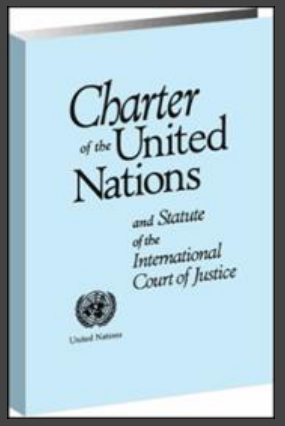
Cyber attacks
and the law of armed conflict

Andrew Carswell
Senior Delegate to Canada
International Committee of the Red Cross

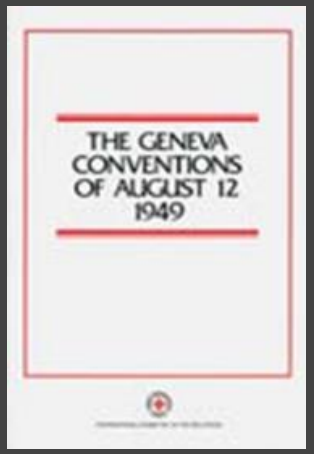
ICRC

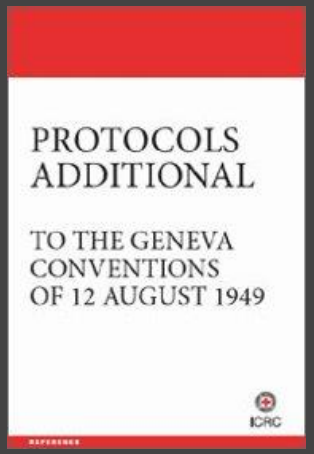
International law governing cyber “attack”

- UN Charter law
  - *Jus ad bellum*



- International humanitarian law
  - *Jus in bello*

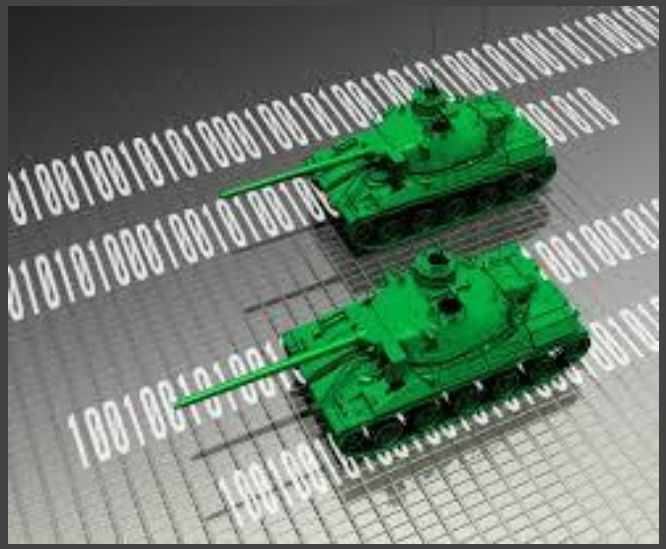




Legal classification of cyber events

International armed conflict

- Common article 2 of the Geneva Conventions
- *Prosecutor v. Tadic*, ICTY
  - *"a resort to armed force between States"*
- Attribution…
  - to State directly
  - or via a proxy



ICRC

Non-international armed conflict

- Common article 3 of the Geneva Conventions
  - ICTY+: organization of parties, intensity of hostilities
- Organization
  - C2, weapons, ability to apply LOAC, sanctions…
  - Virtual organizations?
- Intensity
  - Cyber event within existing NIAC
  - Cyber alone
- Attribution…

Targeting concepts distilled

Attack subject to:

1) Military necessity

2) Distinction
3) Proportionality
4) Precaution

5) Humanity (limitations on means and methods)

Defining “attack” in LOAC

*Acts of **violence** against the adversary, whether in offence or defence*

Art 49(1) AP I

- Tallinn Manual:

  *A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or **damage** or destruction to objects*

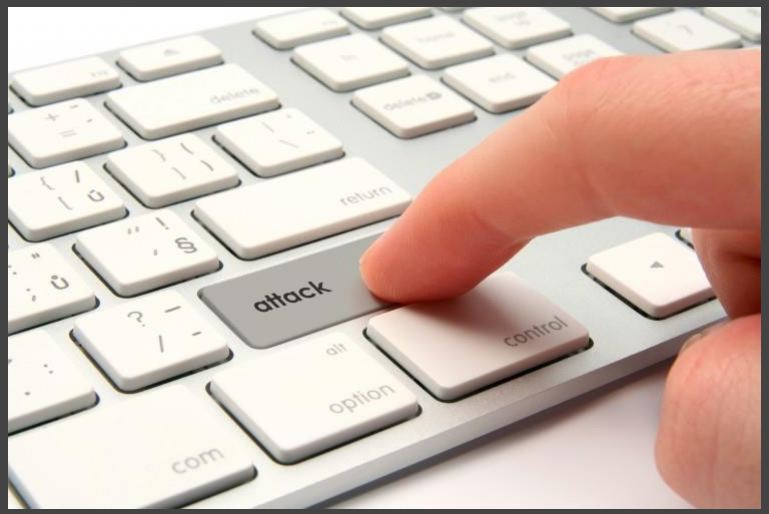
  Tallinn Manual, Rule 30

- Does impairment of function equate to “damage”?

ICRC

“Attacks”?

- Disrupting civilian power grid
- Denial of internet banking service
- Blocking BBC website
- Blocking access to Facebook
- Disrupting water treatment plants



ICRC

Distinction in attack

- Persons
  - Fighting forces vs. civilians
- Objects
  - Civilian objects vs. military objectives
  - Military objectives:
    - Objects which by their **nature, location, purpose** or **use** make an effective contribution to military action
    - And whose destruction, capture or neutralization offers a definite military advantage

ICRC

Distinction in attack

- Dual use objects
- Cyber infrastructure as a target
- Geographical limit of the conflict
- Law of neutrality in cyberspace

Distinction in attack

Indiscriminate attacks are prohibited

Art 51(4)(c) AP I

- Not directed at a specific military objective
- Employ method or means which cannot be directed at a specific military objective
- Employ a method or means which cannot be limited

- How specifically can malware be targeted?

Proportionality in attack

Prohibited:

An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof,

which would be excessive in relation to

the concrete and direct military advantage anticipated

Art 51(5)(b) AP I

- Damage includes impairing functionality
- 2nd and 3rd order effects

ICRC

Precautions in attack
(and other ops)

In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.

Art 57(1) AP I

- Need to understand the target
  - "*…Mission planners should have, where feasible, appropriate technical experts available to assist them in determining whether appropriate precautionary measures have been taken.*"

Tallinn Manual, p. 166

ICRC

Cyber weapons

[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited

Art 36 AP I