Cyberattack as Use of Force
A talk with Professor Duncan Hollis

- Increasing importance and attention on cyber warfare and the laws governing cyberspace
    - 2022 Russian-Ukrainian conflict highlighted cyberattack risks, including increased risks to the U.S. government private sector as a potential response to U.S. for sanctions against Russia and support for Ukraine
    - March 2022, Biden administration stated that it would use every tool to respond to cyberattacks against critical infrastructure and urged private sector entities to bolster cyber defense.

- Cyberwarfare and international laws
    - Development of legal landscape in cyberspace
        - Domestic context: In the early days of the digital age, John Perry Barlow's 1996 A Declaration of the Independence of Cyberspace posited that the U.S. government does not have authority to regulate the internet. Today, it is generally accepted among the states that they do have authority to regulate cyberspace within its borders.
        - International context: Russia's 1998 letter to the UN "Developments in the Field of Information and Telecommunications in the Context of International Security" first began the international conversation around the need for a treaty to regulate information and communication technologies (ICTs). Russia at the time was concerned about the use of ICTs in information warfare. Spurred the creation of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE).
        - In 2013, UN GGE recognized that international law applies in cyberspace.
    - How does international law apply? Issues with international law's application to cyberspace
        - Duncan Hollis, Four Challenges for International Law and Cyberspace: Sartre, Baby Carriages, Horses, and Simon & Garfunkel Part 1 (May 2, 2019) and Part 2 (May 2, 2019), Council on Foreign Relations Blog
        - Existential disagreements about whether certain laws apply
            - E.g., disagreements on whether international humanitarian laws apply. In 2021, UN GGE in its consensus report noted that humanitarian law applies in situations of armed conflict and may apply in cyberspace.
        - Existential debates about interpretation
            - H.L.A. Hart, Positivism and the Separation of Law and Morals, 71 HARV. L. REV. 593 (1958).

        - Lon Fuller, Positivism and Fidelity to Law---A Reply to Professor Hart, 71 HARV. L. REV. 630 (1958).
        - E.g., agreement on the prohibition of use of force in cyberspace (UN Charter Article 2(4)), disagreement on what cyber activities constitute use of force
    - Disagreement on whether we need a law of cyberspace or whether existing rules are sufficient
        - Judge Frank Easterbrook's 1996 Cyberspace and the Law of the Horse argued against the need for new and discrete laws applicable to cyberspace.
        - Lawrence Lessig's 1999 response The Law of the Horse: What Cyberlaw Might Teach argued for the need for cyberspace laws and the importance of studying cyberlaw to learn about how laws affect behaviors and values.
    - Secrecy and attribution complicate cyberwarfare. When states are silent and practices are covert, it makes more challenging construction of customary international law.
        - Customary international law requires states to widely adopt a practice and recognize it as a legal obligation. While some states have started stating positions on international laws in cyberspace, most states are silent.
    - More on issues with international law application: Duncan Hollis, A Brief Primer on International Law and Cyberspace, Carnegie Endowment (June 14, 2021).
  - International law sources
    - Conventions, treaties: express agreement of states
    - Custom: general practice accepted as legal obligations
    - General principles

- What is a cyberattack
  - CIA Triad – general model in information security
    - Confidentiality: protecting against data breaches
    - Integrity: data trustworthy, complete, and not altered
    - Availability: data accessible when needed (e.g., ransomware or DDoS attacks affect availability)
  - Stuxnet attack
    - Stuxnet worm, first discovered in 2010 and believed to be created by the U.S. and Israel to target Iran's nuclear facilities, destroyed centrifuges in Iran's Natanz facility.
    - Duncan Hollis, Could Deploying Stuxnet be a War Crime?, Opinio Juris (January 25, 2011).
  - Use of force
    - UN Charter

- Prohibition on use of force: 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*.

- Exception to prohibition for in self-defense: 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, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*

- Exception to prohibition when authorized by the Security Council: Article 39 — *The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.*

- Tallinn Manual
  - Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press (1.0 and 2.0)
  - Evaluating cyber activity as a use of force
    - Conduct that rose to level of armed attacks and acts that injure or kill people or destroy objects, the effects of which are analogous to previous kinetic conflicts
    - Factors: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, presumptive legality.
- Effects doctrine: if the effects of a cyber activity are analogous to the effects of a kinetic operation, may rise to use of force. Cyber operations that result in death or significant damage more likely to be use of force.
- Differing interpretations of armed attack and use of force
  - U.S. position is that armed attack and use of force is analogous, and any unlawful use of force potentially triggers Article 51 self-defense.

- Most states' position is that the level for armed attack is higher than use of force, thus a higher threshold for lawful Article 51 self-defense.

- Non-state actors
  - Do states have a due diligence obligation or a duty to prevent non-state actors from conducting cyberattacks on other states?
    - When action can be attributed to the state (effective control). Nicaragua v. United States (1986): the International Court of Justice affirmed the effective control standard.
    - Effective control is a high standard; may not be enough to merely fund or arm the non-state actor.
  - Duty of due diligence
    - Due diligence principle – states' general obligation to not allow their territory to be used to breach international rights of other states
  - Challenges in holding states responsible for non-state action
    - Technical attribution
    - When the state is capable but unwilling to act against non-state actor
    - If the harmed state decides to respond with retaliatory cyberattacks, risk of escalation

- Influence operations (IOs)
  - Example: Russia's influence operation on 2016 elections in the U.S.
  - International laws implicated in IOs
    - International criminal law and/or Article 2(4) implicated when IOs involve use of force
    - Duty of nonintervention
    - Sovereignty
    - Human rights law
    - Principle of self-determination
  - Duncan Hollis, The Influence of War; The War for Influence, 32 TEMPLE INT'L & COMP. L.J. 31 (2018).