ICT for peace foundation

WannaCry, the Geneva Digital Convention and the urgent need for Cyber Peace

A commentary by ICT4Peace

Paul Meyer, Senior Advisor, ICT4Peace Foundation
Daniel Stauffacher, President, ICT4Peace Foundation

The mass assault of the “WannaCry” malware that holds computer users to ransom by encrypting their files and demanding a payment for making them accessible has once again demonstrated both the wide-ranging scope of cyber attacks and the continuing vulnerability of many individuals and institutions to them.

Although this action was apparently perpetrated by cyber criminals for financial gain there are official fingerprints on it as well. The cyber payload that contained the malware took advantage of a vulnerability in a Microsoft Windows operating system that had previously been identified and developed by the US National Security Agency as an ‘exploit’ for a covert cyber operation. After this ‘exploit’ was revealed along with a series of other such cyber tools by a mysterious group “Shadow Brokers” (a case of the government hackers being hacked themselves) it became available for further application by cyber criminals or other malicious actors. Some analysts have suggested on the basis of coding and other similarities that the North Korean government may be behind the ransom ware attack. Certainly North Korea has a motivation as it searches for means to gain hard currency in an ever-tightening net of UN Security Council-mandated sanctions against the Pyongyang regime.

In the wake of the “WannaCry” attack, the President of Microsoft Corporation, Mr Brad Smith, decried the state practice of hoarding such identified software vulnerabilities and the applications designed to take advantage of them (known as “zero day exploits” in that they have not been previously identified) in furtherance of their clandestine cyber operations. The role that states play in cyberspace through their intelligence and military establishments is increasingly emerging from the shadows. High profile incidents such as the 2013 revelations by ex-NSA contractor Edward Snowden, the 2014 cyber attack on Sony Pictures attributed by the US to North Korea, and the alleged Russian cyber interference in the US and French presidential elections in 2016 and 2017 respectively have all served to highlight malicious cyber activity undertaken by states.

Microsoft has been in the forefront of the concerned private IT sector in addressing the threat posed to the peaceful use of cyberspace by state cyber operations and in advocating for remedial action. The goal of agreed global norms of responsible state behavior in cyberspace, first articulated by the administration of US President Obama in its 2011 *International Strategy for Cyberspace* policy statement, requires concerted efforts by the private sector and civil society alongside states if this aim is ever to become more than merely aspirational in nature.

In a farsighted speech delivered earlier this year in San Francisco, the President of Microsoft called for a *Digital Geneva Convention* to respond to the increase in state conducted cyber attacks. He noted that "For over two-thirds of a century, the world's governments have been committed to protecting civilians in times of war. But when it comes to cyber attacks, nation-state hacking has evolved into attacks on civilians in times of peace". Making the analogy with the 1949 Geneva Convention in which states agreed to a range of measures designed to protect civilians in times of war, Mr. Smith argued that it was time for states to take action to protect civilians in their cyber activities during peacetime.

It is true that under the auspices of the UN states have been engaged for several years in considering what measures might be taken in cyberspace to prevent conflict and reduce risks to international peace and security. Through the mechanism of UN Groups of Governmental Experts (GGE), successive groups of 15-20 governmental experts drawn from UN member states have been involved in a series of studies of cyber activity in the context of international security. These groups have produced consensus reports in each of 2010, 2013 and 2015. A fourth group is currently underway with a reporting deadline of this fall.

The 2015 GGE report was the most substantive to date in elaborating suggested norms and measures to govern state conduct in cyberspace. The report enumerated a series of confidence building measures to advance transparency and predictability regarding state action and to lessen the risk of cyber conflict. Notably among these was a commitment not to engage in cyber operations directed at critical infrastructure on which publics depend. Furthermore, it was proposed that states refrain from targeting computer emergency response teams (the "first responders" in the cyber world with roles analogous to the emergency response teams in the real world) as well as not employing such teams for any offensive cyber actions. These proposals seemed designed to accord a protective status to infrastructure and computer response teams critical for public safety and well being in a manner similar to the protection assigned to humanitarian actors and entities under the Geneva Convention. The proposals from the 2015 GGE however remain just that – a set of recommendations from a small set of experts that will require state acceptance and implementation to be effective.

