

Navigating the Spectrum

The U.S. is taking big steps to claim its territory in electronic warfare.

Electronic warfare sounds more novel than it is. In 1904, Japan used radio to communicate the location of Russian fleets to its warships. Russia's decision against attempts to interfere with the radio signals ultimately lead to its staggering loss to Japan in the Russo-Japanese War. During World War II, the British Air Ministry jammed and distorted radio waves used by the Luftwaffe for navigation in the "Battle of the Beams", and radar technology was critical to U.S. military operations in the Vietnam War.

Electronic communication technologies have matured dramatically in recent years. These capabilities and the spectrum they occupy are critical to national defense today, which gives advantage to the nation most able to rapidly and securely share intelligence between its forces and allies.

The electromagnetic spectrum, or EMS, is crowded, and software has proliferated the systems communicating to and through it. As adversaries expand their technologies and learn how to intercept, block, and beguile our communications, the United States has strengthened its efforts to keep pace. The Department of Defense is prioritizing the modernization of its electronic warfare systems, with plans to spend \$47 billion during the next 5 years¹ in order to outmatch China and Russia. It's not enough to just keep up— to maintain a competitive advantage, we are working to stay a step ahead.

To compete and win against peer and near-peer adversaries in modern conflict, the joint force should place a high priority on achieving control of the EMS in order to ensure freedom of action in all other domains."

Air University, Curtis E Lemay Center for Doctrine²

¹ <https://www.c4isrnet.com/electronic-warfare/2020/02/21/getting-the-services-on-the-same-wavelength-about-electronic-warfare/>

² https://www.doctrine.af.mil/Portals/61/documents/Annex_3-51/3-51-Annex-EW-EMSO.pdf



The Paradigm Shift

The Department of Defense is deeply invested in changing the way all Defense systems are managed. The U.S. finds itself at an overall disadvantage in maintaining military systems, largely due to time-consuming engineering processes. We face barriers to implementing modern technologies, including vendor lock and differences in standards between branches of the military. The defense and communication systems we rely on were suited for electronic warfare when they were first designed, but they need to be continuously modernized for today's landscapes.

Modern electronic warfare is demanding. The military needs to send and receive intelligence in real time, which requires not only protecting communication paths from outsiders but also making sure one branch isn't blocking another. The commercial industry has largely embraced software-centric engineering, which focuses on building modular, task-oriented, and quickly adaptable systems. With this shift, new technologies are being added to the electromagnetic spectrum faster than ever before.

The processes the DoD has traditionally used cannot match the speed small and mid-sized companies are demonstrating. **So, what makes our adversaries and commercial entities so adept at developing new solutions in electronic warfare?**

1

First, they are not constrained by the same acquisition policy. They build modular, adaptable systems and are mastering “plug-and-play” techniques which allow them to access new capabilities on the spot. The U.S. is changing the way it builds systems to gain these same benefits.

2

Next, a lack of software portability between EW systems used in different branches of the U.S. military decreases acquisition and operational efficiency and heightens the risk of prohibitive interference. The U.S. is shifting to focus on joint force strategies and broadly prioritizing interoperability and faster, continuous adaptation of Defense systems.

“

We have more understanding of how complicated the electromagnetic spectrum is and how hard integration is. So we are looking at integration earlier in the development cycle. A pillar of our product output is interoperability and EW is part of that.”

Dr. Dino Mensa, senior scientist-technology manager for electronic warfare technologies at NAVAIR³

³ <https://www.militaryaerospace.com/sensors/article/14168864/airborne-electronic-warfare>



There's Still Work To Be Done

There is a lot of potential in our existing defense systems. By following the lead of the commercial industry, the DoD can shift to software-centric engineering and make its systems more survivable and resilient without starting from scratch. Successful electronic warfare is task oriented. Engineers at Tangram Flex are experts in decomposition— we break complex systems down into a set of components, define how each one works on its own, and how they work together. This visibility is the key to making systems adaptable in fast paced missions that require coordination between military forces.

Tangram Flex specializes in software integration services and product-based solutions for systems that send and receive sensitive information. Whether you are integrating new sensor payload software on a UAV or building communication pipelines between Army and Navy systems, our approach is catered to guiding engineers through the transition from traditional engineering practices to secure, software-focused agile development.

Our adversaries have the ability to quickly implement cutting-edge technologies without as much cost or manual work. The DoD needs ways to access that same type of plug-and-play operability across environments, domains, and between branches of the military. Our software integration tool, Tangram Pro™, is designed for that. Tangram Pro™ automatically generates secure code and translates between software languages to connect components together and uses advanced testing tools to provide confidence that systems will function correctly— without causing unintentional disruption to other systems. This approach is key to securing systems and their communication pipelines. Tangram Flex works with customers to create tailored toolkits for their systems, allowing users to scale their existing technology and achieve fast, repeatable updates in pace with our adversaries.

TANGRAMFLEX 

Tangram Flex simplifies software integration for mission-critical defense systems. We understand the challenges of security, speed, and safety. Our team combines engineering expertise with our core product, Tangram Pro™, to arm customers with customized toolkits for meeting mission needs.

hello@tangramflex.com