Hiding in Plain Sight – Camouflage, Concealment and Deception in the EMS

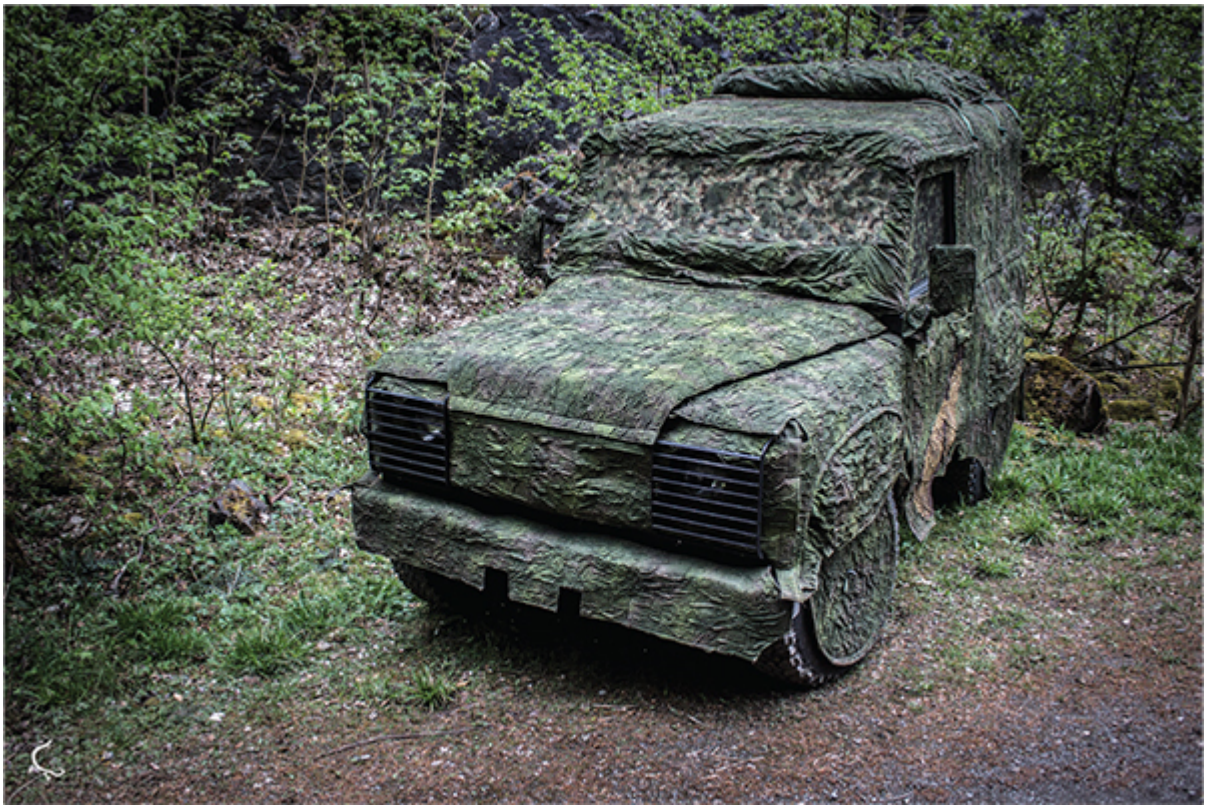
By Andrew White

In the wake of the Great Power Competition between the United States, Russia and China, Europe's land forces are facing the realities of operating in a new and more dangerous battlespace. Over the past decade, Russia and China have been developing new sensor-to-shooter concepts that make use of multispectral ISR platforms, efficient battle networks that can rapidly move target data to commanders and weapons that can engage ground targets at much longer ranges. And they are exporting these capabilities to their allies across the globe. This development poses a new challenge for Europe's armies, which have spent the past 30 years operating in relatively permissive threat environments against adversaries that have been equipped mostly with Cold War era systems. While European armies must continue developing their own sensor-to-shooter networks, they must also focus on technologies, tactics and concepts that enable them to hide from an adversary's sensors.

