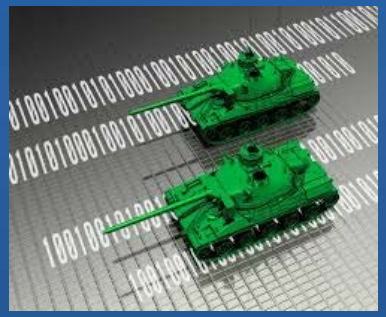
Public international law and cyber attacks

Pascal Brangetto
Kadri Kaska

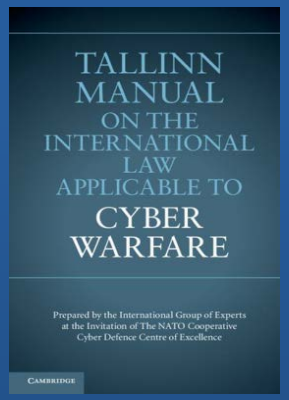
27 November 2015

Outline



Setting the scene

Law and Cyber Conflict



Tallinn Manual

This briefing is a product of the NATO CCD COE.
It does not represent the opinions or policies of NATO and is designed to provide an independent position.

Cyberwar is coming?

Russia-Georgia 2008

Russia-Ukraine 2014

The Sony Hack / The Interview 2014

Features of Cyber Conflicts

- The **attribution** conundrum
- **Low cost** of self entry
- Number of **actors**
- **Ubiquitous** and **transborder**

A classification of cyberattacks

- 3 types of cyberattacks
  - Disruption
  - Destruction
  - Espionage

- Tentative definition of a cyberattack:

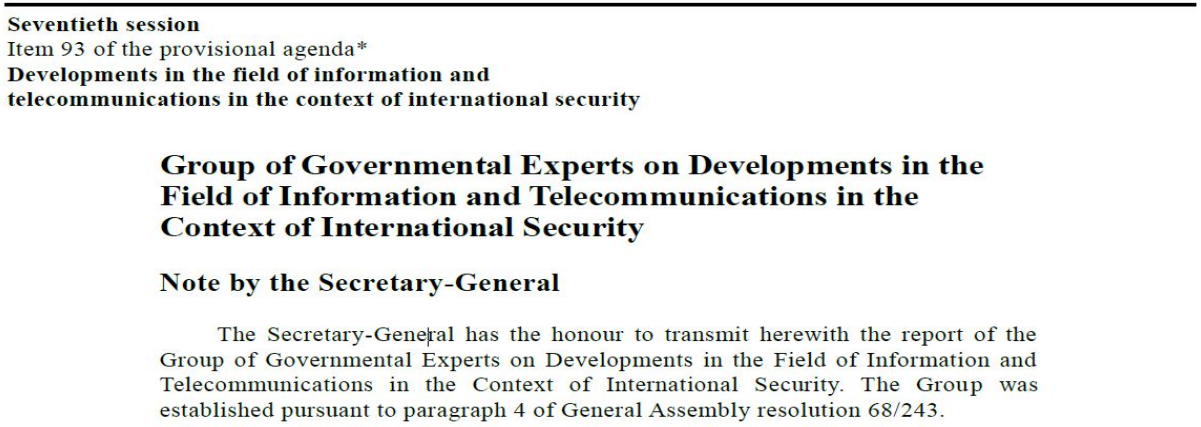
"an act or action initiated in cyberspace to cause harm compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems."

Law vs International Relations

- *"long-standing norms. . . apply in cyberspace"* – U.S. Int'l Strategy (2011)

- *"principles of international law do apply in cyberspace"* – Harold Koh, Legal Adviser to U.S. State Dept

- 2013 UN Group of Gov't Experts agree Int'l Law applies in Cyberspace



Seventieth session
Item 93 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established pursuant to paragraph 4 of General Assembly resolution 68/243.

However, there are some disagreements (Russia – Treaty is Needed or China – Uncertainty over Application).

