Joint All-Domain Kill Webs

The traceability of human agency

by Maj Chris Pavlak

As the U.S. military postures itself for strategic competition, battlefield effectiveness will depend on its ability to outperform the decision-making cycle of its pacing threats. The U.S. military has been developing new concepts for multidomain operations, intended to better integrate operations in the air, land, maritime, space, cyberspace, and electromagnetic spectrum domains. It already conducts multidomain operations today, but current initiatives aim to expand the scope, scale, and speed of such operations resulting in what has been coined "convergence."[1]

Convergence means collecting data from sensors, analyzing it, discerning the important information, sending it to the relevant operators, and optimally responding with the right munitions, from the right platform, at the right time. Achieving convergence will require an increasingly integrated and interoperable force with a shared understanding of the common operating environment.[2] The DOD envisions joint kill webs that can rapidly and efficiently link any sensor to any shooter—the principle of convergence—through the concept of Joint All-Domain Command and Control.[3] In other words:

> The Army has the weapons, observe, orient, decide, act (OODA) loop, and kill chain for land-based problems. The Navy has the weapons, OODA loop, and kill chain for sea-based problems. The Air Force has the weapons, OODA loop, and kill chain for air-based problems. There's also space, cyberspace, and electronic warfare with their own weapons, OODA loops, and kill chains. We need to replace these two-dimensional kill chains (the static linear sequence of events) with a six-dimensional kill web (connect all six domains of warfare into a dynamic network) at all echelons of command.[4]

Conceptualizing and more importantly—understanding—the extended battlespace in which the integrated and distributed force operates in furtherance of secure information parsimony (i.e., the right information, delivered to the right person, at the right time, and at the right place) will require networks, waveforms, connectivity, distributed command and control, and integrated platforms—many of them automated, deciding and acting at the speed of machines.[5] It will occur to such a degree that monitoring the myriad decisions being made across the battlespace with fidelity and transparency may need its own automated oversight akin to the dynamic and emergent environment found in financial sectors.

... it may be difficult ... to distinguish between which inputs and decisions are human and which are machine ...

However, this convergence of capabilities means that machines and sensors are no longer tactical adjuncts within the U.S. military. They are becoming increasingly relied upon and even deferred to as tactical decision aids. As we increase the complexity of the battlespace by weaving kill chains into kill webs across multiple domains and augment human tasks with machines at all echelons of command, humans and machines will both influence each other in an iterative process.

Thus, a hybridization will occur. Humans and machines will become so task-intertwined that they collectively exhibit entirely new emergent behaviors that may obfuscate where a machine's behavior ends and where human agency begins. This leads to iterative interactions between both humans and machines resulting in hybrid organizational systems that exhibit behaviors and produce effects all their own. More specifically, as these new technologies integrate with other existing ones and density increases, it may be difficult or even impossible to distinguish between which inputs and decisions are human and which are

>Maj Pavlak is an Intelligence Officer with the Marine Innovation Unit. In his capacity as a Strategic Capabilities Transition Officer, he identifies existing and emerging capabilities across the DOD and intelligence community for transition to the Marine Corps in furtherance of solving* Force Design 2030 *problems. He is also the author of* From Lawyer to Warrior, *released in January 2023 (https://www.lawyertowarrior.com), and was a guest on the MCA podcast,* Scuttlebutt *(Episode 69).

machine, and how they might be arriving at their decisions, appraisals, or predictions. With this interactive complexity, it is often impossible to isolate individual causes and their effects because the parts are all connected in a complex web.[6] These phenomena are indicative of emergent systems.[7] (They are also known as non-linear systems.) Complicating things further, kill webs are more complex than traditional supported/supporting relationships due to both the engagement density of the assets within the web and the potential simultaneity of requests for approval happening in realtime. What emerges is a complex group dynamic that cannot be divined from the rules for individuals. The global behavior of an emergent system is qualitatively different from the behavior of its parts, and in the act of separating the component parts, they lose their coherence, meaning, and context.[8] Identifying where a machine's agency ends and a human's agency begins becomes problematic.

