RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

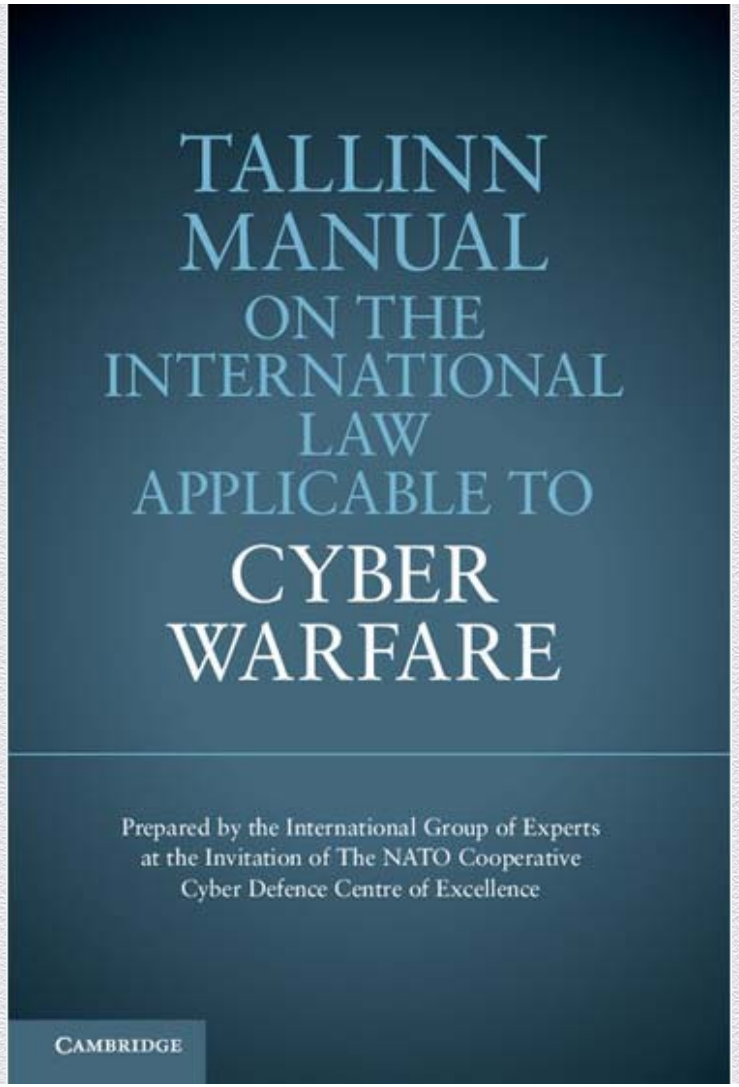
Applying International Law to Cyber Warfare