Law vs International Relations

- **Status quo in international relations**:
  - International law is applicable to cyberspace
  - Need to focus on *how* it applies

Seventieth session
Item 93 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

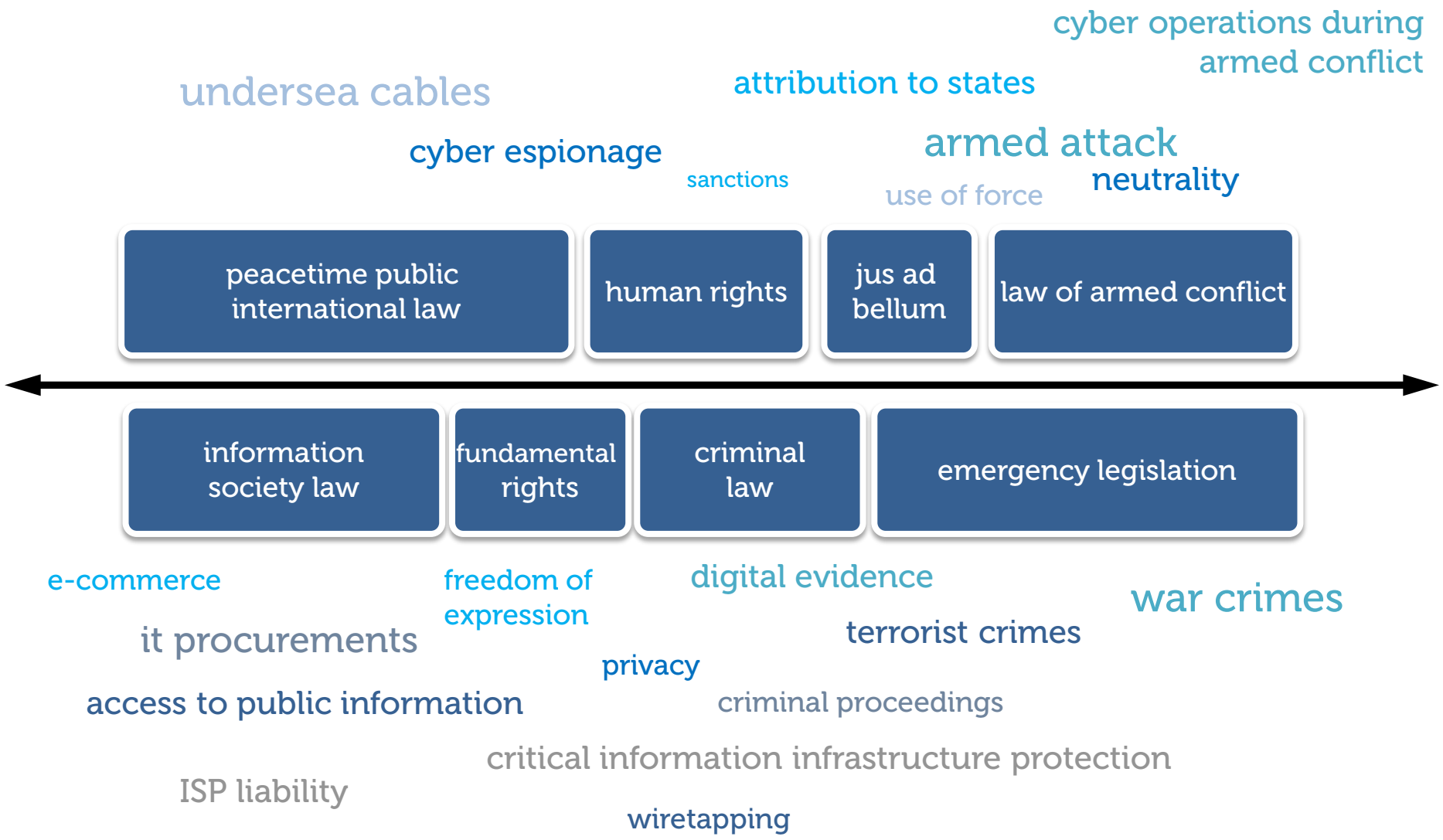
Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established pursuant to paragraph 4 of General Assembly resolution 68/243.

