HUMAN RIGHTS COUNCIL ADVISORY COMMITTEE

QUESTIONNAIRE ON HUMAN RIGHTS IMPLICATIONS OF NEW AND EMERGING TECHNOLOGIES IN THE MILITARY DOMAIN

November 29, 2023

Submission by Project Ploughshares

Questions for All Stakeholders

1. *What criteria and guidelines exist to guarantee the establishment of meaningful human control over the use of force and during the conduct of hostilities, and to ensure compliance with international human rights law and international humanitarian law within the military domain?*

International discussions, including at the United Nations Convention on Certain Conventional Weapons (CCW), have over the past nine years sought to outline guidelines for meaningful human control over the use of force and during the conduct of hostilities. To date there is no universally agreed upon criteria which makes this question all the more critical. While almost all states agree that existing international humanitarian law (IHL) applies, there is disagreement on whether existing IHL is sufficient. At the same time, advances in artificial intelligence (AI) have further crystallized the capabilities that new technologies provide such as object recognition, facial recognition and data analysis that are further diminishing human control over weapon systems as well as decision-making in the military domain.

As such, it has become clear that new law regarding use of AI and autonomy in the military domain is necessary to bolster IHL and indeed, international human rights law (IHRL). Regarding IHRL, some states have been resistant to add it to the discussions at CCW. While recognizing that systems need to be developed in an ethical manner, insufficient attention has been paid to potential human rights implications. **A focus on**

IHRL will therefore need to be advocated for in the forums examining autonomous weapon systems as well as responsible use of military AI.

Nonetheless, over the years, several principles have been noted and some even agreed upon at the CCW that will be relevant beyond this forum and discussions. Fundamental IHL principles such as distinction, proportionality and military necessity have been reaffirmed as key legal principles despite advancement of technology. The majority of states agree that there should be human oversight over weapon systems and that autonomous systems should not simply make decisions without human input. However, there is disagreement on the use of the word 'control,' and some states have instead suggested appropriate levels of human involvement, for example. A stronger focus on defining meaningful human control will be critical to ensure both IHL and IHRL are respected.

States participating in the CCW discussion, along with those engaged in discussions on the responsible military uses of AI held in February 2023 in The Hague, Netherlands, have commonly employed key concepts such as **transparency**, **accountability**, and **predictability**.

This means that states see the benefit of systems that are transparent, meaning that operators understand their functioning, and that errors can be communicated. According to these discussions, transparency would also be a confidence building measure as states would undertake Article 36 reviews and share best practices. Accountability is seen as central in the deployment of weapon systems. States agree that a human operator needs to be held accountable for the actions of a system. Yet there is little clarity on who would be held accountable for a system that can "learn" or change course resulting in actions that a human could not have anticipated. In response, states have called for design and deployment of predictable systems. Majority of states note that unpredictable systems would not be in compliance with IHL and international human rights law. Still, systems can be designed to "nudge" an operator's behaviour, while in other cases human control of some systems may be superficial.

2. *What are the potential risks associated with using NTMD that could be exploited for malicious purposes, such as cyberattacks, espionage, spoofing, jamming, sabotage, or*

bioweapons? How can these risks be mitigated to prevent potential human rights violations and abuses?

New and emerging technologies in the military domain carry both direct and indirect risks. Direct risks such as cyberattacks, espionage, spoofing, jamming and sabotage are some possible malicious uses of the technology. Military systems are increasingly reliant on digital infrastructure, making them susceptible to cyberattacks that can compromise data integrity, disrupt operations, or even take control of critical systems. Advances in biotechnology could lead to the development of new bioweapons with the potential to cause widespread harm to both military personnel and civilian populations.

However, unintended impacts pose a unique challenge for anticipating the full consequences of emerging technologies. These are particularly relevant when examining possible effects on critical infrastructure and possible spillover on civilian populations including those far away from the intended attacks. As such, these deserve sustained dialogue and attention from the global expert community, states, industry, militaries, academics and civil society.

In terms of cyber applications, academic literature and expert opinion already notes the ways in which some larger scale cyber attacks have had unintended consequences. Consider, for example, the 2017 NotPetya attacks initially targeting Ukrainian government and financial entities, but that lead to infection of computers around the world resulting in substantial financial losses globally.

