The Cyber Domain, Cyber Security and what about the International Law?

Dan Efrony

During recent centuries, the history of mankind has witnessed many significant innovations with huge impacts on individual and collective behavior. Yet, the law has been successfully adapted to those innovations, although such process of adaptation often takes time and is met with resistance. Cyber is, however, much more than a specific innovation such as the print machine or others. It is a new and unique environment, often called "cyber domain" or "cyber space" or "cyber sphere" and defined, mostly the same[1] (Hereinafter - the "cyber domain").

The gap between the existing International Law and the activity in cyber, is deep and wide - hard to be bridged solely by interpreting and applying the current law, as it is originally oriented to physical or 'kinetic' activities in the other domains such as, land, sea, and air.

The cyber domain is a new creation; a fifth domain, being added to the well-known four, namely, land, sea, air and lastly, space which became accessible to mankind in the middle of the 20th century. While these four domains are the components of the cosmos, the fifth is a human creation – a pure on-going technological development with continuous and significant impacts on the whole universe. The cyber domain also differs from other domains by its unique characteristics which have a direct and a great influence on the activities within the cyber domain. Our focus rests on two main characteristics; first, the **boundlessness** of that domain. cyberspace does not have physical or geographical borders. It exists and plays major and vital roles in each of the other domains,

[1] **Cyber Domain** - A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Source: Department of Defense Dictionary of Military and Associated Terms

Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants. (https://www.techopedia.com/definition/2493/cyberspace)

Cybersphere the realm of information technology and electronic communication, especially the Internet.

(https://en.oxforddictionaries.com/definition/cybersphere) affording them a technological infrastructure. Any significant activity in any domain and in any field of life currently relies on cyber infrastructure. Thus, in the short time required for tapping on a keyboard, one can destabilize the foundations of our society, completely dissolving fundamental human rights and democratic values. As an example, the rights to privacy and property have already been adversely affected in this global and boundless world. Every digital tapping is exposed to powerful entities which make the most out of digital traces and other forms of digital data - to reveal, analyze and utilize one's personal preferences and habits, fields of interests, intellectual assets, and even health status.

The threats are not limited to fundamental rights and values but even to physical existence. Every kind of transportation in each of the other domains (air, land, sea, and space) can be compromised, paralyzed, or even destroyed through manipulation of cyber-dependent infrastructure. National financial systems could be crushed and countries brought into bankruptcy. All these threats are not theoretical. They could be executed, in the twinkling of an eye, by irresponsible cyber superpowers operating in a hazardous playground. It is pointless to describe the chaotic potential consequences of activities such as these.

Secondly, the ability to **anonymously** execute any cyber operation in any dimension, holds no price or risk to the perpetrators. This creates legal problems, as the operation cannot be attributed to a specific individual, organization, or state. This unique characteristic has the most influential and decisive role in making the enormous threats, such as those mentioned above, tangible, and easily executed.

Bearing in mind this backdrop the Tallinn Project - the Tallinn Manual on the International Law Applicable to Cyber Warfare, and the revised and extended version, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - proposed a full set of rules and principles to regulate the cyber domain, above and below the threshold of use of force, both in time of armed conflict and in time of calm. Although the International Group of Experts did not pretend to provide the international community with a perfect proposal, ready to be accepted as binding rules, one cannot overestimate the importance of this initiative in triggering and inspiring international efforts, to meet the essential challenge of regulating and enforcing law and order in the all-encompassing cyber domain. This is especially so, since the international community, through its institutions, such as the UN and others, have not yet succeeded in promoting a professional international process, aimed at meeting that challenge.

The Tallinn Project is an important step albeit an insufficient one. Unfortunately, many doubts, reservations, questions, and more importantly, threats, remain unresolved, following the prevailing ambiguity that stems from lack of knowledge - on the technical level and consequently on the legal level. Moreover, very frequently, an ambiguity is deliberately being used, to mitigate the risk of disclosing secret cyber capabilities. It also restrains countries, specifically the most influential ones, from collaborating with one another in a manner displaying a high level of mutual trust and transparency, although their goal should have been to reach international agreement on the sustainability of the global structure, inter alia, national, and international structures.

The complexity and the peril of the situation as described above, have been rapidly increasing in conjunction with never-ending technological developments and the growing involvement of various players, mostly unknown, who assume significant roles in the global net, reflecting a variety of tangible risks with hardly any constraints.

During the recent decade, the international community has witnessed and experienced a great deal of problematic incidents and developments occurring in this unique domain. Almost each of them has exemplified the risky global situation and could be considered a wake-up call for an urgent change in the strategy of action, adding to the passive-defensive approach a proactive approach, relying basically on international cooperation to take the lead, and ultimately introduce binding rules in that domain.

Having said that, the coincidence that occurred this week, might or should be a turning point. On May 11,2017 President Trump issued a US presidential executive order on cybersecurity, titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The executive order is in line with the prevailed perception on focusing combined national efforts on defense strategy with the option of strengthening it by an international cooperation. ("The Secretary of state shall provide a report to the President…, documenting an engagement strategy for international cooperation in cybersecurity"). The day after, unprecedented cyber-attacks were launched simultaneously, aimed at civilian institutions, some of which related to critical facilities, in one hundred countries and even more. According to the press, the scale of the cyber - attacks was the largest ever conducted while the consequences are still unknown. Would the International community change the current mode of operation by overcoming political obstacles and adopting a proactive approach in the realm of international law as an essential component in assuring cybersecurity? Or would it continue to adhere to the reactive approach, waiting for an inevitable 9/11 cyber catastrophe, to push it sooner rather than later to do what should and must be done without further delay? Time will tell.