“The UN and the Cyber Security Challenge” - UNOG Briefing March 21, 2014

1. Cyber security has emerged rapidly as a hydra-headed subject that the multilateral system has had to confront and has now begun to address in a substantial fashion.
2. The UN General Assembly ‘s 68th session adopted three major resolutions regarding cyber security, each one generated by a different committee, namely the First on “Developments in the field of information and telecommunications in the context of international security”; the Second on “Information and communications technologies for development” and the Third on “The right of privacy in the digital age”. All of these resolutions addressed cyber security-related themes, yet they did so from the respective perspectives of international security, development and human rights.
3. This fact speaks to the complexity and interrelationship of the issues associated with cyber security, but also underscores the challenge the UN and other multilateral bodies face in trying to come to terms with this multi-faceted subject.
4. Part of the solution to this problem lies in its disaggregation. There is no unified field theory of cyber security and hence no comprehensive solution to the problems it generates.
5. In other words, if we are going to make progress in developing international cooperation on this intrinsically global public policy issue, we will need to delineate specific topics and focus on devising norms and measures relevant to these. Trying to bring into the process too many concerns and priorities is likely to proliferate counter-productive linkages and complicate problem solving in general. Less may be more when it comes to defining the object of our diplomatic efforts.
6. There is some urgency in activating these efforts. Diplomacy has lagged behind developments in the political, military and intelligence spheres which threaten to present the international community with a series of *faits accomplis* that we might prefer to avoid. Cyberspace is a human creation and humans are currently shaping its nature – multilateral diplomacy can and should have a role in determining the character of this new domain.
7. A challenge to that activism is the lack of clarity about what cyber security entails and the confused use of terminology associated with it. The term “cyber attack” is attributed to everything from a sophisticated, destructive cyber payload like Stuxnet to a crude denial of service assault against a website. To some a “cyber weapon” is a frightening, but non-existing armament, while to others it constitutes a piece of electronic surveillance kit that might be put to nefarious ends. We need to start exercising some discipline and precision as to our use of terms. Such clarity will also be a condition for agreeing to eventual arrangements governing this realm.
8. In an attempt to practice what I preach, I will focus on one facet of cyber security, one which I believe is ripe with promise for international cooperation at the same time as it is heavy with the potential for international conflict. This is the international security dimension of cyber security, the conduct of states in their cyber security interactions with other states.
9. The GA’s First Committee has already taken initial steps in this realm, having authorized no less that three GGE’s on the subject, the last two of which in 2010 and 2013 respectively have yielded consensus reports. These reports have usefully pointed the way to further action, in what could be viewed as preventative diplomacy. The latest GGE report notes the increased risk to international peace and security posed by “the absence of common understandings on acceptable State behavior with regard to the use of ICTs” and suggests consideration be given to “cooperative measures that could enhance international peace, stability and security”.
10. The GGE report outlines several important norms for responsible state behavior: i) the applicability of international law, ii) the relevance of state sovereignty and iii) the responsibility of states for unlawful cyber acts carried out on their territory. Beyond norms the report also recommends the “development of practical confidence-building measures to help increase transparency, predictability and cooperation”. It proceeds to enumerate some CBMs such as consultative mechanisms, information exchange and communication links between national Computer Emergency Response Teams (CERTs). While espousing a “regular institutional dialogue with broad participation under the auspices of the UN” the report also encourages action at the bilateral and regional levels as well. It is noteworthy that such parallel efforts have already borne fruit in the form of CBMs agreed bilaterally between Russia and the US and regionally in the context of the OSCE. The report also takes note of the proposal for an international code of conduct for information security that was circulated by the Permanent Representatives of China and Russia, Tajikistan and Uzbekistan at UNGA 66th session in 2011.
11. A further GGE is to get underway later this year and report to the GA’s 70th session in 2015. Its mandate would build on the existing work, but also consider two new elements: the use of ICTs in conflict and how international law applies to the use of ICTs by states. These expert deliberations are significant inputs to multilateral consideration of cyber security, but they are not substitutes for state action itself. Sooner or later, and obviously I would like it to be sooner, states will need to take purposeful action at the multilateral level to translate expert advice into approved norms and measures. Differences of perspective and priority certainly exist and will pose challenges for this multilateral effort, but considerable common ground is also evident. It is time to begin building the cooperative structures that will ensure the cyber security that both governments and their people crave.