RISKS TO PEACE AND STABILITY
FROM THE CYBER DOMAIN

Gian Piero Siroli, Götz Neuneck, Paolo Cotta Ramusino

Working paper - 15.10.20

1. Introduction

Since its foundation, the Pugwash Conferences on Science and World Affairs (Pugwash) has continued to bring together, from around the world, influential scientists, scholars, experts and public figures concerned with reducing the dangers of armed conflict, especially regarding nuclear weapons and other weapons of mass destruction, and with understanding the new threats related to new technologies, while seeking cooperative solutions.

Pugwash held three workshops on the topic of cyber security and warfare between December 2018 and January 2020, gathering a total of about 60 experts and practitioners from Europe, North and South America, and Asia, focusing on a broad set of specific themes. The first workshop (Geneva, Switzerland, December 2018, hosted by the GCSP) discussed battlefield digitalization and offensive cyber capabilities, weapon-system vulnerabilities, and the implications of Artificial Intelligence (AI). The second workshop (Bariloche, Argentina, October 2019, supported by INVAP, Global Security Foundation and KPMG) focused on "Cybersecurity in Latin America". The third workshop (Geneva, Switzerland, January 2020, sponsored by the Mission of Brazil to the UN Office in Geneva) focused on "Cyber Security and Warfare," and included discussions on international cooperation, the multi-stakeholder approach, and implications of AI and autonomous weapons systems. Reports are available on the Pugwash website[1].

The participants, who came from many countries, carried out an analysis and reflection on various aspects of the cyber ecosystem in the context of international stability and security, and reviewed current initiatives included within the international agenda.

Better definitions, a common nomenclature, and reliable communication between responsible stakeholders—based on the principles of International Humanitarian Law and the experiences of arms control for risk reduction, self-restraint and crisis

[1] Reports and summaries can be found here:
Dec 2018, Geneva https://pugwash.org/2018/12/21/geneva-workshop-on-cyber-security-and-warfare/
Oct 2019, Bariloche https://pugwash.org/2018/12/21/geneva-workshop-on-cyber-security-and-warfare/
Jan 2020, Geneva https://pugwash.org/2020/03/02/geneva-workshop-on-cyber-security-and-warfare-2/

management--might be useful or necessary. Sound technical analysis and forensics are a precondition to understanding the different threats and vulnerabilities of the cyber-sphere. Detailed proposals for discussion and implementation were elaborated during the workshops.

2. General Context

Pugwash intends to analyze and understand the possible role of the cyber domain in stimulating and variously supporting—or providing opportunities to resolve or prevent—existing and future conflicts.

Within the international debate many different important topics related to the cyber dimension are being discussed and analyzed, in many cases without a definitive or generally agreed solution; the main ones are briefly described in the following, non-exhaustive list:

- The two distinct but not mutually exclusive approaches that are being followed at the international level to promote international security and stability in the cyber sphere: the development of Trust and Confidence Building Measures (TCBM), and the discussion of more formal binding agreements;
- The development of a multi-stakeholder approach (in particular in the context of the UN Cyber Open-ended Working Group [OEWG]) which would include and integrate in the international debate not only governments but also private actors, civil society, NGOs, academia, etc. Such a wide approach is driven and justified by the intrinsic, deeply multidisciplinary context of the global cyber ecosystem, in order to be able to involve the very wide spectrum of phenomena that need to be taken into account at various levels (political, social, individual and technical);
- The need to foster technical, ethical and legal discussions on Lethal Autonomous Weapon Systems (LAWS) and emerging Hi-tech weapon systems (in particular those using AI applications);
- The fostering of public/private sector cooperation. Analyze and define how to apply state/non–state responsibility in the digital domain, including the concepts of software and hardware liability and supply chain integrity. Within this context, it is necessary to discuss state vs. non-state relations and public/private initiatives and approaches, including proposals already developed by some private actors;
- The discussion of arms control initiatives in the digital domain in comparison with other warfare domains;

- How international laws apply to the use of Information and Communication Technologies (ICT). Discussion of criteria to define when a cyber-attack should be considered as a “use of force” or as an “armed attack”;
- The need to understand the debate on privacy and human rights: supporting fundamental freedoms (including freedom of expression) in the use of information and communications technologies, without raising antagonisms and increasing risks of conflict;
- Raising awareness in political decision makers at all levels, in particular about crisis management in the cyber domain and protection of critical infrastructures and pertinent resilience measures;
- The use of internet as a global communication “medium”, considering the networks at the semantic level. Information warfare and information operations for information manipulation purposes at the social level; propaganda; disinformation; consensus building to condition perceptions, emotions, reasoning and behavior; focusing on human-related aspects of information flow;
- Assessment of the cyber strategies and policies of states, sharing national views in order to build confidence and foster international cooperation toward a global stability.

3. Elements that emerged and were discussed during Pugwash cyber workshops.

During the three workshops many topics were dealt with and analyzed. Some of them could constitute the basis for future discussions.

