The Future of Army Maneuver–Dominance in the Land and Cyber Domains

Lieutenant General Edward C. Cardon

INTRODUCTION

The year is 2025. Just before dawn, several independent 5-man teams from an Army Combined Arms Battalion prepare to launch an attack on a terrorist-insurgent stronghold outside a mega coastal city in a sub-Saharan nation. Before the commander sends in his attack forces, his cyberspace maneuver force has already established a secure communications network using Free Space Optics and Li-Fi and are conducting defensive cyber maneuver to protect and defend key cyber terrain. While monitoring local social media, cyber operators have intercepted insurgent communications, and located their operations center. They begin sending messages on social media to confuse the insurgent network and interfere with their command and control. Next, the cyber operators launch an offensive cyber maneuver, cutting power to the insurgent headquarters. In another offensive maneuver, the cyber force employs electromagnetic pulses to destroy the adversary's electronic systems followed by a Radio Frequency capability to disable all insurgent vehicles. As dawn breaks, the insurgents awaken to the sound and fury of the Battalion's direct and indirect fires…

This scenario describes a future when the Army conducts combined arms maneuver simultaneously across the land and cyberspace domains. To be ready for this future, the Army must continue to make significant strides so that cyberspace is inextricably linked to the Army's ability to fight and win in the land domain. For decades the Army has eagerly adopted networked technologies to enhance its warfighting capabilities. As a result, the Army's tactical dominance is unprecedented. However, these same technologies are also significantly changing our world, creating asymmetries that profoundly disrupt future operating environments, and the Army's ability to conduct unified land operations. We must look beyond these expected disruptions to understand how they both enhance

Lieutenant General Edward C. Cardon was born in Texas, raised in California and was commissioned as an Engineer Officer from the United States Military Academy in 1982. LTG Cardon has commanded at every level from company through division. Prior to assuming command of the United States Army Cyber Command, he was the commander of the 2nd Infantry Division based in South Korea. His education includes a Bachelor's of Science Degree from the United States Military Academy and two Master's Degrees—one from the National War College and the other from the United States Naval Command and Staff College, both in National Security and Strategic Studies. Lieutenant General Cardon is married and has three children.

and become integral elements to how we fight and win. In short, we must envision a future where the information environment and the physical environment converge, and adapt our operating concepts to make the most of the opportunities this presents.

The Army Operating Concept is a foundational document. We must understand cyberspace as a warfighting domain, and demonstrate maneuver in this domain both independently and in support of land operations. With this in mind, what does our future force look like, and how does it fight with and through cyberspace? To remain the world's dominant landpower, the Army must reimagine how it conducts 21st century unified land operations.

Cyberspace as a Warfighting Domain

Future dominance on land, by its very nature, will require dominance in cyberspace. To achieve mission success, Joint and Army commanders must possess a basic understanding of the cyber domain and how it achieves inter and intra domain effects. Cyberspace is a uniquely man-made domain that includes physical, logical, and cyber-persona layers. Similar to other domains, cyberspace operations allow the Army and the Joint force to maintain freedom of action within the land domain by providing operational commanders additional avenues of approach against adversaries. Conceptualizing cyberspace as something separate or discrete is shortsighted, and isolating cyber within a separate domain is an approach we take at our own peril.

Cyberspace operations are increasingly inseparably linked with operations across all other domains. For example, mission command requires network defense and platform resiliency, air targeting supports, and is supported by cyber fires, and cyber effects allow commanders to set necessary operational conditions for ground based maneuver.

In other words, future war should be imagined across the land, air, and space domains that will occur by, with, and through the cyber domain. Because of these emerging conditions, to dominate the land domain, the Army must also do so in cyberspace.

Maneuver in Cyberspace

Traditionally, Army maneuver forces conducted combined arms maneuver on land to seize, occupy, and defend terrain in order to achieve physical, temporal, and psychological advantages over the enemy. The Army's Operating Concept now recognizes that combined arms maneuver actually occurs across all five warfighting domains and acknowledges cyberspace operations as one of seven core competencies.

In future operating environments, the full integration of cyberspace operations into our lexicon, organization, and understanding of maneuver is imperative. Commanders will recognize that the principles of maneuver warfare: targeting critical vulnerabilities; audacity; surprise; focus; decentralized decision-making; tempo; and combined arms are equally applicable in cyberspace.

ARMY CORE COMPETENCIES

- Shape the security environment
- Set the theater
- Project national power
- Combined arms maneuver in the air, land, maritime, space, and cyberspace domains
- Wide area security
- Cyberspace operations in the land domain
- Special operations
- The Army operating concept

Cyberspace operations also have a critical defensive component. Defensive maneuver in cyberspace includes hardening and reconfiguring systems, limiting and protecting network access points, continually maneuvering data, conducting reconnaissance and surveillance on physical and virtual avenues of approach to key cyber terrain, and using passive and active network sensors. Like other domains, the cyber environment is dynamic. We already see in Eastern Europe how Russian cyberspace capabilities can render radio and satellite communications useless, prevent precision fires, and interfere with Global Positioning Systems (GPS). Through denial of service and malware attacks aimed at the opposition, adversaries use online proxies to control their narrative and support their regional objectives. The ability to conduct defensive maneuver will be an operational and tactical imperative in the future as well.

