to illegally monitor Amnesty International (http://www.amnesty.ca/blog/the-uk-government-spied-on-us-and-we-won’t-take-it-lying-down). In Canada, as mentioned above, the Quebec police force actively surveilled journalists (http://www.cbc.ca/news/canada/investigators-lagace-surveillance-1.3837270) who were investigating corruption within Quebec’s police department. The U.S. government’s mass surveillance programs target civil society groups from human rights organizations (https://www.theguardian.com/world/2014/apr/08/edwards-snowden-us-government-spying-human-rights-workers) to non-profit medical groups (https://theintercept.com/2016/08/10/how-the-u-s-spies-on-medical-nonprofits-and-health-defenses-worldwide/). These threats occur amidst excessive and sometimes illegal surveillance of citizens. That situation, made clear in the U.S. through documents leaked by Edward Snowden (https://theintercept.com/2016/05/16/the-intercept-is-broadening-access-to-the-snowden-archive-heres-why/), has been highlighted in other countries recently. Earlier this month, a court ruled against CSIS for

Civil society groups suffer digital attacks and intrusive surveillance everywhere, from tiny independent media groups in Sudan (https://accessnow.cshp.co/digital-security-helpline-case-study-defending-freedom-of-expression-in-sud) to the massive Open Society Foundations (https://www.theguardian.com/commentisfree/2016/sep/09/open-society-hack-politically-motivated-cyberattack) in New York, from China to Kazakhstan to Canada. These cyber intrusions can lead to detention, torture and murder. At a minimum, they chip away at people’s freedom of speech and association.

**Who is responsible for these threats?**

When it comes to the digital insecurity of civil society groups, the experts we consulted were clear that there is a lot of blame to spread around. Certainly, the authors of digital attacks and surveillance are responsible, such as the Assad regime in Syria, the cyber criminals for hire who sometimes do the dirty work for governments, or conflict actors like ISIS’ Cyber Caliphate. But many other actors play a role, including governments and private companies that may be more susceptible to regulation and public pressure.

As shown by the chart below, the experts told us that some actors are more responsible than others for digital threats to civil society. Though as several noted, “responsibility” is a somewhat ambiguous term: it can mean those blameworthy for digital attacks (like repressive governments), and it can also mean those who have the opportunity to address threats even if they shouldn’t be blamed for them (like civil society groups under attack).

![Chart on responsibility for digital threats to civil society](https://opencanada.org)

Topping the list of responsibility for digital threats to civil society are repressive governments — at least for civil society groups within authoritarian states. These governments have the resources, legal authority and motivation to crack down on those who oppose them. “There was a time when authoritarian regimes seemed like slow-footed, technologically challenged dinosaurs whom the Information Age was sure to put on a path toward ultimate extinction,” observes (http://muse.jhu.edu/article/386479) Ron Deibert, the director of the University of Toronto’s Citizen Lab. “As resurgent authoritarianism in cyberspace increases, civil society will struggle.”
Most experts did not see repressive governments as significantly responsible for digital threats to civil society in countries like Canada. A few did, however. Indeed, the alleged Russian interference in the U.S. presidential election suggests that repressive governments may increasingly interfere in civil society and democracy beyond their borders.

If governments do want to monitor and disrupt civil society activity, they can turn to a wide range of private companies that can provide them with the tools they need. Indeed, there is a robust market for surveillance technologies, provided by companies like Hacking Team, Gamma International, NSO Group and Blue Coat. There are also "security" companies that centre around the use of hacking. According to our experts, these private companies take second place as the actors most responsible for digital threats to civil society in repressive countries, and they also endanger civil society in countries like Canada.

People do not install and run their own seat belts. They should not have to do [the equivalent] for Internet safety.

In addition to companies that specialize in surveillance and hacking, our experts argued that private technology companies such as Facebook, Google, Samsung and Cisco can and should do a better job on digital security. These tech giants own and profit off of the apps, social media platforms, devices and digital infrastructure we use, and often make it unnecessarily difficult for individuals and civil society groups to stay safe online. As Oktavia Jónsdóttir (https://freedom.press/about/tech/oktav%C3%ADa-j%C3%B3nsd%C3%B4ttir), advisor to the Freedom of the Press Foundation, puts it: "People do not install and run their own seat belts. They should not have to do [the equivalent] for Internet safety.”

