Private Actors' Self-Help in Cyberspace – Conference Summary

On June 5th, 2019, a conference was organized by the Cybersecurity Institute in Grenoble, France, and entitled *Private Actors' Self-Help in Cyberspace*. Four members of the Federmann Cyber Security Center were present: Professor Yuval Shany, Major-General (ret.) Dan Efrony, Dr. Thibault Moulin and Mr. Nimrod Karin.

A first presentation by Mr Wyatt HOFFMAN (*Carnegie Endowment for International Peace*) underlined that it was necessary to civilize cyberspace (i.e. bringing predictability, rules, and responsible behavior). On the one hand, it was highlighted that the current *status quo* was not working and that – partly due to the risk of collateral damage – reckless hack-back by private companies was not desirable. On the other hand, the main argument of the presentation was that some activities short of 'hack-back' might be acceptable, such as 'self-help'. This means that, to civilize cyberspace, some extent of self-help might be desirable, necessary and unavoidable. It was argued that a large spectrum of activities, more or less disruptive, were conceivable in cyberspace, and that there were situations where corporations should be able to self-help. To the extent that most problems in cyberspace were rooted in the private sector and corporations' decisions, they should not be made totally dependent upon governments. It was also argued that the private sector needs to bear responsibility for the risks it is creating (emerging market of services), that there was an enforcement gap (less than 1% of cybercrime in America result in arrests and indictments, but 90% of attacks might also be avoided with good cyber hygiene), and that actions within the network were acceptable (in contrast with answers outside the network).

A second presentation by Professor Yuval SHANY (*HUJI*) highlighted that international law, by large, underregulates cyber-operations and the ways to react to them. While Tallinn Manual is a convenient starting point, it is often criticized for its definition of use of force, and it appears that most cyber-operations would not qualify as such. There are even controversies regarding sovereignty, and when it is possible to resort to counter-measures. For instance, there is a grey zone surrounding some transborder cyber-operations (theft of data, backdoor theft etc.). Even if economic consequences might be serious, they are insufficient to affirm that lines have been crossed. Another problem allegedly stems from article 52 of the *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. This provision mentions that, before resorting to counter-measures, it is necessary to notify the other party and ask him to change his behaviour. In addition, the responding state must be confident of the source. A problem with cyberspace is that operations are quick, clandestine, and anonymous.

Another problem comes with slave computers, for which automatic hack-back would not constitute an appropriate solution. It was also underlined that limited regulation might come from criminal and civil law, while standards of conducts are emerging (for instance in the financial sector). Retorsions (i.e. withdrawing privilege or benefit) were also presented as a possible solution.

In the continuation of the second presentation, the third presentation by Professor Nicholas TSAGOURIAS (*University of Sheffield*) focused on automatic forms of defence, and questioned their use by private actors. Again, the problems of attribution and proportionality were discussed. It was underlined that, albeit computers can recognize military infrastructures, they hardly recognize dual-use infrastructures or who was behind the attack (a private person? A state?). Likewise, the capacity of a computer in responding in a proportional way was questioned. The main argument was that, unless the computer develops cognitive capacity (i.e. the capacity to reason in complex situation), automatic answer would be unlawful, and there is a need for a human to be on the loop.

The fourth presentation by Mr Nimrod KARIN (*HUJI*) referred to four companies in the USA that admit the resort to self-help (Google, Facebook, SPE and Delta). It was underlined that everyone is contradicting everyone in this field, that no one is elaborating a methodology (including to evaluate the costs of attacks). In a nutshell, international law would be left behind and finding a way to catch up is necessary.

The fifth presentation by Mr. Christian DAVIOT (*ANSSI*, i.e. the National Cybersecurity Agency of France) revealed that every state has an approach of its own with respect to 'what' is hack-back. It was underlined that the best defence was perhaps not an attack. Actually, it appears that organizations lack cybersecurity, that it takes in average 6 months to detect an attack. Usually, companies do not detect attacks themselves, but they are reported by consumers. This issue should thus be addressed, before considering retaliation. It might also be necessary for service providers to be on the battlefield's frontline.

A final presentation by Mr. Laurent BERNAT (*Organisation for Economic Co-operation and Development*) brought light on the role of the Organisation for Economic Co-operation and Development, which is to help governments with the development of better policies (rather than intelligence or law enforcement).