Norwegian Institute of International Affairs

Policy Brief
[11 / 2018]

International Cybersecurity: Orchestral Manoeuvres in the Dark

Eneken Tikk & Mika Kerttunen

Summary

Tikk and Kerttunen inform new entrants and nonparticipating governments of the discussions and outcomes of the UN First Committee Group of Governmental Experts (GGE) and discuss prospects for the 2019/2020 GGE. They explain why the Group will not able to provide answers to practical cybersecurity issues facing the majority of states. The authors call states to critically review their reasons for and expectations towards the UN First Committee dialogue on international cybersecurity.

For the sixth time since 2004, an expert group is being convened under the UN First Committee to discuss international security in the context of information and communication technologies (ICTs). The mandate, composition and outcomes of this group are carefully crafted as the UN GGE provides a closed-door negotiation of acceptable and unacceptable behaviour in cyberspace.

A closer look at leading and participating states is useful to get the tone, context and perspective of these negotiations. Russia incepted the format in 1998 with the basic plea that ICTs and the very information itself constitute weapons in the hands of states and a treaty is needed to ban their use.

The main addressee of Moscow's claim is Washington. The US, another permanent member of the UN GGE, has the most advanced military ICT capabilities and a declared appetite to use them. The US also controls a major portion of global communications by way of its ICT and telecommunication infrastructure and industry.

The US superiority also rests on alliances like one with the UK, the main landing of cross-Atlantic cable connections. Together with Canada and Australia, the UK and the US are part of the Five Eyes, the global powerhouse of intelligence.

Essential for the US counter-narrative of a free and open cyberspace and unrestricted flow of information are cyber pioneers like Estonia and the Netherlands that, in the past years, have all shifted the balance between internal and external cyber affairs from socio-economic to politico-military.

Another key player in the game is China. Often aligning with Russia due to its appetite for national level control of information, Beijing shares economic incentives with the US, while at the same time deliberately assimilating itself to developing countries. China might be best placed among the cyber superpowers to offer views that balance the economic, developmental and political features of ICTs. However, to gain at least silent recognition from the US and like-minded, Beijing would have to downplay her claim for strong governmental controls.

The three leading cyber powers have made no secret of their operational interests related to ICTs. While their modus operandi differs, they all share the lack of interest in any international regime that would curb their freedom of operation.

All of the mentioned countries have been among those deliberating security issues in state use of ICTs. Together, they make recommendations to other states about responsible behaviour in cyberspace and call the international community to uphold the rule of international law.

The US has often been accused of exercising a hegemonic position in the development and use of ICTs. In fact, however, each of the leading cyber powers is seeking their own form of digital hegemony, a leading or controlling position to the exclusion of others.

2 Whither process?

At a first glance, the issue in the UN GGE is one of international peace and security – one of developments that, if left unattended at the UN level, would endanger every state's and society's wellbeing and even survival. The Group has, however, not been able to make a compelling case that ICTs carry a threat of that grade.

In this context, the outcomes of five rounds of expert discussions held so far should be read cumulatively. The first attempt, 2004/2005 was too early to find the international community receptive to the destabilizing role of ICTs. After a series of politically motivated cyberattacks against Russia's neighbours in 2007 and 2008 such a conclusion was no longer alien and the 2009/2010 group opened the door to discussing both the threat and possible remedies.

The governmental experts list a number of cyber trends – from intensifying cybercrime to terrorist use of ICTs to supply chain exploitation. However, the link between these developments and international peace and security remains unclear. Detailed and substantiated accounts of the cyber threat, its root causes, consequences and required remedies are missing. Meanwhile, the Group has concluded that cybercrime, terrorist use of ICTs, cyber espionage and data protection do not merit discussion in the First Committee.

Experts' decisiveness in countering the arguable existential threat has been low, indicating no urgency of solution. Indeed, experts have been able to name a few rules and principles of international law, which they consider relevant and useful to mitigating cyber threats. Importantly, these do not cover state responsibility, due diligence, or the protections afforded to civilian population and objects in case of conflict.

In the process, experts have worded a set of 'voluntary, non-binding norms, rules and principles' for the international community to consider. Among these, alarmingly, is adherence to states' international *obligations*.

Thus, acknowledging that some uses of ICTs could endanger international peace and security, the UN GGE has so far not been able to constructively address which exactly and in what way. The past groups have proven nothing but shy of negotiations between diplomats. The ability of opposing sides to circle around their polarization of treaty-no treaty in the 2012/2013 and 2014/2015 rounds is a fine example of diplomacy. Characteristic to this dialogue is also the (lack of) framing of the concepts of international law, norms, rules and principles as well as the exact situation they are expected to remedy.

Curious are the recently expressed positions of some of the leading cyber powers. A 2018 statement of the UK reads that the Whitehall is not convinced of the existence, in international law, of the rule of sovereignty in the context of ICTs, a view to echo the US Cyber Command's thinking.[1] On the other hand, Russia and China attach to a very absolutist reading of sovereignty trumping any international obligations a state has or may have.[2]

Furthermore, the fact that the UN GGE has come to promote voluntary norms of behavior, testifies of no real prospect of consensus. Moscow likely regards the norms process as a stepping stone towards treaty negotiations, while for all countries with operational interests voluntary norms comfortably mean no meaningful restraint in the exercise of their ambitions. Moreover, prioritizing voluntary commitments over international law erodes the respect for the rule of law

in international relations, emphasized by the Security Council as a cornerstone of the maintenance of peace and security. The UN GGE seems to be unwilling or unable to commit to the purposes and principles of the Charter of the United Nations, international law and justice and to an international order based on the rule of law that the Security Council has regarded as indispensable foundations for a more peaceful, prosperous and just world.[3]

Consequently, expecting the UN GGE to strike any decisive clarity in international cyber affairs is a mistake. The Group can only move within very defined margins and only in the interests of states with strong cyber operational ambitions. In the end of the day the question is of controlling information and its flows. For the time being, the US and the so-called like-minded can still lean on their technological superiority. Meanwhile, Russia, China and a number of developing countries keep playing with the prospect of an international treaty process that is likely to invoke stronger governmental controls.

