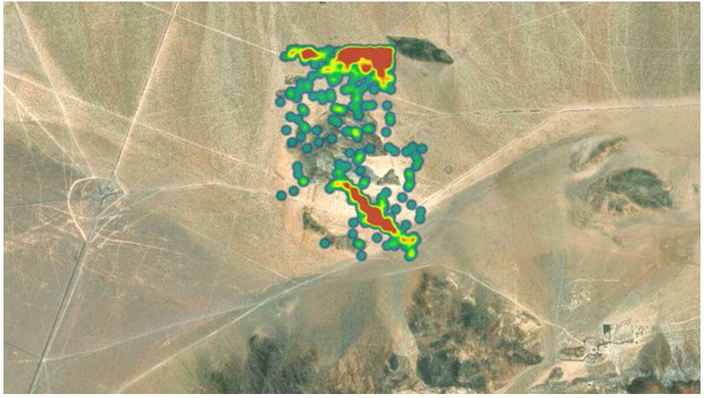
This Is What Ground Forces Look Like To An Electronic Warfare System And Why It's A Big Deal

Modern units generate a large electromagnetic signature from their radios, sensors, and other systems that opponents can spot, track, and attack.

By Joseph Trevithick   May 11, 2020

https://www.thedrive.com/the-war-zone/33401/this-is-what-ground-forces-look-like-to-an-electronic-warfare-system-and-why-its-a-big-deal



US Army

The head of the U.S. Army's 11th Armored Cavalry Regiment has offered an interesting and unusually detailed look at the threat that electronic warfare and electronic support measures pose to American troops on the modern battlefield. The likelihood of a potential adversary monitoring friendly movements via electronic emissions and launching electronic attacks, as well as kinetic ones, on those units has only grown in recent years, with Russia, in particular, demonstrating just how effective these capabilities can be in Ukraine and Syria. American forces in Syria, as well as troops in Europe, have been also subjected to Russia's electronic harassment, as well, underscoring these threats.

On May 7, 2020, Army Colonel Scott Woodward, the commander of the 11th Armored Cavalry Regiment, posted an annotated satellite image on Twitter that showed the electronic emissions signature of a battalion-sized element, along with support units, or "trains," during an exercise at the National Training Center at Fort Irwin in California. The 11th is the unit at the NTC that is dedicated to playing the role of enemy troops, or the Opposing Forces (OPFOR), during exercises and has a fleet of modified vehicles and other systems to mimic the capabilities and visual appearance of potential adversaries.

Woodward's Tweet was in response to a question about the value of certain types of modern visible camouflage. He did say that under the right circumstances that traditional methods of concealment, especially nets that break up the general outline of vehicles and make them harder to immediately identify, an important general camouflage concept, could still be useful.

"Concealment will help you stay alive a little longer in the close fight," he wrote along with sharing the image. "What does your EW [electronic warfare] footprint look like is the larger question. If I can see you like this, it doesn't matter how much camo you have."

The colonel said that the specific force seen in the image had thought the natural cover in that area of the NTC, known as Moose Gardens, had sufficiently concealed their positions and that they were also protected by the fact that it was dark. He said that his opponents in the exercise used their electronic warfare systems to spot his troops from a distance of 12 kilometers away, or nearly seven and a half miles.

Woodward did not explain exactly what systems were generating the electronic signature that his opponents were able to spot, but communications and data-sharing systems certainly produce regular emissions, as do certain kinds of sensors, especially radars. The colonel also pointed out that these dangers were only going to grow as time goes on and new systems begin to enter service.