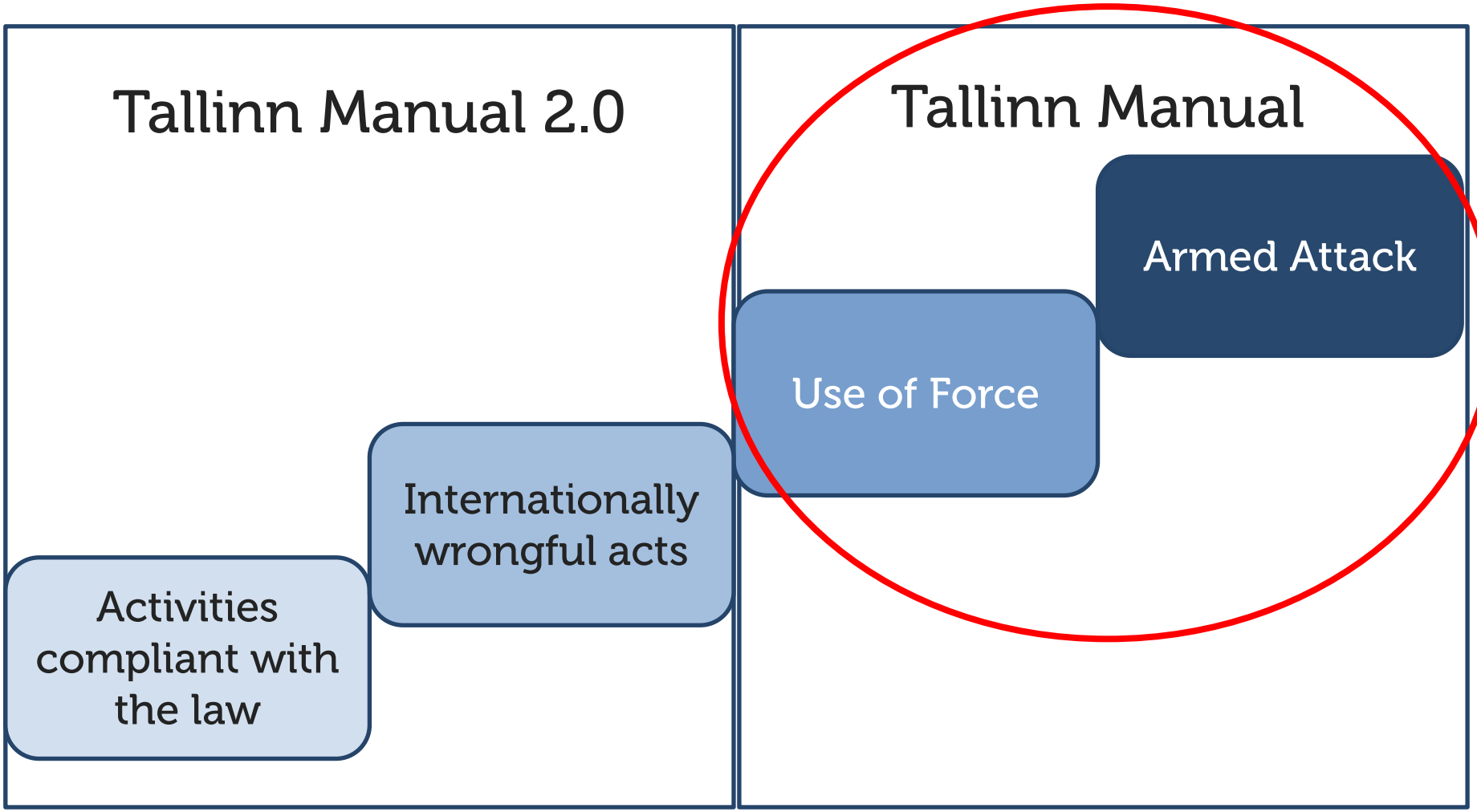
Law vs International Relations

- **Status quo in law**:
  - Tallinn Manual and other scholarly works: detailed analysis of how law applies to and in conflict
  - Certain key issues that are subject to varied interpretations, states need to get involved to shape the debate
  - Current focus on the international law governing cyber operations outside an armed conflict

