



TECHNICAL AND JURIDICAL PROTECTION OF INFORMATION INFRASTRUCTURES - International legislation in cyber space –

Cybersecurity Romania - Bucharest Talks,
June 4, 2019 – Bucharest, Bucharest University of Economic Studies

Features regarding **cyber space**

Cyber space is characterized by threats against **CRITICAL INFORMATION INFRASTRUCTURES**

Cyber threats can be classified, according to their nature and results, in **CYBER OPERATIONS** and **CYBER ATTACKS**

A question to which specialists and literature in cyber security are trying to answer - **ARE CYBER THREATS SIMILAR TO ARMED ATTACKS?**



CYBER THREATS

CYBER OPERATIONS

Cyber operation is defined as the **employment of cyber capabilities** with the primary purpose of achieving objectives *in* or *by* the use of cyber space.

CYBER ATTACKS

A cyber attack is a **cyber operation**, whether offensive or defensive (self-defence), that is reasonably expected to cause **injury or death to persons, or damage or destruction to objects.**

Applying Law in **cyber space**

JURISDICTION IN CYBER SPACE

- ❖ States have jurisdiction over the ICT infrastructures located within their territory;
- ❖ In their use of ICTs, states must conform to the principles of international law (state sovereignty, sovereign equality, non-intervention in the internal affairs of other states etc.);
- ❖ States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts (*due diligence*).

ONU

JURISDICTION APPLIES
IN
CYBER SPACE

—2015—

SOVEREIGNTY

—

During a cyber attack, the state which launched the attack is violating the **SOVEREIGNTY PRINCIPLE** – meaning, one state *should not interfere with the internal affairs of another state* - otherwise, the attacked state has the right to use **countermeasures** in its defense.



Countermeasures apply gradually, according to the threat level (starting from *unfriendly acts* to *self defense*).

States can act in **self-defense** when the cyber attack against them:

- **constitutes a breach of international obligation;**
- **is attributable to a state.**



Cyber attack attribution



!! It is *one of the main challenges* taking into consideration the complex technology and the resources that a cyber attacker can use (mainly, a state actor) in order to *hide its identity*.



A state is entitled to act in *self-defense* with regard to an armed attack (*kinetic or otherwise*).

Condition: a state must be responsible for the attack in order to apply international law – firstly, the following questions should be answered to:

- **Who** is attacking and on what basis?
- If the attack is initiated by non-state actors, are they getting any *state support*?

Cyber attack attribution



!! The attribution of cyber attack is ESSENTIAL – international law applies only to those attacks attributed to **states, and not to individuals or groups.**

- *Example:* a company or a hacker group conducts hostile cyber ops to compel state to adopt policy – not intervention, unless “attributable” to a state (international law does not apply)



The obligations of the state who launched the attack and was discovered:

1. ***Cease the cyber op***, if it is continuing (ex: on-going DDoS attack);
2. Assurance and guarantees of ***non-repetition***;
3. ***Full reparation*** (injury includes material and moral damage).

DUE DILIGENCE

—

States have the obligation to **not allow their territories** (or cyber infrastructures under their governmental control) **to be used for purposes against international law**, and they must exercise all measures for preventing such situation.

⊘

There are three involved parties:

1. **TARGET STATE** of the attack
2. **TERRITORIAL STATE** – its territory is used for launching the cyber attack
3. **AUTHOR STATE** of the cyber attack

*Case study: A hacker group located in state A that carries out a destructive cyber operation against state B using cyber infrastructure located in state C. Therefore, state C must take all the feasible measures to put an end to the operation (otherwise, it is **violation of due diligence**).*



“Blame and Shame” initiatives

!! **DETERRENCE BY DENIAL** – *public exposure and coordinated attribution* of cyber attacks conducted or sponsored by state actors.

- 2018: UK and Netherlands – **public attribution campaign** of the cyber attacks initiated by state actors from Russia
- *Result:* the association of **APT28/SOFACY group** with the military intelligence service of Russia – **GRU**.

The purpose:

1. **Public exposure** of the "irresponsible" actions and hybrid threats conducted by Russia;
2. **Gaining support** from international community;
3. **Reducing Russia's credibility** on international level;
4. More **severe sanctionary measures** for Russia.

Cyber Diplomacy Toolbox

The cyber threats conducted by state actors may constitute **wrongful acts under international law** which can give rise to a joint EU response – “*the cyber diplomacy toolbox*”

Conflict prevention



Mitigation of cyber threats



Greater stability and cooperation
in international relations



Influence the behavior of potential
cyber aggressors



Purpose

Use of measures

Measures within the **Common Foreign and Security Policy**

Restrictive measures

Proportionate with cyber attacks

Conclusion

- *International law enforcement **CANNOT SUBSTITUTE** the network security measures in order to rise the **RESILIENCE LEVEL***
- *The measures conducted and achieved by EU should determine Romania, and the other member states as well, to take action in cyber space:
SCOPE: prevention, before intervention.*
- ***COOPERATION** – the key for assuring cyber security.
Public organizations will need to find incentives to get to **partnership** with all the key parties in order to promote and support **national and international cooperation.***





Thank you!