The security deficits in our everyday digital technologies are partly the result of private companies’ business models, such as their excessive retention of users’ data and frequent security failures. But our experts pointed out that the Canadian government and others have severely compromised the digital security of civil society, within their borders and around the world. Almost all experts criticized the massive, and often illegal, surveillance operations by intelligence and security agencies. Most experts also called for governments to stop trying to undermine end-to-end encryption, and many criticized intelligence agencies for exploiting vulnerabilities in technologies rather than seeing that they get fixed.

Finally, while the experts we consulted did not blame civil society organizations or the general public for the digital threats they face, many argued that civil society organizations and individuals should take reasonable steps to protect themselves.

As can be seen in the chart above, there were some differences in the degree of responsibility for digital threats when comparing civil society groups in repressive countries to those in countries with stronger rule of law. But by and large, according to the experts we consulted, the causes of digital insecurity are the same throughout the world, and similar policy responses should be applied everywhere.

Here are the six responses that resonated across the board.

1. **Make digital technologies safer to use.**

Of all the actions that could address digital threats to civil society, just one was universally advocated by the experts we consulted: the digital technologies we all use should be made more secure. If these technologies are made safer, they argued, it will be much harder for malicious actors to monitor and disrupt legitimate activities by civil society groups. And as several experts pointed out, these security fixes should be ubiquitous and easy to use, or the default setting for all our technologies.

However, making digital technologies safer is a complex proposition. Each of the components of digital communications can be insecure, including the apps we use, the operating systems that run the apps, devices like smartphones and laptops, and the Internet service providers that connect individual devices to the rest of the Internet. Different experts emphasized important safety improvements at all of these points.

As John Scott-Railton (https://www.johnscottrailton.com), senior researcher at the University of Toronto’s Citizen Lab (https://citizenlab.org), argues:
In the long run we need operating systems and platforms that are more secure. Some companies are doing these things, and making it more difficult for aggressive actors to take advantage of them. For instance, the preview feature in Gmail allows you to view an attachment before you download it, so you might be able to spot a potential malware file before your device is infected. You also see Google and other companies increasingly pushing people to use two-factor authentication. And you see companies warning people who may have come under a state-sponsored attack. Google started doing that a couple years ago, then Facebook and a few other companies.

Railton-Scott, like nearly all of the experts we consulted, also stated that people should be able to securely encrypt the data they store and the messages they send. Molly Sauter (https://twitter.com/OddLetters?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor), McGill PhD candidate and author of *The Coming Swarm: DDoS Actions, Hacktivism, and Civic Disobedience on the Internet*, puts it this way: “Strong cryptography for people’s data and communications should be seen as a right that people should have for their own personal security.”

Similarly, Eva Galperin (https://www.eff.org/about/staff/eva-galperin), global policy analyst for the Electronic Frontier Foundation, claims that end-to-end encryption is critical for civil society to be digitally secure. “The Canadian government should support the use of strong encryption among activists and support the development of open source, end-to-end encryption tools,” she says.

While some experts claim that technology companies should take it upon themselves to design more secure products, others highlighted a role for governments. Caleb James DeLisle, a research engineer at XWiki SAS in France, suggests:

> A trusted neutral party should identify and promote more secure and private alternatives of the various technologies and services we use. For instance, they could be given grades from an A to F. The Canadian government could do this evaluation, like it does for food safety, or it could be a civil society organization.

> This is particularly important for mobile phones, since they are the chief means of Internet connectivity in repressive countries and conflict zones. So to improve the security of activists, the Canadian government or another trusted body should establish a testing lab which publically grades mobile phones based on their relative security level.

Different experts suggested a broad spectrum of policy measures, including government regulation, private company self-regulation, and the empowerment of non-state and non-corporate bodies to promote security standards. But the ultimate aim was the same: to improve the safety of the individual components and the overall digital ecosystem that are used by everyone.

### 2. Rein in private technology companies that assist rights-abusers.

While some digital threats to civil society organizations are cheap or require little technical sophistication, other threats — including mass surveillance — use expensive and hard to develop technologies. These include sophisticated internet filtering systems that states can use to silence civil society organizations or their messages, as well as surveillance tools developed and sold by private companies like Gamma International (UK), NSO Group (U.S. and Israel), and the Hacking Team (Italy). The UK-based Privacy International recently issued an extraordinary report on the global surveillance industry (https://privacyinternational.org/node/911), documenting the trading of technologies used to monitor and repress populations.

