Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity not only opportunistic, it is ongoing and persistent. It originates from many sources, but state and state-backed actors represent some of the most advanced threat actors in cyberspace. State to state relations are the responsibility of the Government of Canada, as is the responsibility to protect Canadians and Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government would take domestically to address the cyber security threats to Canada. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase cyber security.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders, Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cybersecurity issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada is responsible to defend and protect Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The National Cyber Security Strategy outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats that face Canada in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the National Cyber Security Strategy and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment to protect

Canada's elections, the Canadian-led G7 Rapid Response Mechanism, and the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015, with negotiations advancing on a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar challenges in cyberspace and the international context is evolving in response to these challenges. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order. The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada to prosper as a country. And Canada is not alone in this, many countries have similarly prospered. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, indiscriminate and irresponsible use of malware, and compromising Managed Service Providers (MSPs).

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. As outlined in the introduction, the Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy, Strong, Secure, Engaged, the updated National Cyber Security Strategy published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID pandemic. Collective security was increased when Canada publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

Using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, and taking into account foreign policy guidance from Global Affairs Canada, [redacted]

Not all cyber incidents will necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace by conducting malicious activity.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy can be read as a transparency and predictability measure.

Canada believes that the international law and agreed norms are largely sufficient to guide state behaviour in cyberspace. Canada acknowledges there remains some questions on how international law applies and that further work is needed to clarify the law, and on understanding and implementing the norms. Human rights and the rule of law are core values that Canada will promote in its understanding and implementation of the norms.

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

Canada does not support the creation of new norms at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms. Canada has further supported the implementation of the norms by sharing with the UN Canada's best practices and lessons learned from its own norms implementation.

For instance, Canada believes states should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet, to ensure the protection of all human rights online.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions. Pillar 3 of this document, Multilateral Engagement to Increase Canada's Security, provides more specificity to Canada's views.

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware; malicious activity by North Korea in the case of the use of WannaCry ransomware; and the compromise of Managed Service Providers (MSPs) by China.

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response to assist a partner regardless of the domain of the malicious activity. This could include joint statements of attribution or coordinated diplomatic activity and it could also include joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada and its partners and allies present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

Information sharing regarding potential compromises and cyber incidents is ongoing and continuous. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

GAC will build on its current relationships, developed through collaboration in numerous forums. This work will take place in existing forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs, as detailed in Pillars 3 and 4.

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan (SEAP). Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Within GAC, the SEAP will look to incorporate other divisions' efforts undertaken for advocacy and engagement in areas of security and contribute to increased Government of Canada coordination in international cybersecurity.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Government Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights online in the context of international security. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defence against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to encourage stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace by supporting the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are trying to use the institutions of the RBIO to further their authoritarian views. Contentious discussions at the intersection of security and privacy, freedom of expression, and internet governance continue. Canada has and will continue to keep human rights at the centre of these discussions. Increased cyber security is paramount to counter the threats facing Canada and Canadians, and our allies and partners. Canada believes that security and human rights are mutually re-enforcing; this is true in cyberspace as well.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

International Law

Canada has more many years affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorse by the UN General Assembly, the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The reports also provided some initial guidance on how it applies. While all States have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in this space.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

<u>Norms</u>

Voluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada will use these norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These voluntary non-binding norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, as well as the right to privacy in the digital age, and to guarantee full respect for human rights, including the right to freedom of expression.

Due to the importance Canada places on these norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation (Annex X?). In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms.

Some groups such as the G20 have developed their own additional voluntary norms, such as the G20 norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and conflict. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributed to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the attendance of civil servants from around the world at a course on the applicability of international in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas.

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem. This includes the promotion of human rights, a core principle in the ongoing work to ensure women enjoy the full benefits of their rights.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada has been a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program has supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its initiatives (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring that all states act lawfully and responsibly. Being transparent about the existence of its national capabilities and its views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with its federal partners to clarify and publicise its views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the I~~i~~nternet and an increasing amount of personal, community, and commercial activities takes place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources, but state and state-backed actors represent some of the most advanced threat actors in cyberspace. State to state relations are the responsibility of the Government of Canada, as is the responsibility to protect Canadians and Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government would take domestically to address the cyber security threats to Canada. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase cyber security.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It ~~and~~ states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders, thus Canada must ensure its foreign policy in cyberspace accounts for this reality.

This International S~~s~~trategy outlines the four pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to act, cooperate, advocate, and assist.

This S~~s~~trategy describes how Canada acts and will act in using the full range of its national capabilities, how it will cooperate with allies and partners to protect Canadian interests, how it will advocate and continue to engage in multilateral forums, and how it will look to increase assistance for cybersecurity issues by supporting capacity building internationally~~.~~

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Commented [YR-1]: These key elements may be lost here - perhaps break out as a list and use caps?

Commented [YR-2]: suggest 2 sentences here

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Commented [YR-3]: Do we also want to include here Canada's vision to make cyberspace better for all, not just Canada (i am thinking of capbuilding, ODA, FoC, I&J, and the trending Digital Inclusion - not suggesting to mention all these:) but to add a phrase or two to cover them all. Similarly, do you want to refer to human rights once somewhere in this vision statement - you develop this well later on below but its not explicit here in the vision part

Scope

The Government of Canada is responsible to defend and protect Canada's security and Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The National Cyber Security Strategy (NCSS?) outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats that face Canada in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the National Cyber Security Strategy and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation and cybercrime represent significant threats to Canada and Canadians. States engage in these kinds of activities and efforts are already underway to address these threats. This includes the work by the Communications Security Establishment to protect Canada's elections, the Canadian-led G7 Rapid Response Mechanism, and the RCMP's National Cybercrime Coordination Unit. There are also existing multilateral efforts, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canadian joined in 2015, with negotiation advancing on a new Protocol to strengthen it.~~that are well underway.~~

Commented [YR-4]: Perhaps add a link here?

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar challenges in cyberspace and the international context is evolving in response to these challenges. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada to prosper as a country. And Canada is not alone in this, many countries have similarly prospered. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors [and their proxies]. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, indiscriminate and irresponsible use of malware, and compromising Managed Service Providers (MSPs).

Commented [YR-5]: Suggest an explanation in a footnote or a sidebar box that states can be responsible for their proxies or actors they sponsor, and thus throughout the paper whenever we talk about states we include their proxies - otherwise it takes more space to say proxies each time, and understates how we will hold states accountable.

Commented [YR-6]: perhaspa footnote to explain this in aline or 2?

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. As outlined in the introduction, the Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy, Strong, Secure, Engaged, the updated National Cyber Security Strategy published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious

Commented [YR-7]: I like the use of "us" and similarly "we" and "our" - you might consider using it throughout, including in the Intro activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID pandemic. Collective security was increased when Canada publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

Commented [YR-8]: add a link? - also this sentence has lots in it, sugest brekaing in 2.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A cyber foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

s.23

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- ○ [redacted]
- ○ Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

[redacted]

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

[redacted]

Using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, and taking into account foreign policy guidance from Global Affairs Canada, [redacted]

Not all cyber incidents will necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

Canada has publicly condemnedcalled out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

Commented [YR-13]: suggest a synonym - this is a term widely used amongst experts but perhaps less so by the public.

[redacted]

Commented [YR-14]: is there a link to add?

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences regarding effective costs [redacted]

[redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's international and national legal obligations, and Canada's commitment to agreed-to international norms for state behaviour, and~~ Canada's international and national legal obligations~~.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace by conducting malicious activity.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy can be read as a transparency and predictability measure.

Canada and allies have long taken the position that international law and ~~believes that~~ the agreed-to norms ~~and international~~ law are largely sufficient to guide state behaviour in cyberspace. Canada and our allies acknowledge~~s~~ there remains some questions on *how* international law applies and that further work is needed to clarify the law, and on ~~in~~ understanding and implementing the norms. Human rights and the rule of law are core values that Canada will promote in its understanding and implementation of the norms.

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

Formatted: Font: Italic

Canada does not support the creation of new voluntary norms at this time, whether at the UN or in other fora Rather, we ~~and~~ believe that ~~s~~ states should continue to work in existing forums, such as the UN~~nited Nations~~, and together to implement these norms. Canada has further supported the implementation of the norms by sharing with the UN Canada's best practices and lessons learned from its own norms implementation.

For instance, Canada affirms ~~insists believes~~ that states should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place [national?]cyber security related initiatives or structures including measures to address security concerns on the Internet, to ensure the protection of all human rights online.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions. Pillar 3 of this document, Multilateral Engagement to Increase Canada's Security, provides more specificity to Canada's views.

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware; malicious activity by North Korea in the case of the use of WannaCry ransomware; and the compromise of Managed Service Providers (MSPs) by China.

Commented [YR-17]:

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response to assist a partner regardless of the domain of the malicious activity. This could include joint statements of attribution or coordinated diplomatic activity and it could also include joint cyber operations.

[redacted]

In all cases these activities would respect Canada`s domestic and international legal obligations and the agreed UN norms.

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada and its partners and allies present a united front against this malicious activity and reinforce the RBIO [framework for stability] ~~agreed to norms of state behaviour~~ in cyberspace.

Information sharing regarding potential compromises and cyber incidents is ongoing and continuous. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

[redacted]

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

GAC will build on its current relationships, developed through collaboration in numerous forums. This work will take place in existing forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, ~~and~~ such as working with states to further develop our common understanding of international law and to implement norms of responsible state behaviour through the adoption of practical measures such as CBMBs, as detailed in Pillars 3 and 4.

