# Panel 4: What is an Act of War Under International Law?

**Moderator:**

**Lt. Col. Mark Visger,** Assistant Professor, US Military Academy, West Point

**Panelists:**

**Col. Gary Corn,** Staff Judge Advocate, US Cyber Command

**Michael Newton,** Professor of the Practice of Law, Vanderbilt University

**Richard Andres**, Professor of National Security Strategy, National War College

Lt. Col. Mark Visger,
Assistant Professor, US Military Academy, West Point

Colonel Gary Corn
Staff Judge Advocate, US Cyber Command

Michael Newton,
Professor of the Practice of Law, Vanderbilt University

Dr. Richard Andres
Professor of National Security Strategy, National War College

# Disclaimer

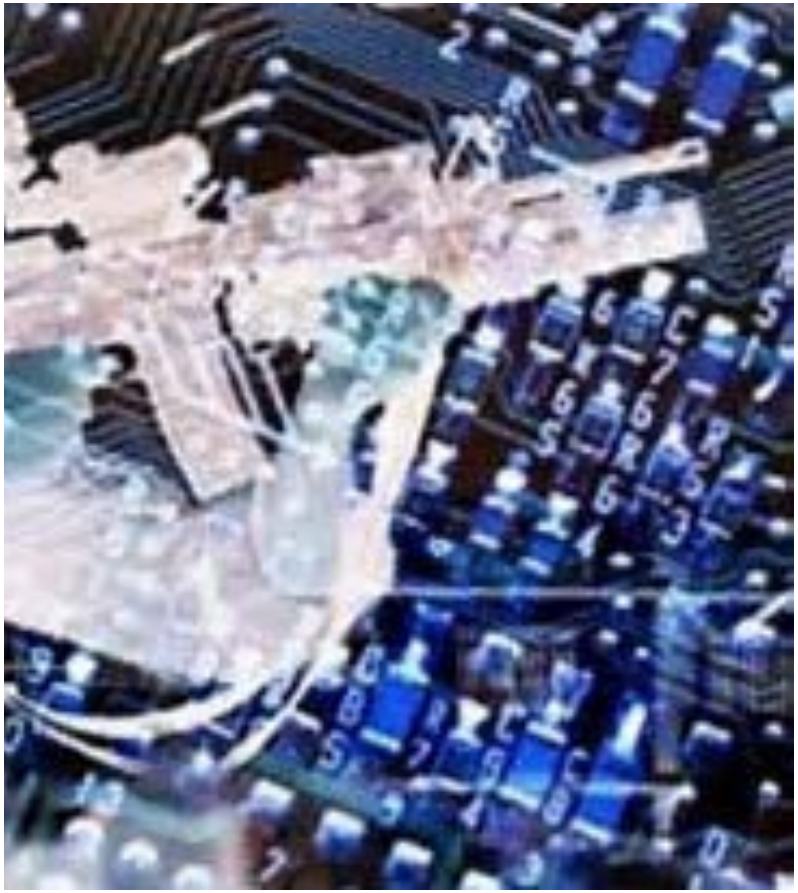
This is not legal advice nor should it be considered legal advice

This presentation and the comments contained therein represent only the personal views of the participants, and does not reflect those of their employers or clients

This presentation is offered for educational and informational uses only

# What is a cyber attack?

- "A cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."
    - Importantly, this definition applies to armed conflict, both in the international and non-international contexts.
- A cyber attack requires an "effort to alter, disrupt, or destroy computer systems or networks or the information or programs on them."



