Working Group 7 Report: "Emerging New Technologies and Security Issues"

Conveners: Richard Guthrie, Gian Piero Siroli

Rapporteurs: Cameron Harrington, Katrin Heilmann

According to the Russell-Einstein Manifesto, even if nuclear weapons were to be abolished, this would only be one step on the path to a world without war. Consequently, a Working Group on emerging technologies was convened to discuss potential future steps on this path. The Group focused on potential threats associated with emerging technologies.

Pugwash sits at the interface where science and technology interact with society and policy. Scientific and technological developments bring many substantial benefits to humankind but also bring with them potential risks for hostile uses. As emerging technologies develop, the Pugwash Conferences are an appropriate forum for identifying such challenges posed to humanity.

Working Group 7discussed an array of emerging technologies and outlined their inherent contradictions. Many were of a dual-use nature, creating challenges for the promotion of their peaceful uses while inhibiting potential harms to mankind.

Furthermore, emerging technologies challenge our preconceptions about what can easilybe defined as a weapon. Basic terms such as 'cyberspace'or'weaponization' pose obstacles to the formulation of policy and the creation of legal regulatory structuresbecause they are multi-faceted and spread across different legal frameworks. The role of independent technical experts in reviewing scientific and technological developments in these areas remains crucial to ensuring proper governance. The group exchanged views onhow emerging technologies impact transparency and invisibility.It is increasingly difficult to attribute the source of an attack and available information is often contradictory.

Attribution, Verification, and Transparency

Emerging technologies fundamentally challenge the traditional understanding of attribution, verification and transparency. The "fog of war" now extends outside the traditional battlefield. It can bealmost impossible to trace back cyberattacks and verify compliance. The transparency of decision-making is impacted when security forces replace humans with machines and algorithms. For instance, if an autonomous weapon system makes the decision to use lethal force, there are few ways to understand the process and the logic behind that decision. This also raises troubling ethical dilemmas.

Among the ideas presented in Working Group 7 was the introduction of an international cyber-monitoring system for early-warning, threat detection and information sharing between specific sensitive network segments. Such asystem would not be comprehensive and global in coverage but only applied to sensitive networks with an interest to share and collaborate.

Participants discussed technical feasibility, security implications, institutional set-up, ethics and confidence building. The group concluded that it may be worth bringing relevant actors together to promote further discussion on the feasibility of this topic.

Working Group 7 concluded that Pugwash's expertise on nuclear weapons might be relevant to the cyber sphere in particular where it touches on nuclear warhead verification, confidence building and nuclear energy safeguards. It was noted that the work of the 2015 Pugwash conference had contributed to the publication of the book *Cyberspace* by Cayon& J. Martin Ramirez under the leadership of the Spanish Pugwash Group, which included chapters on the convergence between the nuclear and cybersecurity spheres.

Legitimacy

The accelerating use of emerging technologies for military applications raises the question of frameworks of legitimacy and governance. The increased access toadvanced technology for individuals and groupsmay spread harmsas governments can no longer guarantee their control and monopolize their use.

In addition, the question of "who decides" is important to consider in the context of emerging technologies. Who is liable for autonomous weapon systems committing war crimes? Is it the designers of the system? The coders? The military who used it? Or the individual soldiers who are overseeing it? Taking into account that there is little existing legislation or policy practice, there is space to shape the developing normative and legislative landscapes.

Working Group participantsagreed that autonomous killing systems should be banned. The discussion emphasised the risks associated with removing humans from the decision-making loop, the lack of a dividing line between civilian and military robotics as well as responsibility and liability. In addition, autonomous killing systems are vulnerable; they could be hacked, disabled, or unable to distinguish between combatants and non-combatants. One suggestion was that Pugwash could contribute by linking its experts with the initiative coordinated by Human Rights Watch that includes NGOs, academics and businesses to develop preventative legislation on autonomous killing systems.

Under-Addressed Issues

The Working Group identified several areas that may be of interest for future discussions. Emerging technologies can have a large impact on conventional military doctrine. It was pointed out that recent technological advances in cyber and in anti-submarine warfare may decrease SSBNs' assured second strike capability or lead to an arms race as adversaries continuously undermine existing defences. Additionally, computational advances, the emerging quantum revolution, and genetic modificationare all poorly understood in terms of their impact on peace and security. Further, potential arms races in space remain of high concern for Pugwash.

The Group further discussed the trade-offs that arise with increased investment (in time, money, and attention) in emerging technologies. There are opportunity costs associated with a focus on emerging technology that may distract from existing arms control regimes. These opportunity costs may not be envisioned and can arise as an unintended consequence. Working group members felt that further attention is needed to the byproducts of emerging technologies.

While threats exist from technologies, it is important to recognize their opportunities as well. Emerging technologies can help alleviate war and increase human and ecological well-being. In this respect, Working Group members called for the empowerment of the individual and the advancement of the peaceful use of technology.

Recommendations

1. Pugwash can play a constructive role in diagnosing and responding to emerging cyber threats and new potential harmful applications of autonomous systems. It should boostits involvement in this area by increasing the participation of natural scientists and technical engineers in future Pugwash dialogues;

2. Emerging technologies accelerate the speed of decision making during crises. Drawing on its expertise on nuclear arms control, Pugwash should consult with nuclear states to advocate measures that wouldincrease in decision making time during crises;

3. Artificial Intelligence constitutes the Third Revolution of Warfare. Autonomous killing systems threaten our existing ethical and legal regimes. Pugwash should therefore contribute to the debate on the ban of autonomous killing robots;

4. Confidence-building measures between states are an essential part of alleviating cyber threats. Pugwash must encourage further dialogue and technical cooperation between militaries and decision-makers, particularly in times of crisis;

5. In preparing for future, and responding to previously unknown threats, national Pugwash groups are encouraged to incorporate more forecasting exercises in their activities. In particular, strategic foresight was singled out as a useful tool;

6. The rise of "fake news" has impacted public confidence in authority figures in general and this impacts upon science and world affairs. Pugwash needs to assess the impact and reach of "fake news" on its activities. The following activities are encouraged:

    a. A survey of national Pugwash group memberson the impact of "fake news" couldbe undertaken and the results shared;

    b. Exchange best practices in educating commentatorsand decision-makers on emerging technologies.