Commented [YR-19]: add reference to capacity-building on I?

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan (SEAP). Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Within GAC, the SEAP will look to incorporate other divisions' efforts undertaken for advocacy and engagement in areas of security and contribute to increased Government of Canada coordination in international cybersecurity.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Government Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights online in the context of international security. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defence against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to encourage stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace by supporting the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are trying to use the institutions of the RBIO to further their authoritarian views. Contentious discussions at the intersection of security and privacy, freedom of expression, and I~~i~~nternet governance continue. Canada has and will continue to keep human rights at the centre of these discussions. Increased cyber security is paramount to counter the threats facing Canada and Canadians, and our allies and partners. Canada believes that security and human rights are mutually re-enforcing; this is true in cyberspace as well.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

Formatted: Font:

Voluntary [Non-binding] Norms

Commented [YR-20]: Please put IL section before norms

In addition to the international legal rules that bind all states, v~~V~~oluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the foundation for sustaining international peace and security in cyberspace. That is why Canada has strongly supported the adoption of voluntary norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada will use these norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These voluntary non-binding norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, as well as the right to privacy in the digital age, and to guarantee full respect for human rights, including the right to freedom of expression.

Commented [YR-21]: Check this wording with JLH/Fetz and/or Utting

Due to the importance Canada places on these norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation (Annex X?). In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms.

Some groups such as the G20 have developed their own additional voluntary norms, such as the G20 norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

Commented [YR-22]: We may need to wordsmith this as we elsewhere say we don't support development of new norms

Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

International Law

Canada has for many years affirmed the application of international law to state behaviour in cyberspace. There is broad support for this position across the international community. It was u~~U~~nanimously endorsed by the UN General Assembly, the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security) ~~concluded that international law applies in cyberspace.~~

Commented [YR-23]: Consider adding links here

The reports also provided some initial guidance on how it applies. While all States have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in this space.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Commented [YR-24]: Not sure this adds value or fits here. I would suggest deleting it/

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use ~~availability of the doctrine of~~ countermeasures in response to internationally wrongful acts.

Canada recognises ~~It is definitive~~ that cyber activities can exceptionally rise to the level of an armed attack. Canada affirmed ~~recognized~~ this when NATO articulated ~~acknowledged~~ that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Commented [YR-25]: check in I Branch if Canada prefers to call it the Washingon Treaty, I have sent a query to JLH

Canada also recognizes that International Humanitarian Law (IHL) (also known as the Law of Armed Conflict, or LOAC)~~,~~ including the Geneva Conventions, applies~~y~~ when cyber operations are conducted during ~~declared~~ hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open up dialogue ~~lines of communication~~ between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and conflict. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributes~~d~~ to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the participation of ~~attendance of~~ civil servants from selected states around the world in training ~~at a~~ courses on the applicability of international law in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas.

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem. This includes the promotion of human rights, a core principle in the ongoing work to ensure women enjoy the full benefits of their rights.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security.

To increase it~~'~~s understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

Commented [YR-26]: Not sure what this adds, i.e., how it relates to the norms.

~~From the perspective of the norms for state behaviour,~~ Canada supports increasing women's participation in decision making and positions of influence in cyber security. For example, ~~at the UN OEWG~~ Canada is~~has been~~ a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program has supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its initiatives (see Annex X). The next step is to ensure the greater participation of all communities whic~~ho~~ may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring that all states act lawfully and responsibly. Being transparent about the existence of its national capabilities and its views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with its federal partners to clarify and publicise its views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources, but state and state-backed actors represent some of the most advanced threat actors in cyberspace. The Government of Canada is responsible for state to state relations and protecting Canadians and Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government would take domestically to address the cyber security threats to Canada. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders, Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cybersecurity issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada is responsible to defend and protect Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The National Cyber Security Strategy outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats that face Canada in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the National Cyber Security Strategy and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment to protect

> Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

Canada's elections, the Canadian-led G7 Rapid Response Mechanism, and the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015, with negotiations advancing on a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar challenges in cyberspace and the international context is evolving in response to these challenges. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada to prosper as a country. And Canada is not alone in this, many countries have similarly prospered. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. As outlined in the introduction, the Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy, Strong, Secure, Engaged, the updated National Cyber Security Strategy published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID pandemic. Collective security was increased when Canada publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

Using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, and taking into account foreign policy guidance from Global Affairs Canada, [redacted]

Not all cyber incidents will necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

s.15(1) - Defence

s.15(1) - International

s.15(1) - Security

s.21(1)(b)

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences regarding effective costs [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace by conducting malicious activity.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy can be read as a transparency and predictability measure.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Summary of Actions:

- Canada will use its capabilities and tools to protect itself and its interests
- Canada will continue to develop the appropriate policies and procedures for using these capabilities
- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response to assist a partner regardless of the domain of the malicious activity. This could include joint statements of attribution or coordinated diplomatic activity and it could also include joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada and its partners and allies present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

Information sharing regarding potential compromises and cyber incidents is ongoing and continuous. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

GAC will build on its current relationships, developed through collaboration in numerous forums. This work will take place in existing forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs, as detailed in Pillars 3 and 4.

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan (SEAP). Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Within GAC, the SEAP will look to incorporate other divisions' efforts undertaken for advocacy and engagement in areas of security and contribute to increased Government of Canada coordination in international cybersecurity.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Government Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights online in the context of international security. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defence against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to encourage stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

s.15(1) - International

Summary of Actions:

- Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.
- [redacted]
- Canada will continue dialogue at multilateral organizations, to support cyber capacity building, and work with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs
- GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach
- GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan (SEAP)
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace by supporting the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are using the institutions of the RBIO to further their authoritarian views. Canada's support to the RBIO, as well as that of allies and partners, is important to continue to sustain the institutions that have allowed Canada to prosper. In cyberspace, this support is demonstrated by Canada's ongoing commitment to international law and norms for responsible state behaviour.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

International Law

Canada has for many years affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorse by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The reports also provided some initial guidance on how international law applies in cyberspace. While all States have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in this space.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

Voluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of norms and continues to promote their endorsement, observation, and implementation in various forums.

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

Canada will use these norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These voluntary non-binding norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Canada does not support the creation of new norms at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms. Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada shared with the UN its best practices and lessons learned from its own norms implementation (Annex X?).

For instance, Canada believes states should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet, to ensure the protection of all human rights online.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms.

Some groups such as the G20 have developed their own additional voluntary norms, such as the G20 norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

reduce the seriousness of state to state cyber incidents by preventing miscalculations and conflict. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use the agreed norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the norms
- Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace.
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributed to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the attendance of civil servants from around the world at a course on the applicability of international in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas.

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security and Canada will continue to ensure human rights values inform its approach to international cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada has been a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program has supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Summary of Actions:

- GAC will continue to engage in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs
- Canada will continue to provide financial assistance in growing international cyber expertise
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring that all states act lawfully and responsibly. Being transparent about the existence of its national capabilities and its views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with its federal partners to clarify and publicise its views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources and state and state-backed actors represent some of the most advanced threat actors in cyberspace. The Government of Canada is responsible for state to state relations and protecting Canadians as well as Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government of Canada would take domestically to address the cyber security threats. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders and Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cyber security issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada is responsible to defend and protect Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The NCSS outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the NCSS and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment (CSE) to protect Canada's elections, the Canadian-led G7 Rapid

Response Mechanism, the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015 and continues to participate in negotiations to advance a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar challenges in cyberspace and the international context is evolving in response to these challenges. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

[redacted]

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada and many countries to prosper. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. The Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy Strong, Secure, Engaged, the updated NCSS published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID-19 pandemic. Collective security was increased when Canada

publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

Guided by Canada's foreign policy, using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence,

[redacted]

Not all cyber incidents necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

s.15(1) - Defence

s.15(1) - International

s.15(1) - Security

s.21(1)(b)

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy is itself a transparency and predictability measure.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions.

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Summary of Actions:

- Canada will use its capabilities and tools to protect itself and its interests
- Canada will continue to develop the appropriate policies and procedures for using these capabilities
- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to develop new, and enhance existing, tools to better deter malicious actors
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications
- Canada will continue to respect its domestic and international legal obligations and uphold responsible state behaviour in cyberspace

s.15(1) - International

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response in coordination with a partner regardless of the domain of the malicious activity. These efforts could include joint statements of attribution, coordinated diplomatic activity, and joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada, its partners and allies will present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

A collective understanding of cyber threats requires ongoing and continuous information sharing of potential compromises and cyber incidents. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

Canada will build on its current relationships, developed through collaboration in numerous forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs, as detailed in Pillars 3 and 4.

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan (SEAP). Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Governmental Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to promote stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

Summary of Actions:

s.15(1) - International

- Canada will continue to call out malicious activity by state and state-backed actors and will continue to support our allies and partners on coordinated attributions.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies and will ask its partners for their support when needed.
- [redacted]
- Canada will continue dialogue at multilateral organizations, to support cyber capacity building, and work with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs
- GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach
- GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan (SEAP)
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors
- Canada will continue to build partnerships and relationships with allies and likeminded states

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace and support the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are using the institutions of the RBIO to further their authoritarian views. Canada's support to the RBIO, as well as that of allies and partners, is important to continue to sustain the institutions that have allowed Canada to prosper. In cyberspace, this support is demonstrated by Canada's ongoing commitment to international law and norms for responsible state behaviour.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

International Law

Canada has affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorsed by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The reports also provided initial guidance on how international law applies in cyberspace. While all states have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in cyberspace.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

Voluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement, observation, and implementation in various forums.

