Pugwash Workshop on Cyber Security and Warfare

Introduction

On 19-20 December 2018 Pugwash held a workshop in Geneva, co-sponsored and hosted by the Geneva Center for Security Policy (GCSP), on the topic of cyber security and warfare. The meeting gathered together 20 experts and practitioners from Europe, North and South America, and Asia, for a broad set of discussions. Below is a summary of some of the key points that arose over the one-and-a-half days of discussions1, followed by a list of possible areas of further future exploration.

Scope of workshop

Introducing the discussion and in terms of clarifying the priorities, it was noted that there remain an unresolved set of definitional issues concerning cyber that need to be addressed in the wider discourse: for example, the notion of ‘cyber weapon’ is not without controversy and could be delineated against a more general issue of cyber ‘capacity’ for both offensive and defensive use, while the distinction between analytical tools for assessment and tools for offense were noted as dual-use technologies. Similarly, the notion of cyber-attack could probably be more clearly defined and used. Moreover the difference between ‘cyber security’ and ‘information security’ as used by different parties complicates the discussion; the two complementary domains of cyber-war and info-war have to be both taken into account. Nonetheless, cyber was used as the most appropriate and widely-understood term for designating the evolving digitalization of conflict on, and through, computers and networks. In any case, very precise definitions should not delay or hinder addressing the analysis of the fast-evolving cyber eco-sphere within the context of international security.

At the same time, there were a number of conceptual issues that recurred in relation to the usage of cyber: while various cyber ‘tools’ may be used either for influencing the minds and perceptions of populations or as a means of propaganda, intelligence/counter-intelligence work, these areas in the social domain were not the focus of this workshop. Rather, the underlying theme was to understand how computer networks are implicated in the creation or exacerbation of conflict at the international level, including where it concerns the traditional Pugwash interests in the nuclear and WMD realm, and what means might be used to address such a situation. The goal of this meeting was thus to discuss the scope of where Pugwash and other relevant partners can make an impact in a future program of

---

1 The points presented here represent a range of opinions expressed in the meeting, and they do not necessarily reflect the personal views of the rapporteur(s) nor of the Pugwash Conferences as an organization. The meeting was held according to traditional Pugwash/Chatham House rules to enable an open exchange of perspectives and exploration of creative possibilities for ways forward: thus, the substance of the discussions can be reported out, but no item discussed is attributed to any one individual. There was no attempt to seek consensus, and in fact the sharing of diverse views was encouraged.
work and contribute to thinking on the development of proposals for possible solutions in the cyber realm in order to mitigate potential conflict or escalation.

**Cyber threats in the existing regulatory framework**

Many participants reflected that a distinguishing quality of emerging cyber threats, when compared to the nuclear or WMD sphere, is the relatively low cost of entry to being a significant ‘player’ even for non-state actors, yet having the capacity for a destabilizing or devastating effects-based strategy. A key problem of cyber security is the inherent vulnerability of computer and network systems, with a wide spectrum of targets ranging from military weapons systems and support to national critical information infrastructures, whose disruption could cause extended damages.

Furthermore, in the current climate there is both a lack of trust and a lack of transparency in terms of capabilities among States, at very different levels for different actors, and little clarification of retaliatory response directives. These factors present both a serious risk of escalation (depending on the target) and a serious challenge to the existing non-conventional (particularly nuclear) and conventional deterrence strategies of States, potentially in very asymmetric scenarios. Although States naturally have different sets of interests to defend, such vulnerabilities were acknowledged to be global and shared by all, thus creating one possible area of overlapping interest in the security domain to be explored towards a more secure and reliable global cyber ecosystem.

Threats and actions in the cyber realm occur regardless of whether there is a state of war (between countries) and this greatly complicates the interpretation of international humanitarian law (IHL) in such scenarios. It was acknowledged by participants that the existing body of IHL is applicable to cyber activity but that cyber, as a category of security threat, has a different set of characteristics from the more traditional means of warfare, in particular through its potential or apparent mobilization by a range of non-State actors.

Indeed, a key problem identified by participants relates to the assessment and attribution of cyber-attacks, where there may exist complex and hybrid relations between different kinds of actors and where certain States have clear limitations on control and enforcement within their national territories. Currently, and probably for a long time, the status of forensic tools for tracing cyber-attacks is weak and thus technical accountability poses an endemic problem. The vast quantities of information to be analysed in assessing any attack hugely complicate the process of reliable data collection at a multinational or global scale. During discussion of a hypothetical internationally-shared ‘cyber monitoring system’, there was convergence towards the sharing of Indicators of Compromise (IOC), data collected by individual actors during the process of incident response forensics which would be useful for early detection of future attack attempts – a kind of malware information sharing infrastructure. Nation States could open lines or channels of communication at the bilateral or multilateral level towards official peer contact points, and each country could then use its domestic technical cyber infrastructures to contribute to this cooperative inter-State exchange of information.

These issues therefore present a serious challenge to the existing international order and the normative landscape of international relations. Clearly, the situation poses a fundamental problem to approaches in the regulation of the cyber realm, which is currently probably the least regulated warfare domain: to address what kinds of activities may be limited or prohibited through binding measures; where
thresholds of activity may be identified or controlled or considered an act of war; and the extent to which legal or voluntary measures would be effective or implementable.

