DCAF
a centre for security,
development and
the rule of law

CONTEMPORARY CHALLENGES TO PEACE AND SECURITY IN CYBERSPACE

PANEL DISCUSSION

19 NOVEMBER 2015

REPORT

f.l.t.r.: Reto Haeni, Jovan Kurbalija, Gustav Lindstrom, Nils Melzer, Anne-Marie Buzatu

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) organised, in cooperation with DiploFoundation*,* an event addressing *"Contemporary Challenges to Peace and Security in Cyberspace"*, as part of the Geneva Peace Week 2015.

In the introductory remarks, the importance for innovative and successful multi-stakeholder initiatives was highlighted. It was further noted that in order to achieve and maintain an open, free and secure cyberspace, state security and human security have to be balanced in a proper way.

The first presentation addressed the applicability of international law. It was stressed that before going *medias in res*, relevant notions for cyberspace have to be defined, especially because differing interpretations were one of the greatest hurdles. It was noted that even though cyberspace was by some authors seen as the "Fifth Domain" in international law, any cyber infrastructure was necessarily placed in the offline world. As a consequence, States are obliged to comply with existing international law. Having said this, it was noted that it nevertheless remained challenging to apply existing principles and norms of international law straight away to cyberspace, because as a matter of fact, international law was not created for that. Concerning emerging customary international law norms, it was pointed out that cyberspace was a far too young domain. Therefore, no long-standing state practice and *opinio juris* could have evolved yet. Hence, applying existing general principles of international law in analogy was considered as the most promising option. Regarding the question of attribution, it was noted that the actual challenge was *factual* attribution, rather than legal attribution. Last but not least, it was stressed that there was no need for developing new norms or adopting a new cyber treaty; rather emphasize should be put on the existing legal framework. In case the existing legal framework would not provide the proper solution, soft law instruments could be used in supporting closing these gaps.

The following presentation focused on trends, commonalities and outstanding challenges with regard to national cyber security strategies. It was noted that there were common visions across national cyber security strategies, in particular with regard to maintaining a secure, resilient and trusted electronic operating environment, promoting economic and social prosperity, strengthening of resilience mechanisms for critical infrastructure, and combating cyber-crimes. However, it was noted that that due to different interpretations by States, these commonalities appear more diverse. Examples for outstanding challenges were the balancing of competing cyber principles, such as openness vs security. Lastly, it was noted that it was important to keep the correlation between cyber defence and cyber offence in mind when dealing with national cyber security strategies.

The following presentation was headed “One Visit & Three Triangles” and addressed issues concerning digital politics and governance. It was critically noted that major information and communication technology companies were missing at the President Obama’s visit in Silicon Valley, at the beginning of 2015. It was noted, that most challenges related to Internet governance could be clustered around three topics: cybersecurity, human rights, and business & economy. At the same time, it was stressed that these three issues were vital for good Internet governance.

The last presentation addressed the topic from a business point of view. It was noted that the most vital aspect in guaranteeing cybersecurity was trust. Trust between individuals and companies as well as trust between companies and Governments. It was stressed that the most vital elements in order to strengthen this trust were security, transparency, compliance with human rights law and accountability. The fact that companies needed generally three hundred days to detect a breach in their security systems, and that companies and States were always lacking behind, was considered quite concerning. It was called for a stronger engagement of States in cyberspace, not only as a regulatory power but also as a protective power. It was further emphasized that Governments and companies needed to learn from each other and effectively cooperate in order to achieve their common goal, namely an open, free and secure cyberspace, where the rule of law and human rights are respected and protected.

During the discussions, it became evident that challenges in cyberspace could only be addressed through an innovative multi-stakeholder initiative. It was further noted that trust between the different stakeholder, i.e. States, private information and communication technology companies, civil society organizations, was a prerequisite for such a multi-stakeholder initiative. But trust was considered very fragile and it was stressed that certain recent State actions, such as restricting encryption technologies, were highly detrimental to building and maintaining this trust. Nevertheless, it was stressed that international human rights law and the rule of law have to be the basement for any actions in cyberspace.