ICT for peace foundation

Another Year, Another GGE? The slow process of norm building for cyberspace

When it comes to defining new norms of conduct in the international realm, states move at a cautious pace. When the norms concern a new and unique environment, such as cyberspace, which has seen little regulation to date, the process can at times seem glacial. However, like a glacier, the impact on the international policy environment can be massive.

This fact is worth bearing in mind when readers consider the latest output of a UN Group of Governmental Experts (GGE) concerned with "Developments in the field of Information and Telecommunications in the context of International Security" that yielded a consensus report this summer.

A track record of consensus

The current GGE was comprised of experts from twenty states, selected by the UN's Office of Disarmament Affairs on the basis of equitable geographical distribution, and chaired by Brazil. It held its four one-week meetings over the course of the 2014-15 time period and agreed on its report at its last session on June 26, 2015 (UN GGEs operate on a consensus basis). The group follows closely upon two earlier GGEs that also produced consensus reports in 2010 and 2013. The principal thrust of these reports is similar in content and recommendations: malicious use of information and communication technologies (ICT) can pose a threat to the security and wellbeing of states and interstate cooperation is essential if these threats are to be countered. This in turn will require the development of common understandings, principles and norms of responsible state behavior in cyberspace. To promote these developments a number of confidence building measures (CBM) could be helpful alongside capacity building actions to assist developing states. The 2013 GGE also affirmed that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment". On the basis of these findings from the earlier GGEs the current group was to pursue its study of the general issue as well as consider two additional aspects: the use by states of ICTs in conflict and how international law is to be applied to state ICT usage.

Conflict Prevention

The 2015 GGE report builds on the basic conclusions reached earlier and tries to enlarge incrementally on them while maintaining the necessary ground for consensus amongst a diverse set of participating states. The GGE reaffirmed "that it is in the interests of all states to promote the use of ICTs for peaceful purposes and to prevent conflict arising from their use". While this espousal of conflict prevention as a goal is laudable it also implies that states may not always act in their best interests or those of society at large. The risk that they might not is underlined by the GGE's acknowledgment that there has been "a dramatic increase in incidents involving the malicious use of ICTS by states and non-state actors". Such uses can harm international peace and security the GGE notes even as it flags that military cyber capabilities are growing and it warns that "The use of ICTs in future conflicts between states is becoming more likely".

Norms of Responsible State Behaviour

So what does the GGE suggest to prevent this potential harm to global peace and help reverse these disturbing trends? The offerings appear relatively modest and revolve around the concept of norms for responsible state behavior. The GGE states that "Voluntary, non-binding norms of responsible State behavior can reduce risks to international peace, security and stability." This formulation however reflects some of the underlying tensions behind this aim. Take for example the "non-binding" nature of norms. If states are not going to be bound or constrained in some fashion by norms what are their utility an observer might well ask? So while states espouse norms, some clearly are reluctant to conceive of these norms as an obligatory rather than discretionary commitment and hence the emphasis on "non-binding".

This reluctance also is manifested in the aversion to considering legally-binding agreements for the new sphere of cyberspace on the part of some states that favour the flexibility of political arrangements. Voluntary norms of course could also be contained in an international legal instrument, in the sense that sovereign states would adhere to such agreements only if they chose to do so. The usage of "voluntary" in this context however is intended to reinforce the sense that conforming to any norms is done at the sole discretion of the parties concerned as a political option.

To the degree that voluntary norms or rules are supported, the GGE recommends a constraint on detrimental cyber operations or what the report describes as "ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security". In particular and most significantly the GGE 2015 goes beyond its predecessors in providing specificity regarding the restraint on state conduct it proposes. States are not to engage in ICT activity "that intentionally damages critical infrastructure". Similarly, the GGE proposes that "states should not conduct or knowingly support activity to harm the information systems of another state's authorized emergency response teams" nor should a state use "authorized emergency response teams to engage in malicious international activity".

The nature of restraint

These proposed restraint measures seek to provide a protective status to critical infrastructure and to the cyber emergency response teams that are crucial to mitigating the effects of a damaging cyber attack. In this respect they mirror the protective status afforded civilian facilities and 'first responders' under international humanitarian law, although importantly the GGE proposal extends this protection to peacetime conditions and not limit it to situations of armed conflict. In this sense it expands the focus of earlier GGEs on how international law and especially international humanitarian law applies to cyberspace, and which was concerned with the limits imposed by that law in conditions of armed conflict, to address the appropriate conduct for states in normal times. This broader context for the exercise of restraint by states can be applauded, but it also raises its own set of questions and concerns. For example if a state excludes its authorized emergency response team from engaging in "malicious international activity" does this mean that any other organ of the state is free to do so? While this was unlikely the GGE's intention, it does point to a danger in this norm building process that specifying certain constraints on state conduct of damaging cyber activity can appear to legitimize that conduct in general. That which is not prohibited is permissible can be an unfortunate inference from such preliminary forays into defining what constitutes responsible state behavior in cyberspace.

The GGE recommends several cooperative approaches to strengthening international cyber security if states are willing to adopt them. One suggestion is for states to "prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions". Given the current predisposition of states to harbor and exploit such tools rather than forswear them, this measure could have a real impact if states were actually prepared to cooperate in countering such pernicious cyber tools. A cynical observer might point out that the measure in reality only enjoins states to prevent the "proliferation" or spread of such tools rather than restrict their own development or use of them. The GGE also encourages states to engage in "responsible reporting of ICT vulnerabilities and share associated information on available remedies". Although these are positive aims, the successful implementation of such cooperative measure would seem to depend on a level of confidence amongst leading cyber powers that at the present is lacking.