OFFENSIVE BATTLE NETWORKS

The creation of modern offensive battle networks is hardly new. The US developed stealth aircraft designs, advanced ISR and targeting sensors, satellite communications, and space-based positioning, navigation and timing (PNT) in the 1970s and 1980s and then integrated these technologies as part of a new battle network concept to challenge the Soviet Union's armor advantage during the last decade of the Cold War. In 1991, the US relied on its nascent sensor-to-shooter network to defeat Iraqi ground forces in the Gulf War. Over the next two decades, China and Russia watched the US and its allies

employ these sensor-to-shooter networks in Bosnia, Kosovo, Afghanistan and Iraq – tailoring the concept and leveraging new sensor and network technologies along the way.



Russia and China watched these developments, and by 2010 they were embarking on modernization programs that could take advantage of tactical unmanned aerial systems (UASs) fitted with compact EO/IR/RF sensors and RF jammers, faster data networks and information networks, precision stand-off munitions to attack high value targets and very accurate long-range artillery (30 km – 70 km range) to break up enemy formations. These technologies have enabled Russia and China to develop new operational concepts for rapidly detecting, identifying, geolocating and engaging large numbers of ground targets and at much longer distances than ever before. In addition to meeting their own needs, Russia and China are selling these capabilities to other countries, who are in the process of developing their own sensor-to-shooter networks. From the standpoint of Europe's ground forces, this is a concerning trend for operations within Europe and expeditionary ops.

MULTISPECTRAL CAMOUFLAGE

According to Saab, today's high-tech battlefield is becoming increasingly sophisticated, making it "ever more challenging to avoid detection and identification and targeting." Company officials described camouflage, concealment and deception (CCD) concepts as a critical necessity for any modern force seeking to optimize their operational effectiveness.

"Today, all peer armies have sensors in all parts of the spectrum," the company said. "There are no scenarios with no multispectral sensor threat. So modern signature management is one of few disruptive technologies that, together with deception and operational adoption, can break an enemy's overmatch in battlefield awareness, detection, target acquisition and long-range fires."

According to Saab's director of strategy and business development for the Barracuda business unit, Niklas Ålund, signature management provides the pre-condition for an armed force to win an engagement in a contested operational environment. "Technology and TTPs will allow an armed force to not become a target, hide its intentions, take the initiative and win an engagement," he said. "Deception is a state of mind. Deceive their minds, disrupt their sensors and destroy their chances to engage first."

Most ground-based weapons systems, from soldiers to APCs to main battle tanks, do not incorporate stealth design principles. In fact, they present significant visual, radar and thermal signatures when measured against the performance of today's radars and EO/IR sensors, including hyperspectral sensors. These signatures can be mitigated to some extent by multispectral camouflage systems, which have been available for more than two decades and can be applied as personal camouflage (ghillie suits), modular systems to cover various types of equipment and encampments, or can be applied directly

to vehicles. One of the first products in this market was the Ultra-Lightweight Camouflage Netting System introduced in the 1990s by Saab Barracuda. Today, however, there are several other companies – many of them in Europe – offering multispectral camouflage systems. These include B.O.I.S. – FILTRY, spol. s r. o. (Blansko, Czech Republic), Lubawa S.A. (Ostrów Wielkopolski, Poland) and TDU Defense Systems (Torbalı-İzmir, Turkey), as well as Fibrotex (Petach Tikva, Israel), Jetcord (New Delhi, India) and Motley Exim Co. (New Delhi, India).

Another approach is to apply stealthy material directly onto a weapons system. In 2011, BAE Systems Hägglunds (Örnsköldsvik, Sweden) introduced its ADAPTIV technology, which can be applied to a ground vehicle's outer armor. First exhibited on a CV90120 tank, ADAPTIV provides a high degree of thermal camouflage. The individual modules can be heated or cooled to create different thermal patterns that can fool thermal sensors.

