The Struggle for Cyber Peace: Norms of responsible state behaviour

Remarks by Paul Meyer, Senior Advisor, ICT4Peace at CANVAS workshop

Cybersecurity Challenges in the Government Sphere – Ethical, Legal and Technical Aspects –University of Applied Sciences, Bern, Switzerland, Sept 5-6, 2018

First I would like to say how pleased I am to be participating in this workshop and on a panel entitled "Cyber Peace". We hear so much about cyber warfare these days, and it is healthy to have a discussion of cyber peace and to remind ourselves that it too can be a goal of states and non-state actors alike. Certainly the NGO I represent here today, ICT4Peace, is dedicated to this end.

In addressing the topic of norms of responsible state behaviour in cyberspace, I will start with describing some irresponsible state behaviour. In particular a vicious cycle of action and reaction fuelled by escalating threat perceptions that is rapidly militarizing this unique, human environment.

Ben Buchanan of Harvard University has described this development as creating "The Cybersecurity Dilemma" – the cyber equivalent of the long-standing concept in international relations of the "security dilemma" whereby one state's actions to provide further security for itself prompts reciprocal action by other states which results in diminished security for all. This dynamic is exacerbated by a particular feature of cyber operations whereby: "From a defender's point of view, it is nearly impossible to separate an act of espionage from preparation for war".

After this brief survey of an increasingly militarized cyber landscape, I will turn to the relatively leisurely diplomatic efforts to develop norms of responsible state behaviour. In particular, the Sino-Russian proposal for a *Code of Conduct for Information Security* and the UN process known as Groups of Governmental Experts. I will conclude with some suggestions as how this desultory pursuit of global norms might be reinvigorated and redirected.

War or Peace in Cyberspace?

The fundamental question about this powerful new human-created environment – whether it should be a realm of peace or a domain of war is one that has not been adequately addressed.
For much of its short period of existence cyberspace and its embodiment the Internet has been in the hands of its creators: that community of enthusiasts in civil society, academia and the private sector who were only interested in its effective use and further development.
But as the Internet and its users grew in size and strength, belatedly governments became involved, bringing their particular concerns and priorities, security

prominent among them, to this novel environment. Although at this early stage there may have been opportunities to seek to enshrine a " for peaceful purposes only" doctrine for cyberspace akin to what had been done via international agreement for outer space, Antarctica, and the seabed, this option was not pursued. Instead we had the national security establishments of leading countries project an adversarial struggle onto this arena and opt to develop capabilities for cyber conflict rather than explore possibilities for cooperative security. We have thus seen in recent years the emergence of state conduct that threatens the well-being of humanity at a vast new scale. In his book *The Darkening Web: the war for cyberspace,* Alexander Klimberg describes the expanding scope of the threat that state action can represent for the billions of "netizens". It is a threat that is no longer confined to traditional, destructive weaponry, the so-called "kinetic effects" in military parlance, but embraces new forms of "information warfare" that is especially damaging for open, democratic societies.

The militarization of cyberspace has come about rapidly and without much in the way of public debate or political direction. This in part relates to the origin of state conducted cyber operations within the intelligence agencies that operate under a thick mantle of secrecy. Their objectives of intelligence-collection through covert penetration of foreign computer networks stressed the exfiltration of information without alerting the victim in the process. It was seen as a contemporary version of SIGINT (signals intelligence) and was referred to as CNE (Computer Network Exploitation). This was distinct from the realm of CNA (Computer Network Attack) that entailed the disruption, damage or destruction of computer systems and the data held in them.

The latter (CNA) evolved out of the former (CNE) and the eventual involvement of the military in this sphere was closely linked to the intelligence community. This explains for example why the head of US Cyber Command is also the head of the National Security Agency. While from an initial capability perspective this was attractive to the armed forces it blurred the institutional and legal lines between state conducted foreign espionage and the undertaking by the military of damaging cyber operations against foreign entities.

With the growing involvement of the military in recent years (and this is all occurring within a short time span – US Cyber Command was only set up in 2010) there has been a belated effort to "normalize" this cyber use of force by situating it within an accepted doctrinal framework. This has taken the form of asserting that cyberspace is just another domain for war-fighting alongside the other domains of the land, sea and air. Increasingly this framing of cyber operations is being used by US and allied militaries in their declarations.
It is noteworthy however that even the military is aware that this usage of cyberspace will be contested by some and the latest policy document from US Cyber Command employs the tactic of blaming this development on "the other guy", thus the quote asserting that the US is only responding to a "militarization" of the domain previously carried out by its adversaries.

