States’ Behaviour and Sovereignty
International Law and Cyberspace

Lisbon 22 June 2017

Karine BANNELIER
Associate Professor, University Grenoble-Alpes
AMNECYS (Alpine Multidisciplinary Network on Cybersecurity Studies)
Worrying Trends
Increase of Malicious Cyber-Activities & Cyber-Attacks

Cyber-Activities & Cyber-Attacks Involving States and Non-State Actors

• A major source of tensions between States

Cyberspace = a “No Law’s Land”?

• UN GGE: “International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment”

Karine Bannelier
States’ Behaviour and Sovereignty
International law and Cyberspace

I. Cyber-diligence as a Key Concept in Preventing Transnational Malicious Acts

II. Responses to Cyber-Attacks and Malicious Acts

III. The Problem of Hack-Back
What is a “Cyber-Attack”?

Canada:

“Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information”

United Kingdom:

“The term cyber-attack can refer to anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as: gaining unauthorized access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)”

Karine Bannelier
State Sovereignty at the Heart of the Concept of Cyber-Diligence

- **UN GGE:** “State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory”
- **ICJ, Corfu Channel Case 1949:** “every State [has the] obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States”

Responsibility of States for Transnational Attacks & Damage

Usefulness of Cyber-Diligence in the Face of Malicious Cyber-Activities and Cyber-Attacks

- **UN GGE:** “States should seek to ensure that their territory is not used by non-State actors to commit such acts”
- **UN GGE:** “States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs”
Cyber-Diligence as a Responsible & Reasonable Standard of Behavior

An Obligation of Conduct and not of Result
- The degree of vigilance expected is that “of a good Government”

Cyber-Diligence & Human Rights
- UN GGE: “State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms”

A Common but Differentiated Responsibility
- UN GGE: “Different levels of capacity for ICT security among different States can increase vulnerability in an interconnected world”

Karine Bannelier
Preventing Cyber-Attacks and Protecting Critical Digital Infrastructures

**The Role of International Organisations**

- UN, OCDE, OSCE, UA, UE...
- UN Security Council Resolution 13 February 2017: *Protection of Critical Infrastructures against Terrorists Attacks*

**The Need of a Public/Private Partnership**

**The Problem of the Trade in Zero-Day Vulnerabilities**

Karine Bannelier
II. Reactions to Cyber-Attacks

States’ Responses to Cyber-Attacks
The Framework of International Law

- Reactions Always Available
  - Mechanisms for international cooperation & dispute settlement
  - Acts of retorsion
  - Exceptional mechanisms of self-protection
- Reactions Available Only if Violation IntLaw by Other State
- Peaceful countermeasures
- Self-defense in case of armed attack ("agression armée")
Hack-Back: Pros and Cons

Interest & Advantages

- Compensate for shortcomings in governmental action
- Efficiency
  - Faster & more efficient
  - Deterrent effect
  - Avoid revealing vulnerabilities
  - Solve problems extra-territoriality
- Good for business!

Disadvantages & Risks

- Escalation & destabilization
- Risks to the authority of the State
- Risks activities of State
  - Foreign policy
  - Intelligence
  - Fight against crime
- Counterproductive
  - Collateral damage
  - Automatic active cyber defense
  - Backlash
  - Selective & hypocritical?

Karine Bannelier
The "Wild" Hack-Back: Legal Problems

No Hack-Back Right for Private Actors

- Impossible rely counter-measures
- Impossible rely on human rights
- Impossible use "self-defense"
- Impossible use "hot-pursuit"

Violation of Domestic Law

- Laws against violations integrity ICT systems & data
- Active Cyber Defense Certainty Act (ACDC) seeks amend US Computer Fraud & Abuse Act
- Transnational consequences of hack-back could expose authors to foreign prosecution + international criminal cooperation
- "Anyone who engages in retaliation should avoid international trips"

Karine Bannelier
A "Wise" Hack-Back? State Control & Regulation

**Ad hoc Reactions**
- State *requests help* private firm to respond specific cyber-attack
- State *accepts request* private firm to respond specific cyber-attack

**Certified Active Cyber Defense**
- Kind of "public/private partnership" with specific companies to respond more effectively to cyber-attacks
- Ensure that values of rule of law (transparency, access to justice, accountability, protection of privacy...) are respected + Control

**Private Military & Security Companies?**
- Various difficulties in practice
- Risk of "cyber privateers"?
States’ Behaviour and Sovereignty
International Law and Cyberspace

Lisbon 22 June 2017

Karine BANNELIER
Associate Professor, University Grenoble-Alpes
AMNECYS (Alpine Multidisciplinary Network on Cybersecurity Studies)