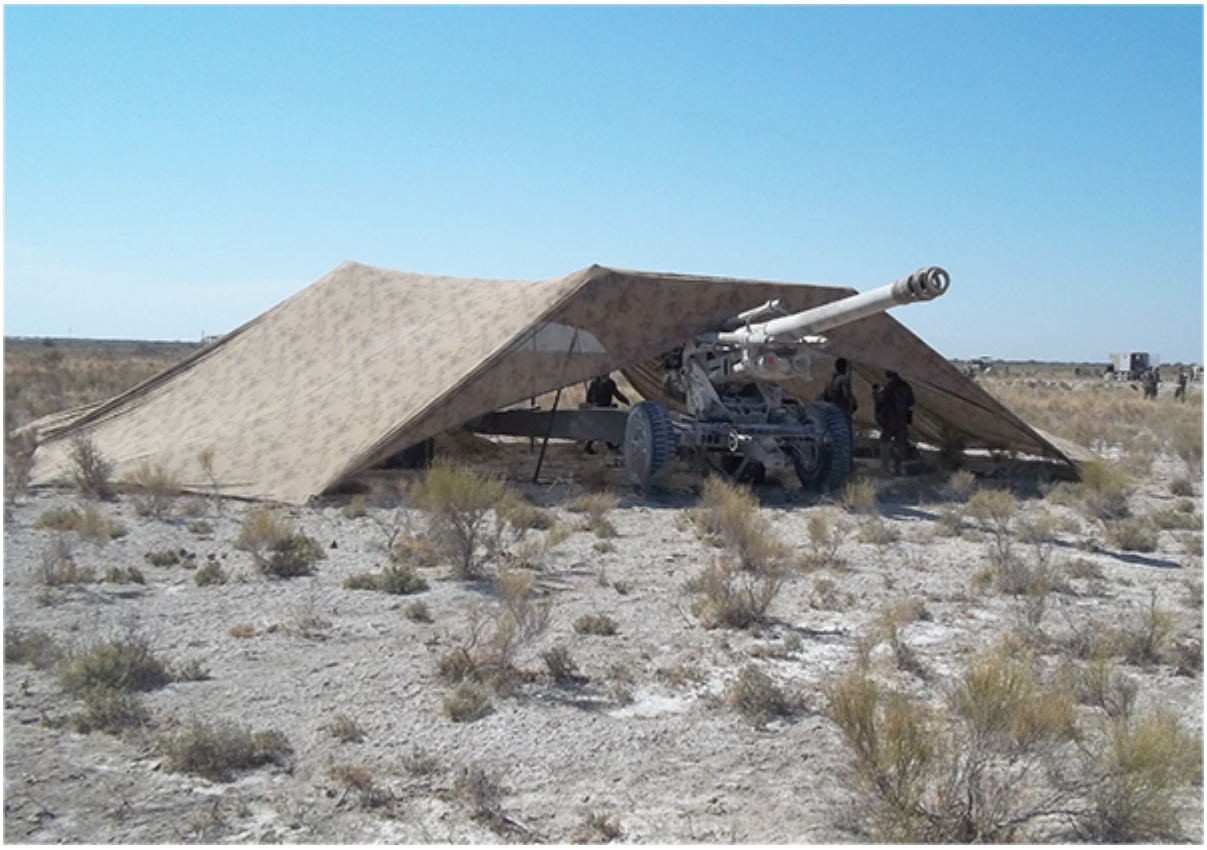
While multispectral camouflage can be added to ground systems, the long-term expectation is that high-value targets, such as tanks and APCs, will eventually incorporate stealth designs to limit their detection by multispectral sensors. In 2013, Research and Development Centre for Mechanical Appliances OBRUM Ltd. (Gliwice, Poland) and BAE Systems Hägglunds introduced a stealth concept design named PL-01 based on BAE's CV90120T light tank. While it never entered full-scale development, it represented a first look at some of the features that stealth tank designs might incorporate, including clean and continuous surfaces and edges, radar absorbing material and a square-shaped covering over its main cannon.

