Russia’s Real-World Experience is Driving Counter-Drone Innovations

by **Samuel Bendett**, published on **Defense News**, May 23, 2021

The Russian military is actively working to develop concepts, tactics, techniques and procedures against aerial drones. The Russian Ministry of Defence has invested heavily to defend its forces against the growing threat and proliferations of UAVs large and small, from those manufactured by foreign states to those used by a growing slate of nonstate actors and terrorist organizations.

This investment comprises the development of technologies, incorporating the lessons learned from its own military and from other forces’ combat, and continuing to refine its electronic warfare capabilities as a key element of counter-unmanned aerial system tactics, techniques and procedures.

Learning from experience

Russia’s own involvement in the Syrian conflict started in 2015 when it brought its military in direct conflict with forces and coalitions fighting the government of President Bashar Assad. While Russia considers Syria its own “*sandbox*” for testing multiple weapons systems, the unpredictable Syrian military battlespace also resulted in nonstate actors experimenting with commercial off-the shelf drone technologies by launching multiple mass UAV attacks against the Russian base at Hmeimim.

At the same time, the Russian military was a keen observer of combat drone use against its allies in Syria and in Libya.

The ongoing drone use by the anti-Assad Syrian forces against

Russian targets, along with Yemen’s Houthi forces against Saudi Arabian targets, and the recently concluded war in Nagorno-Karabakh confirmed the MoD’s conclusion: A robust electronic warfare defense, together with early warning radars and anti-aircraft systems, can provide adequate protection against the growing use of UAVs by global belligerents.

In Syria, the MoD dubbed this triple c-UAS layer as the “*echeloned defense*” that was effective against do-it-yourself-type drones, but that is still unproven against more sophisticated military drones currently in service with multiple combatants around the world.

Following the conclusion of the 2020 Nagorno-Karabakh War, Russian military experts remain committed that the above-mentioned “*echeloned*” combination would have worked well against Azerbaijani drone attacks, especially given that some form of this echelon comprising EW and anti-aircraft systems in service with the Armenian forces was able to blunt certain Azeri UAV operations. As Turkish combat drones in Libya and Syria attacked Moscow’s allies, the older Soviet and Russian-made anti-aircraft systems had limited success against adversarial UAVs, but could not be more effective without other “*echeloned*” elements described above.

The continuous Houthi drone strikes against Saudi targets also expose the limits of modern Western-made anti-aircraft systems like the Patriot; such systems may not be adequate against small UAVs with very low radar signatures. The cost of deploying such anti-aircraft systems against small drones may be prohibitively expensive, necessitating a different approach to dealing with this new and evolving threat.

Finally, Russian support for the separatist forces in eastern Ukraine confirmed the importance of drones as a key intelligence, surveillance and reconnaissance element in today’s combat, and the importance of robust EW defenses should the Ukrainian military start fielding more sophisticated UAVs against pro-Russian forces.

Concepts and Technology

According to Lt. Gen. Alexander Leonov, chief of the Russian air defense forces, the ongoing efforts by nonstate actors and terrorist organizations to improve their UAVs and their usage methods indicate that in the near future, the threats associated with the use of drones may increase not only in Syria but also in other countries.

He points out that Russia gained valuable experience in countering such drone attacks, and that these skills and knowledge are now reflected in air defense combat manuals and are part of tactical, select and reconnaissance training. In fact, the Russian Ministry of Defence notes that today, all military districts across the country have units to counter adversarial drones.

The Russian experience defending its Khmeimim base from UAV strikes has become the foundation of its military’s c-UAS training program. Starting in 2019, all major military exercises and drills include the defense against an adversary’s massed drone attacks. The electronic warfare systems and technologies emerged as a key concept in this training. Across the Russian military services, in numerous drills, exercises and maneuvers, EW training is regularly conducted against adversarial drones, and practically all c-UAS drills feature EW systems as a key element.

Such symbiotic pairing typically unfolds in drills where the “*adversary*” forces use UAVs as key ISR elements against Russian troops, vehicles and systems.

Typically, the Russian military uses a combination of portable and wheeled EW systems. The Borisoglebsk and Zhitel systems are often tested in such drills; the EW specialists conduct electronic reconnaissance, then collect and analyze intelligence data, followed by conducting radio interference to “drown” adversarial UAV control channels along with drones’ communication channels with GPS navigation satellites.

In another typical c-UAS exercise that was conducted this year, the “adversary” force used several UAVs to conduct reconnaissance and coordinate artillery strikes against Russian positions. The Southern Military District’s mobile EW groups used an R-934BMV automated jamming station, the Silok-01 electronic warfare system and the Pole-21 advanced radio suppression system to discover enemy UAVs in order to interfere with their communications and suppress their control channels, rendering them useless for further operations.

In Syria, the MoD confirms that a combination of hand-held and stationary systems are used to suppress and jam drones that continue to harass and attack Russian positions. Using such systems allows the Russian military to directly influence UAVs’ control and navigation channel receivers. The EW troops intercept control channels, and the operator monitors the position of the UAV and proceeds to take control of the drone, giving the UAVs a command to land.

In Russia, military forces started using Stilet and Stupor portable c-UAS rifles, along with the newest Krasukha-C4 EW complex designed to identify adversarial strike aircraft and to suppress their communications and navigation. In a recent Black Sea drill, the EW detachments used the Krasukha system to target and disable multiple drones flying at low and medium altitudes.

Looking Ahead

Today, the Russian military is making c-UAS training mandatory across its services. In July 2018, the MoD announced that all ground forces, marines and airborne troops will have to learn how to shoot down drones with assault rifles, machine guns, sniper rifles and automatic weapons. This c-UAS concept of operations was developed taking into account the Russian military experience in Syria.

There is also evidence that the Russian MoD is eager to expand its c-UAS training and field activity beyond countering small, low-flying drones. In 2018, Russian EW systems jammed American drones operating in Syria, providing the MoD with valuable data and experience in countering more advanced adversarial UAVs.

The Russian military is also making sure its c-UAS systems and concept of operations involve the latest technologies, such as artificial intelligence, for the greatest advantage against the growing sophistication of the global drone force. New counter-drone radars and UAVs capable of targeting other drones are in development by the Russian military-industrial enterprises.

As the UAV threat will continue to persist, Russian MoD efforts will be directed at the continuing refinement of its c-UAS practices, while seeking to introduce technology capable of offering protection against adversaries' drone developments.

Samuel Bendett is an analyst with CNA's Russia Studies Program and an adjunct senior fellow with the Center for a New American Security's Technology and National Security Program.