Threat Perceptions

Of course if one is to justify the pursuit of military superiority in cyberspace it is helpful to have some enemies identified. In the US Director of National Intelligence (Dan Coats) latest presentation to Congress on the global threat assessment, he describes no fewer than four states (Russia, China, Iran and North Korea) "poised for aggression" against the US as well as an unspecified group of "malign actors". It is significant that this assessment and preceding ones since 2013 puts cyber first in its listing of the chief threats to US security. It is worth noting some confusion in the typology being put forward in this assessment: cyber threats are simultaneously depicted as an act of "aggression" (a crime under international law) and as merely a cheap "tool of statecraft", cyber operations are depicted as capable of achieving "strategic objectives" but also simply to enable "propaganda and messaging".

The DNI's world-wide threat assessment marks the growth in the number of states considered to posses offensive cyber capabilities, the Computer Network Attack capacity referred to earlier. From less than a handful of such states in 2007, the ensuing decade has witnessed a steady growth of such capacities with over 30 states now judged by the US intelligence community to possess these offensive capabilities.
The assertion by states of such capacities has not been clear-cut, as several have been reluctant to acknowledge possessing cyber capabilities that go beyond the defensive. In a desire to depict these new areas of operations as essentially benign, states have recourse to various euphemisms. For example the Canadian Defence Policy review outcome document released in June 2017 states that Canada "will develop the capability to conduct active cyber operations focused on external threats". (Well for the layman switching on your computer in the morning is "an active cyber operation" – so why be alarmed?)

The 30+ states now possessing offensive cyber capability are broadly aligned with the leading industrialized states. One reality of developing cyber offensive capabilities is however that they can be acquired without huge investments in human or financial capital (the Iran and North Korean examples are relevant here). The pattern of development of offensive cyber capabilities by states suggests that little thought is given to the eventual consequences of such development on the national interest.

It is noteworthy that in Fred Kaplan's fine account of the history of US development of cyber war capabilities entitled *Dark Territory,* he relates how there was virtually no thought given to the implications of the US unleashing offensive cyber operations including the likelihood of retaliation or the risk of escalation in cyberspace or real space. Kaplan quotes then Secretary of Defense Robert Gates musing aloud that "We're wandering in dark territory".
It was also striking to me, as a former diplomat, that no where in his 300 page book does Kaplan mention any consideration being given to diplomacy to help deal with the emerging threat of cyber conflict among states.

"Someone has crossed the Rubicon"

April 2007 – Estonia: Denial of Service Attacks
September 2007- Syria: Air Defence Radars Blanked
August 2008 – Georgia: Denial of Service Attacks
2010- *Stuxnet* attack on Iranian centrifuges
April 2012-*Flame* attacks Iranian Oil systems
August 2012 – *Shamoon* attacks Saudi Aramco
November 2014 – Sony Entertainment hack
2016 – Disinformation Campaign US Elections
June 2017 – *Not Petya* global impact attack

To illustrate the escalating pattern of malicious activity, I have listed some of the most prominent offensive cyber operations attributed to state conduct in recent years. In this selection there is a major difference between Distributed Denial of Service attacks against Estonia and Georgia, which temporarily crashed several governmental websites in those countries but which did not destroy or distort data and those that entailed deliberate and extensive damage. Such DDOS attacks are essentially disruptive rather than destructive. A hostile act, but not an act of war. The Israeli cyber operation against Syria was in support of the bombing by the Israeli air force of a covert nuclear facility in Syria. The cyber operation was effective in disabling the functionality of Syrian air defence radars (they displayed blank screens to the operators thus enabling the attack to proceed undetected) but did not damage or destroy these systems. This type of cyber attack can be viewed as an extension of earlier forms of electronic warfare designed to disrupt or disable an adversaries communications or surveillance systems.

The "Stuxnet" worm that was directed against the Iranian nuclear program was the first cyber payload that caused the physical destruction of its target (the centrifuges used to enrich uranium) and can be considered the first cyber weapon employed by a state. In June 2012 US officials leaked details of this joint US/Israeli operation code-named "Olympic Games" responsible for the "Stuxnet" attack. Ex-CIA chief Michael Hayden compared it to Cesar's crossing of the Rubicon in terms of its significance for offensive use of cyber down the road. It also means that US claims that it was America's adversaries who first "militarized" cyberspace will be met with some skepticism.