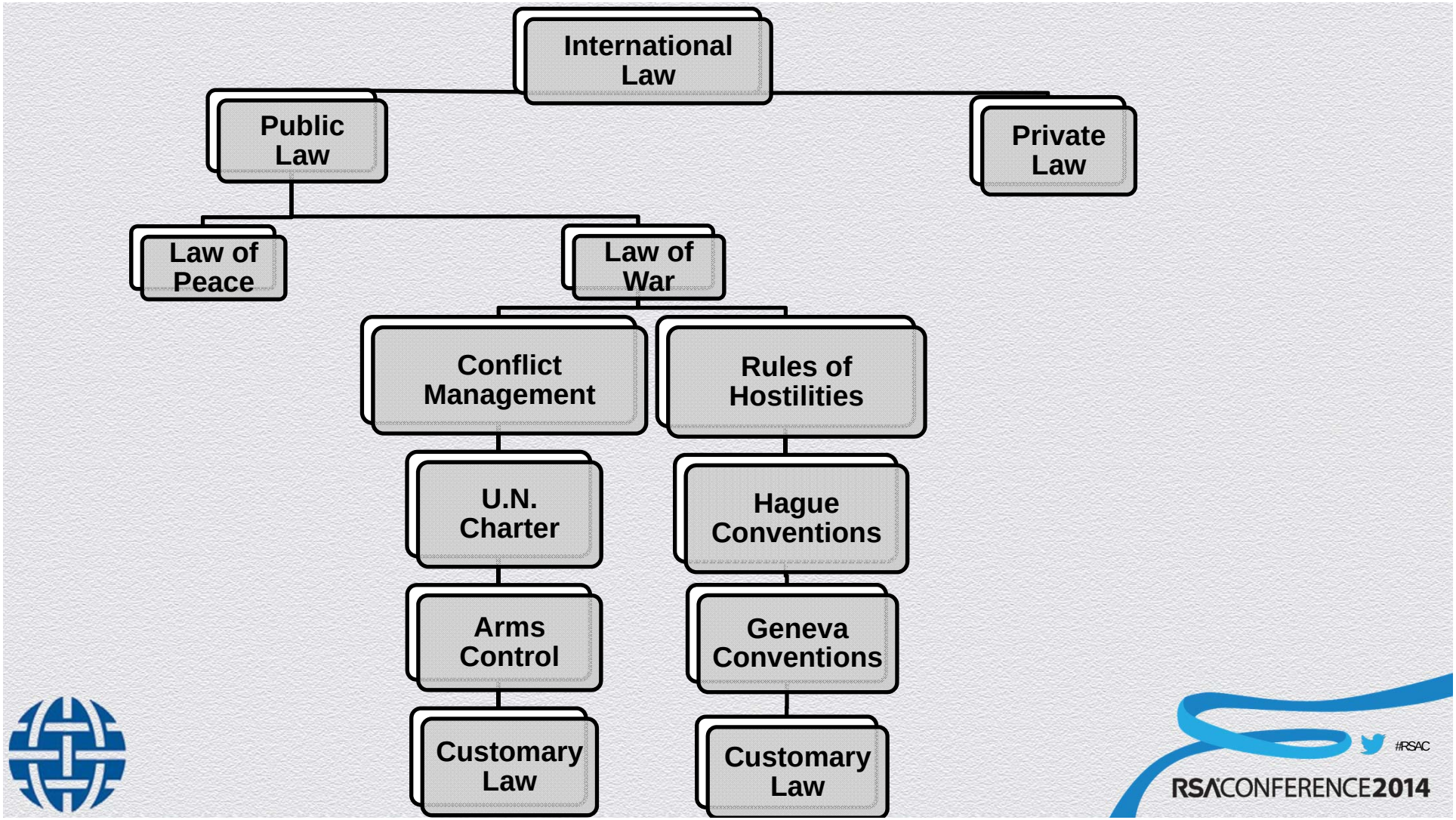
SESSION ID: LAW-F03A

Jason Thelen

Associate Director of the Cyber Statecraft Initiative
Atlantic Council

@AtlanticCouncil





United Nations Charter Article 2(4)

"All members shall refrain in their international relations 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"

Price: 5 Francs
Subscription Rates Listed on Page Two

NEW YORK Herald Tribune EUROPEAN EDITION

50th Year—No. 19,405 PARIS, WEDNESDAY, JUNE 27, 1945

United Nations Adopt World Charter

B29s Bomb 10 Japanese War Plants

Four Industrial Areas On Honshu Blasted by 450 to 500 Super-Forts

Aircraft and Parts Factories Attacked

Osaka Army Arsenal One Of Targets of Raiders

'Boy at the Dike' In a Modern Setting

Crowley Says Reich Policing Must Be Lasting

Asserts Germany Still Has Her Industrial Strength, Despite Allied Bombing

Seized Gold Seen Put to Reich's Use

France Unable to Learn Details of Hoard Seized By American 3d Army

By Geoffrey Parsons Jr.

