On March 12 2021, the UN Open-Ended Working Group on ICTs and International Security (OEWG) adopted a final report and Chair’s summary by consensus after two years of negotiations. The report was an important step forward. It strongly reaffirmed the framework for responsible state behaviour in cyberspace, anchored in the applicability of international law, agreed norms of responsible behaviour and confidence-building measures (CBMs). Overall, all UN member States supported its adoption. On May 28, the UN GGE also adopted a consensus report.

The consensus outcomes at UNGA76 augured well for the UN cybersecurity process underway in 2022: the 2021-2025 OEWG. In addition to this ongoing process, sixty States, including Canada, are cosponsoring the establishment of a UN PoA as a permanent, inclusive, consensus-based and action-oriented international instrument to advance implementation of the acquis on responsible behavior in the use of ICTs in the context of international security.

In this context, Canada endeavoured to research the functions and responsibilities of a cyber PoA. Specific research was conducted to ascertain what operational requirements would look like and how a cyber PoA would relate to the use of ICTs in the context of international security, taking place at the UN and elsewhere.

The research paper submitted aims to flesh out some of these ideas, provide data and or case studies about these issues. It also aims to answer the questions listed above, with a view to informing State’s positions at the UN OEWG, broader policy positions related to cybersecurity, as well as cyber capacity building efforts. Finally, it aims to answer the questions PoA co-sponsors - and potential co-sponsors – about what a PoA would look like in concrete terms and how it would operate.

Discussions about the establishment of regular institutional dialogue are ongoing in the current OEWG. This Research Paper does not pre-suppose the outcomes of those discussions, rather it is intended to share food-for-thought on potential elements UN Member States may decide could be incorporated into any new mechanism. For the purposes of simplicity, this paper refers to the new mechanism as a “cyber POA”. As with all the food-for-thought elements, this is not intended to presuppose eventual consensus agreement on that name.

From May 19-20, 2022 Canada, the Kingdom of the Netherlands, and in collaboration with the CyberPeace Institute, collectively hosted a hybrid workshop on Advancing the Cyber Programme of Action (PoA) in Geneva, Switzerland.

The objective of the workshop, which was held under Chatham House rule, was two fold: first, to present on the design, structure, formation and overview of case studies of past programmes of action. Second, to bring together relevant stakeholders (States, the non-governmental multi-stakeholder community, civil society, industry etc.) and engage in interactive discussions to consider the substantial priorities that need to be considered and reflected into the formation of a Cyber PoA.

The research paper that Canada commissioned the Women’s International League for Peace and Freedom (WILPF) to undertake, was presented in order to provide policy options and operational recommendations with a focus on the formation, architecture and technical guidance of a possible cyber PoA as it relates to cybersecurity.

For further reading, outcomes and recommendations from the workshop are available on the Let’sTalkCyber website here: https://letstalkcyber.org/resources/workshop-on-advancing-the-programme-of-action-full-summary