The Government of Canada

Positions for the North Atlantic Treaty Organization

I. Addressing the Concerns of Member States in Regard to Cyber Terrorism

Article 5 of the North Atlantic Treaty establishes the collective security of all member states, claiming an attack on one ally represents an attack on all. In 2007, The Republic of Estonia experienced a massive denial of service attack (DoS).[1] The attack shut down bank, government, and broadcast services, demonstrating the sensitivity of cyber-reliant technology, and the dire need for advanced security measures. Services that citizens depend upon, such as telecommunication, banking, and public transportation rely on cyber networks to function, and because of their importance, are a prime target for cyber terrorism. Until critical infrastructure is secured, all states will be vulnerable to attacks similar to the one that temporarily incapacitated Estonia. As President of ECOSOC, H.E. Mr. Lazarous Kapambwe, claimed, "We have agreed that cybersecurity is a global issue that can only be solved through global partnership. It affects all of our organization, and the United Nations is positioned to bring its strategic and analytic capabilities to address these issues."[2] The anonymous nature of cyberspace also presents a challenge to Member States in instituting punitive measures to reduce cyber terrorism. The spread of cyber terrorism has lead the North Atlantic Treaty Organization (NATO) to pursue collective cyber defense frameworks that are will be necessary to withstand the numerous threats it faces.

In 2011, Canada sought to enhance cross-border communication by signing a Cyber Security Action Plan with the U.S. under the Beyond the Border Action Plan. Canada is committed to the development of Member State's capabilities and to information-sharing on cyber defense within NATO. Canada has also contributed to the Cooperative Cyber Defense Center of Excellence (CCDOE) in Tallinn, Estonia to bolster regional security. Canada is a founding collaborator of the Global Forum on Cyber Expertise (GFCE), an initiative focusing on cyber security, which was introduced by the Netherlands at the 2015 Global Conference on Cyberspace. By partnering with international cyber security initiatives with the United Nations Office on Drugs and Crime, as well as the Group of Seven, Canada has worked to combat human rights violations over the web. In the latest United Nations Group of Governmental Experts (UN-GGE) report, Canada affirmed the decision of States to uphold the applicability of international law to cyberspace. Canada upholds employing existing international law pertinent to cyberspace such as the UN Charter, International Human Rights Law, and International Humanitarian Law. In 2001, Canada signed the Europe Convention on Cybercrime which acts as a framework for cooperation between states. Canada has developed a Cyber Incident Management Framework (CIMF) that defines roles and duties of all levels of government, and private sector partners so that each organization is able to respond cooperatively in the event of the of a national cyber incident. The CIMF sets clear expectations for all stakeholders in cyber security, such as the federal government, critical infrastructure owners and operators and other public and private sector partners.

Systems which control critical infrastructure, such as electrical grids, dams, and transportation networks, should be a priority for international cyber security to protect by way of framework and punitive measures. Partnering the private sectors of member states with NATO initiatives like the CCDOE will be a crucial objective to building a resilient security network. Canada asserts that in order for collaboration to be possible, trusted protocols for cooperative cyber defense must be adopted, similar to the CIMF currently being utilized by Canada. The CIMF provides blueprint for cyber threat response, by designating responsibilities to each sphere of government, but its use is not contingent on a State's level of development. Much like the open ocean, the Internet is vast and mostly unexplored. Canada supports Member States to implement punitive measures to combat cyber threats by applying the legal frameworks of United Nations Convention on the Law of the Sea (UNCLOS) to Cyber Space. Article 100 of UNCLOS describes the duty of all States to cooperate to repress piracy, or in this case cyber terrorism, and article 105 sets clear protocols for the seizure of rogue vessels. Just as the high seas require cooperative efforts by States to subdue piracy, Cyber Space will require collaboration to combat cyber terrorism. The advent of cyber technology has increased the number of potential threats to Member States and their constituents, but it has, at the same time, strengthened the means by which global cooperation can be achieved.