Ban on Aggression Is Voted, Human Rights Guaranteed

United Nations' New World Charter Provides for Collective Peace Measures and Solution of Social, Economic and Cultural Problems

Closes Conference

President Truman

President Hails Parley's Success

Truman Tells Closing Session of San Francisco Conference It Has Laid Foundation for Lasting Peace

SAN FRANCISCO, June 26. — The charter of the United Nations, a document written in conference here by the representatives of fifty nations to outline their hopes and plans for a future world of peace and security, was formally signed today.

President Harry S. Truman witnessed the signing by delegates of the United States, and addressed the closing session of the conference, praising it for creating "a great instrument for peace and security and human progress in the world."

"But now the world must see it" he said, "otherwise, we shall betray all those who have died in order that we might meet here in freedom and safety to create it."

The delegates, who voted their final approval of the charter at a plenary session late last night, began affixing their signatures at noon. The first was Wellington Koo, of China, who put on his signature with a Chinese writing brush. Sitting in a blue chair before the oval table, Mr. Koo said, "This is a great day for all.

#RSAC

RSACONFERENCE2014

United Nations Charter Article 2(4)

- Outlaws aggressive threats or use of force
- Prohibits 'use of force' rather than 'war'
- Language is complex & subject to various interpretations.

What is a “use of force?”

- **Is use of force limited to physical coercion?**
  - Arming/training guerrillas ***is*** a use of force (ICJ)
  - Economic coercion is ***NOT*** a use of force (Legislative History)

- **Schmidt Test (assessment factors, not formal legal criteria)**
  - *Severity, Immediacy, Directness, Invasiveness, Measurability of effects, Military Character, State involvement, Presumptive legality*

- There is NO clear threshold or standard!

Schmidt Test factors

- ***Severity***: Subject to a *de minimis* rule, consequences involving physical harm to individuals or property will in and of themselves qualify the act as a use of force. Those generating mere inconvenience or irritation will never do so. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scope, duration, and intensity of the consequences will have great bearing on the appraisal of their severity. A cyber operation, like any operation, resulting in damage, destruction, injury, or death is highly likely to be considered a use of force. Severity is self-evidently the most significant factor in the analysis.

Schmidt Test factors

- ***Immediacy***: The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, States harbour a greater concern about immediate consequences than those that are delayed or build slowly over time, and are more likely to characterize a cyber operation that produces immediate results as a use of force than cyber actions that take weeks or months to achieve their intended effects.

Schmidt Test factors

- ***Directness***: The greater the attenuation between the initial act and its consequences, the less likely States will be to deem the actor in violation of the prohibition on the use of force. Whereas the immediacy factor focuses on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, market forces, access to markets, and the like determine the eventual consequences of economic coercion (e.g., economic downturn). The causal connection between the initial acts and their effects tends to be indirect—economic sanctions may take weeks or even months to have a significant effect. In armed actions, by contrast, cause and effect are closely related. An explosion, for example, directly harms people or objects. Cyber operations in which the cause and effect are clearly linked are more likely to be characterised as uses of force.

Schmidt Test factors

- ***Invasiveness***: Invasiveness refers to the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State. As a rule, the more secure a targeted cyber system, the greater the concern as to its penetration. For example, intrusion into a military system (.mil) is more invasive than merely exploiting vulnerabilities of an openly accessible non-accredited system at a civilian university or small business (.com or .edu).

Schmidt Test factors

- ***Measurability of effects***: This factor derives from the greater willingness of States to characterize actions as a use of force when the consequences are apparent. Traditionally, the armed forces carried out operations that qualified as uses of force and the effects of the operations were generally measurable (as in the case of battle damage assessments). In the cyber realm, consequences may be less apparent. Therefore, the more quantifiable and identifiable a set of consequences, the easier it will be for a State to assess the situation when determining whether the cyber operation in question has reached the level of a use of force. Accordingly, a cyber operation that can be evaluated in very specific terms (e.g., amount of data corrupted, percentage of servers disabled, number of confidential files exfiltrated) is more likely to be characterized as a use of force than one with difficult to measure or subjective consequences.

