SOVEREIGNTY IN CYBERSPACE

Hebrew University
Jerusalem
6 December 2017

Principle of Sovereignty

- "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."

  PCA, Island of Palmas (1928)

- External element
- Internal element

Sovereignty and Cyberspace

- Territorial versus “borderless”
- 5th domain?
- Global common (*res communis omnium*)?

State Pronouncements

- UN GGE 2013 report
  - “State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities ...” (pt. 20)
- UN GGE 2015 report
  - “[T]he Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; ...” (pt. 26)
  - “State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities ...” (pt. 27)
  - “In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, ...” (pt. 28(b))

Respect for Sovereignty

- Non-democratic States
  - Control of their “information space”

- Liberal democracies
  - Protection of statehood, independence

Respect for Other States' Sovereignty

- View 1: International law obligation
- View 2 (a few agencies): Sovereignty is underlying principle of international law, but not a primary rule

- Only binding on States
  - Note opposing argument

- Both public and private cyber infrastructure protected

Territorial Integrity and Inviolability

- Borders are inviolable
- Traditional examples
  - Unauthorised entry to airspace
  - Exercise of enforcement jurisdiction absent consent

- Question in the cyber context – when do remotely conducted cyber operations violate the target State's territorial integrity?

Territorial Integrity and Inviolability

- Physical damage
  - Stuxnet-like consequences
- Functional damage
  - Repair or replacement of physical components
  - Reinstallation of the OS or other data?
  - Precise threshold unsettled
- Infringement on territoriality without physical or functional damage

Territorial Integrity and Inviolability

- Violations of territorial integrity and inviolability?
  - Close access cyber operation to insert malware into target system
  - Causing the target cyber infrastructure to permanently stop functioning by overheating hard drives
  - Remotely operating inside cyber infrastructure with the system slowing down
  - Remotely deleting governmental census database / encrypting census database with ransomware
  - Remotely operating inside cyber infrastructure and extracting files
  - Probing for open ports

Inherently Governmental Functions

- Based on a State's exclusive right to perform inherently governmental functions
  - Examples: Delivery of social services, conduct of elections, collection of taxes, conduct of diplomacy
- Interference
  - Example: Persistent DDoS attacks against governmental online resources
- Usurpation
  - Example: Remotely performing law enforcement functions, such as taking down botnet infrastructure, without territorial State's consent

Cyber-Specific Issues

- Unintended consequences?
  - Intend to engage in espionage, but accidentally cause functional damage
- Target State's effective defences?
  - Intend to cause functional damage, but target State effectively defends its systems
- Severe economic consequences without a violation of territorial integrity?
  - Example: Op v. SWIFT banking system in another State

Cyber-Specific Issues

- Transmitting of propaganda, conducting information / influence operations?
- Significant impact on the functioning of the internet?
- Cyber operation manifests on cyber infrastructure located outside the affected State's territory?
  - Governmental data stored abroad

Derivative Principles

- Due diligence
- Jurisdiction
- State immunity
- Prohibition of intervention
- Prohibition of use of force

Principle of Due Diligence

- “[I]t is every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States”

ICJ, Corfu Channel (1949)

Case Study – Estonia 2007

State Pronouncements

- UN GGE 2013 report
  - “States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.” (pt. 23)
- UN GGE 2015 report
  - “States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs” (pt. 13(c))
  - “States ... should seek to ensure that their territory is not used by non-State actors to commit [internationally wrongful] acts” (pt. 28(b))

Threshold of Harm

- Cyber operations that affect the rights of, and produce serious adverse consequences for, other States
  - Cumulative
- Rights of another State
  - Recall *Corfu Channel*: "[I]t is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."
  - Example: State A launches destructive malware against State B's oil pipeline, thereby causing an explosion. The malware reports back to State C. State C is aware of the operation.
    - Right of State B?