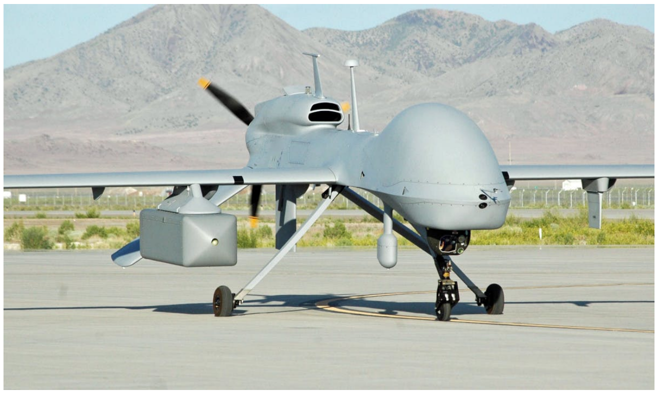
He specifically pointed out that the active protection systems that the Army is increasingly interested in installing on various vehicles to protect against anti-tank guided missiles and other infantry anti-tank weapons can dramatically increase a unit's signature in the electromagnetic spectrum. These defensive systems rely on a variety of sensors, including small radars, to detect incoming threats.

The 11th's commanding officer also did not say what type of system the other side had used to locate his forces. On the ground, the Army has a number of vehicle-mounted and dismounted signals intelligence systems that have secondary abilities to detect, geo-locate, and then track targets by their electronic emissions. The service also has aerial signals intelligence capabilities on both manned and unmanned platforms that can perform these functions. None of these systems have the ability to jam or otherwise attack the source of those emissions.

For some years now, the Army has been working to reinvigorate its ground-based electronic warfare and electronic support measures capabilities with new and improved systems, as well as create new units focused on employing these tactics, techniques, and procedures, as well. Two years ago, the service's Rapid Equipping Force (REF) notably created a prototype Electronic Warfare Tactical Vehicle (EWTV) based on an M1235 Mine-Resistant Ambush Protected (MRAP). The EWTV used a modified version of a system primarily originally designed to spot and then jam remotely-triggered improvised explosive devices (IED) to spot and monitor hostile electronic signals, as well as attack them.

US Army The prototype Electronic Warfare Tactical Vehicle.

The Army has also been looking to expand its aerial electronic warfare capabilities, especially podded systems that its MQ-1C Gray Eagle drones can carry. In 2012, the service had begun development of the Networked Electronic Warfare Remotely Operated (NERO) pod in cooperation with what was then the Joint Improvised Explosive Device Defeat Organization (JIEDDO), primarily as an airborne tool to jam IED triggers. As with the EWTV, NERO's electronic warfare capabilities had the potential for broader applications.



US Army An MQ-1C Gray Eagle drone carrying a NERO pod.

More recently, the Army hired Lockheed Martin to develop the Silent CROW pod, which also has electronic and signals intelligence, as well as cyber warfare capabilities, as part of the service's Multi-function Electronic Warfare-Air Large (MFEW-AL) program. On Apr. 29, Lockheed Martin announced Silent CROW was moving into the second phase of development after initial risk reduction testing using an Army UV-18 Twin Otter fixed-wing aircraft as a surrogate platform to carry the system.

Lockheed Martin An artist's conception of an MQ-1C Gray Eagle carrying the Silent CROW pod under its right wing.

This is all in line with a resurgence of interest in electronic warfare, as well as emerging cyber warfare capabilities, across the U.S. military. The U.S. Marine Corps is pursuing similar efforts to the Army's to improve the ability of its ground forces to fight in the electromagnetic spectrum and the U.S. Air Force and the U.S. Navy both have significant electronic and cyber warfare projects in the works, as well. This is on top of the extensive electronic warfare and electronic support measures systems that both of these services field already.

With even more robust electronic warfare systems that also incorporate intelligence-gathering and cyber capabilities, Army units, as well as those from other branches, will have the ability to spot their opponents at extended distances regardless of how concealed they might be visually, just as they did with the elements of the 11th Armored Cavalry Regiment at the NTC. They will also be able to monitor their activities to glean additional information and launch electronic attacks on them.

