War or Peace in Cyberspace: Whither International Cyber Security? Conference Report

Executive Summary

Cyberspace and the Internet represent a unique human-created environment on which global society is increasingly dependent for its welfare. This space has experienced a major "militarization" in recent years with armed forces establishing cyber security units and many developing offensive cyber capabilities. Diplomatic efforts at developing agreed norms of responsible state behaviour in cyberspace have not kept pace with the growth of cyber security capabilities within national security establishments. The security "frame" imposed on discussions of international cyber policy has tended to marginalize human rights and humanitarian perspectives. The re-emergence of great power rivalry provides an opportunity for middle powers to exercise leadership in promoting cooperative security options for cyberspace. The wider stakeholder community including the private sector and civil society need to be better integrated into state-led discussions of international cyber security policy.

Report: On May 24, 2018, some three dozen experts from the fields of international affairs, cyber security and information technology gathered at the Balsillie School of International Affairs in Waterloo, Canada for a conference sponsored by The Simons Foundation, Project Ploughshares, the Centre for Peace Advancement at Conrad Grebel University College, the Balsillie School and the Canadian Pugwash Group. Participants at the conference, *War or Peace in Cyberspace: Whither International Cyber Security?* considered the current state of the international cyber security policy discussion and its implications for conflict or peace in the vital, if vulnerable environment of cyberspace. The conference engaged perspectives from academia, civil society, the Canadian military and the private sector. This report summarizes the four panels of the conference and describes the main themes and outcomes of the day's discussions, with an eye to potential next steps for civil society and the international community.

Panel A: The Cyber Domain and Threat: The State as Actor

Robert Morgus of the New America Foundation started the first panel of the day by summarizing types of offensive cyber capabilities, including knowledge of software vulnerabilities and methods for exploiting them, as well as tools, infrastructure and platforms used to carry out operations. These operations are generally undertaken with at least one of four objectives in mind: accessing a computer system, not necessarily for the purposes of taking further action at the time but sometimes just for reconnaissance; espionage or theft, in which actors obtain data from the system; attacks aimed at causing disruption, such as distributed denial of service (DDoS) or ransomware attacks (encrypting victims' sensitive data until a ransom is paid); and destructive attacks that can wipe out data or manipulate connected hardware to cause physical effects. Even operations aimed at access, which on the surface may seem less severe than the other types, can have serious consequences: when an unauthorized intruder is found in a computer system, there is no way to know if the intruder is preparing an attack, and that uncertainty could prompt an escalatory response. Morgus said that offensive cyber capabilities have proliferated, becoming both more sophisticated and more accessible. Potent offensive options are now available to actors at the lower end of the spectrum, such as states that have newly obtained cyber capabilities and non-state actors. Such capabilities may not be as sophisticated as those possessed by highly capable states but they are still powerful enough to have significant effects, especially against "softer" targets.

While cyber security is often framed as analogous to armed conflict or military operations, especially when it comes to norms that constrain state behaviour, Morgus suggested some limitations to this analogue. In particular, norms don't matter to states that opt to ignore them; instead, preventing them from acquiring or developing capability may be a better option. As such, alternative analogues may be more effective in framing the problem for the international community, such as collective action on money laundering, disease control and narcotics.

Col. Dave Yarker, director of cyber force development for the Canadian Department of National Defence, described three paradigms used to frame cyber security from a military perspective. The first is that cyber security is a rising threat, which has driven behaviours to reduce the threat. The second is that cyber security is a domain of warfare, similar to land, air or

sea: it is a space that can be contested, where one's actions can remove capability from an opponent or vice-versa. Calling cyber security a domain doesn't mean that a "cyber war" will happen in isolation, but that cyber capabilities need to be integrated into other domains of warfare in the same way that air strikes (air domain) may back up a ground invasion (land domain). Conceiving of it as a domain also underscores that cyber security is not fundamentally different from other domains where conflicts can happen, he said. The third paradigm is that of the invalidated assumption. The assumption in question is that military operations and weapon functions, such as launching a targeted missile, will work as intended, but cyber operations are capable of interfering with those systems and negating those assumptions.

Yarker listed five major cyber security activities outlined in the June 2017 Canadian defence policy review: obtaining cyber defence capabilities and making networks more secure; building an active cyber operations capability; creating cyber mission assurance to build resilience into their systems; setting up cyber security as a trade; and bringing in cyber security reservists. He noted that the latter two are about building human capital rather than technical capabilities, because the current lack of human capital is a "critical problem."