ELECTROMAGNETIC CONCEALMENT

In addition to using passive means such as multispectral

camouflage to mask the electromagnetic signature of a weapons system from EO/IR and radar sensors, today's ground forces must also become more adept at concealing their electromagnetic emissions – radar, communications and jamming systems – from an adversary's electronic support measures (ESM) and signals intelligence (SIGINT) systems. This can be a challenge for ground forces that depend on high-power radars for air defense or airborne surveillance. Most of the emissions from a ground force come from radios with omnidirectional antennas that are used for command, control and communications. A fighting force that employs a highly networked sensor-to-shooter kill chain necessarily sends and receives a lot of signals, and this activity provides a lot of opportunities for adversary EW and SIGINT operators to feed this emitter information into their own sensor-to-shooter kill chains. This is an area where Russia has focused its force modernization efforts, with the introduction of new UAS- and ground-based communications EW systems.

Zoran Dobrosavljevic, senior consulting engineer at Roke Manor Research (Romsey, Hampshire), described how western armies continue to rely upon communications networks to exchange information across a battlespace. "All that assumes a freedom of maneuver in the electromagnetic spectrum, but we don't think we can take that for granted anymore. The current electromagnetic environment and battlespace will be contested, congested and constrained, and all those things that go together with it," he said. "Adversaries can therefore try to deny parts of the spectrum, both actively and passively, to basically force NATO forces to use the radio spectrum in a way that is unfavorable to them," he added, referring to jamming command and control nodes and rebroadcasting stations for example.