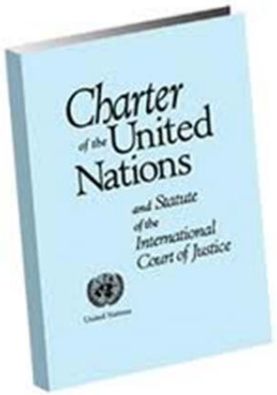
Law and cyber conflict



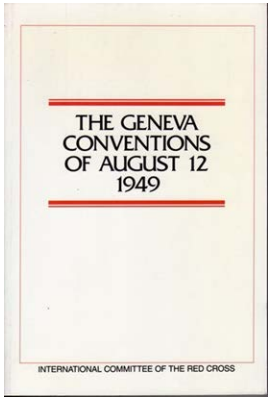
Law of cyber conflict
State Actions and International Law



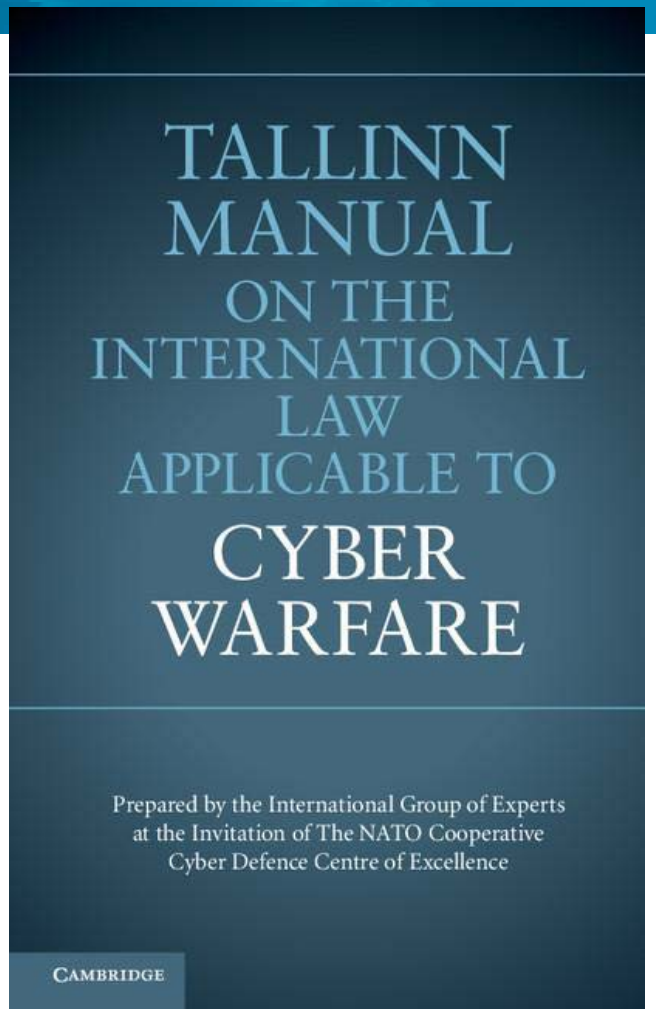
The Tallinn Manual



legal framework of use of force
(Jus ad Bellum)



law applicable in armed conflict
(Jus in Bello)



Self-Defence

- United Nations Charter, Article 51

> *"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..."*

- Legal basis for Article 5 of the NATO Treaty

Self-Defence

- **(Cyber) Armed Attack**
  - No definition
- **Tallinn Manual**
  - "Grave" injury, death, damage or destruction

  vs
  - Brief or periodic interruption of non-essential services

Self-Defence

- **Advisory report to the Netherlands government**
  - “if it causes (or has the potential to cause) serious disruption to the functioning of the state [...] even if there is no physical damage or injury.”

