SOVEREIGNTY

Cybersecurity Law

HISTORICAL DEVELOPMENT

- Key concept
- Location, time frames
- Thomas Hobbes (Leviathan, 1651) → six elements of sovereignty
    - legislation
    - adjudication
    - making war and peace
    - allocating offices
    - reward and punishment
    - aassigning ranks and honors
- Hugo Grotious (1583 – 1645)
    - *“the acts of the sovereign executive power of a directly public kind are **the making of peace and war and treaties** and **the imposition of taxes** and other exercises of authority over the persons and property of its subjects, which constitute the sovereignty of the state.”*

HISTORICAL DEVELOPMENT

- The highest, final decision-making authority, which lent its holder power over others → the highest independent power of disposition
- Sovereignty X Jurisdiction?

LOTUS CASE (1927)

- *" the first and foremost restriction imposed by international law upon a State is that - failing the existence of a permissive rule to the contrary - it may not exercise its power in any form in the territory of another state."*
- Jurisdiction to prescribe → it is the power of a state to assert the applicability of its national law to any person, property, territory or event, wherever they may be situated or wherever they may occur.
- Jurisdiction to enforce

- Physical concept → normative concept
- But sovereignty itself is founded upon the fact of territory → Why?

HISTORICAL DEVELOPMENT

- International law is reactive
- Reduction of territorial exclusivity of the state in international law
- A process of change → statehood is eroding → need for security → creation of supranational organizations
- *Is any state sovereign?*
- Form of external control
- Internal X External aspects (Malcolm Shaw)
  - supremacy of the governmental institutions
  - supremacy of the state as a legal entity

SOVEREIGNTY IN CYBER CONTEXT

PRINCIPLE OR PRIMARY RULE?

- Does it make any difference?
- If sovereignty is not a primary rule of international law, then it is not itself susceptible to violation
- Primary rules impose either obligations or prohibitions on States
- Foundational principle from which primary rules such as the prohibitions of intervention and the use of force emanate

- The level of use of force

PRINCIPLE?

- Reflections of the unique aspects of the cyber domain
- When does a cyber activity constitute a use of force?
- Does sovereignty only guide state interactions? Or does it dictate results?
- The principle of sovereignty does not establish an absolute bar against individual or collective state cyber operations that affect cyberinfrastructure within another state
- Sovereignty is a principle, subject to adjustment depending on the domain and the practical imperatives of states rather than a hard and fast rule

PRIMARY RULE?

- Sovereignty as a principle rejects any directly operative effect of the principle itself
- Other regimes are premised on territorial integrity and inviolability
- Judicial treatment
- State practise and Opinio juris
- International fora

JUDICIAL TREATMENT

- Lotus case (1927)
  - When a State acts without the territorial State's consent, the former is in breach of an obligation owed the latter to respect its sovereignty
- Corfu Channel case (1949)
  - The ICJ dealt with accusations of violations of sovereignty
- Nicaragua case (1986)
  - The ICJ again faced the issue of territorial sovereignty
- Parties never asserted the absence of a primary rule prohibiting violations of sovereignty.

STATE PRACTISE AND OPINIO JURIS

- Political statements
- Georgia and Russia (2009)
- Russia and Ukraine (2014)

SOVEREIGNTY IN INTERNATIONAL FORA

- UN
- GGE (2013 report)
  - “State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.”

CONCLUSION

If we desire to determine an act as an internationally wrongful act than the breach of an obligation must be contained in a primary rule of international law

TALLINN MANUAL

- NATO CCD COE
- Any differences between Tallinn Manual 1.0 and 2.0?
- Tallinn Manual 1.0
  - jus ad bellum (the use of force by States)
  - jus in bello (regulation of the conduct of parties engaged in an armed conflict)
- Tallinn Manual 2.0
  - Cyber operations during peacetime
- Is it an official document? Source of law?

Rule 1 – Sovereignty (general principle)

The principle of State sovereignty applies in cyberspace.

"The principle of State sovereignty applies in cyberspace."

- States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure
- Various layers
  - Physical
  - Logical
  - Social
- No State may claim sovereignty over cyberspace per se → why?

Rule 2 – Internal sovereignty

A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.

"A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."

- **Two legal consequences**
  - Cyber infrastructure and activities are subject to control by the State (enforcement of laws)
  - The right to protect cyber infrastructure and safeguard cyber activity that is located in, or takes place on, its territory (ISP's server)
- **Logical layer**
  - A State may legislatively require electronic signatures to meet particular technical requirements
  - To employ particular cryptographic protocols to guarantee secure communications between web servers and browsers

"A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."

- **Social layer**
  - Child pornography
  - Incitement to violence
  - Any problems?
    - Censorship
  - Blocking access requires limits
    - Non-discriminatory
    - Authorised by law
- *"The authority of a State to independently decide on its political, social, cultural, economic, and legal order."* (Nicaragua judgement)

Rule 3 – External sovereignty

A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.

"A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it."

- Where does it come from?
- Article 2(1) of the UN Charter

  The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

  (1) The Organization is based on the principle of the *sovereign equality* of all its Members.
- A State is independent in its external relations and is free to engage in cyber activities beyond its territory subject only to international law
- The freedom to formulate foreign policy
- The freedom to decide whether to opt into specific cyber treaty regimes

Rule 4 – Violation of sovereignty

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

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

- A scenario
  - A corporation is the target of a malicious cyber operation by a State
  - The corporation hacks back
  - Does the corporation violate the state's sovereignty?
  - Is it lawful? → such operations are likely to violate the domestic law of States having jurisdiction over the persons or activities involved
  - Plea of necessity, self-defence

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

- Private infrastructure
  - The State A conducts cyber operations that cause damage to the cyber infrastructure of a private company located in the State B
  - Does the State A violate the state's B sovereignty?
    - → Rule 2!
- Physical presence in a State
  - An agent of the State A uses a USB flash drive to introduce malware into cyber infrastructure located in the State B
  - Does the State agent violate the state's B sovereignty? → attribution!

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

- Is intent decisive?
  - Cyber operations often affect States other than the State on whose territory the targeted cyber infrastructure is located
  - Such cyber operations do not usually constitute violations of sovereignty BUT
  - It could breach other norms of international law (international trade law)

Rule 5 – Sovereign immunity and inviolability

Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty.

" Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty. "

- The cyber infrastructure aboard the platform in question must be devoted exclusively to governmental purposes
- Sovereign immunity entails inviolability → any interference with an object enjoying sovereign immunity constitutes a violation of international law
  - A denial of service against a State's vehicle
- Are there any limits?
  - The obligation to respect the sovereignty of other States
- Immunity does not prevent the other States from taking those actions that are lawful, appropriate, and necessary