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

Canada views these norms and our obligations under to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These voluntary non-binding norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Canada does not support the creation of new norms for state behaviour in cyberspace at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms.

Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms. (Most recently, see Canada's submission to the UN in Annex X?).

For instance, Canada believes that human rights apply online as they do offline. States should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Some groups such as the G20 have developed their own additional voluntary norms, such as the norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

In seeking stability in cyberspace, Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

escalation. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use the agreed norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the norms
- Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices
- Canada will continue to strengthen existing relationships and establish new ones

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. In addition, malicious actors often practice their abilities against one state before moving on to the next.

State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributed to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the attendance of civil servants from around the world at a course on the applicability of international in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas. [Reference to support to Georgia election? ICC and IOP consult].

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security and Canada will continue to ensure human rights values inform its approach to international cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada is a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Summary of Actions:

- GAC will continue to engage in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs
- Canada will continue to provide financial assistance in growing international cyber expertise
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring all states act lawfully and responsibly. Being transparent about the existence of national capabilities and views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with federal partners to clarify and publicise Canada's views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources and state and state-backed actors represent some of the most advanced threat actors in cyberspace. The Government of Canada is responsible for state to state relations and protecting Canadians as well as Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government of Canada would take domestically to address cyber security threats. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders and Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cyber security issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. In doing so, Canada will ensure our actions respect our values of democracy, rule of law, and human rights.

This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada defends and protects Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The NCSS outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the NCSS and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked

> Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment (CSE) to protect Canada's elections, the Canadian-led G7 Rapid Response Mechanism, the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015 and continues to participate in negotiations to advance a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar difficulties in cyberspace and the international context is evolving in response to this reality. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada and many countries to prosper. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. The Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy Strong, Secure, Engaged, the updated NCSS published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID-19 pandemic. Collective security was increased when Canada

publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

Guided by Canada's foreign policy, using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, [redacted]

Not all cyber incidents necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy is itself a transparency and predictability measure.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions.

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Summary of Actions:

- Canada will use its capabilities and tools to protect itself and its interests
- Canada will continue to develop the appropriate policies and procedures for using these capabilities
- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to develop new, and enhance existing, tools to better deter malicious actors
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications
- Canada will continue to respect its domestic and international legal obligations and uphold responsible state behaviour in cyberspace

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response in coordination with a partner regardless of the domain of the malicious activity. These efforts could include joint statements of attribution, coordinated diplomatic activity, and joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada, its partners and allies will present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

A collective understanding of cyber threats requires ongoing and continuous information sharing of potential compromises and cyber incidents. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

Canada will build on its current relationships, developed through collaboration in numerous forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs, as detailed in Pillars 3 and 4.

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a cyber stakeholder engagement action plan. Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Existing consultation processes will be used, as well as new or innovative processes as opportunities arise.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Governmental Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to promote stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

Summary of Actions:

- Canada will continue to call out malicious activity by state and state-backed actors and will continue to support our allies and partners on coordinated attributions.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies and will ask its partners for their support when needed.
- [redacted]
- Canada will continue dialogue at multilateral organizations, to support cyber capacity building, and work with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs
- GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach
- GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors
- Canada will continue to build partnerships and relationships with allies and likeminded states

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace and support the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are using the institutions of the RBIO to further their authoritarian views. Canada's support to the RBIO, as well as that of allies and partners, is important to continue to sustain the institutions that have allowed Canada to prosper. In cyberspace, this support is demonstrated by Canada's ongoing commitment to international law and norms for responsible state behaviour.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

Canada believes that existing international law and agreed norms are sufficient to guide state behaviour in cyberspace. Canada acknowledges there remains work to be done concerning how international law applies and to ensure states have a comprehensive understanding of their responsibilities stemming from these norms. However, Canada believes international law and the existing norms are clear in governing state activity in cyberspace, including respect for human rights.

International Law

Canada has affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorsed by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The reports also provided initial guidance on how international law applies in cyberspace. While all states have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in cyberspace.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of

international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

Voluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada views these norms and our obligations under to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Canada does not support the creation of new norms for state behaviour in cyberspace at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms.

Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms. (Most recently, see Canada's submission to the UN in Annex X?).

For instance, Canada believes that human rights apply online as they do offline. States should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Some groups such as the G20 have developed their own additional voluntary norms, such as the norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

In seeking stability in cyberspace, Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and escalation. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use the agreed norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the norms
- Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices
- Canada will continue to strengthen existing relationships and establish new ones

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. In addition, malicious actors often practice their abilities against one state before moving on to the next.

State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributed to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the attendance of civil servants from around the world at a course on the applicability of international in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas. [Reference to support to Georgia election? ICC and IOP consult].

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security and Canada will continue to ensure human rights values inform its approach to international cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada is a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Summary of Actions:

- GAC will continue to engage in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs
- Canada will continue to provide financial assistance in growing international cyber expertise
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring all states act lawfully and responsibly. Being transparent about the existence of national capabilities and views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with federal partners to clarify and publicise Canada's views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources and state and state-backed actors represent some of the most advanced threat actors in cyberspace. The Government of Canada is responsible for state to state relations and protecting Canadians as well as Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government of Canada would take domestically to address cyber security threats. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders and Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cyber security issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. In doing so, Canada will ensure our actions respect our values of democracy, rule of law, and human rights.

This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada defends and protects Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The NCSS outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the NCSS and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked

Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment (CSE) to protect Canada's elections, the Canadian-led G7 Rapid Response Mechanism, the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015 and continues to participate in negotiations to advance a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar difficulties in cyberspace and the international context is evolving in response to this reality. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada and many countries to prosper. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. The Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy Strong, Secure, Engaged, the updated NCSS published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID-19 pandemic. Collective security was increased when Canada

publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

Guided by Canada's foreign policy, using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, [redacted]

Not all cyber incidents necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

Commented [LD-1]: When we Canada articulates FP priorities, they are usually organized in some way around the security, prosperity, values triad. So I found it odd to see this sentence without any reference to values.

The document more broadly talks a lot about values (RBIO, human rights, gender etc.), so values are clearly an important part of our cyber foreign policy.

Could that be made more explicit here? For example: "Canada's priorities for foreign policy in cyberspace are protecting the security of Canada and its interests, and advancing our values"?

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy is itself a transparency and predictability measure.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions.

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Summary of Actions:

- Canada will use its capabilities and tools to protect itself and its interests
- Canada will continue to develop the appropriate policies and procedures for using these capabilities
- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to develop new, and enhance existing, tools to better deter malicious actors
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications
- Canada will continue to respect its domestic and international legal obligations and uphold responsible state behaviour in cyberspace

[redacted]

s.15(1) - International

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response in coordination with a partner regardless of the domain of the malicious activity. These efforts could include joint statements of attribution, coordinated diplomatic activity, and joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada, its partners and allies will present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

A collective understanding of cyber threats requires ongoing and continuous information sharing of potential compromises and cyber incidents. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

[redacted]

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

Canada will build on its current relationships, developed through collaboration in numerous forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour through the adoption of practical measures such as Confidence Building Measures~~CMBs~~, as detailed in Pillars 3 and 4.

Commented [LD-2]: This is the first reference, also presumably the acronym is CBM, not CMB

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a cyber stakeholder engagement action plan. Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Existing consultation processes will be used, as well as new or innovative processes as opportunities arise.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely in an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Governmental Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to promote stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

s.15(1) - International

Summary of Actions:

- Canada will continue to call out malicious activity by state and state-backed actors and will continue to support our allies and partners on coordinated attributions.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies and will ask its partners for their support when needed.
- [redacted]
- Canada will continue dialogue at multilateral organizations, to support cyber capacity building, and work with states to implement norms of responsible state behaviour through the adoption of practical measures such as ~~CMBs~~Confidence Building Measures
- GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach
- GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors
- Canada will continue to build partnerships and relationships with allies and likeminded states

[redacted]

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace and support the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are using the institutions of the RBIO to further their authoritarian views. Canada's support to the RBIO, as well as that of allies and partners, is important to continue to sustain the institutions that have allowed Canada to prosper. In cyberspace, this support is demonstrated by Canada's ongoing commitment to international law and norms for responsible state behaviour.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

Canada believes that existing international law and agreed norms are sufficient to guide state behaviour in cyberspace. Canada acknowledges there remains work to be done concerning how international law applies and to ensure states have a comprehensive understanding of their responsibilities stemming from these norms. However, Canada believes international law and the existing norms are clear in governing state activity in cyberspace, including respect for human rights.

International Law

Canada has affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorsed by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The reports also provided initial guidance on how international law applies in cyberspace. While all states have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in cyberspace.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of

international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

Voluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada views these norms and our obligations under to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Canada does not support the creation of new norms for state behaviour in cyberspace at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms.

Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms. (Most recently, see Canada's submission to the UN in Annex X?).