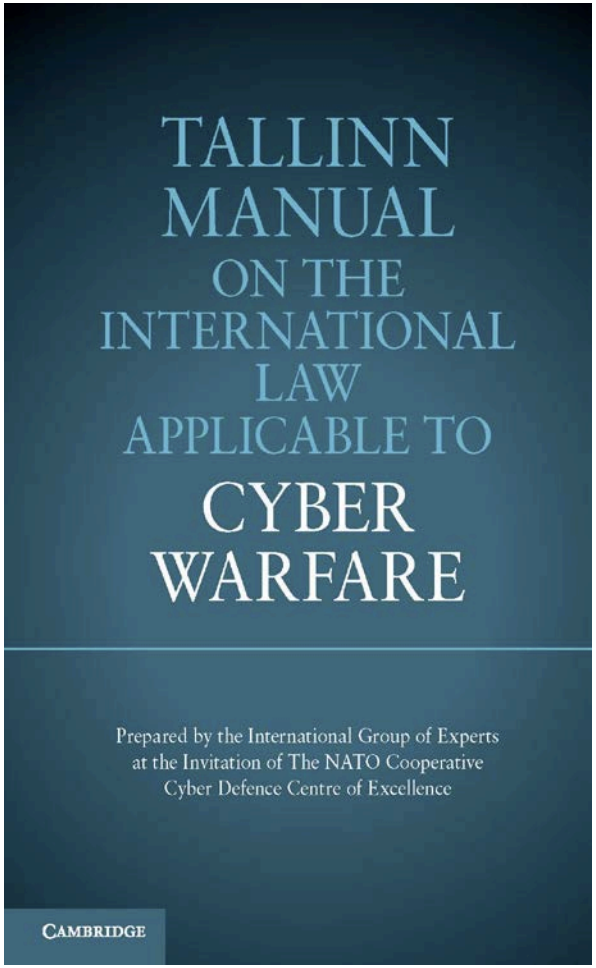
Shamoon 2012

ارامكو السعودية
Saudi Aramco

Attack under IHL

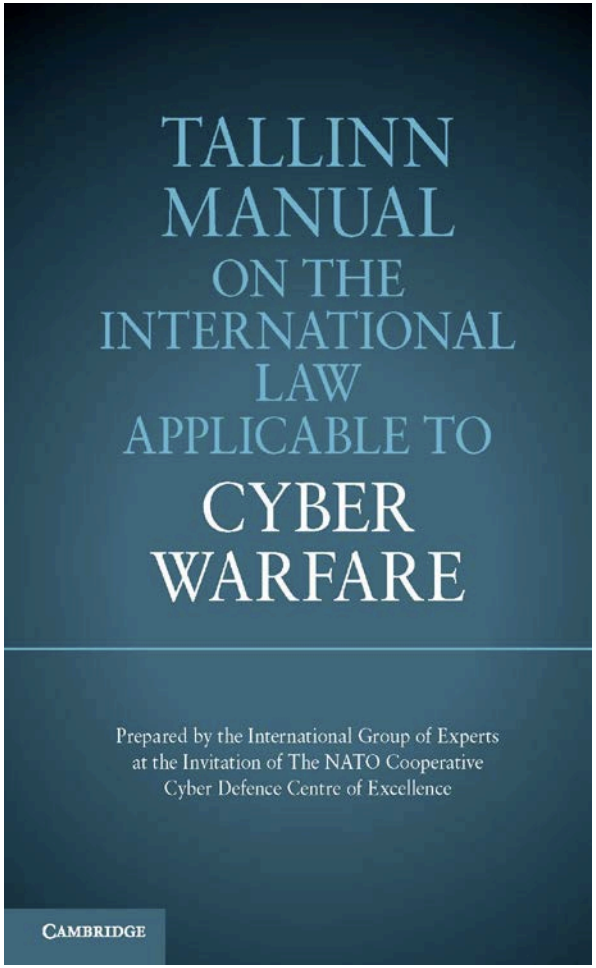
- Definition of attack under Article 49(1) of AP I
  - ""Attacks" means acts of violence against the adversary, whether in offence or in defence."
- Tallinn Manual definition of "cyber attack" under Art. 49(1)
  - "A cyber attack is a cyber operation, whether in offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."