Threshold of Harm

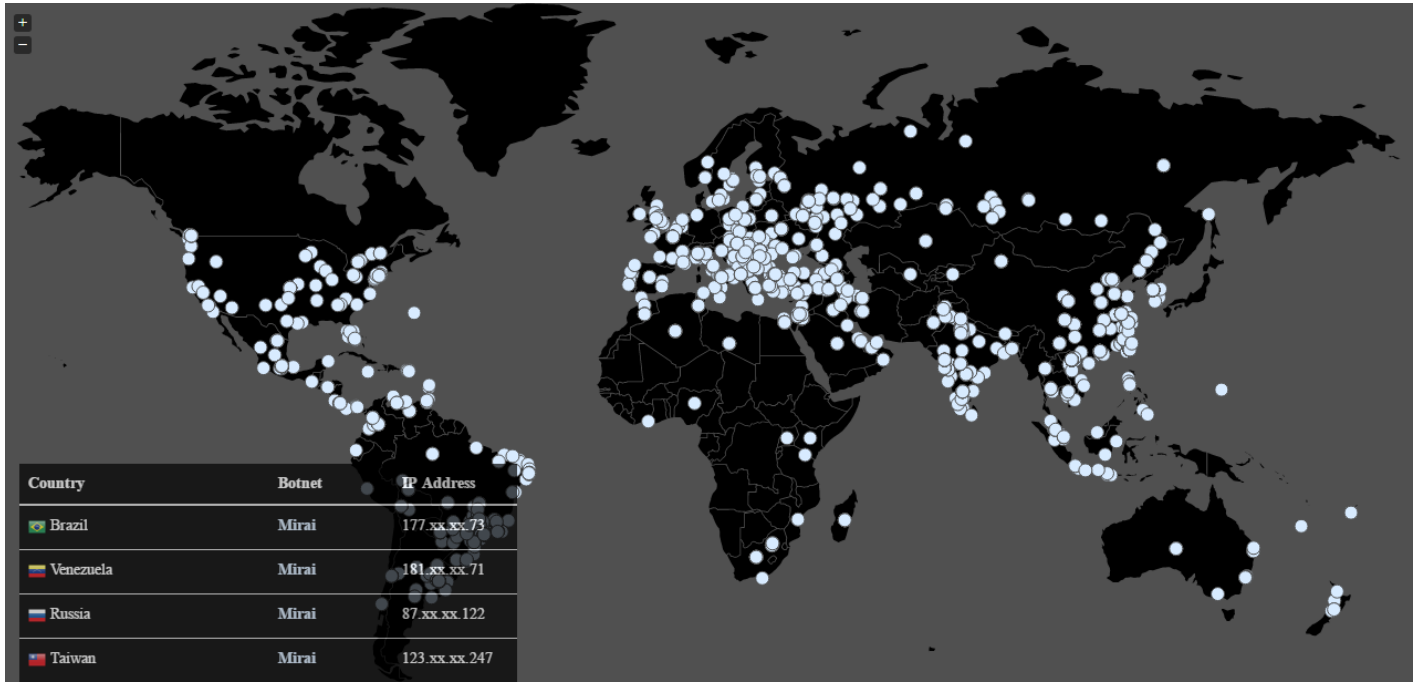
- Rights of another State cont'd
  - Example: State A is in possession of State B's highly classified documents concerning State B's military capabilities. State A makes the documents publicly available via a server that is located on State C's territory. State C is made aware of this fact. Publication of the documents causes serious adverse consequences for State B.
    - Right of State B?

Threshold of Harm

- Rights of another State cont'd
  - Example: State A and State B have concluded a treaty not to conduct cyber espionage against each other. State A designs malware that extracts classified data from State B's systems and sends them to a server on State C's territory. State C knows of the operation.
    - Right of State B?

Threshold of Harm

- Serious Adverse Consequences cont'd
  - Example: transnational botnet



© MalwareTech

Action Required from Territorial State

- Territorial State must stop the harmful activity that occurs from its territory
- Harmful cyber operation that is about to be launched?
  - Example: intelligence agencies have infiltrated a closed online forum and find out about a destructive operation that will be launched soon.

Obligation to Stop Harmful Activity

- Obligation to take general preventive measures?
  - Adopt domestic legislation, set up a CERT, adopt information security policies, raise the public's awareness about information security, monitor cyber communications ...?
  - Problem with the knowledge requirement
    - Territorial State cannot know of potential harmful cyber operations that will occur in the future

Breach of Due Diligence

- Failure to take feasible action
  - Inaction
  - The taking of ineffective or insufficient measures when other measures are feasible
  - Example: State does not require ISP to stop providing services to a customer from whose infrastructure large-scale DDoS attacks are being mounted
- Domestic legal restrictions do not excuse non-compliance

Breach of Due Diligence

- Obligation of conduct, not obligation of result
  - Territorial State does everything feasible, but the target State nevertheless suffers harm → obligation has not been breached
- Territorial State not required to suffer unreasonably in order to avoid harm to another State
  - Example: State has human intelligence that a severe cyber operation will be launched, but does not know its exact signature and timing. The only way to avoid the cyber operation would be to isolate big networks from the internet, thereby causing “self-denial” of service with significant financial consequences

Miscellaneous

- Territorial State finds out about an imminent cyber operation of which the target State is unaware
  - Issue: sharing of sensitive information, thereby revealing capabilities
  - Must stop, but does not need to inform target State
- State that is “unable”
  - Does it need to request assistance from other States if it lacks the capacity to stop the harmful cyber activity?

QUESTIONS?