It can be said that the global war occurring in Cyberspace is just as deafening as traditional warfare. There is much to be conveyed when comparing the two. “The difference between traditional kinetic warfare and cyber warfare is that kinetic warfare exists only in the physical world whereas cyber warfare exists in both a physical world and a cyber one” (A, 2022). Additionally, where we are used to reading about landscapes and Man versus Man, machines, and Man almost seem to become one because “cyberspace is a man-made environment and is therefore unlike the natural domains of air, land, maritime, and space” (A, 2022). Machines meshing with Man in Cyberspace often “encompasses the use of all digital system "tools" available to paralyze or even destroy the enemy's ICT-technology-based systems while keeping one's systems operational” (A, 2022). It can be said in specific discussions that traditional warfare also has similar caveats.

Shifting gears a bit, a stark contrast comes from ethical and lawful discussions. How far is too far? The lines are blurry inside Cyberspace compared to traditional warfare. While discussing the unknowns of Cyber Operations, Peter Stockburger points out, “there are known knowns: there are things we know we know. We also know there are known unknowns: that is to say, we know there are some things we do not know. However, there are also unknown unknowns—the ones we don't know we don't know” (2016, p.546). To sum up another way, Stockburger concludes, “there is simply not enough State practice to say, with certainty, what the customary international law requires when it comes to cyber operations and the prohibition against the use of force” (Stockburger, p.583). For example, in everyday cyber operations on a federal level, we see intelligence in the form of offensive and defensive, policies and procedures, personnel, legal frameworks, training, and awareness as a complete circle approach. An unknown for each area can be seen below:

Intelligence in the form of Data mining against foreign adversaries. Possible Unknown includes undetected not and malicious malware. Policy concerns occurring in the Zero Trust Policy. Possible Unknown includes increased detail-oriented work resulting in decreased efficiency—personnel concerns for Expertise versus Dependability. Possible Unknown includes overlooking better algorithms versus completism of mission on time with an average algorithm—legal battles in International Law. Possible Unknown includes Top Secret Federal entities existing in grey areas of Cyberspace. Training problems with Possible Unknowns include human errors regarding poor cyber awareness.

Another unknown that exists on all levels of Cyber Operations is the pressure on each “combatant command” because each “combatant commands with assigned geographic areas are unique in that each military service has portions of its service networks that fall within the geographic purview of different combatant commands" and each has "functional responsibilities since many global capabilities are provided by the military services (Air Land Sea Space Application (ALSSA) Center, 2022). Arguably one of the most frighting unknowns to occur in Cyberspace. How much pressure is just enough, and where is the line for the mission acceptable too much?

References

Air Land Sea Space Application (ALSSA) Center. (2022). *DOD Cyberspace: Establishing a Shared Understanding and How to Protect It*. Retrieved From https://www.alsa.mil/News/Article/2891794/dod-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/.

A. (2022, September 28). *Cyber Warfare – The game changer in the battlespace - Cyberwatch Finland*. Cyberwatch Finland. Retrieved From https://www.cyberwatchfinland.fi/cyber-warfare/.

Stockburger, Peter Z. (2016) "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum," American University International Law Review: Vol. 31: Iss. 4, Article 2.
Retrieved From http://digitalcommons.wcl.american.edu/auilr/vol31/iss4/2.