Bill Robinson of Citizen Lab described the difficulties of distinguishing between computer network attacks, espionage and defence. The ambiguity around motivations and effects makes it difficult to identify whether an attack has occurred that would merit a response under international law. However, he noted that it's possible for formal or informal restraints to develop among states: for instance, in the field of espionage, norms prohibit states from killing another state's spies. Norms are helpful in establishing a standard against which bad behaviour can be called out, even if it's an informal norm – or "pirate's code" – of mutually reinforcing self-restraint. He also noted that it would be impossible to limit all computer network espionage, so the priority should be on enhancing resilience and cyber defence to minimize the negative consequences of espionage efforts.

Panel B: The Role of International Law and Confidence Building Measures in Defining Acceptable Cyber Activity

Eneken Tikk, of the University of Leiden, opened the panel by noting that in its three most recent sessions, the *United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security* (henceforth the GGE) has discussed at length whether and how international law applies to state activities in cyberspace. But regardless of what the GGE decides, she said, it's up to states to interpret international law and decide to what extent it can be helpful in resolving the issues at hand. So far, states have taken a variety of positions: some, such as Russia, have said or demonstrated through their actions that international law does not or cannot be applied; some say parts of it should not be applied, such as China's argument that addressing the right to self-defence in cyberspace would open the door to the legitimization of cyber conflict and more frequent use of force; some say it applies, such as the participants in the *Tallinn Manual* project, but their views diverge on how it should be interpreted; and very few actually apply it as written. Even Western states that say international law should apply to cyber security have either explored the possibility of conducting cyberspace operations below the threshold that would be considered an act of war, or have accepted other countries doing the same without levelling consequences against them, both of which erode their moral authority and leadership on this issue.

Instead of the normative approach to cyber security favoured by Western states, Russia has suggested a treaty-based model. The prospect of a cyber security treaty should be taken seriously, Tikk said. Over the past 20 years, Russia has aimed to reopen elements of international law for negotiation, such as state sovereignty over cyberspace and related restrictions on the freedom of information, and it has succeeded in moving more countries to its camp, especially from the developing world. A treaty could help address gaps in international law and create clear and consistent red lines, which is helpful because inconsistency contributes to the kind of uncertainty that has been driving states to launch below-the-threshold attacks. At the same time, Tikk also recognized a role for domestic law to address cyber security – especially when it comes to cyber crime, which is far more common than attacks launched by nation-states – rather than expecting international law to solve everything on its own.

Theresa Hitchens, of the University of Maryland's Center for International and Security Studies at Maryland (CISSM), focused on transparency and confidence-building measures (TCBMs), which are designed to build trust and avoid conflict via information sharing. Transparency is important because when one party doesn't know what the other is up to, it is more likely to assume the worst, which can escalate tensions and lead to conflict based on misperceptions. Hitchens outlined the progress of the GGE, which agreed to a set of TCBMs in 2015, but failed to agree on a report in its next session two years later. In contrast, the Organization for Security and Cooperation in Europe (OSCE) has adopted several TCBMs over the years, including such concrete, practical steps as developing contact points for information sharing within states and major tech industries, national reporting of vulnerabilities in cyber systems, cooperating on protecting national and transnational critical infrastructure, and developing a classification system for cyber events to allow for consistency in defining what constitutes an attack and degrees of severity. While both diplomatic processes have stalled in terms of generating new measures, this has shifted the focus to implementation. The OSCE has better prospects here because the OSCE secretariat has powers that allow it to implement TCBMs, she said, while the UN has no similar secretariat mechanism for mandating states to implement its recommendations.

Hitchens suggested a number of priorities for TCBM implementation, such as developing standardized processes to classify cyber incidents, identifying critical infrastructure – possibly including core internet functions such as the domain name system (DNS) – and providing for cooperative protection of it, and clarifying procedures around vulnerability sharing. In any case, cooperation is critical because the cross-border nature of the digital world means a system is only as secure as its weakest link. Active cyber security diplomacy is required, but with the United States backing away from diplomacy, there is a role for middle powers to lead in this space. There is also a role for NGOs and academics to take part in Track 1.5 efforts at defining the way ahead.

