Search for Cyber Norms – Where to Look?
#2 National Views and Positions in the UN

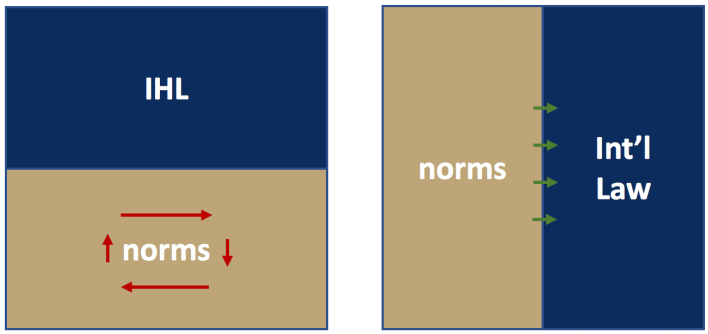
Even though only 38 states have been fortunate to send their experts to the UN GGE, every country has a voice in the cyber norms dialogue. A way to get involved is via national replies to the Secretary-General,[i] views in the broader UNGA discussions, feeds into upcoming consultations, or responding to the call of the UN Secretary-General in the context of Digital Cooperation[ii].

Reading governments' input reveals much more than immediate national positions or recommendations. It reveals a load of assumptions that underpin the cyber norms discourse. Country positions are claims of preferred structure and procedures. They express preferences about how to approach gaps and weaknesses of public international order in the ICT environment.

Before 2014, hardly any government thought of mitigating international cybersecurity with voluntary and non-binding norms – the first public references to this direction are in the Swedish and German contributions in 2014.[iii] It appears that this turn was internalized in and during the GGE and sealed with the 2015 UN GGE report.

In the eyes of the US, the scope of norms is limited to 'peace-time' behavior and any recommendations to that end are to remain voluntary and non-binding.[iv] In the Russian conception, the legal status of norms matters less as they are seen as contributing to the development, over time, of the body of binding international law. As the figure below indicates, in one view the norms dialogue is seen as a self-contained discourse bordering to international humanitarian law (IHL), whereas in the other, it is intended to directly interact with international law more broadly.

Conceptual approaches to cyber norms



The United States | The Russian Federation

There are mainly four angles from which states have addressed "cyber norms":

Conceptual views on norms deal with the question of their normative status and scope. For instance, Germany envisages the process resulting in broad, non-contentious, politically binding norms of State behaviour in cyberspace.[v] Lebanon has put emphasis on unified international standards at the technical level.[vi] Australia has pointed out that new or additional norms for State behaviour must be developed consistent with international law.[vii] In Portugal's view, regulation should primarily stem from international rules.[viii]

Both the Russian and the US conceptions of norms find support in the broader dialogue. Brazil, for instance, argues for a specific legal framework to deal with cybersecurity challenges.[ix] Israel, in turn, has expressed hope that further consensus can be reached on "the voluntary and non-binding nature of new norms".[x]

Countries also engage in the norms discussion by specific **references** to pre-existing instruments, rules and principles. Germany has recommended that states confirm the general principles of availability, confidentiality, competitiveness, integrity and authenticity of data and networks, privacy and protection of intellectual property rights.[xi] Mali has pointed out General Assembly resolution on aggression.[xii] Mexico has made reference to a General Assembly resolution on international terrorism[xiii], as well as the Tunis Commitment.[xiv] The United Kingdom has promoted the global culture of cybersecurity and OECD's "Guidelines for the Security of Information Systems and Networks — towards a culture of security".[xv] Sweden has brought up the International Principles for the Application of Human Rights to Communications Surveillance to assure the legality and legitimacy of any surveillance, while safeguarding the rights of individuals.[xvi]

Of substantive **new norms proposals**, only two contributions stand out: the Dutch call for the protection of the functionality of the Internet[xvii] and Brazil's contribution on a no-first-use norm with regard to offensive operations using ICTs. Such a norm would "reduce the chances of a global ICT-related arms race and reassure the international community that ICTs will not be used as instruments of aggression".[xviii]

Calls for codification are perhaps the most controversial area of norms dialogue. The Code of Conduct on international information security[xix] has been criticized for adding subjective language to established rules and standards of international law.

Several of the above proposals have made it to the texts of the previous UN GGE reports. Here, some correlation can be spotted between national positions and the experts' recommendations. One can observe that the main proposals of states, whose experts have been attending the discussion, have also reached the GGE reports.

When tracking national input, one easily notices that only voluntarism does not even suit all the GGE countries. This scan of national positions leaves little doubt that the preference of UN members is on a binding framework for responsible State behavior.

[i] Under resolutions on Developments in the field of information and telecommunications in the context of international security.
[ii] http://www.un.org/en/digital-cooperation-panel/
[iii] A/69/112 and A/69/112/Add.1.
[iv] The US will promote "adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime" (US NCS 2018). The Department will reinforce voluntary, non-binding, norms of responsible State behavior in cyberspace during peacetime (DOD CS 2018).
[v] A/66/152; A/68/156/Add. 1
[vi] A/62/98
[vii] A/69/112
[viii] A/71/172
[ix] A/C.1/71/PV.4, page 8.
[x] A/C.1/71/PV.4, page 22.
[xi] A/66/152
[xii] A/64/129/Add. 1 (Resolution 3314 (XXIX) of 14 December 1974).
[xiii] 51/210, of 17 December 1996, particularly part I, paragraph 3(c).
[xiv] A/61/161/Add. 1, in particular para 15: "We further recognize the need to effectively confront challenges and threats resulting from use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights."
[xv] A/59/116
[xvi] A/69/112, https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf
[xvii] "States should establish special normative protection for certain systems and networks, including critical infrastructure providing essential civilian services, civilian incident response structures and certain critical components of the global internet, both physical and logical." A770/172, pages 4-5.
[xviii] A/C.1/71/PV.4, page 8.
[xix] A/66/359 and A/69/723.