Cyberspace Operations and Combined Arms Maneuver

In tomorrow's complex operating environment, combined arms maneuver requires coordinated efforts, both defensive and offensive, simultaneously across all domains.

Commanders must be just as adept deploying cyber effects as they are delivering physical effects. This level of synchronization is not new to our force. The Army has demonstrated unparalleled expertise in the synchronization of fire and maneuver at a decisive point. Our competence at the operational and tactical level is perhaps unmatched. However, our commanders' continued ability to effectively employ all the tools in this cross-domain arsenal in the future faces two general challenges.

First, Army and Joint operations are dependent upon networked capabilities enabled by cyberspace and space-based platforms from the strategic to the tactical level. In the past, threats to mission command have been generally well known and reasonably mitigated. However, the proliferation of technology and decreasing barriers to entry combine to present potential asymmetric advantages a savvy adversary can employ against the Army and Joint force. In the future, our enemies and adversaries will use cyberspace to influence populations, degrade the Army's technological superiority and impede our ability to communicate, collect intelligence, operate, and execute mission command.

Full integration of cyberspace operations into our lexicon, organization, and understanding of maneuver is imperative.

Second, in light of these potential emerging asymmetries, we must be able to not only defend our own critical assets, but turn the technology to our advantage. We will only achieve the level of operational dominance we demonstrated in the past if we are able to leverage and integrate cyberspace operations in the future. To do this, the Army must reimagine combined arms maneuver on both the land and in cyberspace. We have to critically examine how we are organized, how we train, and how we fight. Cyberspace operations, information operations, and electronic warfare must become an ingrained component of a commander's scheme of maneuver. Redundant and disconnected communications will take on new meanings.

Therefore, to successfully execute future mission command, the Army must continue operational integration of EW, IO, Cyber, Signal, Psychological Operations and Intelligence to dominate the information environment. In the past, these functions were separated both across staffs and throughout mission execution. The modern battlefield requires these functions to achieve greater operational integration both in planning and execution. This will entail removing organizational and mission command barriers so that these functions become completely integrated. It demands formations designed for rapid task organization through the integration and synchronization of all Army warfighting functions. Ultimately, before synergy of maneuver across cyber and the land domains can be achieved, cyberspace operations will need to be normalized as a regular warfighting capability, and within a commander's vision of the battlespace.

Our adversaries are already adapting and innovating in this way to maximize their own cyberspace capabilities. Today, Russia employs cyberspace capabilities in a world-wide campaign of social media misinformation to shape domestic audiences and achieve strategic objectives in Ukraine and elsewhere. Russian commanders deploy information operations, electronic warfare, social media, and cyberattacks in a decentralized manner that affords them significant operational autonomy. In recent operations, these and other actors have demonstrated the effectiveness of leveraging asymmetric capabilities to overcome their traditional military limitations.

Army Cyber Command continues the important work of integrating cyber capabilities into the Army's conception of maneuver warfare. We are conducting pilot programs at the Combat Training Centers (CTCs) to exercise defensive and offensive cyberspace maneuver. These exercises will inform holistic Army-wide changes to our doctrine, organization, materiel, and training. The next evolution of this initial cyber integration will be significant, generating critical questions to inform how the Army integrates cyberspace capabilities in the "Force 2025 and Beyond." How should the Army task organize to best integrate cyberspace capabilities? Beyond our current Cyber Mission Force construct, will the Army create a Cyber Expeditionary Brigade that can be rapidly task organized to support commanders? Or, will we permanently task organize these capabilities at echelon? How will the Army institutionalize cyber operations at the CTCs and wargames? Permanent changes in resources and personnel for individual and collective cyber training up through institutional changes to CTCs will be necessary. Another evolution of this effort started this year, incorporating civilian technology partners into Army experimentation and initiating a Silicon Valley Innovation pilot to explore social media strategies. Finally, how will the Army develop optimal command and control (C2) frameworks to provide cyber capabilities that can enable commanders' ability to dominate on land and in cyberspace? In doing so, how can the Army best realign network command and control to appropriately match existing land domain authorities? These are just a few critical areas Army Cyber Command continues to address as we look toward the "Force of the Future".

> Army commanders must fully embrace cyberspace as a new maneuver domain to maintain our freedom of action.

CONCLUSION

Determining how the Army will fully integrate cyberspace operations as part of a combined arms maneuver force into Unified Land Operations will be a constantly evolving process. One thing is clear, we have already *crossed the Rubicon* in cyberspace. It is impossible today to effectively conduct combined arms maneuver or Unified Land Operations without leveraging cyberspace. Many of our adversaries are already exploiting the asymmetric advantages they can achieve through cyberspace and quickly adapting their tactics. As part of a combined arms maneuver force, cyberspace operations could significantly amplify the Army's capabilities to prevent, shape, and win. To win on land in the crucible of tomorrow's complex operating environment, Army commanders must fully embrace cyberspace as a new maneuver domain to maintain our own freedom of action and while restricting that of our adversaries. Dominance in cyberspace is essential to win a complex world.