# “New” threats, Article 5 and the Strategic Concept

**Dr. Maria Mälksoo**
**ICDS**

**The Future of NATO’s Nuclear Deterrent: The New Strategic Concept and the 2010 NPT Review Conference**
**NATO Defense College**
**Rome, Italy**
**28 February - 2 March 2010**

# Main problem

- What is the character of potential Article 5 challenges today?

- How to regard the so-called “new” security challenges, such as cyber and energy contingencies, in the context of Article 5 of the Washington Treaty?

# The key issue

- Can we qualify cyber attacks as “armed attacks” in the sense of NATO’s Article 5 and thus as falling under the rubric of the use of force as defined in the United Nations Charter Article 2 (4)?

# Sub-question

- Could states use physical force as a self-defense measure in order to retaliate the attempts to undermine their security with non-traditional means if and when these should result in causing real threat or physical damage to their people's lives?

# The applicability of Article 5 to the "new" security challenges

- What makes "new" threats qualitatively new?
- The application of the traditional definition of an armed attack to cyber conflicts problematic because of the indeterminacy of agency.
- At the same time, the "battle deaths" in the traditional physical sense are no longer necessarily a *sine qua non* for qualifying an attack as "war".

# The qualification problem of cyber attacks

- Cyber attacks are difficult to be territorialized.
- No fixed threshold in international law as of yet about the qualification of cyber attacks as the use of force.
- CNA can be regarded as an armed attack only in case their consequences are equal to those of a physical armed attack.

# No political or legal consensus

- At the moment, there is no political consensus, let alone an international legal one, on the issue whether or not cyber threats could be qualified as use of force according to the UN Charter Article 2 (4) that would activate the self-defense provisions of the North Atlantic Treaty framework.

# Likely NATO practice vis-à-vis CNA

- The implementation of Article 5 in case of CNA will be closely related to the implementation of Article 4 of the North Atlantic Treaty.

- Whether or not concrete cyber attacks should trigger the collective defense provision of NATO Article 5 will remain to be decided *ad hoc* by the Allies in the conceivable future.

# Traditional deterrence difficult to apply to CNAs

- Traditionally conceived deterrence is difficult to apply to the so-called “new” threats since deterrence assumes:

- the scope of an attack can be quickly determined,
- the source of attack clearly recognized,
- the likely damage from offensive attack assessed,
- the possible gains motivating the opponent recognized.

# Strategic aim: deterrence through denial

- Improving NATO's defensive capabilities against potential cyber attacks.

- Developing an adequate capability to undermine opponent's offensive capabilities through a pre-battle information suppression operation, designed with an aim to dissuade the opponent from attacking in the first place.

# Ditto for energy security

- The weight of emphasis of NATO's critical infrastructure protection should lie on prevention, in order to:

- minimize preemptively the probability of energy cut-offs, and
- attacks against respective infrastructures and their possible consequences.

# *Lex lata* and *lex ferenda*

- The existing law and state practice generally speak against qualifying cyber and energy security challenges under Article 5.

- Difficulties with the law-as-we-want-it-to-be: NATO can give new extended substance to its legal duties only as a result of extensive consultations and consensus-building.

# Calibrating deterrence

- Constraining options of both state and non-state actors, traditional and non-traditional threats.

- Weaving nuclear and conventional aspects in a sensible way.

# Thank you!

Full paper will be made available after the conference online at www.icds.ee