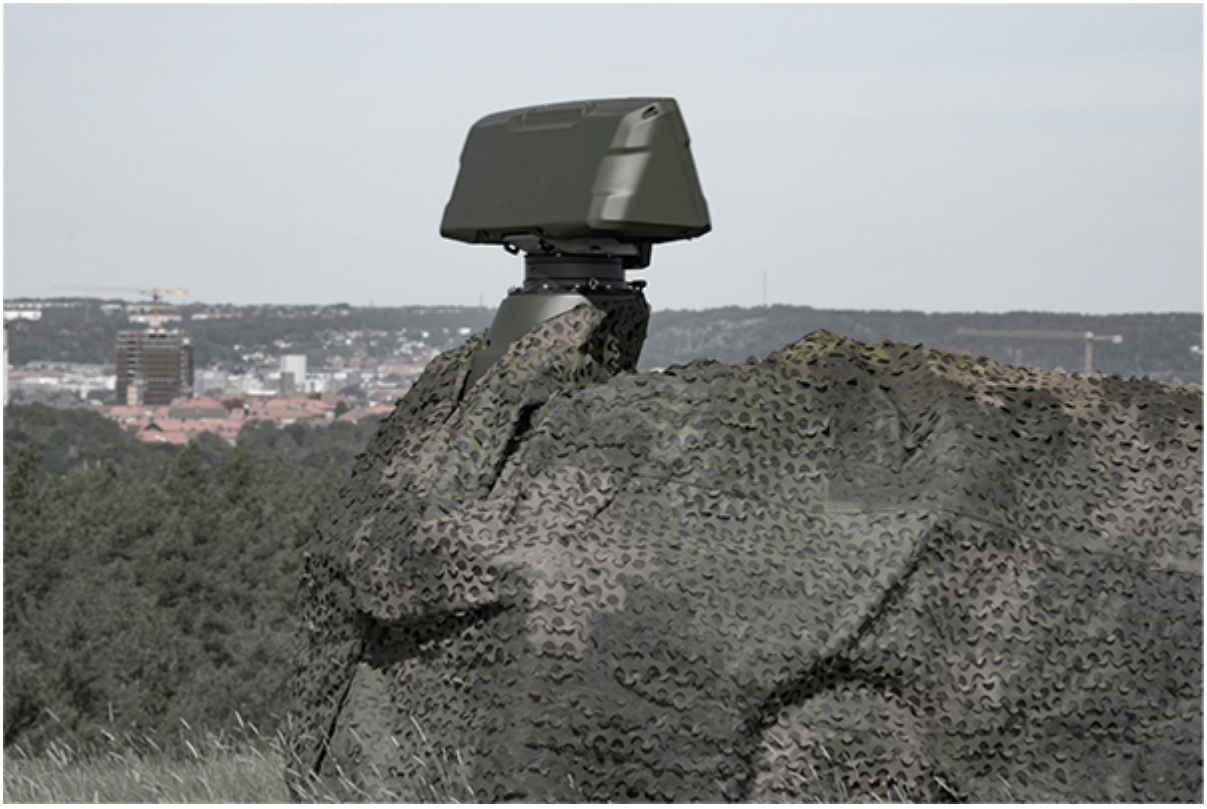


According to Dobrosavljevic, peer/near-peer adversaries are able to deploy man-portable and vehicular ESM and SIGINT systems to confirm ranges of their opponents and detect emissions across the full range of frequencies, including HF, UHF and VHF. “They have sensors that are kind of focusing on specific types of communication systems. So on jammers, you have systems designed to suppress GPS and navigation, as well as a separate capability to exploit mobile cellular communications and systems to attack tactical communication networks,” he said.

Studying ongoing operations in eastern Europe, Eric Herron, Roke’s CEMA business development lead, suggested NATO forces must learn (and train) to emit as little as possible, relying upon tactical communications networks to deliver only critical messages, such as orders that are absolutely necessary to achieve mission effectiveness. “A battlegroup commander should have a good understanding of the risk associated with a certain activity, but on the ground,” he said. “It is difficult to protect an entire formation which is often scattered across a battlefield. But there are lessons to be

learned with [Russian] activities which are currently going on in Ukraine and Syria. These give us an idea of how our adversary operates – and it is very offensive. Now, that can be an advantage to us. And I think that there are probably ways to utilize that in the way we react. The enemy being active in the spectrum means they also expose themselves, which gives us an opportunity to counteract. And that's how the game goes," he explained.

Herron described how NATO forces in particular must revert to lessons learned during the Cold War. "We were very slick with our radio planning and radio silence when necessary," he said. "But it's something that isn't or hasn't been used, [at least] up until the last few years. So, there's a certain amount of skill fade and requirement to go back to basics. We have the ability to do it; it just hasn't been a priority. But we are doing stuff about it with future command and control systems being designed to reduce their signatures and to be resilient as much as possible to any electronic attack measures," he said.



This Giraffe radar system is covered by Saab's Barracuda

multispectral camouflage. Even with the radar antenna exposed, the rest of the vehicle is not clearly visible to EO, IR and radar sensors. SAAB

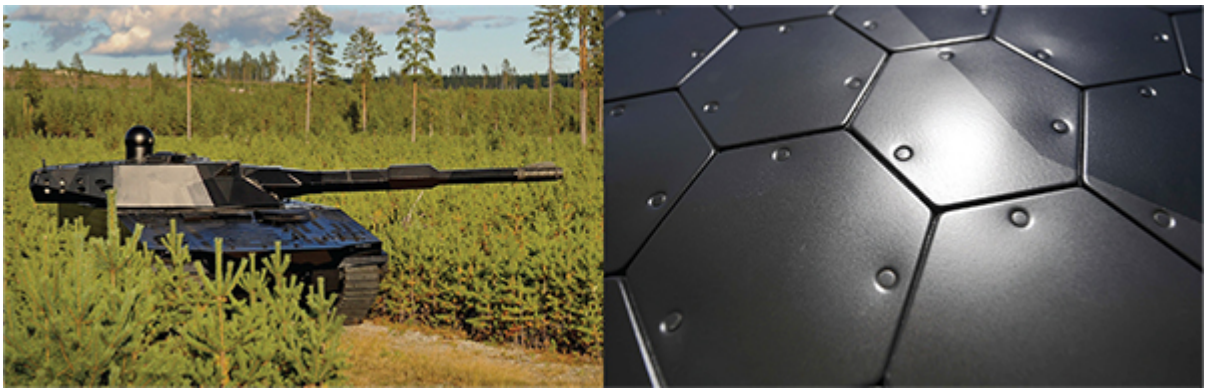
According to Herron, the most suitable starting point to managing the electromagnetic signature of any ground force is awareness. “So first of all, we need to make sure that armies and industry are aware and decision makers are aware of the presence of threat and the importance of enemy capabilities as well. That links into us being aware what our electromagnetic signatures are,” he explained. “How much do we really expose ourselves in the electromagnetic spectrum, particularly when we go about conducting our regular business doing command and control information exchange. So a ground force has to make sure what its signatures are and what they enable a potentially capable adversary to do.”