Panel C: Key Forums and Results to Date

Elana Broitman, of the New America Foundation, discussed the benefits and drawbacks of the UN as a forum for reaching international agreements on cyber security. Two major challenges

are that technology moves much faster than treaty-making, and that distrust among nations, as well as different approaches to cyber security, have contributed to stalemates in UN fora such as the GGE. However, the UN retains its influence when it comes to forms of "soft power" such as socialization, persuasion and ideation. Its global reach also puts it in a position to coordinate and amplify cooperative measures that have been reached at a regional level, and to implement capacity-building activities. She noted that while cyber security at the UN General Assembly has traditionally been addressed by the First Committee, which handles international security matters, aspects of it have also been addressed at the Second (economic) and Third (human rights) committees. This is important to ensure that critical issues such as development and human rights are included in discussions around cyber security.

Despite the failure of the 2017 GGE, major parts of the 2015 GGE recommendations were endorsed by the G20 grouping of leading states and have not been disavowed. Bringing attention to existing normative agreements can help reinforce areas of consensus that have been reached and make it harder to walk them back. New America is currently developing a database of such agreements to help in that effort.

Roy Firestein of Cycura, a cyber security firm, began by describing the recent *Cybersecurity Tech Accord* signed by about 30 private companies involved in different aspects of the digital world, including Facebook, Microsoft, GitHub, Cloudflare, Dell and Symantec. The companies agreed on four main principles: protect all users and their data; oppose cyber attacks on their users, including attacks by governments; build the capacity of the users and businesses that use their technology to keep themselves secure; and partner with other companies to enhance cyber security, through collaboration, threat sharing, etc. This fourth point is particularly important because private companies have traditionally been reluctant to share information, even though it can be mutually beneficial, for fear of exposing their own vulnerabilities or business information. At the same time, even when information about a threat is shared, a company may be reluctant to trust it without knowing how the company that reported the threat came to its conclusions.

Firestein said there is a need for more drivers for companies to promote information sharing. Other potential measures the private sector could take to enhance cyber security would be to

expose parties that abuse their technologies by public shaming and other sanctions that would change their risk calculus; focus on core internet routing technology that everyone relies on; agree on standards that can be deployed globally (e.g. the shift from IPv4 to IPv6); and encourage large tech companies work with small and medium businesses to share information and provide them with tools and strategies to enhance their security.

Alison Pytlak, of Reaching Critical Will, provided a civil society perspective. As a feminist peace organization, her NGO has been challenging the militarization of cyberspace. While disarmament isn't the best or only approach to cyber security, she said it's where most of the conversations in this space have been happening. However, most of the debate has lacked the sense of urgency that civil society has brought to other topics. She outlined a few potential reasons for this: decision-making fora, such as the GGE and OSCE, are closed to civil society; concern that bringing the matter to arms-control discussions further legitimizes the security-based approach to the issue; and the lack of clear humanitarian impact of cyber attacks to date, making arguments more speculative and more difficult to frame. However, she said, cyber security is increasingly coming up in other arms control spaces, such as discussions around autonomous weapons or nuclear systems.

Pytlak offered a few recommendations for civil society groups working in the cyber security space. First, they could do better at interpreting technical jargon, both to galvanize public opinion but also to bolster their work with policy stakeholders, especially in smaller countries that might not have the resources for subject experts. This will likely require building more links with the technical community. Second, they can look beyond traditional multilateral fora such as the UN to nurture core groups of likeminded countries, or to link local or regional efforts to global ones. Finally, they can use human-based security approaches to promote human rights and humanitarian perspectives – where civil society groups often have more resources and expertise – within cyber security conversations.

Panel D: Future Prospects and Canada's Role

Ron Deibert of Citizen Lab introduced the topic of targeted threats and cyber espionage against civil society, often at the hands of governments making use of private tech companies' products,

by presenting recent research by his organization that has uncovered illicit hacking and surveillance of activists by countries such as the United Arab Emirates, Mexico, Ethiopia and Russia. These kinds of capabilities, created and sold by private companies, are proliferating, especially among governments that don't have the resources to build their own advanced cyber security apparatus. Deibert described them as an "off-the-shelf National Security Agency."

There is reason to believe that traditional deterrence models such as mutual entanglement are having an effect in the cyber security space – countries don't want to expose their own vulnerabilities by launching a cyber attack – which has had the effect of pushing most cyber actions down to a more covert domain, such as espionage and influence operations. While most of the discussion around global cyber security is focused on state-on-state actions, authoritarian regimes are at least as likely to include NGOs and even individual dissidents as part of their threat model. With an unregulated surveillance industry with proven abuse potential eager to cater to these regimes, this is a growing area of concern that merits more attention.

