Exploring Technology's Risk in Modern Warfare

Double-edged sword

Maj. Michael Herb
2nd Battalion, 5th Security Force Assistance Brigade

Emerging technologies such as drones, robotics, autonomous weapons, artificial intelligence (AI), electronic warfare (EW), cyber capabilities, and space operations are prominent across the military and industrial sectors. New technologies offer improved situational awareness, communication, collection, and effects.

There are many discussions on the future of warfighting to include how robotics and drones will replace the risk to humans, thus changing how future wars are fought. The conflicts in Gaza and Ukraine highlight the persistent presence of small unmanned aerial systems (sUAS) and/or one-way drone or loitering munitions.

Technology has always been a great tool for warfighters. From the wheel to AI, technology has influenced warfare by changing how a relative advantage can be achieved and exploited at a pace the enemy cannot match. Technologies are designed to reduce human involvement in dangerous tasks, create situational awareness for decisions, cause greater effect on the enemy, and prevent the need for war. Inversely, history and current conflicts demonstrate that technological advances do not limit human casualties in war. Technology exponentially increases casualties when humans apply it to warfare without fully understanding its risks and implications. Technology introduces new risks to mitigate in warfare while also offering new opportunities, as demonstrated by both historical examples and conflicts in Gaza and Ukraine.

Risks of Technology

War has – and will always be – a human endeavor, shaped by the ever-changing character of conflict as humans continuously adapt to new risks introduced by technology. In recent history, machine guns and aircraft revolutionized the battlefield of the early 20th century, and now AI and drones are altering the risks in warfare today. The broad dangers of technology are twofold: overconfidence in technology's ability to achieve an effect or mitigate an enemy effect and failure to understand the risk technology brings by being employed by and against humans.

First, there is a risk of overconfidence in technology's ability to achieve an effect or mitigate a threat. Daylight Precision Bombing was introduced as the answer to end World War II, yet the technology could not achieve the promised effect. Heavy bombers were promised to be all that was needed for victory but did not end World War II. Today, the Army is turning to unmanned sensors to replace human reconnaissance.

Maj. Michael Herb, 2nd Battalion, 5th Security Force Assistance Brigade

I spent two years fighting U.S. Army brigade combat teams at the Joint Readiness Training Center as part of 1st Battalion, 509th Infantry (Airborne) "Geronimo." The battalion had unique enablers, including sUAS, EW (both collection and offensive), as well as space and cyber capabilities. Though employed in innovative ways and with good results, technology never achieved the end state or replaced Soldier fundamentals. Humans are overconfident in technology and have a false sense of security about what it will realistically achieve. On the battlefield in Ukraine, technology for precision munitions is employed, but the effects have dramatically decreased. Overreliance on technology is dangerous, but it can be mitigated by understanding its strengths and limitations.

The second risk is failing to understand how technology changes risk to force. World War I is an example of the technology used in warfare developing faster than the tactics and mitigation. The risk of not using technology is being outpaced by the enemy, but there is a risk in using it. In ongoing large-scale combat operations (LSCO), technology is being employed to receive and process information enabling commanders to make decisions and achieve effects. Conversely, employing technology often makes it easier for the enemy to collect and deliver effects. Whether telegraph wires or using electronics, there is little on the battlefield of yesterday or today that has not been collected on by an adversary to make an assessment. These are hard problem sets. How do you not expose formations to massed fires, yet mass combat power at the decisive point? How can offensive formations be synchronized while keeping command and control (C2) systems undetectable in the EMS to prevent destruction? How do you conceal the main effort when there is near persistent collection within every domain?

Mitigating Risks

Risks from technology can be mitigated, as many fundamental principles remain applicable and effectively address the new challenges. By enforcing strict

control measures, we gain a better understanding of risks and mitigate them more effectively. For instance, implementing restrictions on the use of Bluetooth or Wi-Fi devices, being cautious about social media posts, and taking measures to remain undetected when stationary are crucial control measures. These are not unfamiliar concepts and can significantly contribute to risk mitigation. Understanding the enemy's sUAS and establishing a Security Zone to contest the employment of sUAS and disruption from enemy systems enables the synchronization of the main effort with greater efficiency.

Another example of risk mitigation is rifle companies moving through severely restricted terrain with EMS discipline to thwart enemy attempts to collect data on them. Moving this way to consolidated attack positions allows forces to mass without exposing them on the approach. Simple actions have potential to mitigate risks across multiple domains. The Army recognizes land, air, maritime, space, and cyberspace as domains that influence Army operations, meaning they must be fully considered for risks to operations.

Mitigating risks from technology requires staff to examine protection across all five domains, which is essential to tactical ground formations. This enables staff to convey risks to the commander so that they have a realistic picture of which risks they want to assume to exploit an opportunity. For example, Bluetooth devices in a mobile C2 platform risk identification in the EMS; however, is it worth the opportunity to rapidly issue guidance and synchronize operations effectively on the objective? If that risk is acknowledged and included in the calculation, then probably.

Dozens of systems provide value to commanders while presenting a risk in the EMS. Determining which systems are always required, how to mitigate constant employment, and when is the ideal time to maximize employment must be included in planning factors. Seeing the formation across the domains and not focusing on a singular domain is important. All the domains influence the tactical echelon and must be considered during planning, or units will fail to mitigate the risks present. For example, a command post not being observed from aerial drones is a positive, but ground reconnaissance, space, and electronic means are readily available to all. Active and passive defensive mitigations like camouflage, dispersion, displacing rapidly when identified, and hardening systems across the domains help ensure survivability. Simple things, like power generation being concealed and offset; making a battalion command post mirror a combat train command post to make identification harder; or multiple nodes for C2 dispersion. All these contribute to mitigating threats across the domains. Staffs must understand the unit's signature across all five domains to incorporate the risks into their planning. Staffs must enable commanders to deliberately assume risk when the benefit of employing technology allows a relative advantage and not blindly, assume the risk.

Conclusion

By carefully balancing the benefits and risks of technology, we can maximize our operational effectiveness. As military professionals, it is our responsibility to continuously adapt to these technological changes, ensuring that we not only harness their power but also safeguard our forces against the vulnerabilities they create. We also need to recognize that while technology will support the warfighter and always has, it does not remove the risk for the warfighter. In Eastern Europe and the Sinai, technology is not preventing human suffering; only enabling it at scale. LSCO still, and always will, have an unquenchable appetite for material resources and human life. History and ongoing conflicts demonstrate that technological advances change the character and thus, the risks of war.

Technology is not a coup d'état or an assurance of victory. Technology brings new opportunities and risks. Technology will not end wars or prevent humans from facing risk in war, and it is dangerous to believe technology alone will solve problems in warfare. Technology in warfare punishes unadapted tactics and untrained, undisciplined units. Leaders are charged with understanding the character of war and preparing Soldiers to fight adversaries trying to apply technology against them and mitigate the risks as much as possible. The opportunities to achieve a relative advantage will change with technology, but technology is a tool for the human warfighter, not a substitute for training or eliminating risk for Soldiers.

References

Marcus, Gary., and Ernest. Davis. *Rebooting AI : Building Artificial Intelligence We Can Trust*. Pantheon Books, 2019

Singer, Peter. *Wired for War : The Robotics Revolution and Conflict in the 21st Century*. Penguin Press, 2009.

"Strategic Bombing: Victory Through Air Power." Accessed September 28, 2024 https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/article/195872/strategic-bombing-victory-through-air-power/

"The Russian Momentum Is Back" Accessed June 17, 2024. https://www.youtube.com/watch?v=gk7D_TliAuE