For instance, Canada believes that human rights apply online as they do offline. States should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Some groups such as the G20 have developed their own additional voluntary norms, such as the norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

In seeking stability in cyberspace, Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and escalation. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use the agreed norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the norms
- Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices
- Canada will continue to strengthen existing relationships and establish new ones

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. In addition, malicious actors often practice their abilities against one state before moving on to the next.

State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributed to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the attendance of civil servants from around the world at a course on the applicability of international in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas. [Reference to support to Georgia election? ICC and IOP consult].

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security and Canada will continue to ensure human rights values inform its approach to international cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada is a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Summary of Actions:

- GAC will continue to engage in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs
- Canada will continue to provide financial assistance in growing international cyber expertise
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring all states act lawfully and responsibly. Being transparent about the existence of national capabilities and views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with federal partners to clarify and publicise Canada's views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources and state and state-backed actors represent some of the most advanced threat actors in cyberspace. The Government of Canada is responsible for state to state relations and protecting Canadians as well as Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government of Canada would take domestically to address cyber security threats. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders and Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cyber security issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. In doing so, Canada will ensure our actions respect our values of democracy, rule of law, and human rights.

This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada defends and protects Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The NCSS outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the NCSS and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked

Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment (CSE) to protect Canada's elections, the Canadian-led G7 Rapid Response Mechanism, the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015 and continues to participate in negotiations to advance a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar difficulties in cyberspace and the international context is evolving in response to this reality. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada and many countries to prosper. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. The Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy Strong, Secure, Engaged, the updated NCSS published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID-19 pandemic. Collective security was increased when Canada

publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

Guided by Canada's foreign policy, using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, [redacted]

Not all cyber incidents necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy is itself a transparency and predictability measure.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Summary of Actions:

- Canada will use its capabilities and tools to protect itself and its interests
- Canada will continue to develop the appropriate policies and procedures for using these capabilities
- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to develop new, and enhance existing, tools to better deter malicious actors
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications
- Canada will continue to respect its domestic and international legal obligations and uphold responsible state behaviour in cyberspace

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response in coordination with a partner regardless of the domain of the malicious activity. These efforts could include joint statements of attribution, coordinated diplomatic activity, and joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada, its partners and allies will present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

A collective understanding of cyber threats requires ongoing and continuous information sharing of potential compromises and cyber incidents. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

Canada will build on its current relationships, developed through collaboration in numerous forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs, as detailed in Pillars 3 and 4.

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a cyber stakeholder engagement action plan. Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Existing consultation processes will be used, as well as new or innovative processes as opportunities arise.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Governmental Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to promote stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

Summary of Actions:

- Canada will continue to call out malicious activity by state and state-backed actors and will continue to support our allies and partners on coordinated attributions.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies and will ask its partners for their support when needed.
- [redacted]
- Canada will continue dialogue at multilateral organizations, to support cyber capacity building, and work with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs
- GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach
- GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors
- Canada will continue to build partnerships and relationships with allies and likeminded states

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace and support the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are using the institutions of the RBIO to further their authoritarian views. Canada's support to the RBIO, as well as that of allies and partners, is important to continue to sustain the institutions that have allowed Canada to prosper. In cyberspace, this support is demonstrated by Canada's ongoing commitment to international law and norms for responsible state behaviour.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

Canada believes that existing international law and agreed norms are sufficient to guide state behaviour in cyberspace. Canada acknowledges there remains work to be done concerning how international law applies and to ensure states have a comprehensive understanding of their responsibilities stemming from these norms. However, Canada believes international law and the existing norms are clear in governing state activity in cyberspace, including respect for human rights.

International Law

Canada has affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorsed by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The reports also provided initial guidance on how international law applies in cyberspace. While all states have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in cyberspace.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of

international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

Voluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada views these norms and our obligations under to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Canada does not support the creation of new norms for state behaviour in cyberspace at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms.

Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms. (Most recently, see Canada's submission to the UN in Annex X?).

For instance, Canada believes that human rights apply online as they do offline. States should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Some groups such as the G20 have developed their own additional voluntary norms, such as the norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

In seeking stability in cyberspace, Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and escalation. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use the agreed norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the norms
- Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices
- Canada will continue to strengthen existing relationships and establish new ones

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. In addition, malicious actors often practice their abilities against one state before moving on to the next.

State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributed to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the attendance of civil servants from around the world at a course on the applicability of international in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas. [Reference to support to Georgia election? ICC and IOP consult].

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security and Canada will continue to ensure human rights values inform its approach to international cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada is a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Summary of Actions:

- GAC will continue to engage in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs
- Canada will continue to provide financial assistance in growing international cyber expertise
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring all states act lawfully and responsibly. Being transparent about the existence of national capabilities and views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with federal partners to clarify and publicise Canada's views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources and state and state-backed actors represent some of the most advanced threat actors in cyberspace. The Government of Canada is responsible for state to state relations and protecting Canadians as well as Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government of Canada would take domestically to address cyber security threats. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders and Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cyber security issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. In doing so, Canada will ensure our actions respect our values of democracy, rule of law, and human rights.

This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada defends and protects Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The NCSS outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

> Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the NCSS and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked

challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment (CSE) to protect Canada's elections, the Canadian-led G7 Rapid Response Mechanism, the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015 and continues to participate in negotiations to advance a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar difficulties in cyberspace and the international context is evolving in response to this reality. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada and many countries to prosper. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors or their proxies. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Commented [YR-1]: Suggest an explanation in a footnote or a sidebar box that states can be responsible for their proxies or actors they sponsor, and thus throughout the paper whenever we talk about states we include their proxies - otherwise it takes more space to say proxies each time, and understates how we will hold states accountable.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. The Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy Strong, Secure, Engaged, the updated NCSS published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID-19 pandemic. Collective security was increased when Canada

publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- ○ [redacted]
- ○ Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

[redacted]

Note that it is not until page

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

[redacted]

[redacted]

Guided by Canada's foreign policy, using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, [redacted]

Not all cyber incidents necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation,

s.15(1) - Defence

s.15(1) - International

s.15(1) - Security

s.21(1)(b)

regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's international and national legal obligations, and Canada's commitment to agreed-to voluntary international norms for state behaviour, ~~and Canada's international and national legal obligations.~~

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the agreed voluntary norms for responsible state behaviour in cyberspace.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy is itself a transparency and predictability measure.

Commented [YR-5]: Advise putting legal obligations first as they have more weight than non-binding commitments.

Formatted: Highlight

Commented [YR-6]: See comment on p. 4 advising addition of an explanation of how states can be responsible under international law for the actions of proxies. This is highly relevant in the cyber context. The use here is not incorrect, but it's the first time proxies are mentioned, and then they are not mentioned again.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

[redacted]

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions.

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Summary of Actions:

- Canada will use its capabilities and tools to protect itself and its interests
- Canada will continue to develop the appropriate policies and procedures for using these capabilities
- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to develop new, and enhance existing, tools to better deter malicious actors
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications
- Canada will continue to respect its domestic and international legal obligations and uphold responsible state behaviour in cyberspace

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response in coordination with a partner regardless of the domain of the malicious activity. These efforts could include joint statements of attribution, coordinated diplomatic activity, and joint cyber operations.

In all cases these activities would respect Canada's domestic and international legal obligations and the agreed UN norms.

Commented [YR-7]: Given that this section addresses Canada's responses, including joint responses with partners, assistance to partners and from partners, and including "joint cyber operations", we would advise including a specific mention here that these would in all cases respect Canada's legal obligations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada, its partners and allies will present a united front against this malicious activity and reinforce the framework for responsible ~~agreed to norms of~~ state behaviour in cyberspace.

Commented [YR-8]: Suggest referring to the framework generally for brevity, otherwise would need to add a reference to international law and the voluntary norms. An alternative is to refer to the RBIO, mentioned in the introduction.

A collective understanding of cyber threats requires ongoing and continuous information sharing of potential compromises and cyber incidents. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

[redacted]

s.15(1) - Security

s.15(1) - International

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

Canada will build on its current relationships, developed through collaboration in numerous forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, to further develop our common understandings of international law, ~~and~~ working with states to implement norms of responsible state behaviour, and through the adoption of practical measures such as CMBs, as detailed in Pillars 3 and 4.

Commented [YR-10]: add reference to capacity-building on I?

[redacted]

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a cyber stakeholder engagement action plan. Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Existing consultation processes will be used, as well as new or innovative processes as opportunities arise.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Governmental Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in promoting protection of ~~ng~~ human rights. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.

Commented [YR-12]: In UN discussions the NGOs have not protected human rights (some do it elsewhere for sure) but they have promoted their protection.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with

s.15(1) - International

partners to promote stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

Summary of Actions:

- Canada will continue to call out malicious activity by state ~~and state-backed~~ actors and their proxies and will continue to support our allies and partners on coordinated attributions.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies and will ask its partners for their support when needed.
- [redacted]
- Canada will continue dialogue at multilateral organizations, to support cyber capacity building, to further develop our common understandings of international law, to ~~and~~ work with states to implement norms of responsible state behaviour and through the adoption of practical measures such as CMBs
- GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach
- GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors
- Canada will continue to build partnerships and relationships with allies and likeminded states

Commented [YR-13]: Suggest this revision for consistency

s.15(1) - International

s.15(1) - Security

[redacted]

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace and support the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are using the institutions of the RBIO to further their authoritarian views. Canada's support to the RBIO, as well as that of allies and partners, is important to continue to sustain the institutions that have allowed Canada to prosper. In cyberspace, this support is demonstrated by Canada's ongoing commitment to international law and norms for responsible state behaviour.

