On 10 December 2017, the Cyber-Security Research Center of the Hebrew University of Jerusalem held an international workshop on the Tallinn Manuals on Cyber Operations. The workshop participants included former and current senior practitioners, legal advisers of governmental agencies and ministries, academic experts in international law, and cyber-technology experts. The discussions were held under Chatham House Rules (non-attribution of interventions to specific speakers).

At the beginning of the workshop, the following legal, political, and technological developments were introduced by way of relevant background for the discussions:

- The cyber domain is the only physical domain that has been created, developed, and shaped by human technology. Hyper-connectivity and almost unlimited capacity for action beyond borders, in full anonymity, pose a very serious threat to cause a high level of harm on par with dramatic kinetic means (including weapons of mass destruction). This is an evolving field of activity that affects human behavior and vice versa.

- As of June 2017, more than half of the world’s population, almost 4 billion persons out of 7.5 billion, are global internet users, and two thirds of the world’s population, almost 5 billion persons, use cell phones, mostly smartphones. These figures are increasing. All of them are connected and dependent on the services of global IT mega-companies.

- IoT (the “internet of things”) is spreading rapidly and AI (artificial intelligence) is no longer a matter of science fiction. In a few years IoT and AI will be major features in the virtual world. The Dyn 2016 cyber-attacks using IoT, and resulting in multiple DDoS (distributed denial-of-service) and massive financial losses, marked a new milestone as it became apparent that IoT could easily be weaponized to cause vast and varied types of harm.

- Terrorist organizations such as ISIS have been exploiting cyberspace – mainly social networks but also games consoles – in order to spread their propaganda, recruit supporters, and operate terrorist cells. States and Non-
State Actors use IT technology to spread false information and to manipulate social and political processes. It has already been used to influence the results of elections.

- There is no full consensus concerning the applicable law governing cyber operations, and even less regarding questions of accountability. Initiatives such as the UN Governmental Group of Experts, which was launched two decades ago, reached a dead end in June 2017 when the “Western group”, led by the US, and the “Eastern group,” led by Russia and China, failed even to agree on the basic proposition that international law is applicable to cyberspace. Given that technology advances permanently, whereas the law remains somewhat stuck in the past, the gap between the two has been widening and deepening. Consequently, every individual, group, corporation or nation that has free access to the internet and can covertly exploit the network’s vulnerabilities can achieve many of their goals, be they criminal, commercial, political or national, while ignoring traditional legal restrictions, such as sovereignty, and without the risk of paying a heavy price for doing so.

- Given the inability to obtain broad international cooperation in updating international law through new regulation (international convention), the Tallinn Initiative is the most significant attempt to codify lex lata as the specific international groups of experts (IGE) understand it. Both IGEs made no claim to offer a “silver bullet” manual, and even the rules embraced by the groups through consensus are not necessarily acceptable to the broader international legal or political community as reflecting binding rules of international law.

- One way forward to deal with growing risks to national security posed by cyber operations may be the creation of alliances of like-minded states who could develop joint defensive and reactive capacities.

The general approach expressed by most participants is that international law is applicable to cyber operation. However, in the absence of explicit international regulation, state practice is likely be the leading method in (a) creating new standards, and (b) adapting to cyberspace existing standards originally developed to regulate physical domains. The latter approach would most likely follow the Tallinn Manuals path, i.e. interpreting traditional regulation in an adaptive manner, including by means
of analogy (law-by analogy). The former approach would create a tailor-made legal framework for a digital and deterritorialized domain differing substantively from the regulation of physical-territorial domains.

The participants were mostly of the view that great difficulties will be faced in determining whether state practice has developed in one of the two aforementioned tracks, and even more so, which path has been taken. The main reason for this is the problem of **ambiguity**. In order to protect their national security interests, states intentionally resort to ambiguity regarding policy questions (legal and political) in the context of cyber operations, including with regard to any involvement – defensive or offensive – they have engaged in on cyberspace that might be indicative of their practice or legal policy. Thus, their basic approach is to reduce transparency to the minimal possible degree.

Given this ambiguity and the lack of credible information about cyber operations, it is almost impossible to attribute a legal stance to a state due to its response or lack of response to a cyber-operation conducted against its territory or interests. The thresholds for the use of force or armed attack have not yet crystallized in state practice, and neither have the legal requirements attendant to the principles of sovereignty and due diligence. As in other realms of international law, it will probably take time and the recurrence of significant incidents (in quantity and levels of gravity) to gradually remove that ambiguity, partially or fully.

Meanwhile, the workshop participants noted several topics that could be developed and clarified, despite the policy of ambiguity. The following questions were raised in this regard:

**The use of force** – Should the Tallinn Manual’s narrow approach regarding physical damage as a requisite component in defining the threshold of use of force or armed attack be extended to include damages such as the destruction or severe disruption of data (including by DDoS) in the function of critical infrastructure, and how wide should the definition of “critical infrastructure” be? How should the international community treat global cyber-attacks? Should there be one cumulative threshold for severity or multiple state-by-state thresholds?
Countermeasure response – Should countermeasure means and conditions as included in the Articles on Responsibility of States be extended to include non-state actors who use cyberspace to attack states from the territory of another state? And even when the host state due diligence requirements are implicated, what would constitute a proportionate counter-attack? Judge Simma’s opinion in the ICJ Oil Platforms case was mentioned as a possible basis for hack-backs and other uses of force short of an armed attack.

The attribution process – According to the current laws of armed conflict and state practice, there is no procedural law of evidence or a specific standard of proof which oblige States when executing their military plans and attacks, which mostly rely on confidential intelligence. Should the same standards apply to cyber operations? Or alternatively, should new and specific standards of proof be developed regarding forensic attribution process? Would it be better to integrate a new international agency in the attribution process that is both professional and independent?

The IT Industry – IT giant companies such as Google, Apple, Microsoft, Amazon, and Facebook, are considered superpowers due to their leverage and influence as indispensable tools for every internet user around the globe. This renders those IT companies a most effective facility for collecting technical and non-technical data that could be used to thwart cyber-attacks and to attribute responsibility promptly and accurately. Should the international community look for appropriate ways to integrate those companies in its efforts to assure security and stability in cyberspace? What means should be adopted to ensure the maintenance of due balance between human rights and national security in connection with such efforts?

Espionage – Relying essentially on long and well-established state practice, cyber espionage is considered unlawful if it entails violations of domestic law, though it is not per se unlawful under international law. Cyberspace has dramatically enhanced national espionage capabilities. A significant portion of cyber activities could be considered as espionage. Should states define the legal framework governing espionage? What should be included and permitted under such a framework, and what should be excluded and thus prohibited? For example, how should one treat the theft or destruction of data without the option of recovery as opposed to the copying of data?
Click here to see the photos from the Tallinn Manuals Workshop