Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR

General Joseph L. Votel
Major General David J. Julazadeh
Major Weilun Lin

INTRODUCTION

From Joint Publication (JP) 3-13, the Information Environment (IE) is defined as "an aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." It is within this environment that our adversaries have engaged us persistently below a threshold that could trigger a kinetic response. Within the IE, the cyberspace domain provides our adversaries an asymmetric advantage where they can operate at the speed of war without bureaucratic obstacles or concern for collateral damage, and at relatively low cost. Rapid technological advancements and the lower barriers of entry open the cyber environment for both state and non-state actors to gain and exploit information. To respond to the unique challenge posed by the IE, we consolidated our lethal and non-lethal fires under one single portfolio in our Operations Directorate. This allowed us to maximize impact by synchronizing and integrating multi-domain operations during lethal and non-lethal planning and execution. With the full spectrum of lethal and non-lethal fires linked under one roof, we are better able to connect, integrate, and synch activities along with other Combatant Commands, the broader inter-agency, and the intelligence community. This integration makes us more lethal and disruptive at greater speeds and with greater reach resulting in hundreds of integrated Cyberspace Operations (CO) against our adversaries.

Contesting the Information Environment

Cyberspace as an operational domain is a relatively recent development in the evolution of US military warfare. Leveraging this new domain to enhance the effectiveness of military operations and contest the adversary requires an adjustment of

General Joseph L. Votel serves as the Commanding General of U.S. Central Command, MacDill Air Force Base, Florida, where he oversees an area of responsibility that stretches from northeast Africa, across the Middle East, to Central and South Asia.

The twenty countries within this vast region confront profound social, economic, and political upheaval while simultaneously facing grave security challenges in the form of widespread conflict, expansionist regional powers, violent extremist organizations and destabilizing behavior from outside actors.

GEN Votel is a graduate of the United States Military Academy, Infantry Officer Basic and Advanced Courses, United States Army Command and General Staff College, and the United States Army War College.

current cyber policy, the delegation of cyber operational authorities, expansion of cyberspace security cooperation, organizational doctrine, and interagency synchronization/coordination processes.

At USCENTCOM, we have discovered that Commanders must drive integration and synchronization of lethal and non-lethal capabilities across all domains – Land, Air, Sea, Space, and Cyberspace – in order to fully engage the adversary and create multi-domain dilemmas at the speed of war. In the past, our Information Related Capabilities (IRCs) were generally integrated as an afterthought into fully constructed operational and tactical plans. IRCs are "the tools, techniques, and/or activities employed within the IE that can be used to create effects" and include, for example, Cyberspace Operations (CO), Electronic Warfare (EW), Military Deception (MILDEC), Military Information Support Operations (MISO), Public Affairs (PA), and Civil Affairs (CA).

Over the last two years, we revised our approach and deliberately incorporated and integrated IRCs into our tactical to strategic level plans, developed a significant number of cyber and IO tools, and re-defined our Tactics, Techniques, and Procedures (TTPs) to fight our adversaries in this complex and volatile theater. As we continue to advance our abilities to engage in the IE and normalize how we operate within the Cyberspace domain, we need to proactively execute cyberspace and information operations early in "Phase 0 / steady state" of the planning process – well before operation execution. Only then can we shape the IE, hold our adversaries' capabilities at risk, and execute at the speed of war.

Normalizing the Cyber Domain

My goal is to mature CO within our Command in a way that fully integrates cyber with the physical

Major General Dave Julazadeh is the Director of Plans, Policy, Strategy, and Capabilities, Headquarters United States European Command, Patch Barracks, Stuttgart, Germany. He is responsible to the USEUCOM Commander to formulate, provide staff direction and execute military/political strategy and policy, deliberate planning and security cooperation for command activities involving other U.S. Unified Commands, allied and partner military organizations and subordinate commands. He leads USEUCOM implementation of capability development, theater force posture, countering weapons of mass destruction and partnering programs within the command's area of responsibility.

He has served as an F-16 instructor pilot, functional check flight pilot and flight examiner logging over 2,500 flying hours and over 600 combat hours during Operations Provide Comfort, Deny Flight, Northern Watch, Allied Force, and Freedom's Sentinel.

domains and reduces "stove-piping" and "IRCs as an afterthought" common in the past. By doing so, we strengthen unity of effort in the USCENTCOM AOR and better posture cyberspace forces to support future campaigns, contingencies, and functions. We must not see Cyberspace as drastically different and separate from other domains that we create new processes to prepare, plan, and fight in this new domain. We continue to seek processes that smooth and simplify operations, reducing friendly friction and accelerating decision-making in order to meet the speed of the IE. We have achieved significant successes through better integration horizontally and vertically with stakeholders, which translates into non-kinetic impacts delivered more rapidly in support of the warfighter.

