

ATTACHÉ MERTENS LOÏC

17 September 2026

9TH *SILENT LEGES INTER ARMA? CONFERENCE -BRUGES*



DEFENCE

Position of Belgium on international law applicable to cyber (2025)





DEFENCE

■ Double Disclaimer



■ overview



I

Involved entities and process

II

Belgian position explained and compared

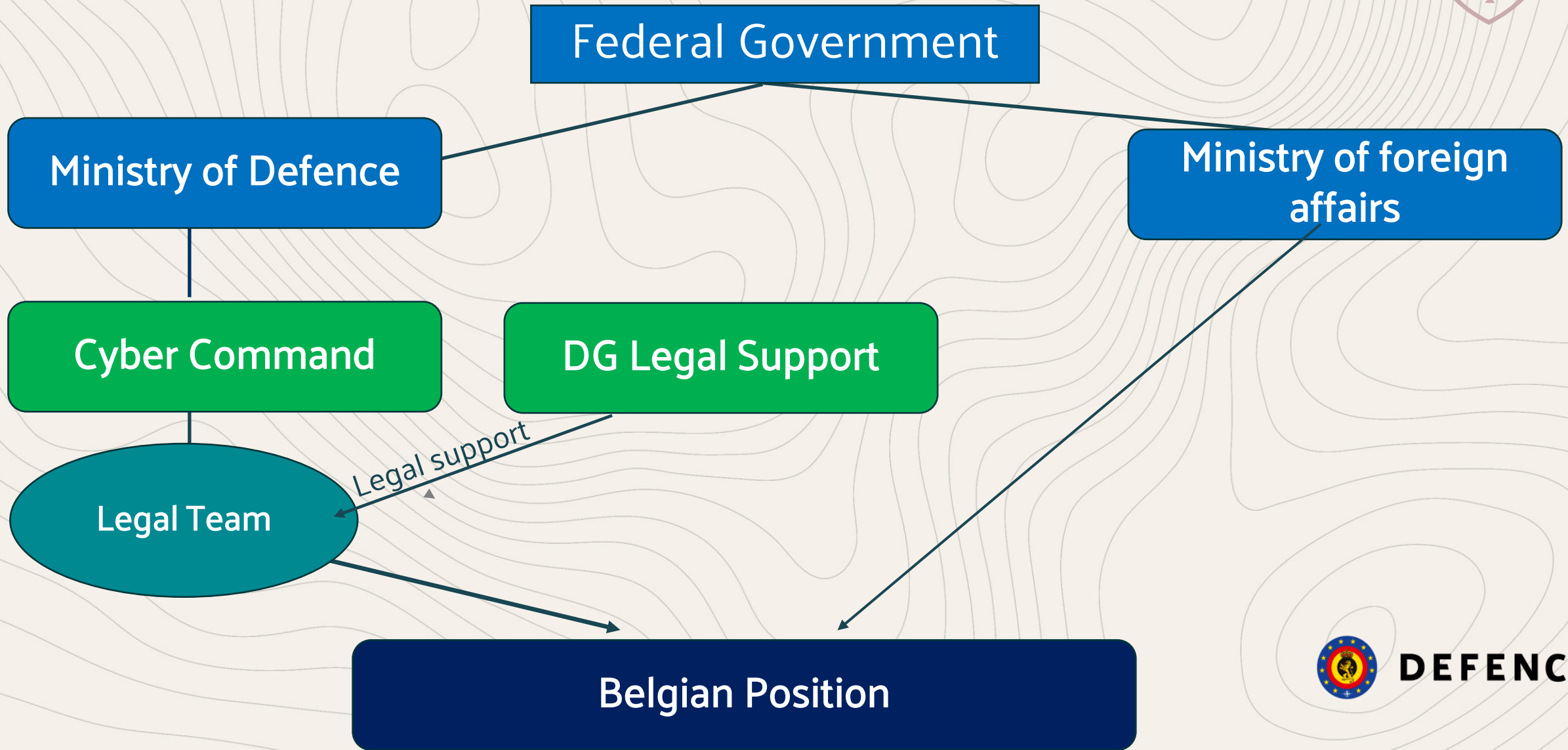
III

Conclusion and way ahead



DEFENCE

I. Involved entities and process



DEFENCE



■ II. Belgian position explained and compared

1

Introduction

2

violations of international law

3

State responsibility

4

Measures in reaction to internationally wrongful acts

5

Specific branches of international law



DEFENCE



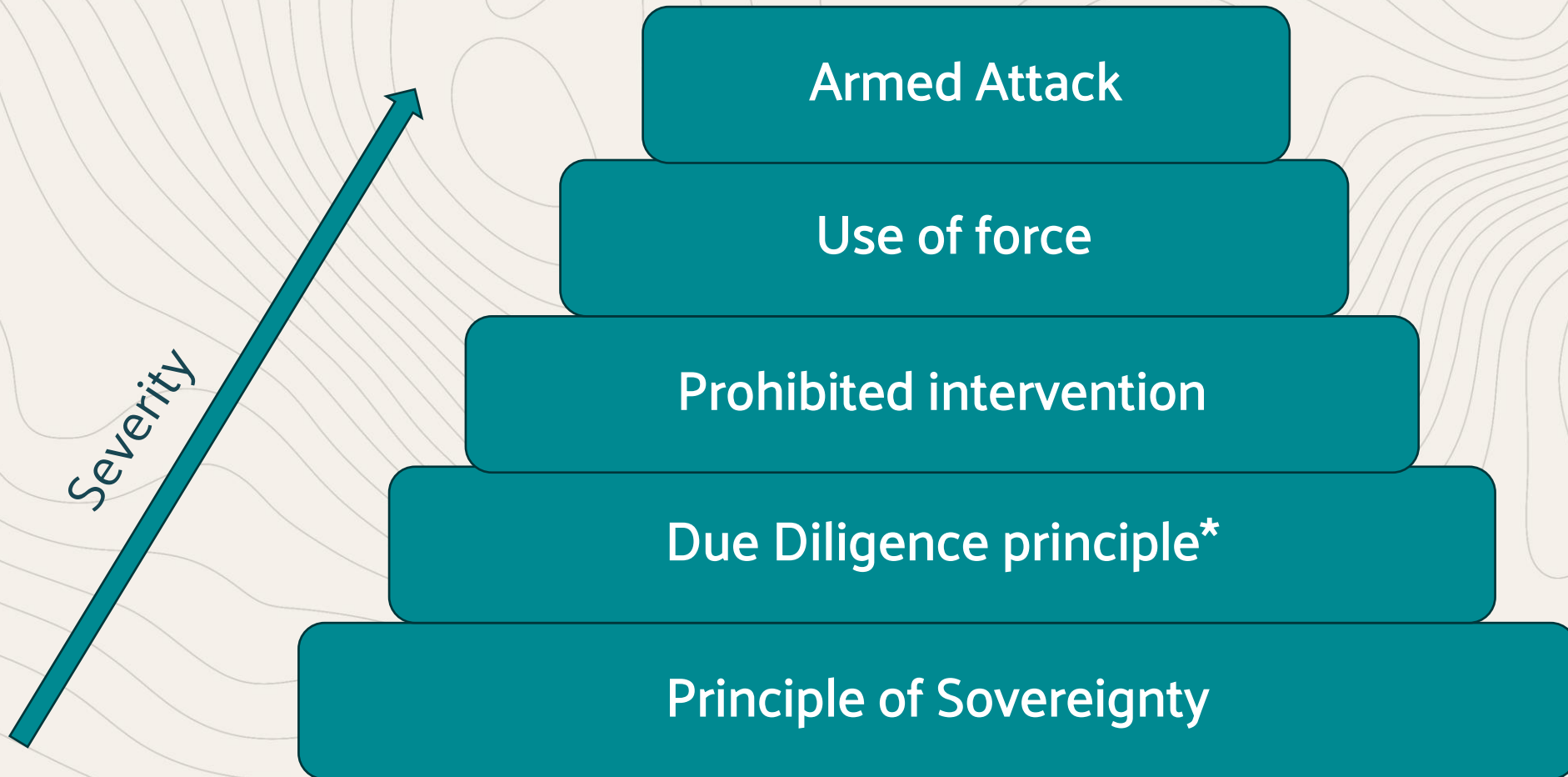
■ II.1. Introduction

- ❖ International law applies to cyberspace
- ❖ Position is temporary and is not to be considered as exhaustive
- ❖ Logically construed position:
 - Violation of norms of international law
 - Attribution
 - Reaction to internationally wrongful acts
 - Specific branches of international law



DEFENCE

■ II.2. violations of international law

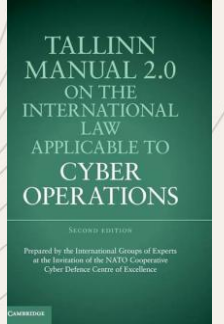


■ II.2. Sovereignty

❖ Island of Palmas arbitral award of 1928 (PCA)

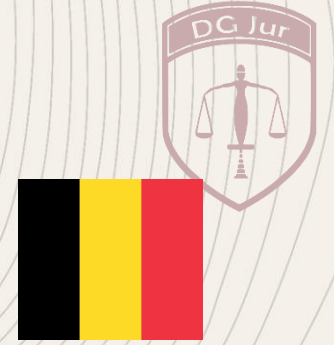
❖ Talilnn manual and cyber law toolkit