According to the experts we consulted, the private companies that manufacture and sell these technologies bear significant responsibility for digital threats to civil society groups. And better regulation of the trade in surveillance technology is one policy lever that can be used to push back against these threats.

Tamir Israel (https://cippic.ca/about-us), staff lawyer and policy analyst at the University of Ottawa’s Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), says:
Canada can use its export regime to prevent domestic entities from selling technologies to repressive regimes that facilitate their surveillance activities. Another way that Canada can export insecurities is if the Canadian government insists that local device manufacturers include backdoors (like the FBI asked Apple to do for their iPhones after the San Bernardino attack), or having social media companies and others build in intercept capabilities so that police can monitor communications. Doing so makes it more likely that companies will export products with insecurities built in, which more repressive governments may take advantage of.

Another expert to recommend that Canada better regulate the sale of surveillance technologies is the hacker “Phineas Fisher,” also known as Hack Back (https://twitter.com/gammagrouppr?lang=en). He’s famous in the cyber-security industry for hacking and leaking the files of several surveillance technology companies (FinFisher and Hacking Team), as well as the ruling party in Turkey (http://motherboard.vice.com/read/phineas-fisher-turkish-government-hack). In an email exchange, he cited reports (http://motherboard.vice.com/read/canadian-government-funded-notorious-censorship-company-for-a-decade-netsweeper-bahrain-citizen-lab) of Internet filtering technologies sold by the Ontario-based company Netsweeper that are allegedly used to limit freedom of expression in repressive countries, and wrote that the first thing Canada should do to help protect activists around the world is “stop profiting off providing the technology that others use to spy on those activists.”

3. Don’t unduly compromise digital safety in order to protect national security.

Many of the experts we consulted were concerned that intelligence and police agencies were using claims about “national security” to undermine people’s rights, including privacy rights. In both repressive countries and in countries with stronger rule of law, civil society groups are frequently the target of intrusive surveillance. Furthermore, the experts pointed out that the countries like Canada and the U.S. are acting in ways that make it much easier for repressive governments to pursue digital threats against civil society groups. Not only can surveillance technologies diffuse around the world (a problem mentioned above), so can policies. That’s one reason that Tanya O’Carroll (https://www.opentech.fund/advisory-council/tanya-ocarroll), a senior adviser to Amnesty International’s Technology and Human Rights program, advocates for Canada and other governments to rein in their intelligence and security agencies:

I think it is also important for there to be litigation within countries like the U.S., the UK and Canada, to challenge the surveillance practices of their own governments. That may not be an immediate way to improve the situation in countries like Ethiopia and Mexico, but I’m very concerned that these extremely intrusive surveillance policies are being normalized worldwide, since countries like Canada and the UK are quietly eroding their own privacy protections. If this kind of intrusive surveillance becomes the norm, then it takes us into a very different world, where it will be even easier for repressive governments to crack down on critical voices and civil society.

Along similar lines, author and McGill University-based researcher Molly Sauter argues that governments should stop undermining the privacy of people’s data and communications. As an example of a government agency going too far, she cites the FBI’s request for Apple to provide a “backdoor” to the data on an iPhone of an alleged terrorist involved in the San Bernardino attack last year. Apple argued that if it did this for the FBI, it may create a vulnerability or precedent that would be leveraged by other actors, including more repressive governments like those of Russia and China (https://www.theguardian.com/technology/2016/feb/17/apple-fbi-encryption-san-bernardino-russia-china). Sauter continues:
Governments should come down hard on the side of strong encryption and say that this is a thing we believe in, this is a thing that should exist. We shouldn’t be distributing back doors and golden keys to governments or other corporations or other investigatory organizations.

Second, governments should disclose vulnerabilities in digital technologies that they find, rather than hoarding them to use for intelligence purposes. If governments disclose vulnerabilities then people can figure out how to fix them and create patches to repair them, so that they can’t be used to compromise the security of civil society groups.

Finally, several of the experts we consulted said that governments should restrict their surveillance of civil society groups beyond their borders. The anti-surveillance hacker Phineas Fisher thus argues:

Another good step the Canadian government could take would be to stop actively spying on activists. It’s important to remember that the relative wealth of Canada and other western countries is based on extreme global inequality and exploitation, and that Canada and other western countries use their intelligence agencies to maintain that. The U.S. is especially notorious for spying on and manipulating the political processes of other countries. But Canada, for example, has a lot of mining companies heavily exploiting natural resources across Latin America, and spies on activists in those countries that threaten Canadian mining interests.