[redacted]

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

Canada believes that existing international law and agreed norms are sufficient to guide state behaviour in cyberspace. Canada acknowledges there remains work to be done concerning how international law applies and to ensure states have a comprehensive understanding of their responsibilities stemming from these norms. However, Canada believes international law and the existing norms are clear in governing state activity in cyberspace, including respect for human rights.

International Law

Canada has affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorsed by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

Commented [YR-14]: [redacted]

The reports also provided initial guidance on how international law applies in cyberspace. While all states have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in cyberspace.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of

s.15(1) - International

international law. International law is shaped in large part by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Commented [YR-15]: This minor change is advised as IL is also shaped by treaties, by the decisions of courts and tribunals, and by legal exerts in academia, NGOs, etc.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Commented [YR-16]: Advise deleting. The first part follows the previous para, and could be developed to support that states should avoid ambiguity by articulating their national views, but that point was clearly made in the previous para. In any event, the second relates to states' responsibilities, and does not fit here.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

Canada recognises ~~It is definitive~~ that cyber activities can exceptionally rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, providing for collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Formatted: Normal, No bullets or numbering

Canada also affirms the application of international human rights law to state behaviour in cyberspace. Canada's views are well known – human rights enjoyed offline are equally protected online.

Commented [YR-17]: Recommend we add a brief mention of IHRL and our public positions on this.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

[redacted]

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

The eleven v~~V~~oluntary norms for responsible state behaviour reinforce the RBIO and are

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada views these norms and our obligations under ~~to~~ international law as the standards for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Commented [YR-19]: This is the first time you mention that there are 11! As noted above, strongly recommend defining these at first use on p. 4 and using a consistent term such as UN voluntary norms.

Canada does not support the creation of new norms for state behaviour in cyberspace at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms.

Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms. (Most recently, see Canada's submission to the UN in Annex X?).

For instance, Canada believes that human rights apply online as they do offline. States should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet.

[redacted]

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Commented [YR-21]: As noted, JLH should be consulted on "right to privacy" language

Some groups such as the G20 have developed their own additional voluntary norms, such as the norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

Commented [YR-22]: Here it says Canada has endorsed additional norms from the G20, but 4 paras above you say Canada supports only the 11 GGE norms and does not support new norms. This needs to be harmonised/clarified.

Formatted: Highlight

Formatted: Highlight

In seeking stability in cyberspace, Canada will continue to advocate for respect for agreed norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and escalation. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use adherence to international law as well as the agreed norms as well ~~as adherence to international law~~ as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the UN voluntary norms
- Canada will continue to advocate for respect for the UN voluntary norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices

- Canada will continue to strengthen existing relationships and establish new ones

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. In addition, malicious actors often practice their abilities against one state before moving on to the next.

State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributes~~d~~ to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the participation ~~attendance~~ of civil servants from selected states around the world in ~~at a~~ courses on the applicability of international in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has contributed over $13.5 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up throughout the Americas. [Reference to support to Georgia election? ICC and IOP consult].

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security and Canada will continue to ensure human rights values inform its approach to international cyber security.

To increase it~~'~~s understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

~~From the perspective of the norms for state behaviour,~~

Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada is a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Commented [YR-23]: Not clear how this relates to the norms for state behaviour, so suggest deleting that first part of the sentence.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). ~~The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem,~~ including neuro and racially diverse communities, among others.

Summary of Actions:

- GAC will continue to engage in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs
- Canada will continue to provide financial assistance in increasing ~~growing~~ international cyber expertise, including on international law
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring all states act lawfully and responsibly. Being transparent about the existence of national capabilities and views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with federal partners to clarify and publicise Canada's views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is not only opportunistic, it is ongoing and persistent. It originates from many sources and state and state-backed actors represent some of the most advanced threat actors in cyberspace. The Government of Canada is responsible for state to state relations and protecting Canadians as well as Canadian interests from these threats.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government of Canada would take domestically to address cyber security threats. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. It states that "the federal government will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour."

Global Affairs Canada is doing its part to meet this goal. Cyber threats and malicious cyber activity are not constrained by borders and Canada must ensure its foreign policy in cyberspace accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

This Strategy describes how Canada acts and will act in using the full range of its national capabilities; how it will cooperate with allies and partners to protect Canadian interests; how it will advocate and continue to engage in multilateral forums; and how it will look to increase assistance for cyber security issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians. Cyber threats and the irresponsible use of digital technologies can undermine Canada's institutions and values.

Canada has and will continue to face these challenges. In facing the challenges and taking action, Canada's security in cyberspace is increased. In doing so, Canada will ensure our actions respect our values of democracy, rule of law, and human rights.

This security is further enhanced by shaping the international environment in favour of Canadian interests and working with allies and partners to increase the predictability of state behaviour in cyberspace.

Working at home to increase cyber security and resilience to cyber incidents, big and small, and working with allies and partners to increase our collective security all contribute to a more stable and prosperous future for Canada.

Scope

The Government of Canada defends and protects Canada's security. Canadians and Canadian organizations also have a responsibility to take reasonable action to protect themselves. However, they should not be expected to independently defend themselves against state or state-backed actors. There are steps only governments can take to reduce cyber threats from state actors.

The NCSS outlines some of these steps; however, in order for Canada's efforts to increase cyber security at home to be successful, they must be supported by Canada's efforts internationally. As part of this effort, Global Affairs Canada will continue to implement a foreign policy for cyberspace that places security at its heart.

This strategy outlines four pillars for Canada's foreign policy that will contribute to increased security. As the most sophisticated threats in cyberspace come from state and state-backed actors, it will focus on state behaviour in cyberspace.

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity, in particular those of the NCSS and its associated Action Plan, and provides foreign policy direction for the federal cyber community.

Challenges such as the misuse of digital platforms for disinformation, domestic cyber espionage for population control, and cybercrime, are closely linked

Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment (CSE) to protect Canada's elections, the Canadian-led G7 Rapid Response Mechanism, the RCMP's National Cybercrime Coordination Unit, and the funding of organizations supporting human rights defenders internationally. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention) that Canada joined in 2015 and continues to participate in negotiations to advance a new Protocol to strengthen it.

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber community will achieve the goals set out by the Government of Canada.

Context

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

Canada is not unique in the challenges it faces. All states face similar difficulties in cyberspace and the international context is evolving in response to this reality. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada and many countries to prosper. For these reasons, Canada is a strong supporter and defender of the RBIO. This support informs our foreign policy. A foreign policy that also remains responsive to the evolving challenges of the 21st century.

A key challenge for Canada is ongoing hostile activity by state actors. With increased technological developments, the range of behaviour by states has expanded, including malicious cyber activity. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. The Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

These actions include the 2015 RCMP Cybercrime Strategy, the cyber initiatives in Canada's 2017 Defence Policy Strong, Secure, Engaged, the updated NCSS published in 2018 and its associated Action Plan, the creation of the Canadian Centre for Cyber Security in 2018, the *Communications Security Establishment Act* of 2019, and the establishment of the RCMP National Cybercrime Coordination Unit in 2020.

Ensuring that all states benefit from the opportunities presented by the digital revolution is an important part of international peace and stability. Equally important are the adoption of cyber security best practices, information sharing, and cooperation. Increasing the security of individual states increases the security of all of us, as it allows less opportunity for malicious activity to take place. For this reason, Canada also supports capacity building for the cyber security of other states and the development of cyber expertise in developing states.

The threats stemming from malicious cyber activity are exacerbated during times of increased vulnerability, such as the COVID-19 pandemic. Collective security was increased when Canada

publicly issued its bulletin on cyber threats to the health sector as it increased the level of awareness of Canada's health sector, and also that of other states looking to protect their own health sectors, by informing them of the potential threat and providing advice on mitigation strategies.

What the future may hold for the evolution of cyber threats is unclear. What is clear is Canada must be prepared to adapt and take action. A foreign policy that protects the national interest and upholds Canadian principles and values is essential to face current and future challenges.

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

Canada will continue to develop the appropriate policies and procedures for using these capabilities, guided by Canadian legislation, relevant international law, government direction, and values such as human rights.

[redacted]

[redacted]

Guided by Canada's foreign policy, using the resources of agencies such as the Communications Security Establishment, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, as well as National Defence, [redacted]

Not all cyber incidents necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

s.15(1) - Defence

s.15(1) - International

s.15(1) - Security

s.21(1)(b)

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in cyberspace are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's priorities for foreign policy in cyberspace, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before action is taken prevents misunderstandings and sets expectations. This Strategy is itself a transparency and predictability measure.

This Strategy represents the first of ongoing efforts to define and publicise Canada's foreign policy in cyberspace, including Canada's international priorities and positions.

[redacted]

Canada's foreign policy for cyberspace will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

Summary of Actions:

- Canada will use its capabilities and tools to protect itself and its interests
- Canada will continue to develop the appropriate policies and procedures for using these capabilities
- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to develop new, and enhance existing, tools to better deter malicious actors
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications
- Canada will continue to respect its domestic and international legal obligations and uphold responsible state behaviour in cyberspace
- Canada will continue to support cyber capacity building that works to improve the cybersecurity of other nations and encourage increased standards of coordination between States to more effectively respond to cyber threats.
- Canada will use capacity building support to provide tailored trainings on the importance of international cyber law, CBMs and responsible state behaviour in cyberspace.