Paul Meyer, of The Simons Foundation and Canadian Pugwash Group, concluded the panel by sharing his experiences as a Canadian diplomat working on cyber security issues. He said the most recent Canadian cyber security strategy, released in 2010, included a call for Canada to develop a cyber security foreign policy, but so far Global Affairs Canada has not released such a policy, and most of the responsibility for the file has been handled by a single official at GAC. By comparison, Australia's foreign affairs department released a comprehensive cyber foreign policy document last year that outlines a whole-of-government approach to preserving "a peaceful online environment," and appointed an Ambassador for Cyber Affairs to oversee the implementation of the strategy, as well as a substantial funding commitment.

In addition to more human and financial resources, Meyer said, Canada would also benefit from stating a clear goal for its cyber foreign policy. While Canada's submission to the GGE spoke of a "free, open and secure cyberspace," he noted that "secure" leaves open the question of what potentially offensive measures could be taken to achieve that security. Instead, he would prefer to see a specific reference to supporting the goal of a "peaceful" cyberspace, as put forward in the Australian policy document, for example. He also noted that given the current atmosphere of

great power disagreement and uncertainty in the cyber realm, a proactive diplomacy is crucial to defuse tensions and foster cooperative security approaches. Such efforts should also involve consultation with the private sector and civil society, which are the principal owners and users of cyberspace and hence key stakeholders in ensuring it is preserved for peaceful purposes.

Conclusions

A number of common threads emerged over the course of the day's discussions. One overarching theme was the need to look at cyber security from a human rights or human security-focused perspective, rather than exclusively from a national security or military perspective. While the vast majority of cyberspace is peaceful, participants expressed concern that policy debates tend to emphasize the risk of state-sponsored cyber attacks that must be defended against, rather than the advantages of a global commons that should be preserved, which makes it easier for conceptions of cyberspace as a domain of contestation to dominate. One participant noted that national security agencies have traditionally taken the lead on cyber security issues, and this could potentially create a "self-fulfilling prophecy" by keeping conversations anchored in that conceptual space, leaving considerations of human rights and societal benefits as an afterthought. A few participants also described this as a negative byproduct of state-level negotiations in fora such as the GGE which have been established within an international security context. Given that "frame" and under pressure to reach as broad a consensus as possible, divisive issues such as human rights are often left out of the discussion. Civil society organizations would be well placed to push states to include human rights and human security considerations in their cyber security deliberations, and to raise public awareness of these issues in order to influence political leadership.

Another theme that ran through all of the discussions was international norms and the limitations thereof. The norms debate has been a major component of the international cyber security conversation, especially given the prominence of the UN GGE as a venue for establishing global norms. With the most recent GGE ending in a stalemate, there has been ongoing debate about whether the normative approach has outlived its usefulness. Rather than abandoning this approach, however, some participants argued that it is important for states to reinforce the gains that have been made so far and to uphold the norms that have already been established.

Amplifying existing norms makes it harder to disregard them, one participant said. More importantly, enforcing existing norms consistently can reduce the insecurity that comes from bad actors taking advantage of normative ambiguity and "grey zones" to see what aggressive actions they can get away with. A lack of consistency in responding to norm-defying behaviour in cyberspace only emboldens these malicious actors to keep pushing the envelope.

There are also alternatives to formal state-to-state agreements that can be used to reinforce norms and establish standards for responsible behaviour in cyberspace. For instance, the conference heard, investors have been successfully dissuaded from buying shares in a company that performs government-sponsored surveillance of civil society actors, which demonstrates how economic incentives can be used to persuade tech companies to work toward improved security and human rights. Private companies can also be incentivized to stand up to illiberal governments and other actors who want to use their technologies in ways that harm human rights and security. Meanwhile, NGOs and other civil society actors can play a role as whistleblowers, by alerting the public and concerned governments about violations of rights and security. They can also help by building capacity, particularly within smaller and developing governments. This doesn't just refer to the technical expertise and capabilities needed to keep cyber systems secure, but also to the legal and policy capacity to develop legislation and participate in global discussions that enables cyber security and protects human rights.

While the prospects for global cyber security agreements are currently dim, there has been progress in reaching more limited agreements and partnerships, either on a regional scale or based on specific issues of mutual interest. Such regional or limited agreements have the potential to be expanded upon by the UN, but even if not, they can still have a net benefit by helping the countries or sectors involved to improve their security. There is great potential for medium-sized countries to play a leading role here, participants said, because they are often more flexible than major powers with entrenched negotiating positions and are more likely to be seen as "honest brokers" in the international community.

