


The slide features a dark blue background with a diagonal split. The left side shows a satellite view of the ocean with white-capped waves. The right side is a solid dark blue. A yellow diagonal stripe runs from the top left corner.

Cyberspace and International Law

- The Tallinn Manual and the Use of Force in and through Cyberspace -

*Prof. Dr. Wolff Heintschel von Heinegg
Europa-Universität Viadrina*




U.S. NAVAL WAR COLLEGE
EST. 1845
NEWPORT, RHODE ISLAND



The slide has a dark blue background with a diagonal split and a yellow stripe, matching the cover slide. The left side shows a satellite view of the ocean. A white box on the right contains the text.

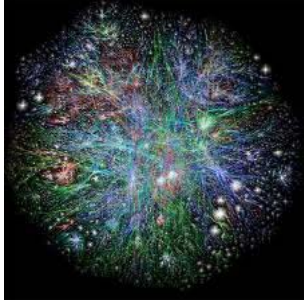

OVERVIEW

- Does International Law Apply At All?
- Cyber Security Issues
- The Tallinn Manual
- Use of Force in and through Cyberspace
- Law of Armed Conflict and Cyber Operations
- Concluding Remarks



Applicability

- Cyberspace =
 - “the interdependent network of information technology infrastructures”
 - ‘Global Common’?
 - ‘5th Domain’?
 - ‘*res communis omnium*’ like the high seas, international airspace and outer space?
- Necessity of ‘new rules’?


Applicability

“The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.”

U.S. President, *International Strategy for Cyberspace* (May 2011)



Applicability


“The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain.”

European Union, Draft Cybersecurity Strategy






Applicability

- Cyberspace requires a physical architecture
- Cyber infrastructure located in territory and subject to territorial sovereignty and jurisdiction
- States exercise jurisdiction over
 - Cyber crime
 - Activities in and through cyberspace
 - Access to cyberspace
- States protect their cyber infrastructure against trans-border interference
- International law applies (subject to necessary modifications)



Cyber Security Issues

- Cyberspace critical resource all economic sectors rely upon
- Offers new opportunities
- Creation of the “digital infrastructure’s architecture was driven more by considerations of inter-operability and efficiency than of security”
- Openness, interoperability and ubiquity created dangerous vulnerabilities

Cyber Security Issues

“Cyber threats to U.S. national security go well beyond military targets and **affect all aspects of society**. Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks and systems that control critical civilian infrastructure. Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause **massive physical damage and economic disruption.**”

DoD, Strategy for Operating in Cyberspace




Cyber Security Issues

- Financial and banking sectors
- Essential services, such as water, healthcare, electricity or mobile services
- Dependence on private sector (“leading role”)
- Threats by private actors, especially by organized crime
- Role of governments?



Traffic Flows (Mbps)

5,000 2,500 1,000 100



Public/Military Dimension

- Growing exercise of State power in and through cyberspace
- “Continued exploitation of information networks and the compromise of sensitive data, especially by nations, leave the U.S. vulnerable”