Formatted: Indent: Left: 1.27 cm, No bullets or numbering

s.15(1) - International

[redacted]

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with non-traditional partners

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace and respond to those that seek to undermine that stability.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response in coordination with a partner regardless of the domain of the malicious activity. These efforts could include joint statements of attribution, coordinated diplomatic activity, and joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada, its partners and allies will present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

A collective understanding of cyber threats requires ongoing and continuous information sharing of potential compromises and cyber incidents. Canada regularly engages with allies and partners to discuss developments in cyberspace that could impact our states and determine how best to support each other. This includes relationships between departments and agencies in the federal cyber community and their international counterparts, cooperating and sharing information, intelligence, threat indicators, and policies, amongst others.

Strengthen relationships, including with non-traditional partners

Strong relationships are critical for advancing Canada's interests abroad. These include both formal and informal relationships and across many forums and many departments. GAC will seek to assist in the development of new relationships and foster existing ones.

Canada will build on its current relationships, developed through collaboration in numerous forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF) and the Global Forum on Cyber Expertise. This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs, as detailed in Pillars 3 and 4.

By leveraging its international affairs expertise and understanding of Canada's foreign policy goals, GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach. Canada will seek to provide capacity building funding to support increased participation from all states in international discussion and negotiations related to cybersecurity and international cyber law.

Through these partnerships, Canada can better understand the nature and scope of hostile cyber threats it is facing. For example, the Canadian Security Intelligence Service maintains valuable information-sharing relationships with more than 300 organizations in over 150 countries, including Five Eyes as well as non-traditional partners.

GAC will also work to increase multi-stakeholder engagement by creating a cyber stakeholder engagement action plan. Its objectives include to develop Canadian expertise by tapping into resources at home and foster relationships with civil society. Existing consultation processes will be used, as well as new or innovative processes as opportunities arise.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Governmental Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

For example, in the context of UN discussion around state behaviour in cyberspace, NGOs have played an important role in protecting human rights. As well, private sector entities have worked with states and with each other to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy in cyberspace, in particular as it evolves to meet the needs of a changing context. Canada is stronger when it acts together with partners to promote stability in cyberspace and respond to those that seek to undermine it. When the group of states acting together grows, so does the strength of their action.

s.15(1) - International

Summary of Actions:

- Canada will continue to call out malicious activity by state and state-backed actors and will continue to support our allies and partners on coordinated attributions.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies and will ask its partners for their support when needed.
- [redacted]
- Canada will continue dialogue at multilateral organizations, to support cyber capacity building, and work with states to implement norms of responsible state behaviour through the adoption of practical measures such as CMBs
- Canada will provide capacity building funding to support increased participation of all states in international discussions and negotiations related to cybersecurity and international cyber law
- GAC will provide assistance and advice to other government departments and agencies on engagement priorities and coordinating international outreach
- GAC will also work to increase multi-stakeholder engagement by creating a Cyber Stakeholder Engagement Action Plan
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors
- Canada will continue to build partnerships and relationships with allies and likeminded states

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability in cyberspace and support the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability in cyberspace

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence. The continued resilience of the RBIO is important for the ongoing prosperity of all states.

The RBIO is facing pressure from states that are using the institutions of the RBIO to further their authoritarian views. Canada's support to the RBIO, as well as that of allies and partners, is important to continue to sustain the institutions that have allowed Canada to prosper. In cyberspace, this support is demonstrated by Canada's ongoing commitment to international law and norms for responsible state behaviour.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

Canada believes that existing international law and agreed norms are sufficient to guide state behaviour in cyberspace. Canada acknowledges there remains work to be done concerning how international law applies and to ensure states have a comprehensive understanding of their responsibilities stemming from these norms. However, Canada believes international law and the existing norms are clear in governing state activity in cyberspace, including respect for human rights.

International Law

Canada has affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorsed by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The reports also provided initial guidance on how international law applies in cyberspace. While all states have agreed that international law applies in cyberspace, there are still differences in opinion regarding exactly how international law applies in cyberspace.

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of

international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory, or to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict, or LOAC), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

Voluntary norms for responsible state behaviour reinforce the RBIO and are important for ensuring security and stability in cyberspace. In particular, Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the

The reports of the UN Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) set out the basis of the framework for responsible state behaviour cyberspace. The consensus reports of 2010, 2013, and 2015 provide guidance for states.

foundation for sustaining international peace and security in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada views these norms and our obligations under to international law as the standard for its own behaviour and to assess the behaviour of other states.

The UN's eleven norms of state behaviour (see Annex X) are particularly important. These norms were endorsed unanimously by the UN General Assembly, and by several regional organizations and in several other forums, including the G7, G20, North American Leaders' Summit, NATO, ASEAN Regional Forum, and the OSCE.

Canada does not support the creation of new norms for state behaviour in cyberspace at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms.

Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms. (Most recently, see Canada's submission to the UN in Annex X?).

For instance, Canada believes that human rights apply online as they do offline. States should comply with their national and international human rights obligations when considering, developing or applying national cyber security policies or legislation. These same considerations are important when designing and putting into place cyber security related initiatives or structures including measures to address security concerns on the Internet.

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Some groups such as the G20 have developed their own additional voluntary norms, such as the norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

In seeking stability in cyberspace, Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace. Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and, trust and cooperation are critical to this. Confidence building measures are one of the most important practical tools available to states. Canada supports and leads on confidence-building measures (CBMs) in a number of forums because of their practicality and their focus on cooperation.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and escalation. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet," and Canada contributes to the ARF's CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices. Canada will also pursue partnerships with other states to increase cooperation in this area.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use the agreed norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the norms
- Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices
- Canada will continue to strengthen existing relationships and establish new ones

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. In addition, malicious actors often practice their abilities against one state before moving on to the next.

State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

For example, Canada contributed to the NATO Cooperative Cyber Defence Centre of Excellence, a multinational and interdisciplinary hub for research, training, and exercises with a focus on technology, strategy, operations, and law. In addition, Canada is supporting the attendance of civil servants from around the world at a courses on the applicability of international law in cyberspace.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. **Canada has committed to ~~contributed~~ over $11~~13.5~~ million to cyber security capacity building since 2015 and will continue to do so.** Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up or improved throughout the Americas. [Reference to support to Georgia election? ICC and IOP consult].

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Commented [NN-1]: We have shifted to speaking to what we are committed to rather than just disbursed. The previous 13.5 was for total disbursed on both cybersecurity and cybercrime.

Currently we are committed to $11M for just cybersecurity alone (includes all disbursed and planned

If you want to just reference cyber capacity building more generally we have currently committed $26.1M since 2015

Commented [NN-2]: If this in reference to the Chatham House project in Georgia I think that was run through IOC.

Commented [NN-3]: We also engage RCMP, CBSA, Justice,

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing. Human rights and gender are important lenses to understand the international context of cyber security and Canada will continue to ensure human rights values inform its approach to international cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada is a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem, including neuro and racially diverse communities, among others.

Summary of Actions:

- GAC will continue to engage in outreach and cooperative activities, as well as workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs
- Canada will continue to provide financial assistance in growing international cyber expertise
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums

Conclusion

The realities of the 21st century necessitate a clear-eyed view of Canada's foreign policy in cyberspace and how best to protect the national interest. This includes acknowledging the threats facing Canada and acting accordingly, cooperation with our allies and partners, supporting and advocating for the RBIO, and assisting other states with capacity building and increased inclusion.

Canada is committed to security and stability in cyberspace and to ensuring all states act lawfully and responsibly. Being transparent about the existence of national capabilities and views on responsible state behaviour in cyberspace contribute to predictability and stability in cyberspace. GAC will work closely with federal partners to clarify and publicise Canada's views on international law and the implementation of norms for responsible state behaviour.

Canada will also work with our allies and partners to implement norms for responsible state behaviour in cyberspace and look at areas of cooperation to increase our collective security. Canada will continue to support efforts for the development and implementation of CBMs, as they are an important tool for the ongoing predictability of state behaviour in cyberspace.

Engagement and support to capacity building raises the bar for discussion and action on cybersecurity issues in the international community. Canada will engage on these issues and assist when it can.

As Canada looks to increase the security of the nation and address malicious behaviour in cyberspace, it will remain engaged in an evolving international environment. Dialogue, cooperation, advocacy, diplomacy, and when necessary, action, each have a role to play in Canada's security and prosperity.

Protecting Canada in the 21st Century – Canada's Foreign Policy for State Behaviour in Cyberspace

Canadians have welcomed the opportunities provided by the Internet and an increasing amount of personal, community, and commercial activities take place online. However, this increase also provides more opportunities for malicious actors to take advantage of this activity.

The threat of malicious cyber activity is ongoing and persistent. It originates from many sources and state and state-backed actors represent some of the most advanced threat actors in cyberspace.

Canada's 2018 National Cyber Security Strategy (NCSS) outlined what actions the Government of Canada would take domestically to address cyber security threats. Led by Public Safety Canada, it outlined the activities of federal departments and agencies to increase the cyber security and resilience of Canada.

The NCSS also recognizes Canada's domestic cyber security does not exist independently from the international context. Cyber threats and malicious cyber activity are not constrained by borders and Canada must ensure its cyber security foreign policy accounts for this reality.