---

[1] "The History of Cyberattacks – a timeline", *NATO Review,* http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

[2] "Cybersecurity: A global issue demanding a global approach", *United Nations Department of Economic and Social Affairs,* http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

II. Security: 'The Women, Peace, and Security' Agenda

The UN Security Council deemed the violence and mistreatment of women unacceptable through its adoption of Resolution 1820 in 2008, but a persistent obstacle to sustained peace has been the exclusion of women from the process of peacekeeping. The lack of women in peacekeeping has hindered operations by depriving the state of unique gender perspectives that can be instrumental to finding solutions that would not occur to male peacekeepers. As Canadian Defense Minister Harjit Sajjan said at the UN Peacekeeping Defense Ministerial: London Communiqué, "In areas of conflict we need to have more women in leadership roles. We are actually handcuffing ourselves if we don't do this."[3] UN Security Council Resolution (SCR) 1325 affirms the necessity for diverse gender perspectives in peacekeeping, and implores Member States to incorporate women into the process of making, sustaining, and enforcing peace. To fulfill the principles of Resolutions 1820, and 1325, institutionalized frameworks must be implemented to ensure the increased participation of women in peacekeeping. Despite the apparent need for women's participation in the peace process, of all personnel involved in peace talks, only nine percent are women.[4]

Gender equality is an essential value to Canada, and is preserved within the *Charter of Rights and Freedoms*, an integral part of the Canadian Constitution. Canada recognizes the need for women to take a larger role in peace operations as Prime Minister Justin Trudeau demonstrated, "Moving forward, we will increase Canada's support to United Nations peace operations: providing more personnel and training to UN peace support missions; increasing our conflict prevention, mediation, and peace building efforts; advancing the roles of women and youth in the promotion of peace and security; and supporting UN reform efforts to make peace support initiatives more effective."[5] Canada's Action Plan utilizes thematic areas articulated by the Security Council in Resolutions on Women, Peace and Security as a framework to direct the government's decision making in the implementation of resolution 1325. Canada has also supported NATO's implementation of SCR 1325 that offers relevant training and education framework with the aim of integrating gender perspectives in military operations. In 2016 Canada was elected to be a part of the United Nations Commission on the Status of Women (UNCSW). By accepting this role, Canada has committed to implementing its diversification techniques and frameworks globally. To understand how policies affect women differently than men, Canada has employed the Gender Based Analysis plus (GBA+) which is used to assess the impact of programs taking into consideration gender and other identity characteristics. To ensure that the recommendations that are suggested as a result of GBA+ are put into action, Canada has appointed specialized gender advisors that are guided by the implementation goals outlined by SCR 1325.

According the the Security Council report in 2005, "Although various actors have made efforts to implement resolution 1325, gender perspectives are still not systematically incorporated in planning, implementation, monitoring and reporting in the area of peace and security."[6] Canada supports current initiatives, such as the NATO Women's Professional Network (NWPN), but asserts that there are areas that must be improved in order to see significant results in female inclusion in peace operations and decision making. Canada affirms that NATO can significantly improve the environment for women peacekeepers by using analytical tools that measure the impact of policies on diverse groups, such as GBA+, by providing gender perspectives current operations. Canada recommends NATO expand its implementation of SCR 1325, by forming a Gender Advisement Board

---

[3] "Ottowa pledges more women for upcoming peacekeeping mission"; Champion-Smith, Bruce; *Ottowa Bureau,* https://www.thestar.com/news/canada/2016/09/08/canada-to-host-peacekeeping-summit-next-year-defence-minister-says.html

[4] "Why Women?", *Inclusive Security,* https://www.inclusivesecurity.org/why-women/

[5] "Statement by the Prime Minister of Canada on National Peacekeepers' Day", *Justin Trudeau, Prime Minister of Canada,* http://www.pm.gc.ca/eng/news/2016/08/09/statement-prime-minister-canada-national-peacekeepers-day

[6] "Women, Peace and Security", *Security Council Report,* http://www.securitycouncilreport.org/monthly-forecast/2005-11/lookup_c_glKWLeMTIsG_b_1141141.php

(GAB), to evaluate current operations. GAB would be selected from a diverse pool of states to oversee existing NATO initiatives for the purpose of recommending integration policies and delivering annual reports to Member States. The reports issued by GAB could be used to determine how foreign aid is to be distributed among Member States.