MANDIANT

APT1
Exposing One of China's Cyber Espionage Units



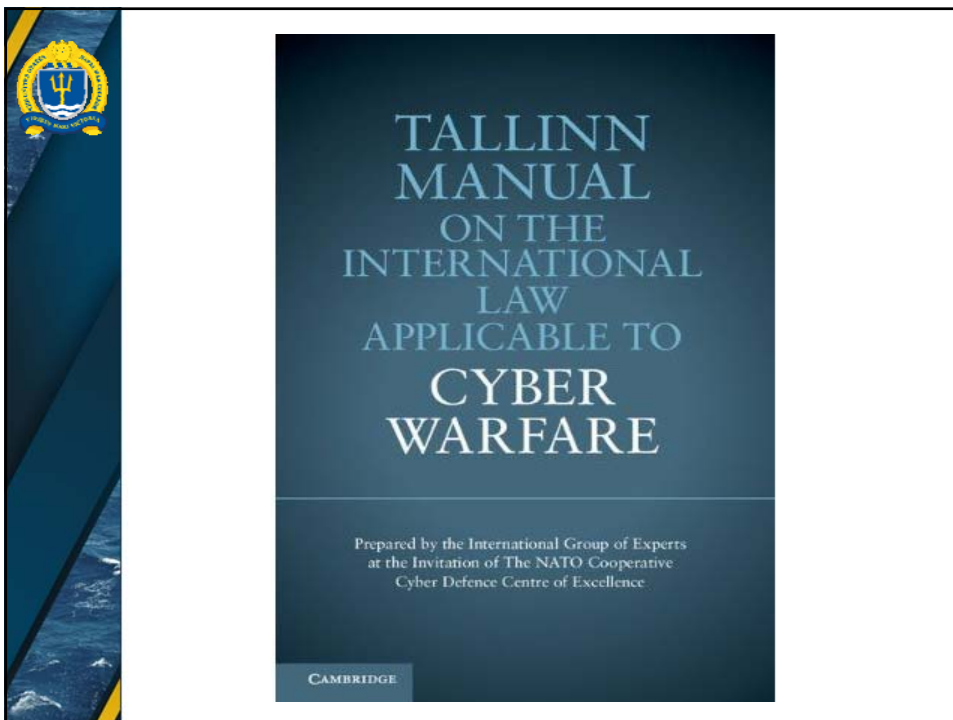
Public/Military Dimension

- Increasing resiliency of critical military/governmental cyber infrastructure
- Defense of critical cyber infrastructure
- Offensive cyber capabilities
- “Military operations depend upon cyberspace for mission success”



Public/Military Dimension

- Estonia (2007), Georgia (2008)
- STUXNET, Drones
- U.S. has “the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests”
- “Significant cyber attacks directed against U.S. economy, government or military” as ‘armed attacks’?







The Tallinn Manual

- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
 - Estonia, United States, Netherlands, Germany, Italy, Latvia, Lithuania, Spain, Hungary, Slovakia, Poland (France and UK joining)
- Three year funding stream
- Final product represents only the views of the experts




Core Group of Experts

- Capt. (Navy) Geneviève Bernatchez, Office of the Judge Advocate General, Canada
- **Air Commodore William Boothby, RAF (ret'd)**
- Col. Gary Brown, US Cyber Command (**Observer**)
- Col. Penny Cumming, Australian Defence Force
- Mr. Bruno Demeyere, Leuven University, Belgium
- Ms. Cordula Droege, ICRC (**Observer**)
- Prof. Robin Geiß, University of Potsdam, Germany
- Prof. Terry D. Gill, University of Amsterdam, Netherlands Defence Academy
- Mr. Ulf Häußler, Allied Command Transformation, NATO (**Observer**)
- **Prof. Wolff Heintschel von Heinegg, Viadrina Europa University, Germany**
- Prof. Eric Jensen, Brigham Young University, USA
- Prof. Jann Kleffner, Swedish Defence College
- Prof. Nils Melzer, Zurich University, Switzerland
- **Prof. Michael Schmitt, US Naval War College**
- Dr. Eneken Tikk, Cooperative Cyber Defence Centre of Excellence
- Brigadier-General (Ret'd) Kenneth Watkin, Canada & USNWC
- Prof. Sean Watts, Creighton University, USA
- Prof. Thomas Wingfield, Marshall Center, Germany (DoD)



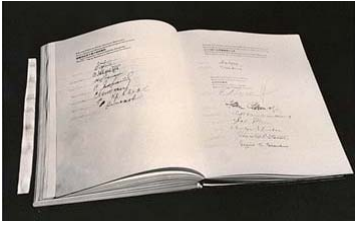
Substance


- Topics
 - Sovereignty
 - Jus ad bellum
 - State responsibility
 - Jus in bello
 - Occupation
 - Neutrality and zones
- Black Letter Rule (unanimity)
- Commentary (includes competing views)



JUS AD BELLUM

Does the cyber operation violate the UN Charter or customary international law regarding the use of force?







Prohibition on the Use of Force

“All members shall refrain ...from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.”

Article 2(4), UN Charter

What is a “Use of Force?”