Just before the official leaks regarding Stuxnet but well after private cyber security firms had revealed its existence a new cyber attack named "Flame" was launched against the Iranian Oil Ministry and Oil company destroying the hard drives of thousands of computers. It prompted a retaliatory strike by Iranian cyber units against the Saudi oil company Aramco that resulted in the destruction of data on 30,000 computers. The victim it would seem had found in short order a way to respond in kind to destructive cyber attacks – unfortunately for the status of cyberspace a damaging precedent had been established.

Importantly, this precedent had been set under a cloak of secrecy absent any form of public scrutiny or debate over parameters. While the US was quick to accuse North Korea of the hack of Sony Entertainment in 2014 the Obama Administration had more trouble in characterizing what had happened, some suggesting it was an act of war, while the President himself described it as "cyber vandalism". The Administration was even more rattled during the summer and fall of 2016 with the Russian-led campaign of cyber interference in the US presidential elections. It had to scramble to add "electoral systems" to a list of "critical infrastructure" to be protected against cyber intrusions and an initial expulsion of Russian diplomatic personnel had to be linked to non-cyber activity. Not only had offensive-centric strategies of "dominance" in cyberspace blurred crucial civil-military distinctions, it also enabled the unleashing of psychological/information warfare against which open societies are especially vulnerable. The "Not Petya" attack, utilizing Ukrainian accounting software as its base proved to be the most rapidly propagating malware in history, crippling companies worldwide and causing an estimated USD 10 billion in damages. Tellingly its effectiveness was due largely to an NSA exploit of a Microsoft vulnerability that was part of a trove of highly classified NSA cyber tools that were stolen and released publicly in early 2017. The cyber weapon was turned back onto its creators, although the victims were the private sector and civil society.

Norms of Responsible State Behaviour

The advent of cyber as a weapon has its parallels in earlier introductions of new military technology. States also have a long experience in developing common standards to manage their relations including their conflicts. International security agreements have been concluded to address action in the traditional domains of land, sea and air. Cyberspace however is a unique domain that raises special concerns and because the manifestations of conflict have only recently emerged in this environment, states have generally been slow to address the problem. The focus has been on developing national cyber security strategies, reflecting the priority attached to domestic over foreign issues.

The U.S. was probably the first country to recognize officially the inter-relationship between national and global cyber security with its far-reaching policy statement, "International Strategy for Cyber Space" issued by the Obama Administration in May 2011. The statement called for the development of a global consensus on 'norms of responsible state behavior in cyberspace'. Although the aim was clear the Obama Administration had trouble devising a diplomatic strategy to realize it. The sense of urgency that initially informed the Administration's strategy dissipated and problems in advancing the strategy led the Obama Administration to put it on a diplomatic back burner. Prominent among these were the revelations courtesy of Edward Snowden in 2013 that exposed a massive cyber surveillance and intelligence-gathering program being run by the US. Needless to say these revelations complicated the American appeal to the international community to agree on norms of responsible state behaviour. The desirability of devising some "rules of the road" however did not disappear.

The Sino-Russian Code of Conduct

The diplomatic opening created by the US call in May 2011 for global norms in cyberspace was filled a few months later by China and Russia. These countries submitted at the fall 2011 session of the UN General Assembly a proposed *Code of Conduct for Information Security*. The proposal was cleverly conceived as a set of politically-binding measures designed to appeal to states that opposed international legal instruments in this new field. The code was comprised of eleven actions, most of which were innocuous, but a couple of which were problematic. The suggestion in the 2011 version that an arms control regime be adopted for cyberspace raised definitional issues – what constitutes 'hostile activities" , what are 'information weapons'? Similarly, a state's right to protect its 'information space' a key aspect of both the 2011 and 2015 versions of the *Code* was open to interpretation – would critical commentary by an NGO be considered a 'disturbance' or 'sabotage' of that information space? It doesn't take a veteran diplomat to point out the problematic nature of such ambiguous language if enshrined in an international agreement.