- Sovereignty as a rule approach (except for UK)
- Violation if:
 - territorial integrity is compromised or
 - interference with inherently governmental functions
- Disagreement as to when territorial integrity is compromised
- What are inherently governmental functions ?



DEFENCE

■ II.2. Sovereignty



❖ BEL position

- Sovereignty as a rule approach
- Principle breached when physical damage or loss of functionality or interference with “state functions”
- not excluded that there is a breach when there is no loss of functionality or if the cyber operation takes place on the territory of another state.



■ II.2. Sovereignty

❖ Own conclusion

- BEL follows Tallinn manual and many other states (CAN, GER, NLD...) and correctly so.
- BEL could have specified what it understands as a loss of functionality (extreme slowing down, reboot necessary)

Noteworthy in this regard :

“any effects produced on French territory by digital means”



DEFENCE

■ II.2. Due Diligence

- ❖ General international law principle (Corfu Channel case, ICJ)
- ❖ Discussion as to its applicability in cyberspace
 - “voluntary, non-binding form of state behaviour” (ISR, NZL, UK, CAN)
 - Legally binding obligation (EST, FIN, FRA, GER, NLD)
- ❖ Discussion as to its applicability criteria



DEFENCE

■ II.2. Due Diligence



❖ BEL position

- Binding obligation
- “**reasonable measures** against cyber operations that violate the rights of another State”
- “persons located on their territory or using servers or networks located on their territory or under their control, and of which they are **aware or ought to be aware**”
- “The obligation of due diligence is an **obligation of means**”



DEFENCE



■ II.2. Principle of non-intervention

❖ General international law principle (Nicaragua Case, ICJ 1986)



❖ Discussion as to its applicability criteria

- When is an act deemed coercive ?
 - Does it need to be forceful or not ?
 - May coercion take on a political or social dimension?
 - In any case, mere propaganda is not sufficient



DEFENCE

■ II.2. Principle of non-intervention



- ❖ BEL follows general international law and declares the principle applicable to cyberspace
- ❖ intervention may take the form of political, economical or social acts of coercion into the “domaine réservé”

Example : “cyber operation, aimed at influencing or tampering with electoral results within a State, where such an operation could undermine or be likely to undermine the country’s political, economic or social system”

Same position as most states.