Confidence Building in Cyberspace

The need to build confidence has been a refrain through all the GGE reports including the present one. The adoption of relevant Confidence Building Measures (CBMs) is reiterated by the GGE, noting that "They can increase interstate cooperation, transparency, predictability and stability". The set of CBMs the GGE recommends repeats many of the earlier proposals although there are some significant new elements. For example states in their “voluntary sharing of national views” are enjoined to include information on “vulnerabilities and identified harmful hidden functions in ICT products”, i.e. the very stuff that states (as well as criminals) fashion their cyber attack payloads from. States are also encouraged to cooperate “with requests from other states in investigating ICT-related crime or the use of ICTS for terrorist purposes or to mitigate malicious ICT activity emanating from their territory”. Again the laudable nature of such information exchange or investigation assistance in theory may well be beyond the current cooperation of states in practice.

To build the levels of trust that could underpin the implementation of some of the more far-reaching CBMs recommended by the GGE will require sustained consultations among states on their cyber conduct. The GGE rightly recommends such activity although its call for dedicated dialogues takes on a very general character: “The development of and support for mechanisms and processes for bilateral, regional, sub-regional and multilateral consultations, as appropriate, to enhance interstate confidence building, and to reduce the risk of misperception, escalation, and conflict that may stem from ICT incidents”. At a time when some key official bilateral dialogues (e.g. US-China, US-Russia) are suspended and no on-going multilateral consultation exists, one can rightly question whether this call represents much more than a pious plea for states to talk to one another about their cyber activity. The GGE recommends “regular institutional dialogue with broad participation under the auspices of the UN”, but it remains to be seen whether UN member states are prepared to establish such an on-going process.

The International Legal Dimension

If the GGE’s results on the tasking to consider the use by states of ICT in conflict are rather oblique (reflecting the conflicted posture major cyber powers are in), the section on “How International Law Applies to the use of ICTs” is more clearly set out. Importantly, it contains language that is supportive of treating cyberspace as a form of “global commons” where state sovereignty is constrained and a primordial responsibility to humanity is explicitly acknowledged. In one of its carefully balanced paragraphs the GGE states: “Underscoring the international community’s aspirations to the peaceful use of ICTs for the common good of mankind, and realizing that the Charter of the UN applies in its entirety, the Group noted the inherent right of states to take measures consistent with international law and as recognized in the UN Charter.” State action must be compatible with the Charter in its entirety (i.e. not just the sections that States might choose to cite) and the overriding goal is one of peaceful use in the interests of all humanity. Of course our cynical observer might remark that such aims are merely “aspirations” of the international community rather than agreed objectives, but it does serve to strengthen a “global commons” status for the special and novel environment of cyberspace.

A central principle of international law is state responsibility and the GGE attempts to reinforce this at several points. It calls for cooperation in investigating malicious activity emanating from the territory of a state and calls on states not to circumvent this responsibility through the employ of surrogates. Specifically the GGE directs that "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non state actors to commit such acts". At the same time and perhaps reflecting the recent public spat of mutual accusations of wrongdoing between the US and China, "the Group noted that the accusations of organizing and implementing wrongful acts brought against states should be substantiated". If states are to be held accountable for possible cyber misuse it should be on the basis of evidence that would withstand scrutiny by the court of global public opinion if nothing more. The GGE consideration of the application of international law does serve to underline the absence of relevant treaty-based governance of cyberspace and of dedicated international tribunals to adjudicate any disputes arising among states.

Next steps

The GGE concludes with a recommendation that a new GGE be established in 2016 with a similar mandate to "promote common understandings on existing and potential threats in the sphere of information security". This recommendation might seem on the surface as a case of a group wishing to perpetuate itself and gives rise to questions as to whether the incremental advances of the 2015 GGE over its predecessors justify another iteration of the GGE. On the other hand, in the absence of any other empowered multilateral process for developing the global norms of responsible state behavior in cyberspace that many advocate, the UN GGEs have taken on a role as a relatively representative mechanism for states to articulate what such norms might look like. Eventually however, UN member states will have to move beyond further studies of the subject to actually taking the decision to act upon the recommendations generated by the series of GGEs. This would entail establishing under UN auspices an inclusive process to negotiate an actual set of norms for state conduct in cyberspace.

To date, there seems little appetite at the UN level to commit to such action. Given the disturbing trends in what the GGE somewhat euphemistically terms "malicious activity" in cyberspace, it is incumbent on states to exert themselves and seek to regulate in some manner state conduct in cyberspace if they truly wish to preserve this critical environment for peaceful purposes. While the easiest path forward may be to simply authorize further group study of the subject, states and other stakeholders interested in preventive diplomacy should consider whether that is an adequate response when the future nature of cyberspace is still so ill defined and the risk of massively disruptive conflict is effectively unaddressed.

*All citations are from the report of the GGE on "Developments in the Field of Information and Telecommunications in the Context of International Security" contained in UN document A/70/174, 22 July 2015.

Ambassador (ret) Paul Meyer is a Senior Advisor to ICT4Peace. He had a 35 year career in Canada's Foreign Service and is currently a Fellow in International Security at Simon Fraser University and a Senior Fellow with The Simons Foundation in Vancouver, Canada