Research seminar
«Reshaping Public International Law in the Age of Cyber: Values, Norms and Actors»

THE INTERNATIONAL LEGAL PRINCIPLE OF NON-INTERFERENCE AND DETERRENCE OF CYBER OPERATIONS

Professor Vera Rusinova, LL.M. (Goettingen),
National Research University "Higher School of Economics"
vrusinova@hse.ru

THE INTERNATIONAL LEGAL PRINCIPLE OF NON-INTERFERENCE AND DETERRENCE OF CYBER OPERATIONS

1. Legal qualification of cyber operations under the non-interference principle
2. State practice in respect of cyber operations
3. Analysis and concluding remarks

1. Legal qualification of cyber operations under the Non-interference principle

- **the content of the Non-interference principle and a dichotomy of states' will**

- **rupture between patterns of state behavior at the domestic (legal and political) and international levels**

- **extreme underinclusiveness of the 'two-pronged test' of the Non-interference principle in respect of cyber operations:**
  - ***domaine réservé***
  - **coercion**

1. Legal qualification of cyber operations under the Non-interference principle

- **underinclusiveness of the two-pronged test:**

(1) *domaine réservé*:

- **'matters in which each state is permitted, by the principle of sovereignty, to decide freely' *(ICJ, Nicaragua case, para. 205)***
  - **meddling into the elections**
  - **cyber attacks on banks, TV stations, oil plants, business companies, etc.**

1. Legal qualification of cyber operations under the non-interference principle

- **underinclusiveness of the two-pronged test:**

(2) coercion:

"no State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind." ***(Friendly Relations Declaration, 1970)***

1. Legal qualification of cyber operations under the non-interference principle

- **underinclusiveness of the two-pronged test**

(2) coercion: ***for what purpose*?**

- **cyber-attack on biggest US banks in 2012:**
  an Iranian revenge?
- **hacking attack on the German Bundestag in 2015:**
  Russians to spoil the image of German political leadership?
- **the hacking of the Sony Pictures in 2014**
  financial compensation + cancellation of the release of "The Interview" – North Korea?
- **the DDoS-attacks at Estonian web-sites in 2007:**
  a revenge for removal of the Bronze soldier statue?
- **the NotPetya virus in 2017:**
  a 'part of the Kremlin's on-going effort to destabilize Ukraine and demonstrate ever more clearly Russia's involvement in the on-going conflict'.

THE INTERVIEW MOVIE, SONY PICTURES

1. Legal qualification of cyber operations under the non-interference principle

➢ Principle of sovereign equality: a principle or a rule?

- **Tallinn Manual: Rule 4 – Violation of sovereignty**

  A State must not conduct cyber operations that violate the sovereignty of another State.

- **designation of 'critical infrastructure' at the national level**

- **The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of 2015**

  a prohibition to commit cyber attacks of critical infrastructure as one of the recommendations for 'voluntary, non-binding norms, rules or principles of responsible behaviour of States'

2. State practice in respect of cyber operations

1) Diversity of the attribution tracks

2) Official qualification of cyber operations

3) Responses of the victim states

4) Typical reaction of the alleged sponsoring states

2. State practice in respect of cyber operations

1) Diversity of the attribution tracks

A) an official attribution to a concrete state:

- cyber attack to Sony Pictures (2014)
- *WannaCry* ransomware (2017)
- cyber attack at Estonian web-sites (2008)
- hacking attack against German Bundestag (2015)
- cyber attacks against Ukrainian electric power stations (2015 and 2016)
- meddling into the US Presidential elections (2016)
- release of the medical files of WADA related to international athletes (2016)
- *Petya/NotPetya* and *Bad Rabbit* viruses (2018)

2. State practice in respect of cyber operations

1) Diversity of the attribution tracks

B) a general attribution:

- **South Korea, "DarkSeoul", 2013**

The Minister of Defense: "we cannot rule out the possibility of North Korean involvement, but we do not want to jump to a conclusion".

- **Attacks against Saudi Arabia and Qatar (Shamoon, 2012-2017 and Triton, 2017):**

'Iran is the only country that has attacked us repeatedly and tried to attack us repeatedly. In fact, they try to do it on a virtually weekly basis'.

- **Attacks against Russian governmental web-sites:**

Press Secretary of the President D. Peskov (2019): 'Russian structures including the Russian presidential website have regularly experienced cyber attacks from the US and Europe'.

2. State practice in respect of cyber operations

1) Diversity of the attribution tracks

C) no official attribution:

- **Saudi Arabia 2012, attack against the biggest oil company Saudi Aramco**: no attribution to Iran, no legal qualification;
- **Attack against leading financial institutions of the US in 2012 (Ababil or Swallows operation)**: no attribution, no reaction in respect of Iran;
- **US Office of Personal Management attack in 2014-15**: no official attribution, China announced the arrest of two suspected hackers.
- **Attack at Iranian oil and gas pipelines and plants in 2016**: no attribution and qualification.

2. State practice in respect of cyber operations

2) Legal qualification: prevalence of the 'soft' techniques

- **Hacking attack against German Bundestag**, **2015:** Teresa May – Russian 'influence campaign'.
- **Cyber attack at Sony Pictures in 2014:** in the statement for press – 'lawless acts of intimidation' which 'demonstrate North Korea's flagrant disregard for international norms', and is 'an attempt to suppress free speech, which is at the center of America's values and a founding principle of the Bill of Rights'.
- **The meddling into the US Presidential elections, 2016**: Obama to Putin: "International law, including the law for armed conflict applies in cyberspace". Nonetheless, later: Russian actions "undermine *established international norms of behaviour*, and interfere with democratic governance".
- **Attacks against Ukrainian electric power stations in 2015 and 2016**: President Petro Poroshenko: 'direct and indirect involvement of secret services of Russia, which have unleashed a cyberwar against our country'.

2. State practice in respect of cyber operations

3) Responses of the victim states

- **Retortions:** economic sanctions, expel of diplomats;
- **'Hacking back':**
  - after the Sony Pictures incident in December 2014 the North Korea internet network was shut down for 9 hours and became blocked for 2 days
  - Shamoon 1 and 2 operations against Saudi Arabia - the 2016 cyberattacks on Iranian petrochemical facilities - Shamoon 3 and 4 and the Triton operations
  - US cyber attack on the Russian NGO "Internet Research Agency" (a "fabric of trolls")
- **Criminal prosecution:** in the USA, Czech Republic, Estonia, China.

3. Analysis and concluding remarks

- an extension of the scope of legal prohibitions or

  a mixture of both legally binding and also non-binding rules?

  - the deterrent function of the Non-interference principle
  - counter-measures as not a practical tool for cyber operations
  - retortions as a deliberate choice of a more advantageous path