The Tallinn Manual(s)



Tallinn Manual

- Project **hosted by** CCD COE 2009-2012
- Published 2013
- International Groups of Experts of **20 scholars and practitioners**
- **Interpretation** of international law in the cyber context
- **Independent** academic research, not the policy or doctrine of NATO or any state
- **Rules** + commentary



Tallinn Manual – So What?

- **“Law doesn’t keep up with technology”**
  “Cyber law – it’s soooo hard”
  - The law can reasonably be applied in the cyber context
  - No grand legal lacuna
  - Better understanding of interpretive controversies and grey areas in the law
- **Informs international dialogue**
  - UN GGE, national strategies
- **One stop shop for legal advisors**

Tallinn 2.0 Facts

- Project **hosted by** CCD COE 2013-2016
- **International Group of Experts**; peer review and State engagement (*The Hague Process*)
- Expands the analysis to **peacetime international law**
- Will result in the **second, expanded edition** of the Tallinn Manual (expected end-2106)
- **Rules** + commentary
- Independent academic research, **not the policy or doctrine of NATO** or any state

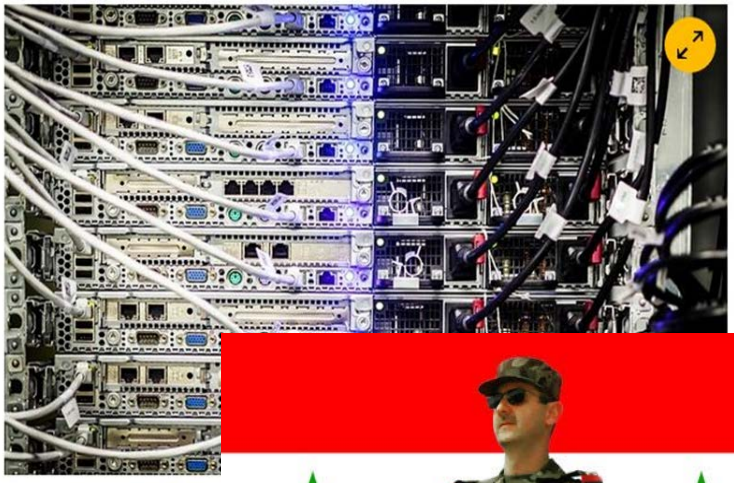
Tallinn 2.0 Topics

- Sovereignty
- Jurisdiction
- Due diligence
- Prohibition of intervention
- State responsibility
- Responsibility of IOs
- Int'l human rights law
- Air law
- Space law
- Diplomatic law
- Law of the sea
- The law of peace operations
- Peaceful settlement of disputes
- International telecommunications law
- Cyber operations not *per se* regulated by international law
  - Cyber espionage
  - Private sector cyber operations