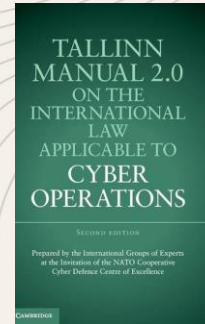
■ II.2. (prohibition on the) Use of Force

❖ art. 2 (4) UN CHARTER Nicaragua Case, ICJ 1986

❖ “Effects based approach”

❖ Use of force without physical damage ?

- If disruption is “significant enough to affect state security”
- Development of criteria to help with the qualification
- Some nations have adopted criteria in their national positions (FRA, NOR, NLD)



DEFENCE

■ II.2. (prohibition on the) Use of Force



❖ BEL position

- Scale and effects theory
- Does not rule out that an act may be qualified as a use of force if there is **no significant physical damage or loss of life** « provided that its scale and effects are similar to those resulting from the use of other weapons and military means”
- Example : “cyber operation deliberately seeking to affect a State, by paralysing its financial system or the operation of its critical/essential infrastructures, with serious consequences for the health, safety or economic well-being of the population”



DEFENCE



■ II.2. Armed Attack

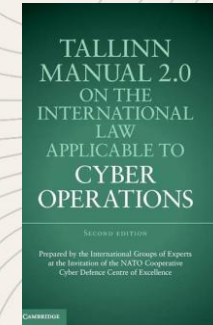
❖ art. 51 UN CHARTER

❖ Only “the most grave uses of force” (Nicaragua case, ICJ 1986)

- “Only cyber operations that seriously injure or kill a number of persons or cause significant damage to, or destruction of, property would undoubtedly constitute armed attacks”

❖ Gives rise to the right of self-defence (subject to certain conditions)

❖ US position : every use of force gives rise to the use of force in self-defence



DEFENCE

■ II.2. Armed Attack



❖ BEL position

- Follows general international law (scale and effects) and applies it to cyberspace. It states that **an armed attack through cyber means is not to be excluded**.
- “The attack must, at the very least, result in substantial loss of life or extensive destruction of infrastructure or systems”.
- Mentions the theory of cumulative events.



DEFENCE

■ II.2. Armed Attack

❖ Own conclusion

- BEL is one of the only states (FRA) to mention the theory of cumulative events. More states should explicitly mention this (if that is their position)
- BEL could have expanded the scope of qualification of an armed attack to apply to non-state actors under the « unwilling or unable » theory. (Austria, Denmark, GER...)



■ II. Belgian position explained and compared

1

Introduction

2

violations of international law

3

State responsibility

4

Measures in reaction to internationally wrongful acts

5

Specific branches of international law



DEFENCE

■ II.3. State responsibility



- ❖ ARSIWA are applicable for the purposes of State responsibility in cyberspace
- ❖ BEL confirms that attribution is difficult in cyberspace
- ❖ Attribution remains a sovereign prerogative, though BEL may endorse attribution by an international organisation or other state.
- ❖ Aiding or assisting other states in committing an internationally wrongful act may incur responsibility.



DEFENCE



■ II. Belgian position explained and compared

1

Introduction

2

violations of international law

3

State responsibility

4

Measures in reaction to internationally wrongful acts

5

Specific branches of international law



DEFENCE



■ II.4. Measures in reaction to violations of international law

Circumstance
precluding
wrongfulness

(Use of force in) self-defence

Circumstance
precluding
wrongfulness

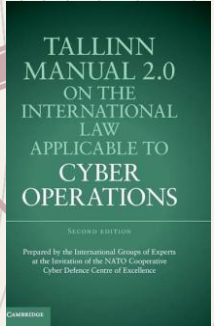
Countermeasures

Retorsions



DEFENCE

■ II.4. Countermeasures



- ❖ Countermeasures are not to be applied to cyberspace (Brazil, China, Cuba). Most experts and other countries disagree.
- ❖ Some conditions with regards to countermeasures are discussed, such as the notification requirement
 - CAN, ISR, NOR, UK and US argue that notification to the responsible state that a countermeasure is going to be taken is not necessary, as to preserve the effectiveness of the measure/to avoid exposing certain capabilities,