The technical community can also play a role here, building trust and working relationships at a level outside of the scope of politics. Historically, computer emergency response teams (CERTs)

have shared information about threats and vulnerabilities. While some private companies and government agencies are understandably leery of sharing threat information, one participant suggested they could use “black box” methodologies established by other industries, such as satellites and banking, to share information about threats or vulnerabilities without divulging sensitive information.

Several participants also spoke of the need to establish clear definitions and standards. A lack of clear terminology contributes to an environment of uncertainty and confusion: what one actor may characterize as a severe attack, another could see as a routine intrusion. Clarifying definitions and degrees of severity for offensive cyber activities would contribute to consistency and help identify appropriate proportional responses.

While most of the discussion at the conference focused on traditional conceptions of cyber security, there was also some discussion of influence operations or information warfare, such as the campaign widely attributed to Russia that used social media in an attempt to influence public opinion during the 2016 U.S. election. One participant said this is one of his greatest concerns, because while propaganda has existed for a long time, today’s technology makes it easy to spread propaganda faster and farther than ever before. Influence operations have implications for security, by increasing societal tensions that could result in real-world conflicts, and for human rights, by targeting marginalized groups or discouraging internet users from exercising their right to freedom of expression. While this was not a main focus of the conference, it does point to an area for future work. Likewise, conference participants from the technology space pointed to quantum computing as a game-changing technology on the horizon, because of its ability to overcome encryption as we know it. This represents another topic that merits attention in future discussion of international cyber security policies.

War or Peace in Cyberspace: Whither International Cyber Security?

May 24, 2018

Balsillie School of International Affairs, Waterloo, Ontario

Panel A) The Cyber Domain and Threat: the State as Actor

Moderator: Paul Meyer, The Simons Foundation

1. Offensive versus defensive cyber operations – Robert Morgus, New America Foundation

2. Military cyber establishments, capacities and doctrine- Colonel Dave Yarker, Director, Cyber Force Development, DND

3. How should cyber espionage be addressed? – Bill Robinson, Citizen Lab

Panel B) The Role of International Law and Confidence Building Measures (CBMs) in Defining Acceptable Cyber Activity

Moderator: Ernie Regehr, Canadian Pugwash Group

1. The Application of International Law: Current status, Eneken Tikk, University of Leiden

2. Cyber Confidence Building Measures: Transparency, Cooperation and Restraint – Theresa Hitchins, CISSM, University of Maryland

Panel C) Key forums and results to date

Moderator: Alistair Edgar, BSIA

1. UN engagement on cyber security (GGEs, First Committee)- Elana Broitman, New America Foundation

2. The role of the private sector – Roy Firestein, Cycura

3. The role of civil society – Allison Pytlak, Reaching Critical Will

Panel D) Future Prospects and Canada's Role

Moderator: Cesar Jaramillo, Project Plougshares

1.The Cyber Arms Race and Collateral Damage – Ron Deibert, Citizen Lab

2.A Cyber Security Foreign Policy for Canada – Paul Meyer, The Simons Foundation/Canadian Pugwash Group

Public Event: "War or Peace in Cyberspace: What Does it Mean for You?"

Moderated by Bessma Momani (BSIA) and featuring Theresa Hitchins (University of Maryland) and Paul Meyer (The Simons Foundation)

Sponsored by:

List of Participants

Elana Broitman, New America Foundation

Scott Campbell, Centre for Society, Technology and Values

Peter Carr, University of Waterloo

Ron Deibert, Citizen Lab

Heather Douglas, Balsillie School of International Affairs

Alistair Edgar, Balsillie School of International Affairs

Roy Firestein, Cycura

Marlene Floyd, Microsoft Canada

Ian Goldberg, University of Waterloo

Rebecca Herbener, Balsillie School of International Affairs

Paul Heidebrecht, Conrad Grebel University College

Theresa Hitchens, University of Maryland

David Jao, University of Waterloo

Cesar Jaramillo, Project Ploughshares

Florian Kerschbaum, University of Waterloo

Stephanie MacLellan, Centre for International Governance Innovation

Paul Meyer, The Simon Foundation

Bessma Momani, Balsillie School of International Affairs

Robert Morgus, New America Foundation

Naomi Pearson, Laurier University

Allison Pytlak, Reaching Critical Will

Ernie Regehr, Canadian Pugwash Group

Bill Robinson, Citizen Lab

Eneken Tikk, University of Leiden

Scott Totzke, ISARA Corporation

David Welch, Balsillie School of International Affairs

Dave Yarker, Canadian Armed Forces