4. **Make social media platforms safer.**

Social media platforms are central to private communication and public messaging by civil society groups. Human rights groups and humanitarian aid agencies use Twitter, Facebook and other platforms to raise awareness of threats and mobilize responses. But the fact that many activists “live on Facebook,” as one expert put it, means that the platform holds critical information about their lives, campaigns and social connections, information that attackers seek to access and exploit.

Ellery Biddle, Director of Global Voices Advocacy, argues:

Too many people are put at risk because of Facebook’s real names policy, which forces people to identify themselves on the platform even if they think it might put them at risk. Also, threats of violence on social media haven’t really been addressed. Even though the big platforms prohibit them, things like incitement to rape and other forms of violence happen all the time. We’ve seen a situation where 45 people have threatened to rape someone for her activism, and that content stays up for three weeks.

In general, Facebook and other social media companies should be a lot more transparent about what they are doing, and about the effects their policies are having. Because it sometimes seems like what they say they are doing and what happens is out of sync.

Deirdre Collings, executive director of the SecDev Foundation, has a deep understanding of the digital threats faced by non-violent civil society groups in Syria over the last four years through her work on the SalamaTech program. Facebook has been essential to the work of Syrian civil society groups, but it has also exposed them to new threats and challenges. For instance, when opponents falsely report them for violating the Facebook’s “community standards” provisions their accounts have been shut down. The SecDev Foundation and other groups helped Facebook develop channels to more quickly restore accounts targeted in this way. But problems continue, says Collings:
We still often have to help non-violent groups in Syria to have their accounts restored after opponents have reported their pages as violating standards.

We also help close down the social media accounts of individuals who go missing or are detained. The risk is that their devices will be taken and their passwords extracted from them, and then whoever has done so can go through all their messages and contacts...

...Facebook has come a long way on these and other issues, but it could do more. For instance, it’s still really hard for people — especially vulnerable populations — to understand just how much information they are sharing, and how much risk they are exposed to. It is still a complicated process to lock down your account and keep it private.

Facebook could provide more support on their platform as well as actual hands-on training to help people mitigate the risks they face.

Several experts cautioned that social media companies record and keep too much information about their users. The Grugq (https://medium.com/@thegrugq), a cyber-security expert, argues that “stronger data privacy laws are needed to make the users of platforms more secure and safe.” Along with several other experts, he claimed that social media platforms are increasingly used to spread misinformation in order to stigmatize or drown out civil society actors:

There needs to be tools to help activists deal with the ‘bullshit is harder to produce than refute’ problem. This is a great problem now and will be in the future. If it is 10 [times] harder to disprove a lie, then repressive regimes can spread lies which are beyond the resources of activists to refute. [To address this problem requires] creating tools to create information that is verifiable and “provable” far beyond what exists today. Make it harder for rights abusers to get technologies.

5. Seek accountability for digital attacks and privacy violations.

Digital attacks don’t perpetrate themselves. Another policy option to help protect civil society organizations is to hold attackers accountable. Accountability measures can help incapacitate attackers, deter future attackers, and reinforce norms against such acts. Scott-Railton of the Citizen Lab argues that while it’s difficult to hold
people accountable for these acts, Canadian authorities could do a better job of investigating and assessing the problem:

There’s a general deficit in the ability of law enforcement in Canada to investigate hacks against normal people. If there were easier mechanisms for individuals to report bad things and crimes against them online, more people might do so. Then you’d get a better sense of how pervasive it is. You might get more cases and have states recognize that this is a real issue.

However, holding actors accountable for cyber attacks is difficult. One basic challenge is the difficulty of attribution; it can be very hard to determine who is responsible for hacking a system or launching a digital attack. Furthermore, the attack can often be launched from anywhere, including from countries that are unlikely to cooperate with Canada or other governments in seeking prosecutions. Craig Forcese, a University of Ottawa law professor and prominent voice in public debates around Canada’s national security policies, observes:

Digital attacks on civil society groups in Canada are likely violations of Canada’s criminal code. Many other countries have similar criminal laws, because Canada, the U.S. and most European countries have ratified the Budapest Convention on Cybercrime. However, criminal law in these areas is pretty much irrelevant unless you can get your hands on a defendant. So this isn’t going to do much good if attacks are coming from a country like Syria.

