ASYMMETRIC THREAT SYMPOSIUM XIII

Cyber, Electronic Warfare, and Spectrum Operations: Critical Capabilities for Protecting America

POST-EVENT REPORT 1 · DECEMBER 2020

The Electromagnetic Spectrum in Modern Conflict and Competition

This report is a summary of topics covered at the Asymmetric Threat Symposium XIII

By many measures, today the United States of America is a dominant global military power. However, the 21st century is revealing that old measures of power are not enough to combat new threats. New capabilities and strategies are needed that are far different than the ones used to dominate 20th century industrial warfare. Already, America's military superiority has eroded to a dangerous degree, and this erosion is most concerning because adversaries are eroding American power through a new avenue – by exploiting the electromagnetic spectrum (EMS) as never before.

While the United States has spent nearly two decades fighting counter-terror and counter-insurgency operations, America's rivals poured great effort into building up EMS technology. Today, innovations in key areas – from 5G cellular networks to cyber warfare to artificial intelligence (AI) – are changing the character of war. As a result, the U.S. no longer controls the when, the how, and where conflicts might begin. The convergence of cyber, electronic warfare (EW), and various forms of intelligence (from signals intelligence, to geospatial intelligence) are seen clearly in modern multi-domain operations. This reveals that all future military operations must be layered, networked, and fully integrated. To accomplish this will require unprecedented innovation, cooperation, and agility both in government and in the private sector.

The EMS is the strategically vital national security arena of our time, where the most decisive challenges, decisions, and actions the United States faces will present themselves for the foreseeable future. While the tools of conflict are still defined by the hard power of troops in battle, military hardware, and the human skill to navigate combat, the "decisive ground" of conflict is increasingly no longer ground at all. Winning and losing in war, competition, and conflict is more and more decided in the EMS, and performance in the physical domain is being steadily reduced to a still important but nonetheless secondary domain.

Today, however, most of the U.S. military's energies continue to focus on improving kinetic capabilities. Though many national security practitioners have spent careers focused on improving combat and kinetic capabilities, now the U.S. and its allies have to embark on a very difficult and probably very uncomfortable effort to improve military power through the EMS.

To meet this challenge, the U.S. needs to close the kill chain and break the ability of our adversaries to do so. The U.S. has to improve its ability to make sense of events in conflict and competition, and to enable human decision-making and action to command and control (C2) effects in any domain – on land, in the air, in space, at sea, and in cyberspace. And to do it at greater scales than ever before.

The importance of the EMS in conflict is not a new phenomenon, but one that gained increasing prominence in the fight against terrorist groups in Iraq and Afghanistan, and now holds even more importance in great power competition. The "find, finish, exploit, and analyze" (F3EA) targeting model used to great effect by special operations forces to unravel terrorist groups in Iraq and Afghanistan is an example of how the EMS is now inseparable from modern war. Only one of those words – finish – is about physical action on a target. All other elements of that set of activities are related to the EMS. Using a powerful network of all-source

intelligence sifting through massive amounts of data to examine and exploit signals intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT), and electronic intelligence (ELINT), and employing state-of-the-art computer and cyber capabilities at the time, these tools and techniques were used to defeat terrorists nearly a decade and a half ago. Now they must be rethought in a threat environment defined by great power competition.

It is the connectivity between military forces, decision makers, and networks that will be targeted by adversaries in any future contest. Well-equipped, modernized military forces will seek to gain advantage over each other through use and manipulation of the EMS, whether through EW, information operations, or cyber capabilities. Whichever nation can build and protect linkages between high speed data networks and military forces – be they unmanned aerial vehicles, low earth orbit satellites, or troops in the field – will generate military advantage as disparate technologies are converged and leveraged together against adversaries.

Both Russia and China have moved to build up EMS capabilities that now call into question the underlying foundations and assumptions of how America projects military power. This has led to the proliferation of anti-access and area denial weapons such as missiles and EW capabilities, the growth of cyber weapons, and the development of new counter-space weapons. Both China and Russia are also focusing on areas such as AI and autonomous systems. Many of these technologies are more resident in the commercial world, though, and this gap must be addressed if the U.S. military is to avoid falling further behind.

Networks, from smart phones to enterprise IT systems, are increasingly perceived as the front line for achieving military advantage in conflict. Conflicts of the not too distant future will feature highly connected soldiers, sailors, airmen, and marines, as young U.S. military service members and their leaders will have an array of sensors at their disposal, from measuring their heart rate to tracking the status of their weapons. All this information is being transmitted back to headquarters, and to commanders in conflict. Being able to develop that data management technology and build fast, resilient networks will prove critical to long term military advantage.

