Cybersecurity Law

HANDOUT – CYBER-GOVERNANCE AND INFORMATION SOVEREIGNTY

A Declaration of the Independence of Cyberspace by John Perry Barlow:

(…) We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

(…) You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

(…) Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

Tallinn Manual 2.0, Rule 1:

2. A well-accepted definition of 'sovereignty' was set forth in the Island of Palmas arbitral award of 1928. It provides that: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'

4. For the purposes of this Manual, the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty. The physical layer comprises the physical network components (i.e., hardware and other infrastructure, such as cables, routers, servers, and computers). The logical layer consists of the connections that exist between network devices. It includes applications, data, and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities.

6. The fact that cyber infrastructure located in a given State's territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty. Indeed, States have the right, pursuant to the principle of sovereignty, to disconnect from the Internet, in whole or in part, any cyber infrastructure located on their territory, subject to any treaty or customary international law restrictions, notably in the area of international human rights law (Chapter 6).

Tallinn Manual 2.0, Rule 2:

2. A State's sovereignty over cyber infrastructure and activities within its territory has two international legal consequences. First, the cyber infrastructure and activities are subject to domestic legal and regulatory control by the State. In particular, the State may promulgate and enforce domestic laws and regulations regarding them. Second, the State's sovereignty over its

territory affords it the right under international law to protect cyber infrastructure and safeguard cyber activity that is located in, or takes place on, its territory.
6. In addition to authority over the physical layer, the principle of sovereignty affords States the right to control aspects of the logical layer of cyberspace within their territories. For instance, a State may promulgate legislation that requires certain e-services to employ particular cryptographic protocols, such as the Transport Layer Security protocol, to guarantee secure communications between web servers and browsers. Similarly, a State may legislatively require electronic signatures to meet particular technical requirements, such as reliance on certificate-based encryption or that the certificates include certain information, such as their cryptographic fingerprint, owner, or expiration date.
7. As to the social layer of cyberspace, a State may regulate the cyber activities of those on its territory, including both natural and legal persons. For example, a State may criminalise the posting of material such as child pornography or that which incites violence online. It must be cautioned that State censorship of, or restrictions on, online communications and activities are subject to applicable international human rights law (Chapter 6).
11. A few of the Experts were of the view that States are also entitled to exercise sovereign rights, including jurisdiction, over government data and that of their nationals stored or transmitted outside their territory, subject to specific restrictions imposed by international law.12 For these Experts, a State's sovereignty over data that is stored or in transit abroad can exist independently of its sovereignty over cyber infrastructure located in its territory and the persons and activities therein. The majority, by contrast, took the position that States do not enjoy such sovereignty over data located abroad unless international law specifically so provides, as in the case of data stored aboard certain objects like warships. They acknowledged, however, that a State may, in certain circumstances, exercise prescriptive jurisdiction over data located outside its territory (Rule 10).
12. Sovereignty not only affords rights, but imposes legal obligations, 13 such as that requiring the exercise of due diligence to terminate harmful cyber activities emanating from a State's territory (Chapter 2).

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue - A/HRC/17/27.

51. Cyber-attacks, or attempts to undermine or compromise the function of a computer-based system, include measures such as hacking into accounts or computer networks, and often take the form of distributed denial of service (DDoS) attacks. During such attacks, a group of computers is used to inundate a web server where the targeted website is hosted with requests, and as a result, the targeted website crashes and becomes inaccessible for a certain period of time. As with timed blocking, such attacks are sometimes undertaken during key political moments. The Special Rapporteur also notes that websites of human rights organizations and dissidents are frequently and increasingly becoming targets of DDoS attacks, some of which are included in the first addendum to this report.
52. When a cyber-attack can be attributed to the State, it clearly constitutes inter alia a violation of its obligation to respect the right to freedom of opinion and expression. Although determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult, it should be noted that States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future.