Moreover, legal causation tests tend to break down when applied to emergent systems. The kinds of phenomena that kill webs exhibit will have profound implications for legal analyses, which rely on evidence of human behavior and agency when determining foreseeability, causal relationships, and ultimately what a human being might be thinking or intending. As machine autonomy intercedes on human agency, both redistributing it and rearranging it, it confounds the norms we have long relied upon for ascribing legal and moral responsibility and for holding people and institutions accountable.[9] As we weave kill chains into kill webs, we are simultaneously increasing the complexity of interactions between humans and machines with subsystems in a single domain and then, those myriad interactions will be integrated across multiple domains at all echelons of command. What happens when we put a single linear path—the chain of legal causation, against a dynamic, modular, and non-linear kill web? A complex adaptive system of both offensive and defensive tactics operating as a kill web may make the traceability of human agency within it nearly impossible to identify.

Recommendation

To fully understand the implications of automation-augmentation, organizational leaders could adopt a relational ontology that accepts that, in the Digital Age, human and machine agents are so closely intertwined in hybrid collectives that the relationships between them determine their actions. Blockchain technology (BCT) may be a new paradigm of risk management that is more proactive, connected, and able to identify relationships and intangible risks to provide layers of mitigation. BCTs have already been posited as a means to mitigate credit decisions in the banking sector to reduce uncertainty; for cyber-threat intelligence-sharing systems for dynamic risk management; and for preventing security breaches while enhancing connectivity between stakeholders.[10] By facilitating risk identification at an early stage as well as periodically reviewing those risks once the commander has implemented risk mitigation measures BCTs may help prevent and combat the negative effects on operational processes (e.g., the targeting cycle) anticipated from a volatile, uncertain, complex, and ambiguous hybrid environment where machines and humans are iteratively interacting.[11] In other words, BCTs can help the commander understand that while there is one area of responsibility, different domains within that area (both geographic and functional) may have different tactical and operational complexions of many human + machine relationships. Understanding these relationships improves the commander's awareness of information parsimony required for convergence, and likewise, auctioning-off targets to those platforms best postured in time and space within the kill web to prosecute them.

What happens when we put a single linear path ... against a ... non-linear kill web?

Notes

1. The RAND Corporation, *Multiple Dilemmas: Challenges and Options for All-Domain Command and Control* (Santa Monica: 2020).

2. LTC Brittany Lloyd and 2LT Jeremiah Rozman, "Achieving Decision Dominance Through Convergence," Association of the United States Army, February 2022, https://www.ausa.org/sites/default/files/publications/SL-22-1-Achieving-Decision-Dominance-through-Convergence-The-US-Army-and-JADC2.pdf.

3. Ibid. *Likewise, as we anticipate fighting alongside our coalition partners, we might even extend it to "Combined Joint All-Domain Command and Control."*

4. Ray Alderman, "Transitioning from the Kill Chain to the Kill Web," Military Embedded Systems, May 30, 2018, https://militaryembedded.com/comms/communications/transitioning-from-the-kill-chain-to-the-kill-web.

5. Robbin F. Laird and Edward Timperlake, *A Maritime Kill Web Force in the Making: Deterrence and Warfighting in the XXIst Century* (Pennsauken: BookBaby, 2022).

6. John F. Schmitt, "A Systemic Concept for Operational Design," (Quantico: Marine Corps Warfighting Laboratory, 2006).

7. See Vince Darley, "Emergent Phenomena and Complexity," *Artificial Life* 4 (1994).

8. See John F. Schmitt, "Command and (Out of) Control: The Military Implications of Complexity Theory," *Marine Corps Gazette* 82, No. 9 (1998).

9. Peter Asaro, "Autonomous Weapons and the Ethics of Artificial Intelligence," in *Ethics of Artificial Intelligence* (Oxford: Oxford University Press, 2020).

10. Soumyadeb Chowdhury, Oscar Rodriguez-Espindola, Prasanta Dey, and Pawan Budhwar, "Blockchain Technology Adoption for Managing Risks in Operations and Supply Chain Management: Evidence from the UK," *Annals of Operations Research* (2022).

11. Ibid.