Short Commentary on Cyberwar and Cyberpeace in International Pugwash Workshop

Mehrnoosh Farzamfar, LL.B., M.Soc.Sci, LL.M. in International and Comparative Law
E-mail: mehrnoosh.farzamfar@helsinki.fi

It is a privilege for me to have this opportunity to present a short commentary on the challenges of international law in dealing with the issues of cyber space and cyber war in this workshop. For the next 10 minutes, I will address what international law could possibly offer as alternatives to the shortcomings of Tallinn Manual on regulating cyber space and cyber war.

It is an undeniable fact that in today's world, cyber operations are powerful tools for States, non-State actors and individuals to convey their political or strategic messages. We are all aware that unfortunately not all these operations are deemed to be for peaceful purposes. That is why in late 2009, the NATO Cooperative Cyber Defence Centre of Excellence invited a group of twenty international law scholars and operational legal advisers, under the leadership of Professor Michael Schmitt of the United States Naval War College, to conduct a three year research project examining the norms applicable during cyber war. The product of this effort is the "Tallinn Manual on the International Law Applicable to Cyber Warfare", published in March 2013 by Cambridge University Press.

Tallinn Manual was designed as a reference tool for State legal advisors, policymakers, and operational planners. It is also a very good brain exercise for scholars and students. However, this document has visible gaps. Its greyest area is to identify the laws applicable in cyberspace and to objectively explore the various interpretations of that law, which States might wish to adopt. What this manual suffers the most is 'lack of enforcement'. In the hierarchy of sources in international law, it is categorized as so-called "soft law". Hence, it does not have the enforcement mechanisms which international agreements have. States are generally unwilling to bind themselves to what they have not expressed their explicit consent to.

Alternatively, although the international law in general does not address the issue of military operations within cyberspace, this does not necessarily mean that cyber space and cyber warfare could not be regulated by the international humanitarian law or the laws of armed conflict. There is no specific mention of cyber warfare or computer network attacks in the Geneva Conventions or their Additional Protocols. But the principles and rules in these treaties governing the means and methods of warfare are not restricted to situations that existed at the time of their adoption.

International Humanitarian Law clearly anticipated advances in weapons technology and the development of new means and methods of waging war. For example, Article 1(2) of the 1977

Protocol I Additional to the 1949 Geneva Conventions provides that in cases not covered by the Protocol or other international agreements, civilians and combatants remain protected under the authority of the customary international law, the general principles of international law, the principle of humanity and the dictates of public conscience. To give an example, I shall remind you of the decision of the International Court of Justice (ICJ) in its advisory opinion on the legality of the threat or use of Nuclear Weapons. In its decision, the ICJ held that the absence of regulation on the use of nuclear weapons and nuclear warfare in the 1949 Geneva Conventions and its Additional Protocols does not prevent the applicability of the international humanitarian law or the customary international law in this regard.

It is worth mentioning that Tallinn Manual has been indeed a pioneer by explicitly classifying cyber attacks as a use of force, in Rules 10 and 11, once they reach 'the scale and effects of a kinetic use of force'. What it means by 'the scale and effects of a kinetic use of force' is that the attack causes injuries or kills people or damages and destroys objects. These Rules make it clear that a cyber attack committed by a State's armed force is a military operation which would constitute a use of force. Therefore, cyber-attacks like other armed conflicts need to respect the principles of armed conflict, meaning the principles of distinction, proportionality and pre-caution. Sub paragraph b of Article 8(2) of the Rome Statute of the International Criminal Court is the elaboration of these principles, according to which it is prohibited to intentionally launch attacks on civilian individual or population who do not take part in hostilities or against civilian objects which are not military objects.

In addition to the issues of enforcement and identifying applicable law, if a State has been the victim of an unlawful cyber use of force, the question of reprisal and responsibility arises. Most commentators so far have focused merely on the shortage of the law enforcement in Tallinn Manual, and regrettably little attention has been paid to the law of State responsibility. Tallinn Manual briefly touches upon this subject in Rules 6 to 9. However, as set forth in Articles 22 and 49 to 53 of the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts, victim States are entitled to resort to ***non-forcible countermeasures*** in reaction to internationally wrongful acts committed by offending States. While these Articles do not enjoy treaty status, the customary right of States to exercise countermeasures, subjected to various limitations, is confirmed by this jurisprudence.

In conclusion, we need to bear in mind that at the end of the day it is up to the States to choose which law they want to practice, especially in matters where controversy exists, like interpretation of applicable laws. States must comprehend that their actions and counter-actions in the cyber space inevitably has significant influence on civilian objectives.