This strategy outlines the pillars by which Global Affairs Canada will do its part to protect Canada, Canada's interests, and increase Canada's security. These pillars are to Act, Cooperate, Advocate, and Assist.

Canada will act by using the full range of its national capabilities; it will cooperate with allies and partners to protect Canadian interests; it will advocate for the Rules-Based International Order and continue to engage in multilateral forums; and it will look to increase assistance for cyber security issues by supporting capacity building internationally.

All of these activities play a role in protecting and increasing Canada's security. Global Affairs Canada's international engagement demonstrates its commitment to security through cooperation, diplomacy, and advocacy. These are also essential tools to ensure Canada's future prosperity in the 21st century.

Vision

A stable and prosperous future for Canada by working at home and partners to increase cyber security and resilience to cyber incidents.

Scope

This strategy builds on existing initiatives and activities by the Government of Canada to address malicious cyber activity and increase cyber security, specifically those of the 2018 National Cyber Security Strategy (NCSS) and its associated Action Plan.

As the most sophisticated threats in cyberspace come from state and state-backed actors, this strategy will focus on state activity related to international cyber security, including how the Government of Canada will work to shape the international cyber security environment in Canada's favour.

Challenges such as the misuse of digital platforms, disinformation and misinformation, and cybercrime are closely linked challenges. Efforts are already underway to address these threats. This includes the work by the Communications Security Establishment (CSE) to protect Canada's elections, the Canadian-led G7 Rapid Response Mechanism, and the Royal Canadian Mounted Police (RCMP)'s National Cybercrime Coordination Unit. There are also existing multilateral efforts to address some of these challenges, such as the Council of Europe's Convention on Cybercrime (Budapest Convention), that Canada joined in 2015 and continues to participate in negotiations to advance a new Protocol to strengthen it.

Canada's National Cyber Security Strategy defines cyber security as "The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."

This Strategy complements these efforts, helping to ensure there are no gaps in the federal government's efforts to address the challenges facing Canada. Taken together, these efforts represent a Whole-of-Government approach to increasing Canada's security. Working together, the federal cyber security community will achieve the goals set out by the Government of Canada.

Context

To protect Canada's economic prosperity, national security, and democratic values, Canada must be realistic about the threats it faces. The international environment can be a hostile place and malicious cyber actors pose significant threats to Canada and Canadians.

The nature of the threats and the challenges they pose are rapidly evolving. In this context, Canada stands with our allies and partners, keeping a determined eye on potential adversaries, continuing dialogue with all states, and keeping Canadian policies firmly rooted in support for democratic and multilateral institutions.

According to Canada's 2020 National Cyber Threat Assessment, state-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations. In particular, China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.

Canada is not unique in the challenges it faces. All states face similar difficulties in cyberspace and the international context is evolving in response to this reality. Multilateral and regional organizations play an important role in facilitating dialogue, debate, education, and cooperation related to cybersecurity.

These multilateral and regional organizations also play a key role in the Rules-Based International Order (RBIO). The principles of the RBIO, including the rule of law and respect for human rights, have allowed Canada and many countries to prosper.

Ongoing hostile activity by state actors is key challenge for Canada. The range of behaviour by states has expanded with increased technological developments, including malicious cyber activity, as states seek advantage and dominance over potential adversaries. This activity includes hacking into protected systems to steal commercial information and intellectual property, cyber intrusions into critical infrastructure, and indiscriminate and irresponsible use of malware.

Such activities can undermine Canada's core values of democracy and human rights, threaten our social cohesion, and, at times, threaten our national security. The Government of Canada has taken action to protect Canada in response to the growing malicious cyber activity.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

Pillar 1 Act: [redacted] Defend Canada and Canadian Interests

- [redacted]
- Define and publicise Canada's international priorities and positions on state activity in cyberspace

[redacted]

States have a responsibility to protect their citizens; developing and using instruments of state power in accordance with international and domestic legal obligations to address evolving security threats is the activity of a responsible state.

Develop and use national deterrence and response policies and capabilities

Canada will further develop and use its capabilities and tools to protect itself and its interests. [redacted] but it should be recognized that stopping malicious activity altogether is not a realistic possibility.

[redacted]

[redacted]

Guided by Canada's foreign policy, [redacted] This includes using authorities such as those in the *CSE Act*, as well as the resources of agencies such as the CSE, the Canadian Centre for Cyber Security, the Canadian Security Intelligence Service, the RCMP, as well as National Defence.

Not all cyber incidents necessitate a cyber response. [redacted] Canada will use the most appropriate response for the situation, regardless of how the incident occurs. At all times, Canada's response will be in accordance with our domestic and international legal obligations.

Canada has called out malicious cyber activities in the past and attributed these activities to specific states. Canada will continue to do so and will continue to raise awareness of the threats facing Canada and its allies.

[redacted]

s.15(1) - Defence

s.15(1) - International

s.15(1) - Security

s.21(1)(b)

[redacted]

[redacted] Canada works closely with its allies to learn from their experiences [redacted]

Signalling, transparency, raising awareness, and modeling appropriate state behaviour are essential to reduce the risk of escalation when action is taken. [redacted]

Define and publicise Canada's international priorities and positions

Canada's priorities for foreign policy in international cyber security are the security of Canada and protecting Canadian interests. Foreign policy guidance to federal partners will take this into account.

The use of instruments of state power and national capabilities to protect Canada and Canadian interests will be guided by Government priorities, GAC's international security foreign policy priorities, Canada's commitment to agreed-to international norms for state behaviour, and Canada's international and national legal obligations.

Canada will communicate clearly and transparently its positions on activities in cyberspace, including when Canada believes a state is violating international law or failing to respect the norms for responsible state behaviour in cyberspace.

Calling out states for irresponsible behaviour and for failing to meet their commitments is an important step in signalling what Canada considers malicious cyber activity by states and their proxies. Communicating what Canada believes is wrong before it takes action prevents misunderstandings and sets expectations. This Strategy is itself a transparency and predictability measure.

This Strategy represents the first of ongoing efforts to define and publicise Canada's views on international cyber security, including Canada's international priorities and positions. Canada's foreign policy for cyber security will continue to evolve in response to a fast-paced environment rapidly changing with emerging technology. Canada will continue to detail its foreign policy through statements, speeches, and publications.

s.15(1) - Defence

s.15(1) - International

s.21(1)(b)

Summary of Actions:

- [redacted]
- Canada will employ the full range of our collective resources to protect Canada and mitigate cyber threats
- Canada will continue to develop new, and enhance existing, tools to better deter malicious actors
- Canada will continue to call out malicious behaviour and will continue to raise awareness of the threats facing Canada and its allies
- [redacted]
- Canada will continue to detail its foreign policy through statements, speeches, and publications
- Canada will continue to respect its domestic and international legal obligations and uphold responsible state behaviour in cyberspace

s.15(1) - International

Pillar 2 Cooperate: Work with Allies and Partners to Deter and Respond to Threats to Canadian Interests

- Coordinate national deterrence and response capabilities with allies and partners
- Strengthen relationships, including with diverse stakeholders

Coordinate collaborative deterrence and response mechanisms

Canada does not have to act alone in responding to malicious cyber actors and promoting responsible state behaviour. Canada is always stronger when it acts together with partners and allies to encourage stability in cyberspace.

In the past, Canada and its partners have called out malicious cyber activity. This includes malicious activity by Russia in the case of the indiscriminate use of the Not-Petya malware (indiscriminate and irresponsible use of malware that cost billions of dollars in economic damage around the wold); malicious activity by North Korea in the case of the use of WannaCry ransomware (criminal ransomware activity); and the compromise of Managed Service Providers (MSPs) by China (economic espionage and theft of intellectual property and private sector data).

Canada will continue to call out malicious activity by state and state-backed actors and will continue to consider requests for attribution support from allies and partners. Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies at their request and will ask its partners for their support when needed.

As in its own response, Canada will choose the most appropriate response in coordination with a partner regardless of the domain of the malicious activity. These efforts could include joint statements of attribution, coordinated diplomatic activity, and joint cyber operations.

[redacted]

By working with allies and partners to publicly attribute unacceptable behaviour in cyberspace, and support each other's efforts to deter malicious cyber activity, Canada, its partners and allies will present a united front against this malicious activity and reinforce the agreed-to norms of state behaviour in cyberspace.

Strengthen relationships, including with diverse stakeholders

Strong relationships are critical for advancing Canada's interests internationally. Canada will build on its current relationships, developed through collaboration in numerous forums, such as the Organization for American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF). This will include dialogue, continued efforts in cyber capacity building, and working with states to implement norms of responsible state behaviour.

With much of cyberspace infrastructure and software being owned and run by private sector entities and the Internet having been developed largely an academic setting, it is clear that a multi-stakeholder approach is essential to protect Canadian interests. Academia, Non-Governmental Organizations (NGOs), civil society, and industry representatives all have important contributions to make.

GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors. The knowledge and experience gained in working with stakeholders to inform will help inform Canada's foreign policy for cyber security, in particular as it evolves to meet the needs of a changing context.