- *Cyber arms control:* analyze which approaches/tools of arms control are relevant for the cyber sphere, focusing on distinctive characteristics of this warfare domain and considering possible lessons of other regimes (e.g. the Biological and Chemical Weapons Conventions). Development of P-5 work/statement on “Cyber and Nuclear Forces”.
- *Critical infrastructures:* Prohibit cyber attacks on critical infrastructures, particularly nuclear installations and facilities. Propose TCBMs to strengthen national ICT infrastructures and Early Warning Systems to prevent any nuclear incident or war. Reiterate commitment of existing IHL obligations on the non-attack of nuclear or critical infrastructures and non-military targets. Develop an agreed list of critical infrastructures to be out-of-bounds for attacks.
- *Communities:* computer scientists and the various scientific and technical communities should be urged to engage and participate in discussions on the impact of these technologies. There should be a call to discuss the role of responsible science and scientists, with more commitment to concrete research

contributions that would mitigate or control destabilizing developments in the cyber sector.

- *Awareness raising:* active initiatives for raising awareness on the impact of ICT technologies on civil society is of fundamental importance, including also discussions on the role and responsibility of those technologies in mitigating or controlling destabilizing developments in the cyber sector and future domains of warfare. The rapid development of AI and Machine Learning challenges societies not only technically but also on ethical grounds, in a full interdisciplinary context.
- *Cyber regulation of the chain of products:* prohibit implanting “backdoors” or malware into products. States could be compelled to publish malware codes, and companies incentivized to disclose vulnerabilities and produce secure products, as a means to increase global security in the cyber ecosystem. Put in place national and international “bug-bounty” programs in collaboration with already established organizations. Endorse the integrity of encryption protocols by opposing any process of weakening. Explore how to prohibit the proliferation of cyber weapons (e.g. disruptive malware) and the pre-emptive deployment of those for later offensive usage.
- *Glossary:* propose a common understanding as to what defines defensive and/or offensive cyber weapons. Try to use operative definitions based on tools, techniques, targets, and consequences (more criteria if necessary) to avoid the convoluted debates on definitions that plague intergovernmental discussions. Technical details and specifications can change very quickly, thus the need for a general definition that is more stable, applicable and useful.
- *Point-of-contact network:* establish an independent global “point-of-contact network for cyber security and severe incidents”, which includes both technical and political levels and an emphasis on establishing a dialogue between them. This framework could provide a coordination mechanism (for example through hotlines) to facilitate State interactions regarding tracing, assessment, and attribution of cyber attacks and activities. Such an infrastructure could foster cooperation at a bilateral or multilateral level, including regional arrangements, of State actors. Alternative centers and capability of communications and analysis relying on public/private partnerships.
- *Capacity building:* promote capacity-building to address international cooperation and confidence-building measures to close the asymmetry between cyber-advanced states and newcomers to cyber security.
- *Information sharing:* encourage the distribution of cyber-attack technical details (Indicators of Compromise [IoC]) via established methods, possibly through a trusted entity for cyber-threat intelligence sharing at the international level. Large-scale publication of incident reporting in cyber attacks.

- *ICT dual use technology:* understand the dual-use character of cyber technologies. How to deal with the dual-use nature of cyber technology? There are important debates on dual use in the biological and nuclear fields influencing national and international arms export and arms control regulations. Lessons from these debates can be applied to the cyber field.
- *Impact of Battlefield Digitization.* Cyber vulnerabilities of nuclear weapon systems. AI/XAI/ML and military applications. Information Operations & PSYOPS (dualism cyber/info-war).

4. Conclusions - Pugwash position

The nature of cyberspace strongly indicates the need for a wide multidisciplinary approach and global cooperation to minimize risks and threats, and to maximize opportunities for the peaceful use of the entire fast-developing ICT domain.

The international debate on the regulation of the cyber dimension, and in particular the UN discussions within the cyber GGE and OEWG, is strongly supported, especially considering the multi-stakeholder approach, which includes not only nation-states but also additional actors from civil society, the private sector, regional organizations and NGOs.

With limited resources, Pugwash must find allies and partners in other areas of the multi-faceted cyber dimension, but many alternative paths can be pursued at different levels (political decision makers, academics, awareness raising) to make a significant contribution through initiatives of a different nature.

Pugwash could focus on a few high-priority topics, as mentioned in the previous points above; some of these topics could be dealt with in meetings, working groups or diverse Pugwash initiatives:

1. Discuss future TCBMs for reducing tension and mitigating conflict, and consider measures that would avoid potentially catastrophic events. Evaluate the proliferation of military malware and cyber hacking tools used by governments in the context of national and international security. Establishment of norms, rules and principles of responsible behavior of States in the cyber dimension.

2. Understand the impact of cyber technologies on strategic stability. This impact has to be carefully and thoroughly tackled in order to mitigate misunderstandings and the risk of the accidental use of nuclear weapons, weapons of mass destruction in general, as well as conventional weapons. Protection of nuclear infrastructures, both civilian and military, is a very important element as is the protection of civilian critical infrastructures.

3. Engage the scientific ICT community in analysis, discussions and the drafting of new proposals about dual-use applications, measures of restraint, and product development, raising also awareness for risk reduction in the public, industrial and governmental domain. Support educational outreach and awareness raising.

4. Contribute to the international debate about Lethal Autonomous Weapon Systems (LAWS) and correlated Artificial Intelligence (AI) techniques, in the general context of battlefield digitization. Discuss the ethical aspects arising from widespread use of AI. Ban on autonomous weapons systems that select and engage targets without meaningful human control.

5. Understand the importance and the effects of Information Warfare at the semantic level, of the messages flowing in the global Internet, containing not only information but also propaganda, disinformation and manipulation of the cyber medium for destabilizing the global environment.

* * *