THE LAW OF WAR IN CYBERSPACE

Jessica Malekos Smith, sources cited in-text

Terminology:
The *Tallinn Manual* (2013) defines a **CYBER ATTACK** as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."

U.N 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."
Article 51:
"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense 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."

Cyber Intrusion **–** "(a cyber operation short of an attack) into another state's cyber systems would not constitute a use of force, nor would it violate international law." (*See* Gary D. Solis, *Cyber Warfare*, 219 Mil. L. Rev. 1, *15, (2012).

(1) ***De minimus*** **damage/injury threshold;**
"'Attacks' means acts of violence against the adversary, whether in offense or in defense (*See Additional Protocol I, Article 49.1)*

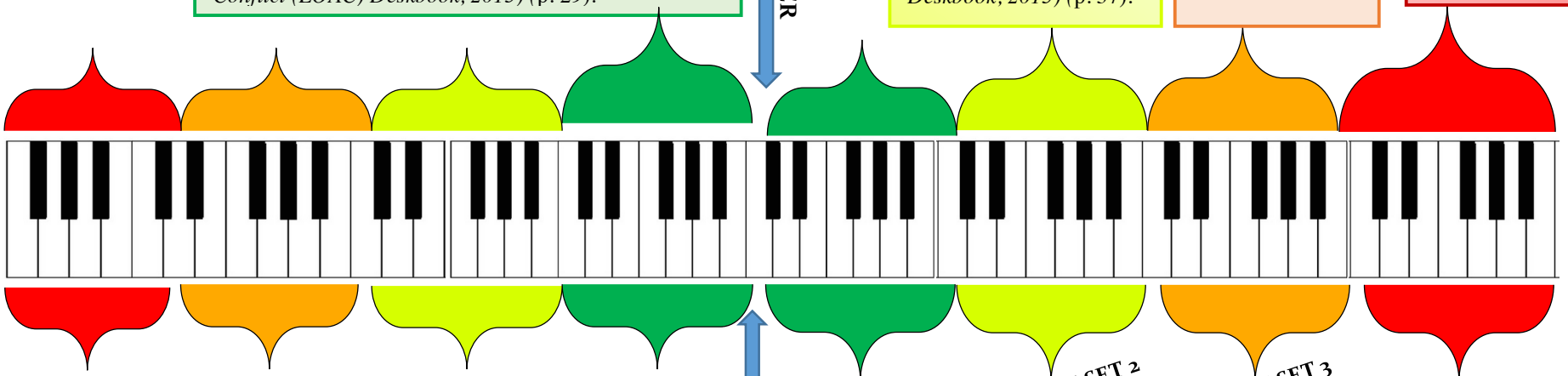
(2) "Any decision to employ force must rest upon the existence of a viable legal basis in ***International law*** **as well as in** ***domestic law*** (including application of the 1973 War Powers Resolution (WPR), Public Law 93-148, 50 U.S.C. §§ 1541-1548)." (*See Law of Armed Conflict (LOAC) Deskbook, 2015)* (p. 29).

U.N. CHARTER

Anticipatory Self-Defense "justifies using force in anticipation of an **imminent armed attack."** (*See LOAC Deskbook, 2015)* (p. 37).

Victim state's response to kinetic attack launched by **non-state entity –** answer may rest on issues of state responsibility and ability to satisfy higher burden of proof to invoke a use of force in self-defense (*See LOAC Deskbook, 2015)* (p.39).

Preventative Self-Defense **–** employed to counter non-imminent threats is **illegal under international law.** *(See LOAC Deskbook, 2015)* (p. 39).



OCTAVE SET 1: Permissible State Action

OCTAVE SET 2 Likely Permissible State Action

OCTAVE SET 3 'Somewhat' Permissible State Action

OUT OF RANGE

"MIDDLE C"

A ***cyber attack*** requires an "effort[] to alter, disrupt, or destroy computer systems or networks or the information or programs on them[.]" (Matthew Waxman, 36 YALE J. INT'L L. 421, 422 (2011). Next, if the act produces "death, damage, destruction or high level disruption," it yields a ***violent effect***. (*See Gorman & Barnes, Cyber Combat: Act of War,* WALL ST. J (May 31, 2011).

According to USAF MAJ GEN. Charles Dunlap, Jr. JAG, (ret.) "cyber attacks that have a violent effect are the legal equivalent of armed attacks, or what the military calls a 'use of force.'" In military parlance, "use of force" is regarded as an armed attack. (*See Gorman & Barnes*).

Thus, a theoretical equation for calculating a "Use of Force" in Cyberspace → Cyber attack(s) + Violent Effect(s) = Use of Force under Article 2(4)