USE OF FORCE

Cybersecurity Law

… SOVEREIGNTY

- Principle
  - The right to hack back → solely in cyber domain!
  - UK (Jeremy Wright, Attorney General)
    - *"Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.* ***The UK Government's position is therefore that there is no such rule as a matter of current international law****."*

… SOVEREIGNTY

- Rule
  - An option to resort to countermeasures → international wrongful acts → violation of a primary rule
  - Countermeasures → all domains
  - Michael Schmitt
    - *“ To my knowledge,* ***the U.S. government has not formally adopted the “sovereignty as principle but not rule” approach****; it remains the subject of inter-departmental and interagency discussion.“*

USE OF FORCE

NICARAGUA JUDGMENT (1986)

- Nicaragua (P) brought a suit against the United States (D) on the ground that the United States (D) was responsible for illegal military and paramilitary activities in and against Nicaragua
- ICJ raised several topics
  - The prohibition of the use of force
  - The right of self-defence
  - The principle of non-intervention
  - State sovereignty

Rule 68 – Prohibition of threat or use of force

A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.

"A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."

- Art. 2/4 UN Charter
  - *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*
- Customary int. law
- NJ (par. 188)
  - *"The Court has however to be satisfied that* ***there exists in customary international law an opinio juris as to the binding character of such abstention****. This opinio juris may, though with all due caution, be deduced from, inter alia, the attitude of the Parties and the attitude of States towards certain General Assembly resolutions, and particularly resolution 2625 (XXV) entitled "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations".”*

"A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."

- Scope is broader
- Two exceptions
  - Use of force authorised by the Security Council
  - Self-defence
- Solely undertaken by a State's armed forces?
- Art. 2/4 versus art. 39 UN Charter
  - *"**All Members shall refrain** in their international relations **from the threat or use of force** against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*
  - *"The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."*

Rule 69 – Definition of use of force

A cyber operation constitutes a use of force when *its scale and effects* are comparable to non-cyber operations rising to the level of a use of force.

*"A cyber operation constitutes a use of force when **its scale and effects** are comparable to non-cyber operations rising to the level of a use of force."*

- NJ (par. 228)
  - "In the view of the Court, while **the arming and training of the contras** can certainly be said to involve the threat or use of force against Nicaragua (…) the Court considers that **the mere supply of funds to the contras**, while undoubtedly an act of intervention in the internal affairs of Nicaragua, as will be explained below, does not in itself amount to a use of force." → hackivist group?
- "Use of force" versus "armed attack"
- NJ (par. 191)
  - "it will be necessary to distinguish **the most grave forms of the use of force** (those constituting an armed attack) **from other less grave forms**."
- US opinion

"A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."

- Summary
  - Some cyber actions are undeniably not uses of force
  - Uses of force need not involve a State's direct use of armed force
  - All armed attacks are uses of force
- Analysis of quantitative and qualitative factors (use of force assessment)
  - **Severity** → How many people were killed? How large an area was attacked?
  - **Immediacy** → How soon were the effects of the cyber operation felt? How quickly did its effects lessen?
  - **Directness** → Was the action the proximate cause of the effects? Were there contributing causes giving rise to those effects?
  - **Invasiveness** → Did the action involve penetrating a cyber network intended to be secure? Was the locus of the action within the target country?

"A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."

- Analysis of quantitative and qualitative factors (use of force assessment)
  - **Measurability of effects** → How can the effects of the action be quantified? How certain is the calculation of the effects?
  - **Military character** → Did the military conduct the cyber operation? Were the armed forces the target of the cyber operation?
  - **State involvement** → Is the State directly or indirectly involved in the act in question?
  - **Presumptive legality** → acts such as propaganda, psychological operations, espionage, or mere economic pressure

Rule 70 – Definition of threat of force

A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force.

"A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force."

- Two scenarios
  - A cyber operation that is used to communicate a threat to use force (whether kinetic or cyber) → this cyber operation is only a medium
  - A threat conveyed by any means (e.g., public pronouncements) to carry out cyber operations qualifying as a use of force
- Threat must be communicative in nature
- The mere acquisition of cyber capabilities does not constitute a threat

Rule 71 – Self-defence against armed attack

A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.

"A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."

- Art. 51 UN Charter
  - *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security (…)"*
- Armed attack, trans-border element
- Employment of 'weapons' as a necessity?
- Harm to persons or physical damage to property as a condition?
- A cyber attack against a stock exchange → Yes or No?
- A cyber operation against a State's critical infrastructure→ Yes or No?

"A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."

- Bleed-over effects
- NJ (par. 195)
  - *"(…) an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "**the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State** of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein"."*
- 9/11
- The requirements of necessity, proportionality, imminence, and immediacy

Rule 72 – Necessity and proportionality

A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate.

"A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate."

- Necessity
  - Non-forceful measures are insufficient to address the situation
  - A combination → diplomacy, economic sanctions
- Proportionality
  - How much force is permissible once force is deemed necessary
  - Does not impose a requirement to respond in kind

Rule 73 – Imminence and immediacy

The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy.

"The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy."

- Imminence
  - *"anticipatory self-defence"* (the Caroline incident)
  - *"last feasible window of opportunity"* → whether a failure to act would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts
- Immediacy
  - the period following the execution of an armed attack → the victim State may reasonably respond in self-defence → otherwise it would be retaliation

Rule 74 – Collective self-defence

The right of self-defence may be exercised collectively. Collective self-defence against a cyber operation amounting to an armed attack may only be exercised at the request of the victim State and within the scope of the request.

"The right of self-defence may be exercised collectively. Collective self-defence against a cyber operation amounting to an armed attack may only be exercised at the request of the victim State and within the scope of the request."

- Prerequisite → a request for such an assistance
- NJ (par. 199)
  - *"there is no rule permitting the exercise of collective self-defence in the absence of a request by the State which regards itself as the victim of an armed attack. The Court concludes that* ***the requirement of a request*** *by the State which is the victim of the alleged attack is additional to* ***the requirement that such a State should have declared itself to have been attacked****."*
- An option to limit the assistance to non-kinetic measures or restrict the types of targets that may be made the object of cyber operations while operating in collective self-defence
- Collective defence treaty (NATO)
- Ad hoc arrangement

Rule 75 – Reporting measures of self-defence

Measures involving cyber operations undertaken by States in the exercise of the right of self-defence pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council.

"Measures involving cyber operations undertaken by States in the exercise of the right of self-defence pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council."

- A violation of the obligation
- The failure does not deprive the State in question of the right to act in self-defence

Rule 76 – United Nations Security Council

Should the United Nations Security Council determine that a cyber operation constitutes a threat to the peace, breach of the peace, or act of aggression, it may authorise non-forceful measures, including cyber operations, in response. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures.

"Should the United Nations Security Council determine that a cyber operation constitutes a threat to the peace, breach of the peace, or act of aggression, it may authorise non-forceful measures, including cyber operations, in response. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures."

- The Security Council has never determined that a cyber operation constitutes a threat to the peace, breach of the peace, or act of aggression
- Two situations
  - international terrorism
  - proliferation of weapons of mass destruction
- Art. 41 UN Charter
  - *"The Security Council may decide what **measures not involving the use of armed force** are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."*
  - **interruption of cyber communications with a State or non-State actor**

"Should the United Nations Security Council determine that a cyber operation constitutes a threat to the peace, breach of the peace, or act of aggression, it may authorise non-forceful measures, including cyber operations, in response. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures."

- Art. 42 UN Charter
  - *"Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."*
  - **A state with a nuclear weapon capacity**