Summary of Actions:

- Canada will continue to call out malicious activity by state and state-backed actors and will continue to support our allies and partners on coordinated attributions.
- Canada will also consider the use of its national capabilities for deterrence and response in partnerships with allies and will ask its partners for their support when needed.
- [redacted]
- GAC and the federal cyber community will continue to grow and deepen their relationships with the private sector and civil society actors

Pillar 3 Advocate: Multilateral Engagement to Increase Canada's Security

- Promote responsible State behaviour and accountability and support the Rules-Based International Order (RBIO)
- Reduce risk of conflict with bilateral & multilateral confidence-building measures

Promote responsible state behaviour and accountability

The stability, predictability, and transparency of the RBIO has allowed Canada and many other states to prosper. Based on commitments made by states, the RBIO provides a positive framework for the peaceful development of all states regardless of their size and influence.

Canada believes existing international law and the existing agreed norms are clear in governing state activity in cyberspace, including respect for human rights. Canada acknowledges there remains work to be done concerning how international law applies and to ensure states have a comprehensive understanding of their responsibilities.

The Rules-Based International Order refers to the principles and institutions to govern state behaviour developed over several centuries and codified primarily in the 20th century. Examples include the law of the sea, the United Nations and its associated institutions, as well as treaties such as the Vienna Convention on Diplomatic Relations.

International Law

Canada has affirmed the application of international law to state behaviour in cyberspace. This position was unanimously endorsed by the UN General Assembly, as outlined by the 2013 and 2015 reports of the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now GGE on Advancing responsible State behaviour in cyberspace in the context of international security).

The public articulation of a state's position on how international law applies in cyberspace is an important way to contribute to international stability in cyberspace and in the shaping of international law. International law is shaped by state behaviour, by the actions states take or do not take, and by the public statements accompanying these actions.

Ambiguity is a particular challenge in cyberspace, this ambiguity risks escalation, destabilization and potential unnecessary confrontation. To reduce ambiguity and destabilization, states have a responsibility to ensure malicious cyber activity does not emanate from their territory and to do something about it when notified.

Canada reaffirms that the United Nations (UN) Charter applies in its entirety to state actions in cyberspace, including the prohibition on the use of force (Article 2(4)), the peaceful settlement of disputes (Article 33), and the inherent right of states to act in individual or collective self-defence in response to an armed attack (Article 51). The international law on state responsibility applies to cyber operations, including the option to use countermeasures in response to internationally wrongful acts.

It is definitive that cyber activities can rise to the level of an armed attack. Canada affirmed this when NATO acknowledged that malicious cyber activity of a serious enough nature could trigger Article 5 of the North Atlantic Treaty, collective self-defence in the event of an armed attack against one or more members.

Canada also recognizes that International Humanitarian Law (IHL) (also know as the Law of Armed Conflict), including the Geneva Conventions, applies when cyber operations are conducted during hostilities.

Canada has been transparent about its intent to develop and employ active cyber capabilities, which were outlined in our defence strategy Strong, Secure Engaged and in the *CSE Act*. Canada has stated that it will use these capabilities according to international law and existing agreed-to norms. In addition, as a member of NATO, Canada acknowledged that cyberspace is a domain of military operations, just as land, air, and sea.

Public statements on the applicability of international law communicate a state's intent and open lines of communication between states. Canada encourages other states to be open about the existence of their cyber capabilities and the conditions under which they would use them. Canada also encourage states to pledge that they will follow international law and agreed-to norms if they use their cyber capabilities.

Canada will continue to publicly state its views on the applicability of international law, through statements, speeches, and publications.

Norms

Canada sees the applicability of existing international law and norms for state behaviour in cyberspace as the foundation for sustaining international peace and security in cyberspace. This is why Canada strongly supported the adoption of norms and continues to promote their endorsement, observation, and implementation in various forums.

Canada views these norms and our obligations under to international law as the standard for its own behaviour and to assess the behaviour of other states. The UN's eleven norms of state behaviour (see Annex X) are particularly important.

Canada does not support the creation of new norms for state behaviour in cyberspace at this time and believes states should continue to work in existing forums, such as the United Nations, and together to implement these norms.

Due to the importance Canada places on these norms, and to further support the implementation of the norms, Canada was the first state to share with the UN its best practices and lessons learned from its own norms implementation. In sharing this information, Canada hopes to provide guidance and encourage other states to observe and implement the norms. (Most recently, see Canada's submission to the UN in Annex X?).

Many of the norms correspond closely with Canadian values, including that states should respect the promotion, protection and enjoyment of human rights on the Internet, including the right to freedom of expression, as well as the right to privacy in the digital age.

Some groups such as the G20 have developed their own additional voluntary norms, such as the norm proscribing cyber enabled intellectual property theft for commercial purposes. Canada has also endorsed the G20 norms and is actively working to promote their implementation.

Reduce risk of conflict with bilateral & multilateral confidence-building

Reducing the risk of conflict must be the goal of all states and trust and cooperation are critical to this. Confidence building measures (CBMs) are one of the most important practical tools available to states. Canada supports and leads on CBMs in a number of forums because of their practicality and their focus on cooperation.

CBMs can be defined as commitments or actions taken by states to reduce uncertainty between states. They can be formal or informal, bilateral or multilateral, political or military. At their heart, they build mutual trust by creating predictability in behaviour or actions and increase information sharing.

Canada believes that cyber CBMs promote stability and security in cyberspace and can reduce the seriousness of state to state cyber incidents by preventing miscalculations and escalation. Canada has been working closely with regional organizations such as the ARF, the OAS, and the OSCE to develop, implement, and disseminate cyber CBMs.

For example, Canada currently leads the effort to implement OSCE cyber CBM 4 “Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet,” and Canada contributes to the ARF’s CBM efforts by organising workshops and implementing the CBMs.

Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices.

Summary of Actions:

- Canada will continue to publicly articulate its position on how international law applies in cyberspace
- Canada will use the agreed norms as well as adherence to international law as the standard for its own behaviour and to assess the behaviour of other states
- Canada will continue to support the implementation of the norms
- Canada will continue to advocate for norms and encourage more states to adopt, observe, and implement the existing norms for state behaviour in cyberspace
- Canada will continue to highlight and advocate for the importance of these norms in bilateral relationships and in regional and multilateral forums as it has done at the UN, OAS OSCE, and ARF
- Canada will continue to pursue opportunities with regional partners to implement CBMs, whether through hosting workshops, leading working groups, or sharing best practices

Pillar 4 Assist: Support Capacity Building and Inclusion to Increase Security in Cyberspace

- Increased capacity of state partners to engage in international forums on cybersecurity issues
- Promote gender equality in international cybersecurity

Increased capacity of state partners to engage in international forums on cybersecurity issues

All states are safer when each state is made safer. The size, scope, and borderless nature of the Internet means that threats posed by malicious cyber activity places all states at risk. In addition, malicious actors often practice their abilities against one state before moving on to the next.

State capabilities and capacities to respond to these threats vary. Helping each other to understand the issues at play, the potential avenues for threat reduction, and working together to mitigate the impact of malicious acts increases the security of all states.

To help grow state expertise in cybersecurity, GAC engages in outreach and cooperative activities and hosts workshops and seminars, including on how and why Canada is implementing the norms for responsible state behaviour and CBMs. Canada also provides and will continue to provide financial assistance in growing international cyber expertise.

Canada will also remain responsive to the requests of partner countries and multilateral institutions regarding their needs and plans for capacity development and how Canada can best support them.

Capacity-building efforts are vital as they increase the resilience of states to malicious cyber activity. Canada has committed over $11 million to cyber security capacity building since 2015 and will continue to do so. Among other outcomes, these projects have helped a number of countries in the Americas develop their national cyber security strategies. Thanks in part to Canada's support, seventeen Computer Security Incident Response Teams were stood up or improved throughout the Americas.

GAC also works with federal partners to seek their support in cyber capacity building, including Public Safety and the Canadian Centre for Cyber Security, such as the development of national cyber security strategies.

Promote gender equality in international cybersecurity

Canada is committed to the promotion of gender equality and the participation of women in the international cyber security ecosystem.

Security, whether physical or virtual, is tied to human rights. The two concepts are mutually re-enforcing and gender is an important lens to understand the international context of cyber security.

To increase it's understanding of gender and cyber security in this context, Canada commissioned two reports on gender and cyber, "Why gender matters in international cyber security," by Deborah Brown and Allison Pytlak, and "Making Gender Visible in Digital ICTs and International Security," by Sarah Shoker. These reports are the first of their kind to address the gender and cyber security nexus and are important resources for states, including Canada, looking to improve their understanding of this issue and inform their policies.

From the perspective of the norms for state behaviour, Canada supports increasing women's participation in decision making and positions of influence. For example, at the UN OEWG Canada is a donor country for the Women in International Security and Cyberspace Fellowship, a program that promotes greater participation by women in discussions at the UN OEWG. It is a joint initiative of the governments of Australia, Canada, the Netherlands, New Zealand, and the United Kingdom. The fellowship program supported the participation of over 30 women from states in Africa, Asia, the Pacific, Latin America, and the Caribbean.

Increasing women's participation is a positive development and a good start. A Gender Based Analysis (GBA) + was done for this Strategy and will continue to be used in the implementation of its activities (see Annex X). The next step is to ensure the greater participation of all communities who may not have full participation in the international cyber security ecosystem.

Summary of Actions:

- Canada will continue to support cyber capacity building that works to improve the cybersecurity of other nations and encourage increased standards of coordination between States to more effectively respond to cyber threats.
- Canada will use capacity building support to provide tailored trainings on the importance of international cyber law, CBMs and responsible state behaviour in cyberspace.
- Canada will continue to support increased women's participation in decision making and positions of influence in international cyberspace forums