Schmidt Test factors

- ***Military Character****:* A nexus between the cyber operation in question and military operations heightens the likelihood of characterization as a use of force. This contention is supported by the fact that the United Nations Charter is particularly concerned with military actions. Its preamble provides that "armed force shall not be used, save in the common interest", while Article 44 uses the term 'force' without the qualifier 'armed' in a situation that clearly refers to the use of military force. Further, the use of force has traditionally been understood to imply force employed by the military or other armed forces. U.N. Charter, Preamble.

Schmidt Test factors

- ***State involvement***: The extent of State involvement in a cyber operation lies along a continuum from operations conducted by a State itself (e.g., the activities of its armed forces or intelligence agencies) to those in which its involvement is peripheral. The clearer and closer a nexus between a State and cyber operations, the more likely it is that other States will characterize them as uses of force by that State.

Schmidt Test factors

- ***Presumptive legality***. International law is generally prohibitive in nature. Acts that are not forbidden are permitted; absent an express treaty or accepted customary law prohibition, an act is presumptively legal. For instance, international law does not prohibit propaganda, psychological operations, espionage, or mere economic pressure *per se*. Therefore, acts falling into these and other such categories are presumptively legal (although in a particular situation they may in fact violate an international law norm). This being so, they are less likely to be considered by States as uses of force.

Exceptions to Article 2(4)'s Prohibition of the Use of Force

- States' right to individual & collective self-defense (Article 51)
- UN Security Council Chapter VII Authorization

Self-Defense

- **Article 51 of the Charter of the United Nations provides that states may respond in self-defense if an armed attack occurs.**
  - Use of force response can be by cyber or physical means.
- **...but what is an "armed attack?"**

Armed Attack

- **U.S. Position**
  - Use of Force = Armed Attack
- **Tallinn Manual Position (Rule 11)**
  - A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.
  - Must also comply with other requirements (necessity, proportionality, immediacy, and eminency)

Armed Attack (Expert Commentary)

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

Armed Attack (Expert Commentary)

- **The case of actions that do not result in injury, death, damage, or destruction, but which otherwise have extensive negative effects, is unsettled.**
  - Some of the Experts took the position that harm to persons or physical damage to property is a condition precedent to the characterisation of an incident as an armed attack.
  - Others took the view that it is not the nature (injurious or destructive) of the consequences that matters, but rather the extent of the ensuing effects.

Countermeasures (Rule 9)

- **A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.**
  - Countermeasures are necessary and proportionate actions that a 'victim-State' takes in response to a violation of international law by an 'offending State'.

The *Tallinn Manual* is a NATO directive: **FALSE**

The project's conclusions are the opinions of the authors in their private capacities, and not a statement of official policy by NATO, any of its member governments, or any other participating organization.

According to the *Tallinn Manual*, Stuxnet was an act of war by the US: **FALSE**

The International Group of Experts agreed that significant legal and practical challenges stand in the way of definitively declaring an international armed conflict. The group was divided as to whether the operation had reached the armed attack threshold that allows a State that is the target of a cyber operation to exercise its inherent right of self-defense.

The *Tallinn Manual* gives governments permission to kill hackers: **FALSE**

While Rule 33 of the manual states: “[i]n case of doubt as to whether a person is a civilian, that person shall be considered to be a civilian,” the International Group of Experts agreed that an act of direct participation in hostilities by civilians renders them liable to be attacked, by cyber or other lawful means. The group was, however, divided as to whether a presumption against direct participation applies. For example, whether the causal connection between the act of providing malware and a subsequent attack would be sufficiently direct to qualify as direct participation.

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

@AtlanticCouncil

QUESTIONS?

Cyber Statecraft Initiative

- International conflict, competition and cooperation in cyberspace
- Publications at AtlanticCouncil.org
- Public and Private Events