Similarly, AI-enabled systems and use of generative AI introduces new vulnerabilities as more states adopt these technologies in their critical infrastructure as well as security and defence institutions. Poisoning attacks can include deceiving AI systems to make mistakes, accessing training data, and manipulating variables. Additionally, attackers may add false data in the training process, among other methods. While intentionally poisoning data or manipulating machine learning algorithms may be done with specific objectives, the potential impacts of such changes on global security could be significant. This is especially true if the targeted systems are not identified and are subsequently deployed by various states.

Additionally, given the dual-use nature of AI technologies, civilian technology can be adapted for nefarious purposes. Generative AI used for civilian purposes in one demonstration came up with 40,000 new possible biochemical weapons.

In order to mitigate these risks, states require clear guidelines in responsible use of technologies, developing contingency plans for spillover effects and keeping channels open to ensure any significant manipulation can be clearly communicated, particularly between more adversarial states. Strengthening international agreements and treaties that prohibit the development and use of biological weapons will also be key, including the implementation of strict controls on access to and handling of dangerous biological materials. International cooperation and verification mechanisms can also help monitor and enforce compliance with these agreements. A crucial challenge currently is the lack of political will and cooperation and the international level to develop regulatory frameworks and strengthen existing ones to counter both direct and indirect impacts.

3. *How can both States and private entities effectively establish mechanisms of accountability and responsibility to address violations and abuses of international human rights law and violations of international humanitarian law committed using NTMD, including AI and ADS, cross-border and long-distance use of force, neurotech and brain interface controls, as well as dual-use technologies employed for both military and civilian purposes? Additionally, how can monitoring the design, development, training, and use of NTMD play a role in ensuring accountability and addressing potential violations and abuses?*

Establishing mechanisms of accountability and responsibility for violations and abuses of IHRL and IHL related to new and emerging military technologies is crucial for maintaining ethical standards and preventing harm. Both states and private entities have a role to play in shaping a **multilevel governance framework** that includes both hard law as well as norms and standards. Ultimately, it is states that have the responsibility and the power to ensure international obligations and national policies are aligned and protect citizens and the global community.

Key recommendations to effectively establish mechanisms of accountability:

1. **Develop and strengthen regulatory frameworks**
    - Support the development of new treaties and robust national legal frameworks, including on autonomous weapon systems.
    - Ensure that these laws are in line with international norms and provide mechanisms for accountability.
    - Strengthen exisiting treaties to reflect changes and challenges presented by new and emerging technologies.
    - States should develop and disseminate ethical guidelines for the use of new military technologies, incorporating IHRL and IHL principles. As well as to provide training for military personnel to ensure awareness of and compliance with these guidelines.

2. **Address insufficient industry standards and codes of conduct**
    - Private entities should adhere to and support compliance with national and international legal frameworks.
    - Develop internal policies that align with these legal standards and establish accountability mechanisms within the organization.
    - Codes of conduct are welcome and should reflect legal norms.

3. **Require Human Rights Assessments**
    - States should integrate human rights impact assessments into the planning and deployment of new military technologies.
    - Evaluate the potential effects on civilian populations and take preventive measures to minimize harm.
    - States should require private entities to adopt human rights assessments in high-risk AI applications.

4. **Design Transparency**
    - States should ensure thorough documentation of the design, testing, and deployment of military technologies.
    - Ensure transparency in the decision-making processes related to the use of force, and disclose information when appropriate.
    - Industry should maintain transparent practices regarding the development and use of military technologies.

Questions for civil society, scientific community and academic institutions

1. *Please describe the relevant work that your organization has done on the issue of new and emerging technologies in the military domain (NTMD) and human rights. What have been your key accomplishments? What challenges have you faced?*

Project Ploughshares has paid sustained attention to the emerging military and security technologies file for the past eight years. Throughout the years we have consistently participated in international discussions at the CCW and recently contributed to the 2023 Summit on Responsible Military AI held in the Hague, Netherlands. We have contributed to numerous consultations with the Government of Canada, as well as participated in consultations with the United States Department of Defense. We have published several reports of interest on key principles on responsible military AI as well as opinion pieces in national and international publications. We have also engaged in numerous expert panels and public facing events on the issue of autonomous weapon systems and military applications of AI.

Key accomplishments include elevating the public debate on the issue in Canada and beyond. Project Ploughshares has raised awareness and highlighted key challenges posed by emerging technologies to diverse audiences and has been critical to bringing a spotlight on these topics. Alongside civil society colleagues, we have promoted the need for an international dialogue and a legally binding instrument on autonomous weapons.