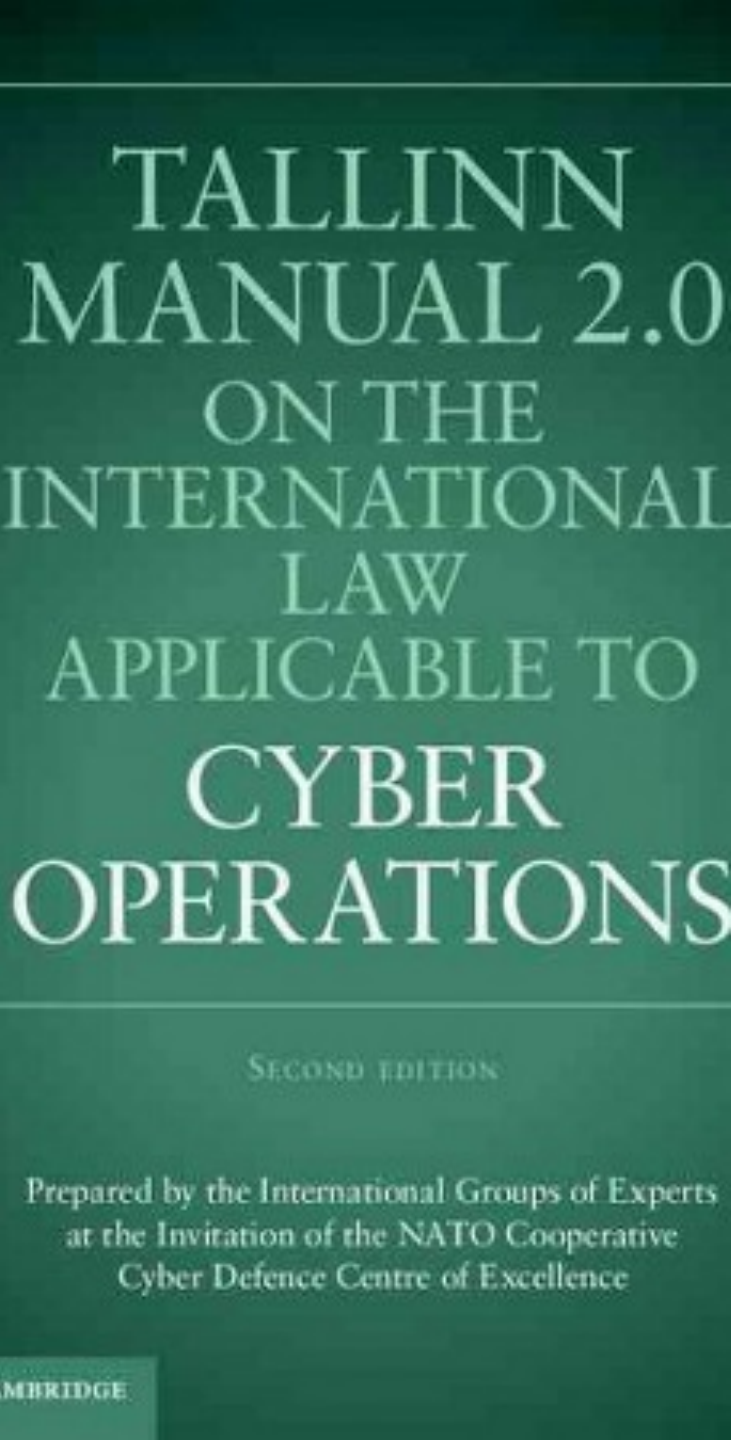
# What is an “act of war?”

- “Act of war” retains political meaning.
- As technical legal matter, this term has been replaced by provisions in the U.N. Charter.
    - UN Charter prohibits the use of “force” by states against each other, and it affirms that states have a right of self-defense against “armed attacks.”
    - State military response to a cyber hostility would only be legal under the UN Charter if the cyber hostility rose to the level of “armed attack.”
- A decision to employ force must rest upon the existence of a viable legal basis in international law and domestic law.[1]



# What is considered a “use of force” and an “armed attack?”

- “Use of force” and “armed attack” are not defined in the UN Charter
  - No consensus on the exact threshold at which a cyber activity crosses into the use of force or when a use of force qualifies as an armed attack.
- Minority US position: “Use of force” and “armed attack” are equivalent for purposes of international self defense
- Tallinn Manual approach: not all cyber actions are uses of force, and not all uses of force qualify as an armed attack.
  - The scale and effects of an act
  - Applied by analogy to kinetic acts.