DEFENCE

■ II.4. Countermeasures



- ❖ BEL confirms that the law of countermeasures applies to cyberspace
- ❖ notification of the responsible state is necessary



DEFENCE



■ II. Belgian position explained and compared

1

Introduction

2

Cyber operations amounting to violations of international law

3

State responsibility

4

Measures in reaction to internationally wrongful acts

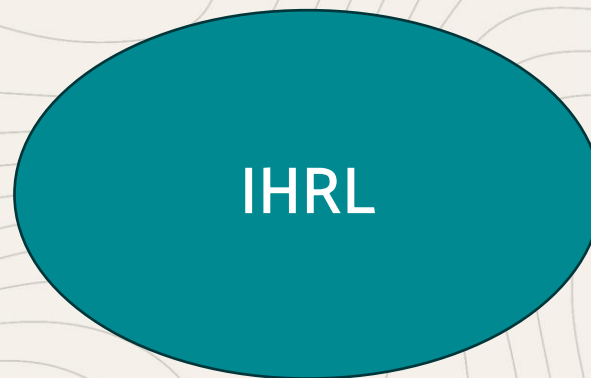
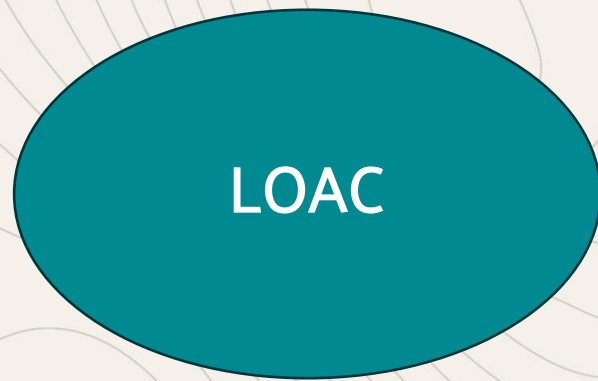
5

Specific branches of international law



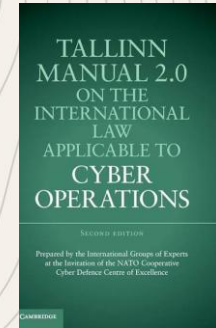
DEFENCE

■ II.5. Specific branches of international law



DEFENCE

■ II.5. LOAC – notion of attack

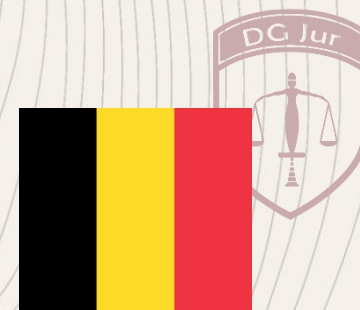


- ❖ Article 49 API : “acts of violence against the adversary, whether in offence or in defence.”
- ❖ Threshold for some obligations under IHL
- ❖ Discussion concerning the standard of harm :
 - Physical damage (DK, ISR, PERU)
 - Loss of functionality (majority of states)



DEFENCE

■ II.5. LOAC – notion of attack



- ❖ BEL position

- ❖ Loss of functionality approach (FRA)

- Considered as an attack if “*restoring the functionality requires intervention, such as replacing parts or a re-installation.*”

- ❖ Is not an attack :

- Desinformation campaigns, DDOS, jamming



DEFENCE



III Conclusion and way ahead

- ❖ Decent first positioning, in line with most experts and most like-minded states
- ❖ Still a lot of stones left unturned :
 - LOAC: conflict classification, DPH, application of principles (precaution, proportionality), military objectives....



DEFENCE



DEFENCE

■ Questions?

