Cybersecurity Law

HANDOUT – CYBERSECURITY AND CYBER-DEFENCE

John F. Murphy, Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests? 89 Int'l L. Stud. Ser. US Naval War Col. i 2013:

Similarly, according to a recently released document, "[t]he United States will oppose efforts to broaden the scope of the ITRs (International Telecommunication Regulations) to empower any censorship of content or impede the free flow of information and ideas."
In sharp contrast, during a meeting in 2011 between then Russian Prime Minister Vladimir Putin and ITU Secretary-General Dr. Hamadoun Touré, Putin reportedly told Touré that Russia was keen on the idea of "establishing international control over the Internet using the monitoring and supervisory capability of the International Telecommunications Union." It is hardly surprising that countries like China and Iran would support Putin's proposal. But it is at least disappointing to learn that democratic countries like Brazil and India reportedly "share the belief that the Geneva- based UN agency the International Telecommunications Union (ITU) would do a better job if put in charge of international cyber-security, data privacy, technical standards and the global web address system."
In response to the Russian challenge, at least within the U.S., condemnation of the ITU's dangerously amateurish behavior has been universal. Republican and Democrats, Congress, the White House and the FCC [Federal Communications Commission], along with major industry representatives, consumer advocates, and engineering groups including the highly-respected and international Internet Society, have all raised alarms over both the content and the process of upcoming negotiations.

Rule 92 – Definition of cyber attack
A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

10. Within the International Group of Experts, there was extensive discussion about whether interference by cyber means with the functionality of an object constitutes damage or destruction for the purposes of this Rule. Although some of the Experts were of the opinion that it does not, a majority of them was of the view that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components. Consider a cyber operation that is directed against the computer-based control system of an electrical distribution grid. The operation causes the grid to cease operating. In order to restore distribution, either the control system or vital components thereof must be replaced. The cyber operation is an attack for the majority.

13. The International Group of Experts discussed the characterisation of a cyber operation that does not cause the type of damage set forth above, but that results in large-scale adverse consequences, such as disrupting all email communications throughout the country (as distinct from damaging the system on which transmission relies). The majority of the Experts took the position that, although there might be logic in characterising the operation as an attack, the law of armed conflict does not presently extend this far. A minority took the position that should an armed conflict involving such cyber operations break out, the international community would generally regard them as attack. All Experts agreed, however, that relevant provisions of the law of armed conflict that address situations other than attack, such as the prohibition of collective punishment (Rule 144), apply to these operations.

14. Notwithstanding disagreement over the precise definition of 'attack' in the cyber context, the International Group of Experts agreed that not all cyber operations qualify as attacks. For instance, it is clear that the term does not encompass cyber espionage per se unless the means

or method by which it is conducted cause consequences that qualify as an attack (Rule 89). Moreover, it should not include cyber operations that would be akin to jamming because 'the jamming of radio communications or television broadcasts has not traditionally been considered an attack in the sense of [the law of armed conflict]'. In this regard, the Experts noted general agreement that cyber operations that merely cause inconvenience or irritation to the civilian population do not rise to the level of attack, although they cautioned that the scope of the term 'inconvenience' is unsettled.

Rule 93 – Distinction
The principle of distinction applies to cyber attacks.

1. The 1868 St Petersburg Declaration provides that 'the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy'. This general principle is the foundation upon which the principle of distinction is based. The principle of distinction is one of two 'cardinal' principles of the law of armed conflict recognised by the International Court of Justice in its advisory opinion on the Legality of the Threat or Use of Nuclear Weapons. The other is the prohibition of unnecessary suffering (Rule 104). According to the Court, these principles of customary international law are 'intransgressible'.

Rule 110 – Weapons review
All States are required to ensure that the cyber means of warfare that they acquire or use comply with the rules of the law of armed conflict that bind them.
States that are Parties to Additional Protocol I are required in the study, development, acquisition, or adoption of a new means or method of cyber warfare to determine whether its employment would, in some or all circumstances, be prohibited by that Proto- col or by any other rule of international law applicable to them.

8. With regard to both lit. (a) and lit. (b), the fact that a supplying State has already reviewed a method or means of cyber warfare does not relieve an acquiring State of its obligation to consider the means by reference to its own international law obligations. In complying with this obligation, the acquiring State may consider a legal assessment conducted by the supplying State, but retains the obligation to satisfy itself as to compliance with the legal rules by which it is bound. A determination by any State that the employment of a weapon is prohibited or permitted does not bind other States.

9. The determination of the legality of a means or method of cyber warfare must be made by reference to its normal expected use at the time the evaluation is conducted. f a means or method of cyber warfare is being developed for immediate operational use, the lawyer who advises the commander planning to use it will be responsible for advising whether the cyber weapon or the intended method of its use accord with the State's international law obligations. Any significant changes to means or methods necessitate a new legal review. A State is not required to foresee or analyse possible misuses of a cyber weapon, for almost any weapon can be misused in ways that would be prohibited.

13. The Experts recognised that there may be significant difficulties in accumulating sufficient and reliable information on which to base the legal review. For instance, replicating in advance the environment in which a new cyber weapon is intended to be used can be problematic, thereby frustrating such activities as advance testing and computer modelling. Nevertheless, they agreed such difficulties do not relieve States of the obligation to review the lawfulness of new cyber weapons.