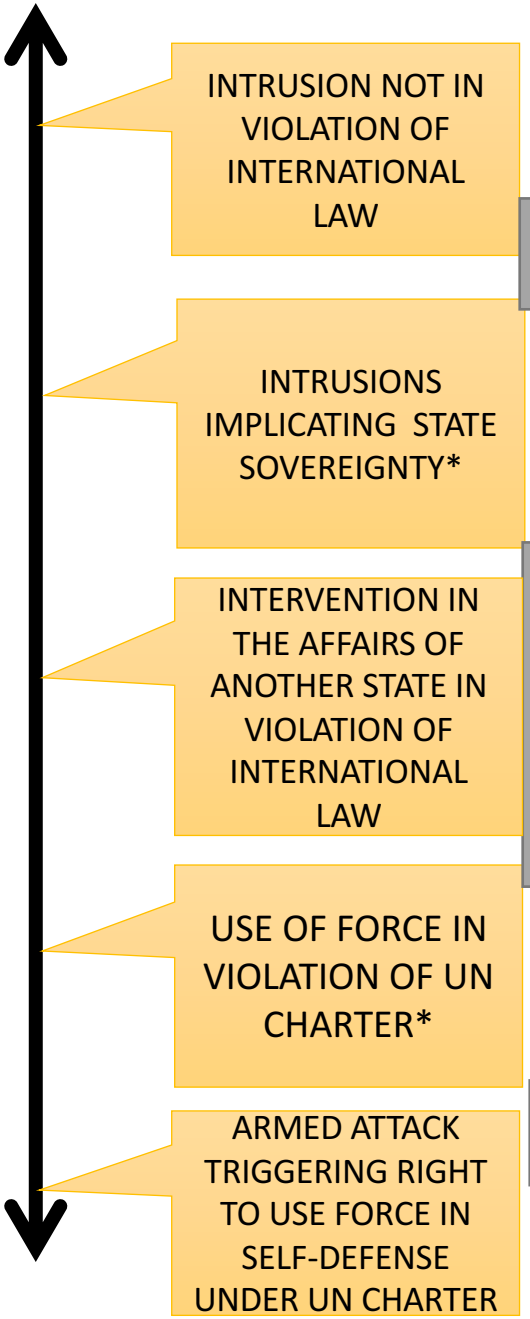





# What is the Tallinn Manual?

- An academic, non-binding study on how international law applies to cyber conflicts and cyber warfare.
- Written at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence by an international group of approximately twenty experts.
- Main tenet: cyber warfare is governed by international law already in force, particularly the rules that regulate the commencement of an armed attack and the rules that regulate the conduct of armed conflict.

# SPECTRUM OF CYBER INTRUSIONS UNDER INTERNATIONAL LAW




## TRIGGERS RETORSION BY NATION-STATE

Sovereignty includes "right to exercise therein, to the exclusion of any other State, the functions of a State." (Island of Palmas arbitration) *Ambiguity as to role of sovereignty in cyberspace

"States [may not] intervene directly or indirectly in internal or external affairs of other States." (Nicaragua ICJ Judgment)

## TRIGGERS COUNTERMEASURES, RETORSION BY NATION-STATE

UN 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."
*U.S. position: All uses of force trigger state's right to use force in self-defense

## TRIGGERS RIGHT TO USE OF FORCE IN SELF-DEFENSE BY NATION-STATE

# Tallinn Manual's Position on the Spectrum of Cyber Intrusions

Rule 4: "A State must not conduct cyber operations that violate the sovereignty of another State."

Rule 66: "A State may not intervene, including by cyber means, in the internal or external affairs of another State."

Rule 69: "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."

Rule 71: "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."

# What is considered the "use of force" and an "armed attack" in the Tallinn Manual?

Use of Force: 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.

- Acts that injure or kill persons or damage or destroy objects are unambiguously uses of force
- Cyber operations that are analogous to other kinetic actions that would be described as uses of force
- Factors: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, presumptive legality

Armed Attack: the scale and effects required for an act to be characterized an armed attack (prompting right to use force in self-defense) necessarily exceed those qualifying as a use of force.

# What does U.S. consider to be a "use of force"/"armed attack"?

U.S. government has definitively taken the public position that *some* cyber-attacks, even though carried out through digital means rather than kinetic violence, *could* cross the UN Charter's legal thresholds of "force"/"armed attack."

- *"Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action …, the target and location, effects and intent, among other possible issues."* Harold Koh (Legal Advisor to State Dept.) CYBERCOM speech (2012)

# What other issues remain?

- Attribution/Law of State Responsibility
- Private individual attacks
- Issues with hacking back
- Attacks with Economic Impact Only
- Attacks with Data Loss Only
- Attack on Network Infrastructure
- Foreseeability of Adverse Effects
- Criminal Activity or Terrorism or “Act of War”?
- Posse Comitatus
- Government- Private Sector Cooperation
- Espionage

# Questions?

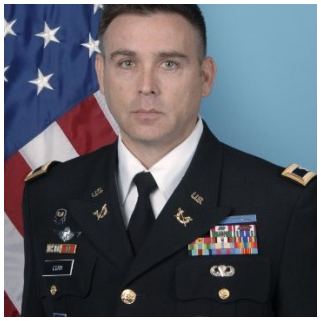
# Appendix

Lt. Col. Mark Visger,
Assistant Professor, US Military Academy, West Point

Contact:
E: Mark.Visger@usma.edu

Lieutenant Colonel Mark Visger currently serves as an Assistant Professor in the Department of Law at the U.S. Military Academy at West Point. During his four-year tenure as Assistant Professor, Colonel Visger has served as course director for three courses—Cyber Law, International Law, and National Security Law; and he also teaches Constitutional and Military Law. In addition to his teaching experience, Colonel Visger has served as a Judge Advocate (military attorney) in the U.S. Army since 1997.