China and Russia have proceeded with caution in promoting their proposal, holding multilateral consultations and circulating in 2015 a revised version. A basic thematic and practical issue inherent in the proposed *Code* is the distinction between the concept of "information security" and that of "cyber security" favoured in the West – the former implying that information content itself can threaten security. Although the intentions of the co-sponsors of the *Code* are not clear, there has been a recent indication that Russia will seek to have the *Code* adopted at this fall's session of the UN General Assembly.

The UN Group of Governmental Experts

Although consideration of cyber security norms have occurred in several multilateral bodies (notably in the OSCE and ARF) the universality of the Internet has made the UN a natural nexus for this diplomatic discussion. Within the UN the principal mechanism for this discussion has been Groups of Governmental Experts (GGE) created by the First Committee (Disarmament and International Security) of the UN General Assembly.. These GGEs normally consist of 15-20 national "experts" that study new issues and offer up recommendations for UN member states. The original mandate of the GGE was to study "existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States". A series of these GGEs have issued consensus reports in 2010, 2013 and 2015. All of these reports have acknowledged that states have an interest in preventing conflicts arising from the use of this technology and have noted that "international cooperation is essential to reduce risk and enhance security".

The reports have also suggested a series of confidence-building measures (CBMs) to "increase interstate cooperation, transparency, predictability and stability". In the 2015 iteration these have included restraint measures such as the non-targeting of

"critical infrastructure" or states' computer emergency response teams (CERTs). They have also encouraged an enhanced level of cooperation to embrace the sharing of information on "vulnerabilities and identified harmful hidden functions in ICT products". These vulnerabilities of course are the very features that states engaged in offensive operations seek to acquire in order to develop cyber payloads to exploit them.

While the GGEs *faute de mieux* perform a certain function in providing a broadly representative forum under UN auspices for the discussion of international cyber security norms their recommendations remain just that in the absence of some official multilateral process to ensure their codification and adoption by states. For many a degree of GGE fatigue has set in and there is concern that the GGE process gives the appearance that the international community is addressing the problem of cyber conflict while actual state behaviour remains largely unchanged. The most recent GGE (20016-17) failed to agree on a report, with differences of opinion on how international law should be applied to state cyber activity being the key matter of dispute. Although Russia may lead again at UNGA this fall a resolution authorizing another round of the GGE, the intrinsic limitations of this mechanism (lack of transparency and inclusiveness being prominent among them) calls into question the continued viability of the GGE process for generating a consensus position on state cyber conduct. Attempting to forge common understandings on the law may also be premature when, as one analyst put it, "the principal questions of the international cyber security discourse are far from settled politically".

Time for a Cyber peace process?

Against a backdrop of relentless "militarization" of cyberspace it is not sufficient to simply call for the development of global norms – a dedicated diplomatic process is necessary to accomplish this task. States will have to move beyond the initial expressions of interest in such an undertaking and agree on a mechanism to negotiate these norms and supporting measures of restraint. Bilateral and regional arrangements involving leading cyber powers, can assist in this enterprise, but they are not sufficient.

The global character of cyberspace suggests that the norms to govern it should ideally be global in nature. This points to a multilateral diplomatic process under UN auspices as the way to progress the endeavour to moderate state conduct in cyberspace. The priority should be given to negotiating cooperative measures to restrain destructive, offensive cyber operations. The threat to international (and human) security posed by destructive state cyber actions should be the focus, putting to one side the issues of state cyber espionage, which are far less amenable to negotiated interstate restrictions.

The language and assumption of cyber war need to be rejected. A civil society statement on cyber delivered at the UN General Assembly last year challenged the trend towards militarization: "it's not too late to turn back the clock. States can

choose to elaborate methods to preserve cyber peace, rather than resign themselves to formulating the norms of cyber war". Cyberspace is an environment that need not be reduced to just another domain for warfare - international cooperation has effectively demilitarized other special environments in the past. The same status could be accorded to cyberspace.

For this to occur a cyber peace lobby must find its voice. Given their huge stake in cyberspace and the strong interest in preserving it for peaceful purposes, it is incumbent on the private sector and civil society to engage. We are beginning to see signs of such engagement (for example the President of Microsoft's call for a *Digital Geneva Convention)* but it will take a much more concerted effort if governments are to be influenced and diplomatic alternatives to inter-state cyber conflict given a chance. A cyberspace dedicated to peaceful purposes and the benefit of humanity is a cause worth championing. Thank you.