ICT for peace foundation

The year that cyber peace became non-binding

In 2017, discussions broke down in a UN group of government experts about guarantees of peace and security in the context of the use of information and communication technologies by states. One could have expected an upcurve in 2018. **After all, not only have the UN experts agreed that cybersecurity had become a matter of peace and security – reports of state-sponsored or otherwise government-affiliated cyberattacks keep stacking.** The Center for Strategic and International Studies (CSIS) and the Council of Foreign Relations (CFR) list more than 200 publicly known state-sponsored incidents that have occurred since 2005. The vast majority of these incidents constitute cyber espionage, distributed denial-of-service, data destruction and sabotage. The accounted incidents feature the US, UK, France, the Netherlands alongside Russia, China, North Korea and Iran as state actors with considerable operational interests and capabilities put in use in cyberspace.[1]

Instead, **2018 brought a wave of cyber norms.** The suite started by the UN experts in 2015 has since been followed by G7, G20, ASEAN and others. The Dutch-initiated Kaljurand Global Commission on the Stability of Cyberspace and the Paris Call for Trust and Security in Cyberspace both produce and reproduce recommendations of responsible state behavior. There seems to be a *norm* for everything that could possibly be wrong in cyberspace – against tampering the elections or planting backdoors, against botnets and hack-backs, against proliferation of malicious activities and against letting a state's territory be used for internationally wrongful acts using ICTs. **There are so many norms that their main quality gets lost in the translation – all of them are voluntary, non-binding and not addressing the issue of international peace and security.**

This course of action is confusing. The governments who call and opt for the voluntary and non-binding norms, are also behind cyber operations. Even if we believe that the Western cyber operations are well-meaning and minor, shouldn't the liberal, like-minded governments be much more decisive about the rule of international law applicable to the cyberoperations of others? Given that the vast majority of known state-on-state operations are cyber espionage, widely considered lawful, how can norms offer any effective remedy? Are diplomats trying to do the job that essentially does not belong in their area of expertise? If so, are they perhaps missing, or even undermining, the effort and resources that could be spent on national resilience, public awareness, personal and corporate cyber hygiene, and routine security measures? As curiously, nothing in the CSIS and CFR data points to any real threat to international peace and security that the chosen venue of the dialogue – the disarmament committee – should be occupied with.

Many of these norms propositions come with some very disturbing small print about international law. Not only have the UN experts declared state responsibility and due diligence non-binding. The UK has also singled out sovereignty as 'not a rule but a principle' and therefore no clear threshold to be violated under international law.[2] The violation line, they

1 https://www.cfr.org/interactive/cyber-operations; www.csis.org.
2 https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

argue, runs along 'prohibited intervention', the area of international law, whose clear parameters are variable and challenging to determine.

The most important shift in 2018 involves Russia. Moscow has been a steady proponent of *lex specialis* on international information security. Their 2018 move towards a UN open-ended working group (OEWG), however, reveals an at least temporary settlement on "rules, norms and principles of responsible behavior of States".[3] Although the new resolution elevates the 2015 recommendations from expert consensus into a resolution, it is clear that a lower gear towards treaty negotiations currently suits both Kremlin and the White House.

In sum, 2018 closes with a troublingly wide conclusion that peace, in the context of state use of ICTs is voluntary and non-binding. To believe governments, nothing is wrong in the world when it comes to cybersecurity. For the super powers, the common nominator of peace is absence of a major war. Anything else is optional. In other words, meet the peace as the international community is expected to embrace it in 2019 – an ugly peace, characterized by the state of sub-security, securitization and obscurity.

In this light, it becomes understandable why it does not matter that none of the norms proposed or called for are shared or commonly implemented. States and experts are at this point satisfied with simple normative sentences, wishful thoughts and no clear end game. **They are coming from political promises, with no questions asked about any backing by relevant practices, policies, legislation or jurisprudence – the material, that real expectations of behavior are made of.** Those questions are left to be tackled.

If we take norms proposed by government-appointed experts and prominent scholars at their face value, we can make some predictions towards 2019. According to the Global Commission on the Stability of Cyberspace, we will have to tolerate offensive cyber operations conducted by governments and tampering of products as long as it does not 'substantially impair' the stability of cyberspace. According to the UN Government experts, international obligations are only voluntary in the context of state use of ICTs as is the notion of states preventing their territory to be used for cyberattacks against other states. Pursuant to the Paris Call, hacking back is allowed to states but denied to non-state actors. **Full of levelling thresholds for substantial and unsubstantial damage and justifying government actions, calls remain silent on human rights and basic public order.**

As of 2019, the recently agreed UN open-ended working group (OEWG), acting on a consensus basis, has been called to further develop the rules, norms and principles of responsible behavior of States and the ways for their implementation. Whether the OEWG will be able to accommodate states' actual needs and priorities, remains to be seen as currently, both the US and Russia call for norms, while backpedaling on international law.

3 A/RES/73/27, 11 December 2018.

It is not clear whether one should wish the international community a safe and happy cyber-2019 or should we, indeed, hope for something forcing the governments out of the shadows and from behind each other's shoulder. **Perhaps a happier wish for 2019 is for concerned citizens to rely on paragraph 1.13[4] of the UN Resolution to unite and think of ways to hold governments accountable for not just their actions but also for their inaction.**

Dr. Eneken Tikk, Senior Advisor, ICT4Peace Foundation

Geneva, 31 December 2018
ICT4Peace Foundation

4 1.13. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behavior in information space with regard to their potential role.