During his tenure as a Judge Advocate, Colonel Visger has served in a number of legal positions, including serving as the Staff Judge Advocate (general counsel) to the Commanding General of First Army Division West at Fort Hood, Texas. He has also worked extensively in prosecuting and defending cases under the Uniform Code of Military Justice, and has earned an Expert Military Justice Practitioner qualification. In addition, Colonel Visger has deployed to Iraq and Bosnia-Herzegovina, where he advised the command on the International and Operational Law aspects of re-building each country. Colonel Visger received his J.D. (Magna Cum Laude) from Washington and Lee University School of Law and his LL.M. (Harlan Fiske Stone Scholar) from Columbia Law School.



Colonel Gary Corn
Staff Judge Advocate, US Cyber Command

Contact:
E: gpcorn@cybercom.mil

Colonel Corn is presently assigned as the Staff Judge Advocate (General Counsel) to US Cyber Command, the Department of Defense's strategic headquarters responsible for organizing and developing cyber resources, defending all U.S. military networks, and, when directed, synchronizing and conducting the full spectrum of cyberspace operations. He has previously served in a number of assignments as a legal advisor at the brigade, division and corps level, to include on deployment to the Former Yugoslav Republic of Macedonia as part of the United Nations Preventive Deployment Force and as the Chief of International Law for Combined Forces Command, Afghanistan. His assignments included multiple tours as both a line and supervisory military prosecutor, a Senior Litigation Attorney with the United States Army Litigation Division, and a Deputy Legal Advisor to Joint Task Force Six, the Department of Defense command responsible for providing counterdrug support to civilian law enforcement agencies within the United States.

Colonel Corn has also served in a number of strategic-level positions within the Department of Defense, to include as a Special Assistant United States Attorney with the United States Attorney's Office for the District of Columbia, the Staff Judge Advocate (General Counsel) to United States Army South, a Deputy Legal Counsel in the Office of the Legal Counsel to the Chairman of the Joint Chiefs of Staff, and the Chief of the Operational Law Branch in the International and Operational Law Division of the Office of the Judge Advocate General of the Army.

Colonel Corn earned a BA cum laude in International Relations from Bucknell University in 1987, a JD with honors from the George Washington University in 1993, an LLM in International Law from the U.S. Army Judge Advocate General's Legal Center and School in 2002, and an MA in National Security Studies as a Distinguished Graduate from the United States Army War College in 2013. He is also a graduate of the Escola de Comando e Estado Maior do Exército do Brasil (Command and General Staff College of the Brazilian Army).

Michael Newton,
Professor of the Practice of Law, Vanderbilt University

Contact:
E: mike.newton@Law.Vanderbilt.Edu

Michael Newton is an expert on accountability, transnational justice, and conduct of hostilities issues. Over the course of his career, he has published more than 80 books, articles and book chapters. He is an elected member of the International Institute of Humanitarian Law and the International Bar Association. At Vanderbilt, he developed and teaches the innovative International Law Practice Lab which provides expert assistance to judges and lawyers, governments, and policy-makers around the world. Under his leadership, Practice Lab students have completed projects for ongoing litigation, international organizations such as the UN Office of Drugs and Crime and the Conduct and Disciplinary Office, and Foreign Ministries in a number of nations.

Professor Newton is presently serving on the Advisory Board of the ABA International Criminal Court Project. As the senior advisor to the Ambassador-at-Large for War Crimes Issues in the U.S. State Department, Professor Newton implemented a wide range of policy positions related to the law of armed conflict, including U.S. support to accountability mechanisms worldwide.

Professor Newton began his distinguished military career as an armor officer in the 4th Battalion, 68th Armor, Fort Carson, Colorado, until his selection for the Judge Advocate General's Funded Legal Education Program. He deployed on Operation Provide Comfort to assist Kurdish civilians in Northern Iraq, as well as a number of other exercises and operations. From 1993-95 he was reassigned as the brigade judge advocate for the 194th Armored Brigade (Separate), during which time he organized and led the human rights and rules of engagement education for all Multinational Forces and International Police deploying into Haiti. He subsequently was appointed as a professor of international and operational law at the Judge Advocate General's School and Center in Charlottesville, Virginia from 1996-99.