If the hack was coming from a state with whom we had good relations [and] that had some functioning rule of law, you could work through our mutual legal systems and liaison relationships with the security and intelligence services, and try to persuade them to take action. But by and large there’s little prospect that we could extraterritorially enforce Canadian law.

Another avenue is to hold corporations accountable for selling technology and assistance to rights-abusing states. There are ongoing cases against private technology companies in France, the UK and the U.S. In 2013, a distribution company paid a civil penalty fine of US$2.8 million for violating U.S. sanctions against Syria, when it sold Internet monitoring technology to the Assad regime. Tanya O’Carroll, senior adviser to Amnesty International, argues that other accountability processes should be pursued in addition to legal cases against private companies:

Naming and shaming countries and companies also plays an important role. Amnesty International does it, and so do other civil society groups. The companies that develop and sell so-called lawful interception technologies don’t just make one-off sales; they provide regular updates and ongoing technical assistance to governments to deploy their products against specific targets. Companies are not exempt from international law and must be pressured to put human rights due diligence processes in place so that they neither directly, nor indirectly, facilitate human rights violations in their operations.

6. Government, tech companies and cyber-security organizations should help civil society groups protect themselves.

While civil society organizations may not be responsible for causing digital threats, it is in their power to protect themselves from them. Several experts recommended that civil society — perhaps with assistance from governments and private technology companies — should take steps to become aware of security risks and learn to resist them. Tamir Israel of CIPPIC explains that the Canadian government and cyber-security experts can assist in these efforts.
The Canadian government could look at creating a centralized entity mandated with helping NGOs facing digital attacks. The government can fund research and education initiatives around security tools, threat modelling and data hygiene. The cyber-security community can help civil society more too, in addition to their work for government and private companies. It would be great to see a pro bono momentum in the cyber-security community, since their services can be more expensive than many civil society groups can afford.

There are also civil society organizations that have taken lead roles in helping other civil society groups around the world address digital threats. For instance, Canada’s SecDev Foundation works with nonviolent Syrian groups by providing extended training and digital tools, and through helping them develop their own digital security practices. Amnesty International provides digital security training to some of the human rights organizations they work with around the world, and has been campaigning for people to use safer communication tools and to push back against onerous government surveillance.

One prominent non-governmental organization in this space is Access Now, which promotes policies to protect the privacy of citizens and civil society groups. Access Now also operates a Global Security Helpline that is accessible day and night around the world, in order to provide rapid advice to civil society organization in need of help. Fanny Hidvegi, the European Policy Manager at Access Now, suggests several big picture policies to address digital threats:

Every human rights organization, and not just digital rights organizations, should be aware of these digital insecurities and have strategies to secure their communications, their stored data and, in some cases, their office premises as well. Many organizations are doing a lot better than they were doing five years ago, but there’s still not enough information out there that is specific enough for groups in different countries and written in different languages, so people have access to materials not only in English.

**A long-term challenge**

Overall, the recommendations from these experts reveal the complex policy landscape and the competing aims of stakeholders in this space. At the same time, there is general agreement about key actions that the Canadian government, private companies and interested citizens can and should take to better protect civil society from digital threats.

For better and worse, national borders rarely stop digital communications, digital threats or the policies that shape them. Thus, while the experts identified some differences in the sources of risk to civil society in more repressive states versus those with stronger rule of law, the general sources of risk were similar and the policy responses are inextricably linked. For that reason, weakening security in countries like Canada, where the consequences of government surveillance may not be as severe, can directly lead to greater threats elsewhere — especially if Canada and similar countries weaken encryption, export surveillance technologies, and hypocritically disregard their own domestic and international commitments to privacy standards.

It is also clear that digital insecurity will long be a problem for civil society groups and for average individuals. Fanny Hidvegi of Access Now says:

Ultimately, I think a long-term goal should be to make digital security part of our primary education. It’s that fundamental. We are fighting not just for privacy but for the ability of people to communicate without being afraid, which is necessary for democracy. My feeling is that our perception of democracy has changed so much in the last few years, as we’ve gotten used to continual surveillance and privacy issues. That’s what Snowden says, too: This isn’t about privacy, this is about democracy.