Global Cyber Security Norms: A Proliferation Problem?

By Amb. (ret.) Paul Meyer

Global Cyber Security Norms: A Proliferation Problem?

By Amb. (ret.) Paul Meyer

Summary

The international community's effort to develop norms of responsible state behaviour in cyberspace is currently facing a crisis that may also be an opportunity. The crisis is the breakdown of what had been a consensus at the United Nations as to how work on such norms should proceed. The failure of a UN expert group to agree on a report last year and the adoption of parallel and competing processes at this year's General Assembly has cast a shadow on and much uncertainty as to the future direction of inter-governmental discussions.

This situation has however also presented an opportunity for other cyber security stakeholders in the private sector and civil society to highlight their own proposals for norms to govern state conduct. While there may be a risk of norms proliferation down the road, the near-term challenge will be for these stakeholders to find a way to engage states in a process to adopt and implement such norms of responsible state behaviour which they alone can realize.

* * * * *

Not so long ago an analyst of international cyber security policy could write an article entitled "The End of Cyber Norms" suggesting that the failure in June 2017 of a UN expert group to come to agreement meant that "a nearly seven-year process to write the rules that should guide state activity in cyberspace came to a halt". [i] It was perhaps a bit premature to signal the demise of the pursuit of cyber security norms for responsible state behaviour in cyberspace, as the failure of one international process seems to have prompted both an expansion in such processes and the increased role in them of non-governmental entities. We are now facing something of a proliferation of recommended sets of norms which may make it more difficult to gain support from states for implementing any of them. To appreciate what this recent spurt of activity on cyber security norms portend for the future, we must first briefly consider the inter-governmental process that preceded it and for which in part it is a response to.

The UN effort on norm development: the good years

The search for norms of responsible state conduct in cyberspace from an international security perspective originates with a 1998 Russian initiative to have the UN take up the question. Russia and its partners were successful in gaining consensual support within the UN General Assembly for a series of UN Group of Governmental Experts (GGE) to consider "Developments in the Field of Information and Telecommunications in the Context of International Security". The GGEs consisted of 15-20 representatives of member states who would examine the issue, usually over a two year period and report back to the General Assembly if they were able to come to consensus agreement on a report. Three of these GGEs were successful in producing such reports, in the years 2010, 2013 and 2015 respectively.

Already in the 2010 report there was recognition that "States are developing information and communication technologies (ICTs) as instruments of warfare and intelligence, and for political purposes". The first of the five recommendations from the 2010 GGE stated "Further Dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure". [ii] This principal recommendation received further amplification when a leading cyber power, the United States, issued in May 2011 its International Strategy for Cyber Space. This policy statement expressed concern that international peace and security could be endangered "as traditional forms of conflict are extended into cyberspace" and called for the development of an international consensus on "norms for responsible state behavior" in cyberspace. The statement promised early action to achieve this goal: "We will engage the international

community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace..."[iii]

The Obama Administration encountered difficulties in implementing this policy goal and did not seem to have a clear diplomatic strategy for building the international consensus envisioned. The UN GGE process continued to serve as the primary vehicle for the inter-governmental discussion of cyber security norms. This reflected both a recognition that given the universal nature of the Internet, the UN context for developing norms of conduct made sense as well as the fact that the GGE process was yielding results. The 2013 GGE report made notable progress in relating existing international legal norms to state practice by affirming "The application of norms derived from international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability"[iv].

The 2015 GGE report represented something of a high-water mark for the development of thinking as to what norms of responsible state behaviour would consist of. This expanded grouping of 20 states, building on the previous GGE outcomes produced the most elaborated set of "norms, rules and principles for the responsible behaviour of States" that the international community had seen so far. While noting the "voluntary, non-binding" nature of the norms it was recommending, the report set out 11 norms ranging across a wide spectrum of state cyber security activity. Prominent among these norms was one specifying that "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure to provide services to the public;". In a similar vein, authorized cyber emergency response teams were to be immune from attack and also were to be excluded from engagement in "malicious international activity" undertaken by a state. States were also to encourage "responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities..."[v]. Given the rising publicity and concerns regarding malicious state activity in cyberspace during the 2014-2015 period in which the GGE was active, these recommendations appeared to set a high standard for state conduct and an emphasis on the potential of cooperative measures to help "build an open, secure, stable, accessible and peaceful ICT environment"[vi].