Jamming and cyber attacks could make it difficult for them to coordinate other friendly units and cut them off from other sources of information. It could also disorient and confuse hostile forces, including by creating virtual decoys that appear to an adversary's sensors, or even on their own electronic warfare systems, to draw their attention away from actual American troops.

US Army The RC-12 Guardrail has been one of the Army's most powerful signals intelligence tools for decades. Now in its latest RC-12X form, it provides multi-mission electronic surveillance support.

Just being able to geolocate enemy forces electronically, which they might not be aware is even happening, opens up the immediate possibility of launching artillery or airstrikes against those positions. Mixing those strikes together with additional electronic or cyber attacks could be particularly devastating.

American forces are also at risk of having the same things done to them. The role that electronic warfare, alongside electronic and other intelligence activity and cyber attacks, has played in Russian operations in Ukraine has been a major factor behind this renewed focus on similar capabilities within the U.S. military.

Christian Brose, a senior fellow at the Carnegie Endowment for International Peace and the head of strategy at tech startup Anduril Industries, described a prototypical series of events during an engagement in Ukraine in his new book *The Kill Chain: Defending America in the Future of High-Tech Warfare*. Brose describes an incident in which someone, likely a member of Russia's intelligence community, spuriously called the mother of a Ukrainian commander and told her that her son was dead. She then hurriedly called his unencrypted cell phone to try to confirm whether this was true. When he called her back to tell everything was okay, Russian troops geolocated his forces' positions from his cell phone signal and hit them with a rocket artillery barrage, killing him in the process.

Steve Trimble, *Aviation Week*'s Defense editor and good friend of *The War Zone* shared the full passage on Twitter.

This is just one of a number of similar anecdotes that have come out of Ukraine's conflict with Russia, as well as Russian-backed proxies, in its eastern Donbass region since it began in 2014. There have also been reports that American troops in Europe have been victims of similar cyber attacks and other electronic espionage seeking to gain information about their families, among other things. Geo-locating and attacking forces by their electronic emissions, as well as jamming those transmissions to sow further confusion, has become an important component of Russia's tactical doctrine. GPS spoofing is another emerging capability that Russia has been quick to embrace.

Russia has not limited these activities to Ukraine, either. There have been numerous reports of Russian electronic warfare attacks in Syria that are either directed at American forces or otherwise impact their operations indirectly. Electronic warfare has become such a major component of large-scale exercises in Russia that the effects often spill over into neighboring countries, as well.

Vitaly Kuzmin   A Russian R-330Zh Zhitel electronic warfare system, which is used to jam cellular satellite communications.

The Kremlin hasn't been the only one to embrace these capabilities, either. China, as well as other smaller countries, also see a clear benefit in developing electronic and cyber warfare systems, especially to counter countries, such as the United States, that have long held advantages in areas including long-range communications and data-sharing, electronic and signals intelligence, and satellite navigation.

So-called "emissions control" tactics, or EMCON, are valuable to reduce the risk that electronic surveillance and attacks pose, but can also limit a friendly forces' general situational awareness and their ability to coordinate with each other. As such, forcing an opponent to go into a reduced emission state or a fully radio-silent operating mode can still have the effect of degrading their capabilities to some degree.

US Army The Wolfhound is a backpack-mounted radio direction-finding system that can detect enemy communications signals and determines their approximate location.

This is driving separate work in the U.S. military, among others, on electronic systems, especially sensors, such as radars and communications systems, that can work effectively in passive modes or otherwise have a low probability of intercept, making them more difficult to detect and more resilient against jamming or spoofing. You can read more about this in these past *War Zone* pieces.

Regardless, these electronic threats are definitely real and it's good to see the U.S. military taking them seriously now, as well as working to give its own forces their own electronic and cyber warfare tools. When it comes to exercises at the National Training Center, it looks like Colonel Woodward and the 11th Armored Cavalry Regiment will be faced with a growing array of capabilities in the electromagnetic spectrum that will keep challenging their ability to stay hidden and get the drop on their opponents.