Dr. Richard Andres
Professor of National Security Strategy,
National War College

Contact:
E: AndresR2@ndu.edu

Dr. Richard B. Andres is Professor of National Security Strategy at the National War College. Before coming to NWC, Andres served in a number of policy positions within the Department of Defense including Special Advisor to the Secretary of the Air Force. His research focuses on the national security implications of new technology. He has led senior strategy development teams for the White House, Office of the Chairman of the Joint Chiefs of Staff, Office of the Secretary of Defense and other civilian and military organizations on topics such as national cyber security strategy, military energy policy, deterrence strategy, and military planning for the wars in Iraq and Afghanistan.

# Case Law

# Doe v. Fed. Democratic Republic of Ethiopia 851 F.3d 7 (2017)

- **Facts:** Plaintiff John Doe ("Kidane")—claims he was tricked into downloading a computer program. The program allegedly enabled the Federal Democratic Republic of Ethiopia to spy on him from abroad. He wants to sue the Republic of Ethiopia. But foreign states are immune from suit unless an exception to the Foreign Sovereign Immunities Act (FSIA) applies. Kidane invokes the FSIA's exception for noncommercial torts.
- **Holding:** The non-commercial tort exception did not apply because the entire tort (the placement of spyware in an email attachment that infected the user's computer when he opened it) did not take place within the United States as required; rather, the tortious intent aimed at the user plainly lay abroad and the tortious acts of computer programming likewise occurred abroad.
    - The noncommercial-tort exception abrogates sovereign immunity for a tort occurring *entirely* in the United States. Kidane, by contrast, alleges a transnational tort. Therefore the court affirmed the district court's dismissal for lack of subject matter jurisdiction.

# Legislation and Executive Orders

# Legislation

- H.Res.200 – 115th Congress:

Expresses the sense of the House of Representatives that the United States should adopt a comprehensive cybersecurity policy that clearly defines acts of aggression, acts of war, and other related events in cyberspace, including any commensurate responses to any such act or event.

- Introduced Mar. 16, 2017 & referred to House Committee on Foreign Affairs
- Cyber Act of War Act of 2016
- S.2905 — 114th Congress (May 9, 2016)
- H.R.5220 — 114th Congress (May 12, 2016)

This bill directs the President to: (1) develop a policy for determining when an action carried out in cyberspace constitutes an act of war against the United States, and (2) revise the Department of Defense Law of War Manual accordingly.

In developing this policy, the President shall consider: (1) the ways in which a cyber attack's effects may be equivalent to a conventional attack's effects, including physical destruction or casualties; and (2) intangible effects of significant scope or duration.

- Failed – Adjourned, executive deadline past (had 180 days)

# Exec. Order No. 13800

- "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (May 11, 2017)
- Holds heads of executive departments and agencies responsible for IT security
- Outlines best practices and risk management strategy – such as upgrading from outdated or unsupported O/S
- Required Risk Management Reports to appropriate oversight agencies and agency heads within 90 days
- Specifies "Resilience Against Botnets and Other Automated, Distributed Threats
- References PPD-41 "United States Cyber Incident Coordination" (July 26, 2016) – requires joint level assessment of the potential scope and duration of… power outage[s] associated with a significant cyber incident

# Other Cyber Related Exec. Orders

**Exec. Order No. 13757**

"Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (Dec. 28, 2016)

- Response to Russian Election Interference
- Election interference added as a reason for freezing assets
- Added a list of specific entities and individuals whose assets are frozen (all Russian)
- Permits Sec. of Treasury, with A.G. and Sec. of State to determine when & if property can be unblocked
- Added to: Exec. Order No. 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"

**Exec. Order No. 13694**

"Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 1, 2015)

- Prevents all property and interests in property in the United States, or that come within the control or possession of and U.S. person, belonging to entities or individuals deemed to be engaged in "malicious cyber-enabled activities" from being transferred, paid, exported, withdrawn, or otherwise dealt in
- References PPD-21 "Critical Infrastructure Security and Resilience" (Feb. 12, 2013) definition of "critical infrastructure sector"

# United States Cyber Command

- Announced elevation to the status of a Unified Combatant Command focused on cyberspace operations on Aug. 18, 2016
- "The elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries." — Statement by President Donald J. Trump on the Elevation of Cyber Command
- Signed into law on Dec. 23, 2016 as part of NDAA FY2017 – created by 10 USCS § 167b
- Unifies command of Army Cyber Command, Fleet Cyber Command, Air Forces Cyber and Marine Corps Cyberspace Command