International Law Applicable to "Cyber Attack"

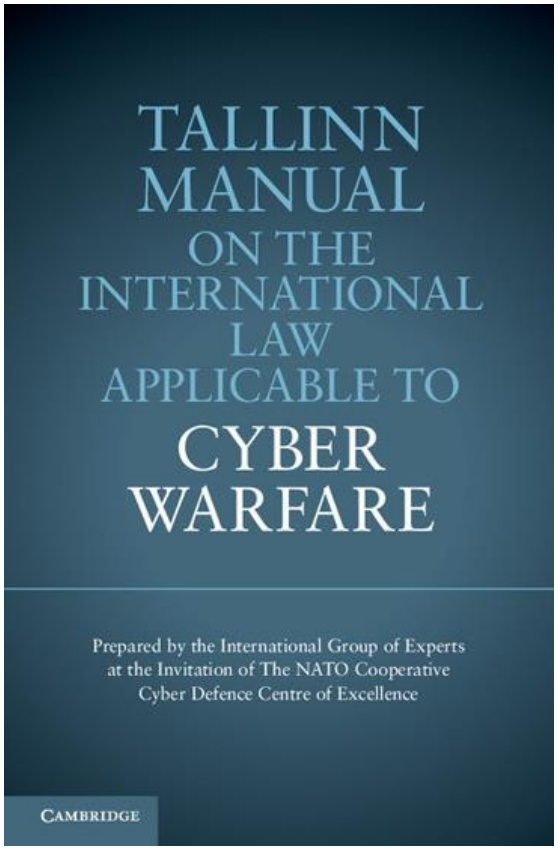
Image credit: Ed Mahoney, Cyber War

Professor Sean Watts

Creighton UNIVERSITY School of Law

The Tallinn Manual

- International Group of Experts
- Format:
  - Black Letter Rules
  - Commentary
- Coverage:
  - *ius ad bellum*
  - *ius in bello*
- Central Thesis: international law applies to the context of cyberspace



Creighton UNIVERSITY School of Law

Cyber-Specific IHL: Virtual Groups and NIAC

- **GC, art. 3:** '… *armed conflict not of an international character …*'
- **AP II, art. 1(4):** '*organized armed groups under responsible command, … control territory, …sustained and concerted military operations, … implement this Protocol.*'
- **ICTY, *Tadić*:** '*protracted armed violence … between organized armed groups.*'

Tallinn Manual, Rule 23:

'*… a minimum degree of organization.*'

Commentary Consensus:

- cyber NIAC will be exceptional
- not intrusions, data deletion, exploitation
- 'established command structure'

No Consensus:

'whether non-destructive but severe cyber operations satisfy intensity criterion'

Majority:

- organized armed group requirement distinguishes NIAC from riot/banditry
- group need not meet physically

Restrictive Minority:

groups must convene physically

'Potential Viewpoints':

- collaboration is sufficient
- collective effort is sufficient
- 'armed conflict' undefined
- denying applicability of NIAC no longer keeps international law at bay

Cyber-Specific IHL: 'Attack' Threshold

AP I, art. 49: '… *acts of violence against the adversary whether in offence or defence.*'

Tallinn Manual, Rule 30:

'A cyber attack is a cyber operation … reasonably expected to cause injury or death to persons or damage or destruction to objects.'

Commentary Consensus:

- can be non-kinetic (e.g. bio.)
- not cyber psy-ops or espionage
- effect-focused not means-focused
- data loss resulting in death or injury to person, or damage or destruction to object is attack

Majority:

- disruption of functionality requiring component replacement is attack
- split on disruption of functionality requiring reinstallation of OS
- communication disruptions are not attacks

Restrictive Minority:

mere disruptions of functionality are not attack – destruction is required

Inclusive Minority:

interference requiring data restoration is attack

Creighton UNIVERSITY School of Law

Cyber-Specific IHL: Dual-Use Objects

AP I, art. 52(2): '*military objectives … by their … use … make an effective contribution to military action … destruction … offers a definite military advantage*.'

Tallinn Man., Rules 38 & 39:

'may include computers, computer networks, and cyber infrastructure.'

Commentary Consensus:

- '*Any use or future use contributing to military action …*'
- military use can render entire network a military objective
- BUT entire Internet unlikely to qualify

Emerging Concerns:

- greatly susceptible to abuse
- Internet protocol directs traffic broadly
- toward a *de minimus* military use standard? e.g. packet transit
- a separation duty? AP I, art. 58(c)
- can 'effective contribution' be refined for cyber contexts?

Replies:

- proportionality a significant safeguard **but** only for civilian objects
- AP I, art. 52(2) and Tallinn require 'effective contribution to military action'

Creighton UNIVERSITY School of Law

Cyber-Specific IHL: Cyber Combatant Status

- **GC III, art. 4(A):** '*armed forces … militia and volunteer corps … unrecognized armed forces …* levées en masse'
- **AP I, art. 43:** '*members of the armed forces are combatants*'

Tallinn Manual, Rule 26:

'armed forces … who … fail to comply to comply with the requirements of combatant status lose their … combatant immunity'

Commentary Consensus:

- Combatancy is limited to IAC (c.1)
- 'belonging to' requires a *de facto* relationship to a State (c.7)
- 'carry arms openly' little cyber application (c.13)
- no international war crime (c.19)

Majority:

- State's own nationals are not owed POW status and do not enjoy combatant immunity
- four militia criteria (command, distinctive sign, carry arms openly, law of war compliance) are implicitly applicable to armed forces
- *levee en masse* requires physical invasion of territory; limited application to cyber

Plurality:

no cyber exception to distinctive sign or uniform requirement

Minority:

- no nationality disqualification
- membership is sufficient for armed forces

Creighton UNIVERSITY School of Law

General IHL: Contributions from Cyber Warfare

Does the cyber context provide any insight or opportunity to develop or clarify persistent issues of IHL interpretation?

- Economic targets …….. TM, Rule 38, c.16
- Presumptions, standards of proof…….TM, Rule 33, c.2; 40, c.4
- Differential obligations …….. TM, Ch. 4,Sec. 7
- Direct participation in hostilities ..... TM, Rule 35
- Geography of IHL …….. TM, Rule 23, c.4

Creighton UNIVERSITY School of Law

Tallinn Manual 2.0 (forthcoming 2017)

- Sovereignty
- Jurisdiction
- State Responsibility
- Due Diligence
- Peaceful Settlement of Disputes
- Espionage
- Non-Intervention
- Cyber Operations at Sea
- Human Rights Law
- Air Law
- Space Law
- International Telecommunications Law
- International Organizations
- Law of War (Tallinn 1.0 update and reissue)

Creighton UNIVERSITY School of Law

Questions and comments

seanwatts@creighton.edu

Creighton
UNIVERSITY
School of Law