Herron explained that decision support tools must also be made available to commanders on the ground, providing them with the ability to balance risk with effectiveness. “When they plan their operations, commanders must be aware of calculated risks in terms of setting up a course of action and whether they may or may not be exposed to certain electromagnetic spectrum risks,” he said.

Ground forces will need to introduce more flexibility into their electromagnetic maneuver strategies. As Mat Willmot, EW sales director at Saab, explained, “Propagation prediction and spectrum management tools are nowadays deployed in dynamic mission planning, as opposed to the traditional pre-mission planning process.”

Another aspect of concealing the electromagnetic signature of a ground force is for it to rely more on passive sensors, such as ESM and EO/IR systems, instead of using emitting sensors, such as radars, to build a situational awareness picture. A company official at Italy’s Elettronica described how soldiers (particularly those conducting clandestine operations) must be capable of undertaking “passive engagement to the maximum

extent" possible. "This provides the user with a tactical advantage with respect to the enemy," the company official confirmed before describing how, in general terms, passive engagement focuses on the exclusive use of passive sensors to provide ranging and complete situational awareness. "Both radio frequency (RF) and infrared/electro-optical (EO/IR) sensors can be used effectively. In fact, the real-time cooperation between passive sensors adopting RF data links allow for an effective geo-location capability. Then, both passive RF and EO/IR sensors can perform ranging on the back of low probability of intercept/low probability of detection data links. This approach can be integrated into overall electromagnetic spectrum operations (EMSOs), including spectrum operations that require dynamic spectrum management (DSM)," the official said.



Demonstrated on a CV90120T, BAE Systems' ADAPTIV technology reduces the ability of IR sensors to detect the thermal signature of the tank. BAE SYSTEMS

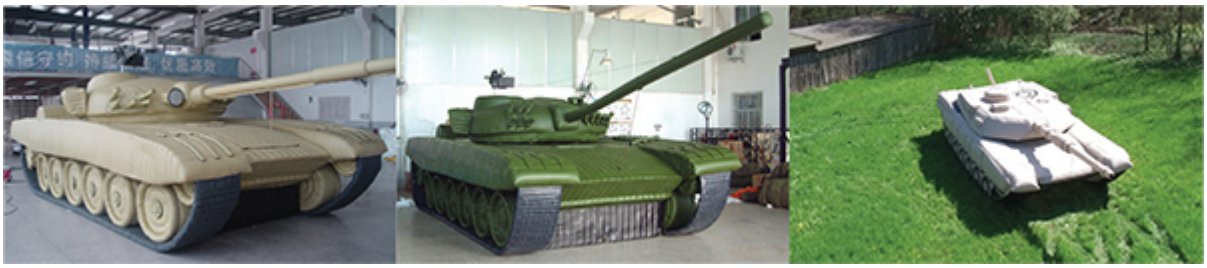
GROUND DECOYS

Just as some companies, such as Saab, are developing materials to meet multispectral camouflage requirements, so others are utilizing new materials, inexpensive commercial electronics and autonomous vehicle technologies to develop maneuvering multispectral decoys that are designed to deceive adversary ISR sensor operators.

In the past, employing ground decoys that could mimic a tank,

an artillery piece or a surface-to-air missile (SAM) system usually meant fooling an adversary mainly in the visual realm. During World War II, wooden and inflatable decoys were utilized in large numbers as part of the Allies' "Ghost Army" in southeast England leading up to the D-Day invasion of France. In the 1990s, Serb forces used very basic materials (lumber, wooden boxes and sheets in some cases) to create decoy tanks and air defense systems that in at least some cases successfully fooled NATO strike aircraft.

Not a whole lot has changed. Most of the "decoys" available today are basically inflatable targets operating in the visual spectrum and are mainly used for training applications. Many companies across Europe, as well as Russia, China and India, manufacture several types of these inflatable targets, although some are used as decoys. The Russian Army's 45th Separate Engineer-Camouflage Regiment, nicknamed the "inflator" regiment according to some Russian news reports, makes extensive use of these inflatable devices.