What about the activities below the threshold of an armed attack

OPM hack: China blamed for massive breach of US government data

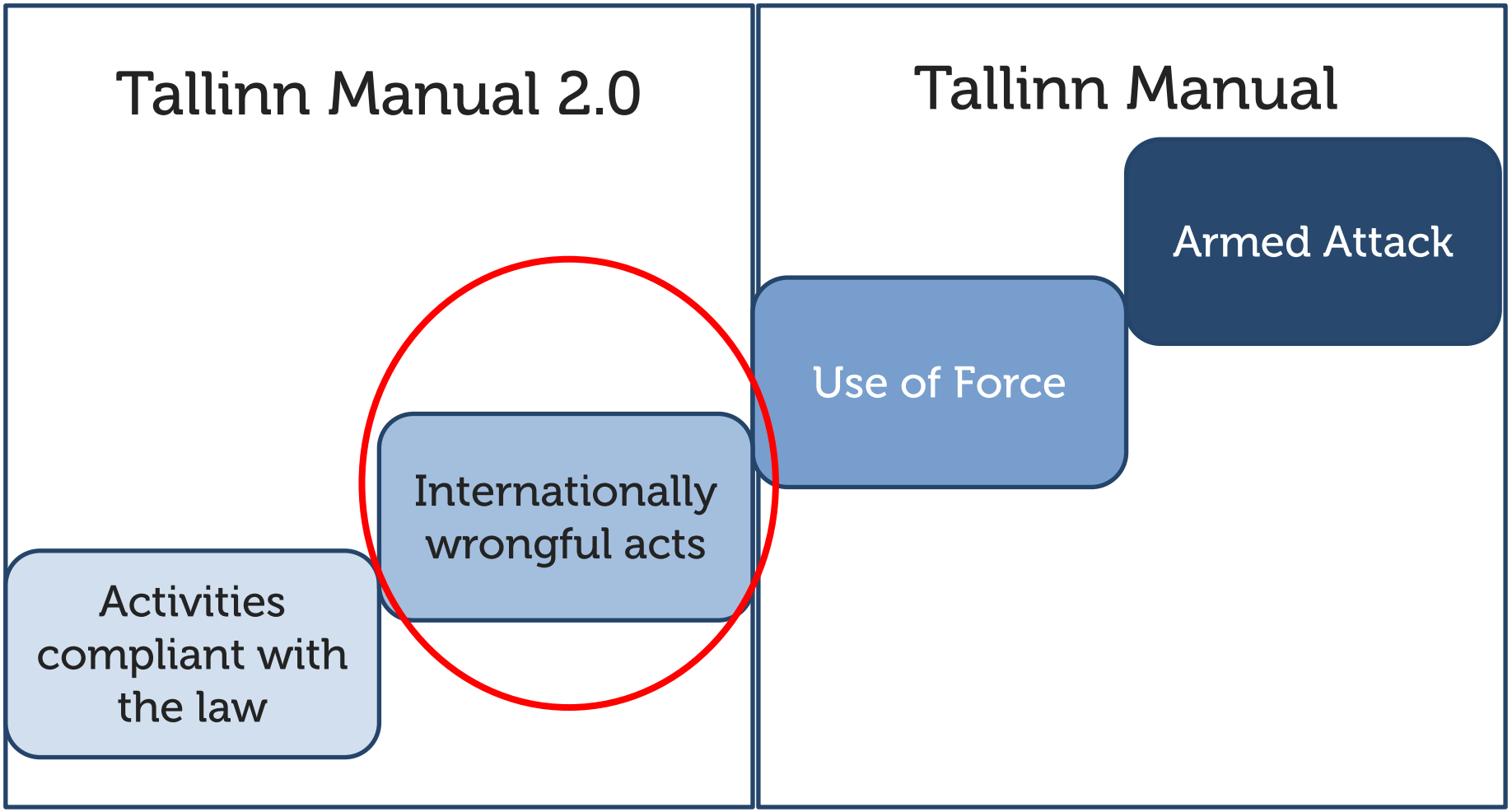
Denials from Beijing after computer systems are targeted at Office of Personnel Management, which holds details on entire staff of US government



The hack at the Office of Perso
100,000 taxpayers. Photograph: T

- Endangering critical infrastructure
- Website defacement
- Malware campaigns
- DDoS attacks
- Large-scale espionage