At the tactical level, we have integrated CO and fielded cyberspace capabilities to support Special Forces and, more recently, conventional ground forces. These tactical cyberspace and EW capabilities are synchronized with the ground scheme of maneuver providing an additional level of force protection to the warfighter by disrupting the adversaries' ability to command and control their forces in the battlespace. During our operations to defeat ISIS, our first success at true multi-domain operations through synchronized lethal and non-lethal effects was against ISIS's critical media operatives; we denied key infrastructure and degraded their ability to execute external operations through social media. These operations against ISIS have informed efforts across CENTCOM as well as other Combatant Commands.

Across the Central Command AOR, we are targeting Violent Extremist Organizations (VEO) propaganda distribution capability and command and control networks. On a daily basis, as our forces are operating in hot spots like Afghanistan, Iraq, and

Major Weilun Lin is Chief of the Central Asia and South Asia Cyberspace branch, Joint Cyberspace Center, Operations Directorate, United States Central Command, MacDill Air Force Base, Florida, where he plans and synchronizes cyberspace authorities, effects and capabilities for combat and contingency operations in the USCENTCOM area of responsibility.

Major Lin's notable staff tours include 17th Air Force (U.S. Air Forces Africa) as Chief, East and Central Africa Communications Engagement and at the 25th Air Force as the Chief, Air Force Intelligence

Community Security Coordination Center. Major Lin was commissioned through the Air Force Reserve Officer Training Corps at Texas A&M University, College Station, Texas.

Syria. Cyber Operators from CONUS Mission Centers, linked via chat, provide critical overwatch and are routinely demonstrating responsiveness at the tactical level. Further, cyberspace-enabled Military Information Support Operations (MISO) deliver content to discrete or broad target audiences giving us another venue to contest and compete in an environment. Combined, these efforts disrupt VEO C2, support and enable kinetic operations, and provide an opportunity to respond directly to high profile attacks, false claims of victory or simply to provide maneuver space (time) for US and Coalition forces to disseminate the facts.

Our intelligence community is a critical component of placement and access to physical and virtual infrastructures. Integrating the IRCs into the planning process early on is dependent upon accessing cyberspace-related intelligence which requires greater Cyberspace-ISR authorities throughout our AOR. Requesting and gaining those early authorities allow for the shaping of the cyberspace domain to occur in Phase 0 of operations to keep pace with the constant restructuring of this man-made domain. Within Phase 0, activities such as access, exploitation, deterrence activities, surveillance, and reconnaissance need to occur in order to support combat operations. These continuous discovery and analysis activities within the IE also support staff estimates and military decision-making, ultimately allowing the commander to selectively apply and maximize his combat power at the time and space of his or her choosing. Additionally, we've taken great care in refining our targeting processes to enable the execution of lethal and non-lethal fires from conceptualization of the plan to execution. Normalizing CO requires us to treat cyberspace-related intelligence and target development the same as other warfighting domains.

Lessons Learned

Modern conflict requires streamlined processes, rapid deployment of technology, complementary partnerships, and flexible authorities to fully leverage cyberspace as an operational domain. CO uniquely requires those authorities, capabilities, and permissions early in Phase 0 to gather intelligence and operationally prepare the information environment. Improvements in the targeting process and synchronizing the IRCs provide the Command with processes that are robust enough to react to adversary actions but nimble enough to seize upon emerging opportunities. Just as on the kinetic battlefield, our enemy is highly adaptive in their cyber TTPs. While our cyber operations have been technically successful, authorities, capabilities, and permissions currently inhibit us from significantly increasing the overall effects in the information environment.

We must leverage the incredible knowledge and strengths of interagency, industry, and academic partners to create better cyber capabilities that better enable our IRCs. We must prioritize to get properly resourced so that we can rapidly procure, develop, test, train, and field them to our forces. Our warfighters need tomorrow's technology today. We've made significant progress, especially over the last eighteen months, in gaining these authorities for the Combatant Commander. We have taken the lessons learned from our operations against ISIS and our successes in Afghanistan and applied them to subsequent operations to enable our warfighters to combat our adversaries. We have also shared these lessons and plans with other Combatant Commands such as U.S. Africa Command (USAFRICOM) in support of their operations ISIS in the Sahel and other ISIS affiliates.

Conclusion

The continued advancements in technology have changed the employment and conduct of warfare; however, the fundamental nature of war remains the same. We are contested across all dimensions of power and must integrate the IRCs into how we fight. It is essential for Commanders in all domains to understand and incorporate the cyberspace domain across the other warfighting domains in order to disrupt the adversary's capabilities and will to wage war. Normalizing the cyberspace domain means broader authorities that are more responsive than current bureaucratic processes. It also means we need simple and streamlined organizations and processes to increase lethality and enhance performance. We need technology and capabilities to keep pace with the operational environment and continue to build the partnerships to do so. This also requires shaping the IE early and continuously so we hold our adversaries' capabilities at risk.

Today's commanders must drive integration of lethal and non-lethal effects across Land, Air, Sea, Space, and Cyberspace in order to create unity of action while maintaining our competitive military advantage on the battlefield. Our failure to operationalize and normalize the cyberspace domain effectively cedes it to our adversaries, gives them a competitive advantage, and ultimately, creates an increased attack vector against our objectives.