In calling for the negotiation of a *Digital Geneva Convention*, Microsoft is looking for a more ambitious and far ranging set of constraint measures. States should not just refrain from targeting critical infrastructure, but forgo targeting technology companies and the private sector as a whole. He also called upon states to cease stockpiling vulnerabilities and to work with the private sector to remedy them. To support a *Digital Geneva Convention,* Microsoft envisions a neutral implementing organization akin to the International Committee of the Red Cross (ICRC). Microsoft presses the ICRC analogy even farther in suggesting that the global technology sector should reject "rising nationalism" and become a "trusted and neutral Digital Switzerland". Ultimately, if unchecked the damaging use of cyberspace by states for perceived security aims will compromise this special domain for all. As Brad Smith states: "…we need to persuade every government that it needs a national and global IT infrastructure that it can trust".

While this vision of the global IT industry serving the world as a "neutral Digital Switzerland" may seem farfetched to many (including some skeptical Swiss) it speaks to the need for the private sector and civil society more broadly to be vocal in the defence of *their* cyberspace and to bring pressure on governments to act responsibly in this vulnerable domain. At the same time, Microsoft cannot afford to be a solitary advocate for greater private sector engagement in developing norms of responsible state behavior for cyberspace. There is a need to mobilize the broader IT sector if governments are going to be receptive to the message of maintaining a peaceful cyberspace. This will entail real coordination and coalition building to have an impact on the intergovernmental discussion, akin to how the International Chamber of Commerce mobilized to influence the proceedings and outcomes at the World Summit on the Information Society (WSIS) over a decade ago.

There is also a concomitant requirement for the UN GGE process to open itself up to interaction with the broader stakeholder community represented by the private sector and civil society. However convenient it is for states to operate behind closed doors and generate their own products, the utility and credibility of their reports would be greatly enhanced if they reflected some inputs from non-governmental stakeholders. Surely there are ways to achieve such a dialogue without compromising the respective prerogatives of each community.

In their *Declaration on Responsible States Behavior in Cyberspace* issued after their April 2017 meeting, G7 foreign ministers expressed support for the sort of confidence building measures generated by the 2015 UN GGE. The G7 however minus leading cyber powers such as Russia and China, not to mention rising ones such as India, is even less representative of the international community than the 2015 GGE members. A broader cross-regional collection of states will be necessary to realize the promise of the recommended measures from the GGE. It is time for the

UN General Assembly to establish a process that would involve member states in the collective formulation of measures to govern their behavior in cyberspace.

A complementary approach would seek to accelerate the on-going work in regional organizations on developing norms to support international cyber security. Regional groupings such as the OSCE, the AU and ASEAN's Regional Forum have all initiated work on cyber security confidence-building measures (CBMs). These CBM initiatives are at different levels of elaboration and ambition, but all aim to improve the secure use of cyberspace and prevent inter-state conflict by enhancing transparency and predictability in state cyber conduct.

Given the wide range of cyber security capabilities amongst the members of the various regional organizations, cyber capacity-building remains a crucial precondition for realizing the promise of international cyber security cooperation.
ICT4Peace has been active in this field for years via customized cyber security capacity building workshops designed to ensure that stakeholders (especially in developing countries) have the means to participate effectively in international cyber-related discussions and negotiations. All these positive actions however will be in vain if a solid commitment to maintaining cyberspace for peaceful purposes is not upheld. Global users of cyberspace should not accept to be passive on-lookers as this environment is compromised by reckless state action. To embark upon even more ambitious collaboration with the private sector as envisaged in the Microsoft's president's address will however require a level of political engagement and leadership not seen to date in the international cyber arena. Perhaps it will take a few more waves of mass cyber assault for citizens to press their governments to get serious about forging international agreements on norms of responsible state conduct in cyberspace.

****

As far back as 2011, the ICT for Peace Foundation called for an International Code of Conduct (or norms of responsible state behaviour) to prevent cyber-conflicts by states and non-state actors. In an op ed of the leading German language newspaper ***Neue Zürcher Zeitung***, Daniel Stauffacher, President of the ICT4Peace Foundation stated that "new online threats such as cyber-espionage and cyber-conflict are very hard to counteract with traditional security policy and instruments. It is now necessary to move forward and develop an international rules-based framework to set standards for the behaviour of states in cyberspace."

The full text in German can be found **here**. The English version "Cyber-conflict: Why the world needs an international code of conduct" can be found **here**.

Geneva June 2017