A key challenge regarding advocacy on emerging military technologies is the lack of political will and the growing great power competition. Both pose a challenge to those calling for greater regulation and the establishment of effective mechanisms to control the development and use of these technologies. Much of the technology being developed is dual-use and as such it may be difficult to ascertain how particular technologies will be introduced into the battlespace.

2. *How can the technical community and academic institutions collaborate with civil society organizations to conduct research, provide expertise, and develop best practices to address the human rights implications of NTMD?*

Collaboration between the technical community, academic institutions, and civil society organizations is essential to comprehensively address the human rights implications of new military technologies. This collaboration can contribute to informed policymaking, ethical guidelines, and the development of best practices.

Here are several ways in which these entities can work together:

1. **Joint Research Partnerships and Collaboration on Guidelines**

Civil society organizations, such as Project Ploughshares, have focused on issues of emerging technologies for several years. Civil society organizations bring unique insights as observers and advocates that can lead to research avenues to investigate the ethical and human rights concerns regarding the development and deployment of autonomous systems. Along with research projects, the different stakeholders can collaborate on the development of ethical guidelines and best practices for the design, development, and use of military technologies. This would ensure that these guidelines reflect both technical considerations and key human rights principles.

2. **Civil society representation on advisory panels, expert forums**

Advisory panels have tended to include representatives from academia and industry and at times there has not been sufficient representation of more critical civil society voices. In order to understand and benefit from diverse perspectives, greater attention should be paid to ensuring advisory boards and expert forums include civil society. This will allow for the exchange of information and networking opportunities necessary for collaboration. Workshops, conferences and seminars should bring together academics and technical experts with civil society practitioners.

Moreover, civil society plays a unique role in this collaboration as it can more freely monitor developments and hold various actors accountable. Unfortunately, civic space has been shrinking globally, and in international discussions some states have pushed for the exclusion of civil society. Disallowing civil society to engage at meetings on emerging military and security technologies diminishes the debate and the ability of the "third sector" to fulfill their role of monitoring and bringing attention to communities that are often overlooked or underrepresented in these forums. As such, we urge states and

international institutions to enable and champion civil society participation on these issues.

3. *Are current international law, international humanitarian law, and human rights law, as well as government policies, effective in addressing the human rights challenges arising from NTMD? If not, what improvements can be made to ensure more effective protection of human rights in this context?*

Existing laws are important in addressing the human rights challenges arising from new and emerging military technologies. However, there is a need for new laws, including treaties and protocols, as well as clarification of the application of existing frameworks to new technologies. The dual approach of bolstering existing law while developing new laws and norms is necessary to address the full impact of these technologies on human rights.

Additional aspects that need to be considered include the need to strengthen mechanisms for monitoring, accountability and enforcement as many of the technologies are dual-use and may pose challenges to traditional ways of monitoring the spread of the technologies. For example, less than tangible technologies, including AI-enabled software, can be added to existing platforms and weapon systems with little outward visibility.

The development and dissemination of clear ethical guidelines and best practices can supplement legal frameworks. These guidelines can be developed collaboratively by governments, international organizations, the technical community, and civil society.

All of this will require political will and cooperation between states. Given the existing global security environment, more effort is needed to bring together more adversarial states to develop policies that ensure the benefits of new technologies while minimizing the associated risks.

4. *What strategies and initiatives can civil society, the technical community, and academic institutions undertake to ensure the inclusion and meaningful participation of marginalized or vulnerable groups in discussions and decision-making processes related to NTMD?*

Collaboration between different stakeholders can ensure that diverse voices are included in these discussions. Women are still underrepresented in multilateral forums on international security issues. This is compounded by the fact that women are also underrepresented in the technical community on emerging technologies, such as artificial intelligence. Women account for less than 25% of AI specialists and only 14% of the cloud computing workforce. States should devote greater effort to addressing this incredible gender gap.

Indeed, governments should support initiatives that provide technical skills training to individuals from marginalized communities, enabling them to actively contribute to discussions on emerging technologies. Academics can employ participatory research methodologies that involve community members in the research process, ensuring that their insights and concerns are considered. All stakeholders need to recognize the intersecting identities and experiences within marginalized groups. It must be ensured that discussions and decisions consider the unique challenges faced by individuals with multiple marginalized identities.