The UN effort: the difficult years

The promising result of the 2015 GGE proved elusive when it came to states actually embracing its recommendations. The "lucky streak" of three consecutive GGEs producing substantive consensus reports also came to the end with the 2016-2017 GGE that failed to agree on a report when it concluded its last session in June 2017. Although the opaque nature of UN GGEs (which meet behind closed doors and normally only issue a report at the end of their proceedings if they agree upon one) makes it difficult to ascertain what were the specific impediments to agreement, there are indications that disagreement over how exactly international law was to apply to state conduct was a major cause. As Alex Grigsby has remarked: "While Washington wanted to further develop how concepts such as neutrality, proportionality and distinction might constrain cyber conflict, Moscow and Beijing saw Washington trying to find justifications in international law for the use of cyber means during a conflict or of conventional means as a way to respond to cyber conflict, leading to destabilizing activity". [vii]

If the failure of the 2017 GGE represented a set back for the effort to forge norms of responsible state behavior in cyberspace, what came next at the UN constituted a diplomatic debacle of sorts. During the 2018 fall session of the UN General Assembly's First Committee, states were unable to sustain the tradition of consensus resolutions on international cyber security policy that hitherto had been the basis for the series of GGEs. Instead Russia and the US submitted competing resolutions setting out different processes for future UN work on the subject. The Russian resolution created an open-ended working group (a mechanism open to any interested UN member state) to pursue development of norms with a reporting deadline of 2020. The US resolution adhered to the previous pattern of limited membership GGEs with a reporting deadline of 2021. Although considerations of coherence and economy would have militated in favour of negotiations to produce a single compromise resolution, this in the event was not achieved. The First Committee adopted both resolutions, thus creating two parallel and competing processes at the UN level, which does not bode well for the goal of building an international consensus on a set of norms of responsible state behavior.[viii]

Other stakeholders step forward

With the deterioration of the inter-governmental process at the UN on devising international cyber security norms, a new impetus was given to the efforts of other stakeholders to propose norms to govern state conduct in cyberspace. In particular, the private sector and civil society, with an overwhelming interest in the continued secure operations of cyberspace became more active on this issue. While the private sector had long deferred to governments when it came to discussing any norms to

regulate state conduct (whether as a result of concerns over commercial relations or simply a lack of interest in this sphere is not clear) this silence was beginning to change. An early leader in this regard was Microsoft, which did not shy away from critiquing state behavior or from offering up its own ideas as to what norms should apply to inter-state cyber security activity. Already in 2015 it published International Cybersecurity Norms that proposed six norms for state conduct. Significantly these did not limit themselves to actions to enhance defences, but also addressed the threat of offensive operations. The document supported: "Norms for limiting conflict or offensive operations, which will serve to reduce conflict, avoid escalations, and limit the potential for catastrophic impacts, in, through, or even to cyberspace"[ix]

Microsoft's President, Brad Smith, followed up this initial policy contribution with a high-profile call in February 2017 for a Digital Geneva Convention that would seek to bind states to respect a neutral status for the entire IT industry in a manner analogous to the protective status accorded certain humanitarian entities under the existing Geneva Conventions. In the fall of 2018, Microsoft also launched in collaboration with some relevant NGOs (including ICT4Peace) a Digital Peace Now campaign that aims to mobilize wider public constituencies in direct opposition to state pursuit of cyber warfare and in favour of sustaining a peaceful cyberspace.
Microsoft has also been the prime mover behind the Cyber Tech Accord, which engaged many ICT industry companies in support of a broad set of cyber security principles, including rejection of state cyber attacks against innocent civilians.

Civil society is also finding its voice on the issue of state conduct in cyberspace. At the same 2018 UN General Assembly First Committee session that had produced the rival resolutions on cyber security, 11 civil society organizations endorsed a statement expressing their concern "about the growing militarization of cyberspace and supportive of solutions that move the global community closer to cyber peace…To counteract this trend, states should establish the strongest norms against such operations and not drift into an acceptance or legitimization of problematic emerging practice".[x]

Among other public-private partnerships addressing the challenge of cyber security norms, The Global Commission on the Stability of Cyberspace has issued in November 2018 a set of six proposed norms, which were preceded by two other norms (on protecting the "public core" of the Internet and "electoral infrastructure"). These norms seek to restrict certain types of state cyber action, such as tampering with ICT components or commandeering of ICT devices into botnets, while leaving latitude for other forms of offensive state cyber operations. This careful delineation of acceptable and unacceptable state practices presumably reflects the judgment of the

commissioners of what was feasible in the current international security environment. This blue-ribbon commission has recognized that the articulation of a norm, however relevant and practical, does not suffice for its effectiveness, there is the need to have it implemented. As their document states "A norm works best when the international community is seized by it, when it shapes both the behavior of public and private institutions and the decisions of national leaders, and when it makes clear to all that some actions fall outside the bounds of what is acceptable."[xi]