- **Is “use of force” limited to kinetic force?**
 - Arming guerillas IS a use of force (ICJ)
 - Economic warfare IS NOT (Charter history)
- **Manual’ s suggested approach**
 - Severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement, presumptive legitimacy
- **No clear standard**



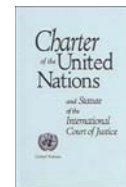
What Cyber Ops Do Not Violate Article 2(4)?

Acts authorized by Security Council

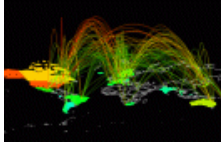

Self-defense under Charter Article 51 or customary international law



Self-Defense When may I Shoot Back?




- Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs ...
UN Charter, art. 51
- May **shoot back** kinetically OR with Cyber Op that is a “use of force”



The Answer?

➤ Key = a cyber “**armed attack**”

- Higher threshold of violence than the “use of force” issue; they meant “armed”



Rules

- A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence
Whether a cyber operation constitutes an armed attack depends on its scale and effects.
 - Must comply with other requirements of self-defense
 - May be exercised collectively



Commentary


The International Group of Experts agreed that any “use of force” that **injures or kills to persons or damages or destroys property** would satisfy the “scale and effects” requirement.

...also agreed that acts of **cyber intelligence gathering** and **cyber theft**, as well as cyber operations that involve brief or **periodic interruption of non-essential** cyber services, do not qualify as armed attacks.”

The case of actions which do not result in this sort of harm but which **otherwise have extensive negative effects** is unsettled.




JUS IN BELLO




Neutrality


- May not use neutral cyber infrastructure for **hostile actions**
- May use “a **public, internationally and openly accessible network** (such as the Internet)” in neutral territory
- Neutral State **must not knowingly allow** acts of cyber warfare to be launched from cyber infrastructure in its territory or under its exclusive control.
- If the belligerent use of neutral cyber infrastructure constitutes a “**serious violation**,” opposing belligerent may (absent feasible & timely alternative) **employ force to terminate** violation of neutral



Lawful Targeting?




- “The Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly direct *their operations* only against military objectives.” AP I, art. 48
- The question: *Does LOAC rule out all cyber mil. ops against other than mil. objectives?*




“Military Operations” Operationalized: “Attacks”

- “The civilian population as such, as well as individual civilians, shall not be the object of *attack*.” AP I, art. 51.2
- “Civilian objects shall not be the object of *attack* or reprisal.” AP I, art. 52.1
- See also, for example:
 - ✓ Indiscriminate *attacks* forbidden (art. 51.4)
 - ✓ *Attacks* limited to military objectives (art. 51.4)
 - ✓ No *attacks* on objects indispensable to civilian population (art. 54.2)
 - ✓ Precautions in *attack* (art. 57)
 - ✓ Precautions against the effects of *attacks* (art. 58)




Attacks?

- AP I, Art. 49: “Acts of *violence* against the enemy, whether in offence of defence”
- Cyber not violent, but violent *consequences* poss.
 - Attacks by analogy to biological/radiological attacks
- Key = prohibitions on “*attacking* protected persons/places, not *targeting* them




The Manual Approach

- A cyber attack is a cyber operation, whether offensive or defensive, which is **reasonably expected to cause death or injury to persons or damage or destruction to objects.**
- **Functionality**
- **Data** if affects functionality




Civilians and Cyber Rules

- “Civilians **are not prohibited** from **directly participating in cyber operations** amounting to hostilities, but **forfeit their protection from attacks** for such time as they so participate.”
- “Civilians enjoy the protection afforded by the law of armed conflict **unless and for such time as they directly participate in hostilities.**”



Commentary

- **Direct participation**
 - Conducting cyber attacks related to the armed conflict
 - Any actions which made possible specific attacks (e.g., identifying vulnerabilities or designing malware specifically to take advantage of particular identified vulnerabilities)
- **Not direct participation**
 - Designing malware without the specific intention that it be used in the conflict
 - Maintaining computer equipment generally, even if such equipment is subsequently used in the hostilities.”



Concluding Remarks

- Tallinn Manual limited in scope but important first step in identification of applicable international law
- Elements of progressive development (State practice?) or ‘slaved to lex lata’?
- ‘Geographical proportionality’
- Contribution to a further fragmentation of international law or to a coherent approach to international cyber security law?