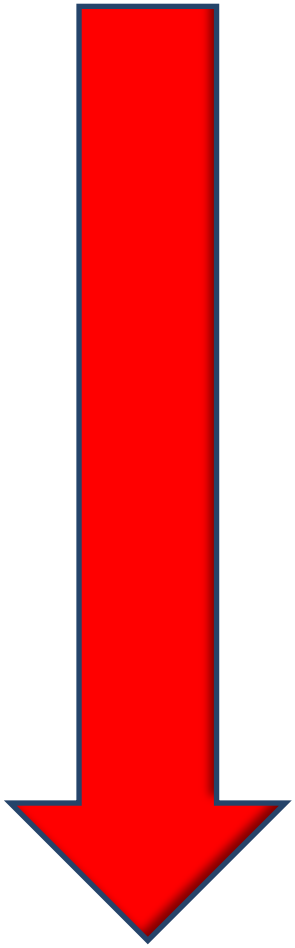
Law of cyber conflict
State Actions and International Law



Law of cyber conflict
State responsibility

- Responsibility of States for internationally wrongful acts
- These rules were drafted in 2001
- Wide recognition as customary international law
- This is a way to regulate States' conduct

Internationally Wrongful Acts
State options



- Negotiation and diplomacy
- Arbitration, mediation, international tribunals
- Law enforcement
- Measures based on consent
- **Retorsion (e.g. sanctions)**
- **Measures based on plea of necessity**
- **Countermeasures**

Retorsion: The Interview 2014

- US: “North Korea Sony Hack is not an act of war”
- US will respond proportionally
- Announces new sanctions against North Korea

“We will respond proportionately [to North Korea’s hack of Sony], and we’ll respond in a place and time and manner that we choose.”

President Barack Obama, Dec. 19, 2014

Retorsion:
Office of Personnel Management 2015

OPM hack: China blamed for massive breach of US government data

Denials from Beijing after computer systems are targeted at Office of Personnel Management, which holds details on entire staff of US government

The hack at the Office of Personnel Management follows an attack on the IRS that compromised the details of 100,000 taxpayers. Photograph: Thomas Trutschel/Photothek via Getty Images

OPM hack: 21 million people's personal information stolen, federal agency says

- OPM background check applicants since 2000 'highly likely' to be affected
- Office of Personnel Management computer networks infiltrated in late May

Office of Personnel Management keeps sensitive information for federal employees and co-habitants, including social security numbers, residency, health records and financial history. Photograph: Patrick George/Alamy

Retorsion:
DDoS Against US Banks 2012

REUTERS EDITION: U.S.

HOME BUSINESS MARKETS WORLD POLITICS TECH OPI

Mr. Lewis said the amount of traffic flooding American banking sites was "multiple times" the amount that Russia directed at Estonia in a monthlong online assault in 2007 that nearly crippled the Baltic nation.

Cyber attacks against banks more severe than most realize

BY JOSEPH MENN

BUSINESS

Banks Seek U.S. Help on Iran Cyberattacks

Bank Hacking Was the Work of Iranians, Officials Say

By NICOLE PERLROTH and QUENTIN HARDY
Published: January 8, 2013 | 332 Comments

U.S. rallied 120 nations in response to 2012 cyberattack on American banks

By Ellen Nakashima, Published: April 11 E-mail the writer

In the spring of 2012, some of the largest banks in the United States were coming under attack, with hackers commandeering servers around the world to direct a barrage of Internet traffic toward the banks' Web sites.

Bank of America
SunTrust
PNC
usbank
JPMorganChase

Countermeasures

- Measures by a state that in themselves would be unlawful, but are used to **compel another state to stop its unlawful behaviour**
- Proportional, temporary, reversible, warning
- Actor has to be known

- Example: State A attacks electrical grid of State B; State B takes measures against State A's irrigation control system

Plea of Necessity

- Measures to protect ‘essential interest’ of the state against a ‘grave an imminent peril’
- Emergency situation

- Example: devastating attack on critical infrastructure, indispensable for the vital functions of society

Training: International Law of Cyber Operations Course

- **Based on the Tallinn Manual**
- 37 nations, 200 students to date
- Resident course
- 1st mobile course
- In Tallinn, Estonia
  - 23-27 May 2016
  - 28 Nov - 2 Dec 2016

THANK YOU