Right now, portions of the EMS such as the C Band, which includes microwave frequencies from four to eight gigahertz and is used for capabilities such as satellite communications and weather radar, are congested with devices in both the private and public sector using valuable bandwidth. But this portion of the EMS is key for future military capabilities – from connectivity for unmanned systems to augmented and virtual reality tools for mobile devices. Being able to use the C Band and the middle of the EMS is critical to allowing 5G networks to reach their full potential quickly. The Department of Defense (DoD) and the U.S. Government need to open up portions of the EMS to private sector innovation, and acknowledge that progress has been made on issues such as deconflicting use of the spectrum for commercial and national security purposes. While China's top down authoritarian model has mined massive troves of data from its own citizens and faced fewer bureaucratic hurdles to opening up the spectrum for 5G innovation, America still has a great deal of innovation potential to bring to bear on the problem. To succeed, the U.S. must figure out how it opens bandwidth and provides the private sector an opportunity to allow investment to occur.

The U.S. military's cyber terrain and data it uses to conduct missions has grown substantially and shows no sign of stopping. Adversaries are constantly attacking DoD networks, from attempts to infiltrate the cloud, to attacking personal mobile devices, and looking for backdoors into weapon systems and networks to steal intellectual property. Great power competition will require even more secure networks, by leveraging automation for better and more consistent configuration, patching, and rapid incident response. To achieve this, the DoD must shift to a "zero-trust architecture" that focuses on securing data, where the constant state of operations must assume that internal military networks are just as hostile as external ones. The urgency of this shift is underscored by the challenges of the COVID-19 pandemic, as the use of non-classified networks and devices soar. Today, the Defense Information Systems Agency (DISA) is working with the National Security Agency (NSA) and U.S. Cyber Command (CYBERCOM) to build a zero-trust reference architecture that will provide guidance to DoD components, and leaders are confident this reference architecture will be delivered by the end of 2020.

Protecting DoD networks is critical to thwarting future cyber espionage and exploitation activities. From intellectual property theft to amplifying divisions via information operations, China, Russia, and other adversaries have shown no sign of scaling back their efforts to use cyber to gain advantage over the U.S. As technology advancements occur, technology developments like 5G and others will add to the cyber threat landscape and will raise the imperative for DoD organizations to work together. This will require more cooperation between agencies such as the NSA and CYBERCOM as they try to plan and execute cyber operations on a global scale that is informed by the latest intelligence.

While cyber capabilities, SIGINT, and EW are converging and overlapping, commanders and leadership have to work to understand what each capability can and cannot do, how they interoperate, and how they can be synchronized to benefit missions from the tactical to the strategic levels.

There is evidence this is now occurring within DoD. Instead of individual capabilities being developed on their own, now customers and U.S. military services are looking more holistically at the challenge of the EMS in conflict. For example, the U.S. military services and defense companies are realizing that with software-defined tools, they can repurpose and combine SIGINT with generating cyber effects. Today, more than ever before, there is a recognition of the importance of the spectrum and the overlap of different tools.

This approach is especially important as U.S. military services and national security organizations grapple with the concept of multi-domain operations. The days of having a single-purpose system or capability are coming to an end. Financial constraints on DoD are certainly a factor, but also soldiers and service members can no longer be burdened with taking more and more equipment with them on missions to go after individual EMS-related threats – especially as they continue to proliferate. The challenge for the U.S. in the coming years will be to take what today resides in individual "boxes" and combine them into a single box or capability. Whether looking at a C2 picture coming from different sources, or a cyber effect talking to a ground system and integrating with that capability, the push to modernize must focus on lightening the load and increasing lethality.

In addition to building interdependent capability, organizations should not just adapt technology in terms of how to target adversaries or how to defend against threats. The military and the defense industry need to look at some of the processes and some of the approaches used to recruit new talent and build new skills. In addition to developing cutting-edge technology, the defense industrial base, the military, and national security agencies will have to keep human capital updated and refreshed and make sure processes and bureaucracies don't slow innovation down.

Keeping innovation alive will be critical to the success of initiatives across the DoD that are now trying to elevate the EMS to the forefront of defense planning. From the Air Force's Advanced Battle Management System (ABMS) to the Army's Project Convergence network experiments, to the Navy's Distributed Maritime Operations concept, managing cross-domain capabilities and effects is increasingly becoming the focus of large, cooperative efforts to build U.S. military advantage.

In closing, while the traditional elements of military combat power, such as aircraft, vehicles, troops, and kinetic weapons, will retain their vital importance in conflict and competition, they are now completely intertwined with the EMS. The U.S. will still require the overmatch of kinetic combat power, but it will need to build that same overmatch in the EMS if it is to prevail in future competition and conflicts. ■