**Speed and artificial intelligence**

This challenge to regulation is particularly acute because of the race toward ever-faster technical development and the potential impact of Artificial Intelligence and Machine Learning upon the various processes. There was a sense that speed would prove a double-edged sword: for example, in relation to the monitoring and analysis issue above, applied machine-learning could enhance data analysis; the flip-side is that there will be an inherently destabilizing technological impact on the horizon, where States do not develop such advances at an even rate. In any case, of course, these new techniques are not exempt from vulnerabilities or malicious manipulation. As such, one participant noted the imperative toward identifying technical solutions sooner rather than later; following the advent of the Internet of Things (IoT), the border between the physical world and cyber domain will fade, which will greatly complicate identifying acceptable measures down the road.

In this context, future ‘warfare’ will not involve only physical battlefields and an intent to kill humans but also forms of cyber-led domination intended to control the digital-battlefield (sensors, communications and weapons systems), and thus bring a country to its knees through cyber-attacks to critical infrastructures. Discussion touched upon human-machine teaming, the balance between human-assisted (semi-autonomous) processes and fully autonomous systems that likely will characterize the future landscape. Artificial intelligence and the retention of human agency in military or civilian systems clearly also carries large ethical questions, which were ultimately beyond the scope of this preliminary discussion and will probably be analysed in future workshops.

Overall, one implication of this future uncertainty may be the degradation of defensive capabilities and deterrence measures, with an overriding emphasis on offensive postures and a first strike attitude. Moreover, it was noted that governments are largely behind in this field and likely cannot qualitatively and quantitively keep up with the rate of technological development in particular in the private sector. It was felt that these challenges to the monopoly of force currently held by States will dramatically change the nature of international conflict.

**Approaches to containing cyber warfare**

There are presently a multitude of both official and non-official initiatives to address the cyber realm. One big question circles around how to implement existing norms rather than developing further law. The Group of Governmental Experts established under the auspices of the UN, in its recent phase, was viewed as having been derailed somewhat by competing resolutions, resulting in two different visions and approaches: the GGE will continue to examine and interpret existing norms while an Open-Ended Working Group would focus on confidence-building measures and the implementation of a legal framework. While the two groups are not mutually exclusive, there was some pessimism for a coordinated approach. More generally, the UN process was seen as compromised by the challenge to establishing an agreed-upon set of norms because of clear political differences and the lack of a level playing field amongst the actors.

One potentially fruitful alternative raised was to seek regional groupings to pursue the implementation of existing norms and development of CBMs, if formal agreements turn out to be
unfeasible. The creation of the Tallinn Manual was held up as one such example and could be built upon within the OSCE area which neatly brings together East and West. Equally, the ASEAN region is perhaps ripe for a similar exercise in exploring a set of measures appropriately determined. There was also a suggestion that such work could be carried out among the UN Security Council permanent members, acknowledging that there are wide political divisions to accomplishing such a project.

Participants also discussed the engagement of the private sector in any future arrangements. While public-private partnerships in the cyber realm may appear idealistic, it was clear that many multinational corporations and companies are active players in the cyber domain, with large infrastructures collecting sensors data and already capable of performing many of the monitoring and analysis tasks over global networks. In a sense, as was suggested, States may look to modulate the incentive structure for such actors, in ways that push them to collaborate or deter them from acting in certain ways and contribute to improving the global cyber-security ecosystem. In general, the highly political dimension of such proposals implied a step-by-step, experimentalist approach rather than blanket regulation.

**Ideas for further exploration and elaboration**

While reinforcement and implementation of existing or future norms and obligations is a key task for the international community, focus was given to thinking of future CBMs for reducing tension and mitigating conflict, and considering measures that would avoid potentially catastrophic events.

- **International database of national points of contact for addressing cyber security threats and actions.** Establishing national contact points for cyber incidents (“cyber defense centers”) could provide a coordination mechanism (for example through hot-lines) to facilitate State interactions regarding the tracing, assessment, and attribution of various cyber-attacks and activities. Such an infrastructure could foster cooperation at a bilateral or multilateral level, including regional arrangements, of State actors; the technical level cooperation (through CERTs for example) would be scaled up at the inter-State level.

- **Alternative centers and capability of communications and analysis** relying on public-private partnerships. As a model, there exists already networks of such communications at academic or private levels, showing that it is technically feasible.

- Encourage the sharing of Indicators of Compromise (IoC) via established methods (e.g. MISP\(^2\) or similar tools), maybe through a trusted entity for cyber-threat intelligence sharing at the international level, taking the business impact for security companies into account.

- Make mandatory the publication of vulnerabilities for the sake of improving the defense of critical infrastructures but also normal constituencies and citizens.

- Put in place national and international "Bug-bounty" programs, with defined revenues on first findings, proportional to distribution of the vulnerable software, paid by the

---

\(^2\) MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing
corresponding manufacture in case of proprietary software and by a central pool for open source software, in collaboration to already established organizations (e.g. MITRE\textsuperscript{3}, CVE\textsuperscript{4}).

- **Endorse the integrity of encryption protocols** by opposing any process of weakening (e.g. by backdoors, reduced key-length, shared decryption keys, etc.).

- Explore how to **prohibit the proliferation of cyber-weapons** (e.g. malware) and the pre-emptive deployment of those for later offensive usage.

- Large-scale **publication of incident reporting** in cyber-attacks.

- Analyze which **approaches/tools of arms control are relevant for the cyber sphere** and focus on the distinctive characteristics of this warfare domain. In this context, the experiences and possible lessons of other regimes should be considered (e.g. the Biological Weapons Convention).

- Development of **P-5 work/statement on “Cyber and Nuclear Forces”**.

- Reiterated commitment of existing IHL obligations on the **non-attack of nuclear or critical infrastructures and non military targets**.

\textsuperscript{3} Mitre Corporation
\textsuperscript{4} CVE - Common Vulnerabilities and Exposures