The most recent contribution to the subject of norms on state conduct is the Paris Call for Trust and Security Cyberspace that was launched in November 2018 during the Peace Forum. A short and carefully worded declaration, the Call builds on existing formulas and affirms that "international law, together with the voluntary norms of responsible State behavior during peacetime and associated confidence and capacity-building measures developed within the United Nations, is the foundation for international peace and security in cyberspace"[xii] The Call is unique to date in being endorsed by a wide array of states, ICT companies and civil society organizations. A diplomatic initiative of France, it perhaps reflects a view that the rupture of the consensus at the UN on how to manage the quest for norms of responsible state behavior has created both a crisis and an opportunity for key actors to engage on this issue. The stakeholders will not want to see this "work in progress" jeopardized by a reemergence of great power rivalry. Despite the success however of the Call in mobilizing a wide cross-section of the concerned stakeholder community, there were conspicuous absentees from the list of states supporting this effort. With major states such as Russia, China, India, Brazil and Indonesia absent from those endorsing the Call, there will necessarily be questions as to its ultimate authority as a normative statement.

Conclusions

For those who care about the future of cyberspace and whether it will be possible to preserve it as a peaceful environment rather than see it transformed into a "war-fighting domain", the current situation must be disquieting. The breakdown in the traditional consensual approach to UN efforts to develop a set of norms of responsible state behavior raises alarm and uncertainty over the status of those norms and confidence building measures that have been generated by the GGE process to date. Clearly an escalation in geopolitical tensions between leading cyber powers and the ongoing militarization of cyberspace (with some 30 states now judged to possess offensive cyber capabilities) does not augur well for states agreeing on a set of norms that will constrain to some degree their cyber operations.

At the same time, the higher profile being given to malicious cyber activity on the part of state and non-state actors alike has prompted greater public attention to and engagement with this problem. It has also spurred a variety of stakeholders to invest in the development of their own proposals for norms of responsible state behavior and to seek support for them in the wider community. While there could eventually be a "proliferation problem" with respect to proposals for norms, leading to a dilution of impact and discord over content, for the moment the handful of substantive proposals that have been brought forward represent a healthy contribution to the norm development effort and a reminder to states that wider interests are monitoring their action (or inaction) on this issue and will hold them to account.

The non-governmental entities that have engaged on the issue of norms of responsible state behavior in cyberspace must appreciate that by definition these proposals will only be effective to the extent that states agree to adopt and implement them. The priority challenge for the wider stakeholder community going forward is to identify the most effective means of persuading states to do just that.

Ambassador (ret.) Paul Meyer is a former career diplomat in Canada's Foreign Service. He is a Senior Advisor for ICT4Peace, an Adjunct Professor of International Studies at Simon Fraser University and a Senior Fellow with The Simons Foundation of Vancouver, Canada.

---

[i] Alex Grigsby , "The End of Cyber Norms" *Survival*, Vol 59 No 6, Dec 2017-Jan 2018, pg 109

[ii] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN* General Assembly, A/65/201, 30 July 2010

[iii] *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World,* The White House, May 2011,pg 4 and 11

[iv] *Group of Governmental Experts on Developments in the Field of Information and* Telecommunications *in the Context of International Security,* UN General Assembly, A/68/98, 24 June 2013, pg 8

[v] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN General Assembly, A/70/174, pg 8

For a comprehensive commentary on the 2015 GGE recommendations see ICT4Peace Senior Advisor Dr. Eneken Tikk's edited analysis: https://ict4peace.org/activities/norms-of-responsible-state-behavior/ict4peace-sponsored-first-global-commentary-on-norms-of-responsible-state-behaviour-in-cyberspace/

[vi] *Ibid* pg 14

[vii] Grigsby, pg 113

[viii] See the author's commentary on these developments: https://www.opencanada.org/features/visions-future-cyberspace-clash-un/

[ix] *International Cybersecurity Norms: Reducing conflict in an Internet-dependent world,* Microsoft Corporation, 2015, pg 2

[x] *Civil society statement on cyber and human security,* UN General Assembly First Committee on Disarmament and International Security, 17 October 2018, (www.reachingcriticalwill.org)

[xi] *Norm package Singapore,* Global Commission on the Stability of Cyberspace, November 2018, pg 7 (www.cyberstability.org)
[xii] *Paris Call for Trust and Security in Cyberspace* , November 11-12, 2018, (www.fdip.fr/call)