This makes the UN GGE a strategic stabilizing platform. The UN is, once again, hosting a waltz between two worldviews.

Promoting National Cybersecurity

Although cyber powers are occupied with the dance around incompatible worldviews, they are not able to fully ignore what dozens of states have said in their contributions to the First Committee – that cybersecurity issues can (and must), first and foremost, be resolved at national level and that the most burning issues for many countries are those that the UN GGE has excluded from the scope of their mandate.

Yet the UN GGE, without fully recognizing it, embarks on the same premises as most of the states (more than 80) that have so far issued a national cyber- or information security strategy. National cybersecurity strategies confirm that most countries see the formula of cybersecurity, both home and abroad, in cooperation, rule of law and transparency. Leading GGE members, however, can hardly be regarded exemplary on any of these leads.

A careful reading of the GGE reports introduces a roadmap comprising of the proposed confidence-building measures and recommendations. Read together, these measures stress the importance of national resilience, promote awareness and call for enhanced national ICT governance practices. These remedies, however, are no match to the alleged international security threat. Instead, these recommendations and observations speak to very different domestic audiences who have little to no exposure of the politico-military dialogue. In other words, the target audience of the UN GGE introduced measures become national authorities in charge of telecommunications, digital development and cybersecurity coordination.

Amidst the leading cyber powers' quest for digital hegemony smaller and developing countries should not forget that enhancing cyber capacity and resilience remains primarily a national responsibility and task. The international community should also recognize that the available advice - global conferences, academic research and capacity building - often become mere construction of coalitions or delivery of targeted messages about both the issue and preferable solutions. It is equally important to adjust one's effort and expectations to avoid the mismatch between the problem, expected solution and venue of choice.

Improving international cybersecurity

Improving international cybersecurity is more than the sum of all national risks, threat and vulnerabilities. Obviously, international attention should focus on issues of peace and war, prevention of conflicts and their escalation and the continuity of peaceful relations both on-line and off-line. Moreover, to follow a 2015 UN General Assembly resolution (A/RES/70/1), our efforts should pursuit a "world order in which the necessary conditions for the sustainable development of the world are created in its three components - economic, social and environmental".

Participating governments should narrow the UN GGE work to the actual maintenance of international peace and security and the prevention of war and conflicts in the context of ICTs. To achieve this end, we recommend experts of the UN GGE to take the Group's mandate more literally. Experts should define (or agree upon) basic notions related to information security and examine relevant international concepts.

In case the countries want to maintain a broad interpretation of the UN GGE mandate, such talks should effectively engage further states and other stakeholders of cybersecurity.

We encourage governments to use the First Committee process for inserting in the discussion further national views and experience that promote cooperation, improve resilience and uphold the rule of law. National views could have more impact when submitted jointly, for instance in regional and sub-regional settings.

Finally, governments should set examples by implementing the recommendations of the 2014/2015 UN GGE in their national legislation or, wherever possible, by reference to applicable international law. In particular, the permanent, past and future GGE members should show global leadership by explicitly committing to and implementing the Experts' recommendations.

Conclusion

Due to its politico-military framing and strong national aspirations involved, the UN GGE remains unwilling to truly tackle issues of international peace and security and unable to solve the issues of national cybersecurity. This shadow theatre is a careful construction of the leading cyber powers.

The key actors are comfortable with lukewarm results that do not jeopardize their preferred state of affairs, be they domestic or foreign, dark or enlightening. Therefore, countries should not expect the UN GGE, or even some anticipated treaty, to solve their issues of information security, cyber security or cyber insecurity.

The shortcomings of the GGE keep stimulating the calls for a 'cyber treaty'. Paradoxically, the enthusiasm to develop new norms will only amplify these calls. Any new norm proposal reveals factual problems and the lack of explicit normative instruments to deal with them. Norms by nature and character voluntary can only provide sub-optimal solutions that do not in the long run satisfy the demand of predictability and stability in cyberspace. The UN GGE as a venue and process is but an interplay in the long orchestration of world politics.

Governments should be very aware of discussions taking place in this dim First Committee format. The reports and omitted or inserted words and expressions are used to push operational interests and to (re-) interpret the boundaries of possible, preferable and permissible. At stake is the world order and the superpowers' freedom of manoeuvre, more than any particular cyber risk, threat or vulnerability. After all, cyber is just another framing of the many issues that remain unresolved around the development and use of ICTs.

Endnotes

1. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century
2. See for example Niels Nagelhus Schia and Lars Gjesvik, "The Chinese Cyber Sovereignty Concept", http://theasiadialogue.com/2018/09/07/the-chinesecyber-sovereignty-concept-part-1/
3. https://www.un.org/ruleoflaw/files/A-RES-67-1.pdf

Norwegian Institute of International Affairs

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

D.Soc.Sc. Mika Kerttunen is Director of Studies, Cyber Policy Institute (Tartu, Estonia), and Senior Research Scientist at the Department of Software Science, Tallinn University of Technology.

D.Jur. Eneken Tikk is Senior Research Scientist at the Department of Software Science, Tallinn University of Technology.

This Policy Brief is published by NUPI's Centre for Cyber Security Studies. The centre is funded by the Norwegian Ministry of Foreign Affairs.