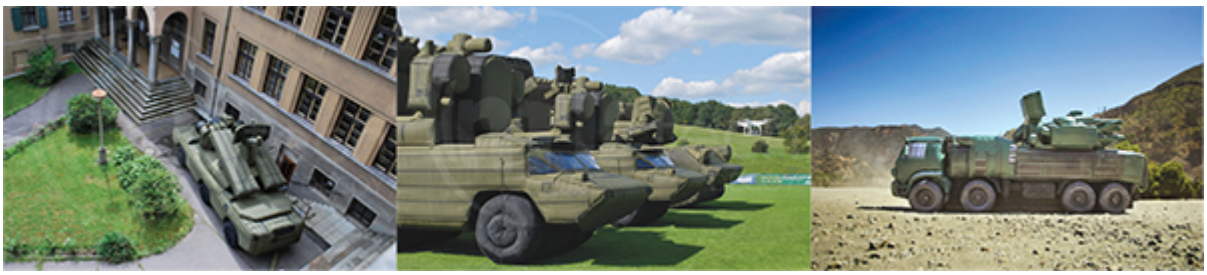
Inflatable targets are sometimes used as decoys. While not presenting much in the way of multispectral signatures and perhaps not very convincing up close either, their visual effectiveness usually increases with distance, especially if viewed through an electro-optic sensor. TCH AND I2KMILITARY.COM

However, simple visual decoys are losing their effectiveness against today's multispectral sensor capabilities. Western ground forces will need a new generation of decoys that present a more realistic signature, including radar return, radio activity and thermal characteristics.

Roke's Dobrosavljevic expressed optimism about the problem:

“I’m not aware of specific off-the-shelf [decoy] solutions at the moment, to be honest, but I’ve seen systems that are being developed. And they’re quite good. I think the technology is pretty much in research and development at the moment, and a number of countries are working on it because there’s a lot of interest in it. But it’s one of the more complicated things to achieve when you’re trying to mimic an entire battlegroup. And unless it is absolutely nailed on, even down to the modulation types and the timings, then a capable adversary will realize that a decoy isn’t real. We’re not talking about simple jammers here.” He went on to say, “However, decoys could basically congest the electromagnetic environment from our side, confusing and keeping the adversary busy over an extended period of time and prolonging their decision loops. That’s one way to maintain the tactical advantage.”

Echoing the thoughts of Saab, Dobrosavljevic also described how disruptive technologies must also be supported by suitable concepts of operation and TTPs: “It’s never just technology itself. You also want to build behaviors, skills and capabilities and ways of working.”



Czech company Inflatech Decoys makes inflatable decoys, such as the SA-8 and T-72 above, that feature thermal and radar signatures. INFLATECH DECOYS

FUTURE

Looking to the future, Roke believes electronic support measures will permeate all the way down to the lowest tactical level, with every soldier on the ground becoming a multi-sensor node in a wider battlefield network. Benefiting from

smaller, lighter, more agile and highly capable solutions, soldiers will be more informed, benefiting from the ability to track their own forces and exploit all of that information. “That’s a double-edged sword,” Dobrosavljevic warned. “If they’re all sensors at the edge, that’s creating a huge signature for potential prosecution by the enemy. But if you have a haystack, which piece of straw is the one you need to stop? So it’s all about either not exposing themselves in the electromagnetic spectrum or creating even more signatures to confuse the enemy across the entire battlespace.”

Saab’s Ålund said, “We think that multispectral deception capabilities are the next big thing. In a potential multi-domain conflict, the most advanced sensors are feeding AI-controlled kill-networks with global reach … Deception will never be obsolete. An 80% reduction of a sensor’s capability to detect is still 50% even when the sensor ranges evolve. We see customers investing to implement a capability now, at the same time as incremental development of technology and doctrine are prioritized in parallel. The future is now. A majority of the customers need state-of-the-art capabilities available now. The threat is not only evolving; it has already been here for a while. The requirement is for a system provider that can deliver incremental developed capacities ahead of the sensor threat.”