MEI
Policy Center

THE NEW FACE OF WAR: DEVASTATING DRONE ATTACKS IN UKRAINE HAVE IMPLICATIONS FOR THE US MILITARY IN THE MIDDLE EAST

ANDREW MILBURN

March 2022

In dramatic video coverage currently going viral on YouTube and TikTok, Ukrainian drones are seen to destroy a Russian convoy, with startling speed — and total impunity. The story of how destructive such drone attacks are proving to be was picked up by several U.S. papers, and brought to light the capability of the Turkish-made Bayraktar TB2 drone — which seems perfectly designed for modern war. Despite its emergence as an inanimate hero of the Ukraine conflict, the story of the TB2, and its employment by various actors over the last three years, brings with it a dire warning for the U.S. military.

In January of this year, Houthi rebels — backed by Iran — launched two attacks, a week apart, against the UAE, using drones and ballistic missiles. Media attention focused largely on the second attack, which targeted the U.S. base at al-Dhafra, and was — according to the headlines — foiled by Patriot missiles. This is true enough, but misses a key aspect of the story. While the second attack relied on ballistic missiles, a threat that the Patriot system is designed to counter, the attack launched a week earlier used only drones that penetrated Emirati air defenses and caused civilian casualties. This incident, the latest in a series of increasingly sophisticated drone attacks directed against the UAE and Saudi Arabia, highlights the vulnerability of U.S. forces in the region, which have no defenses against such an attack. U.S. air defense systems such as the Patriot PAC-2 are simply not designed to defeat relatively slow moving, low flying threats, such as drones or cruise missiles.

Almost three years ago, a drone attack incapacitated Aramco oil processing facilities in Saudi Arabia, overwhelming the Patriot battery that was supposed to defend them. Although that attack was launched by the Houthis, the drones and training in their employment were undoubtedly provided by the Iranians. This should have been a wake-up call for the U.S., spurring us to a concerted effort to counter this threat, and to send an unequivocal message to Iran that it would pay a heavy price for any future attacks.

It's not just our partners who should be concerned. U.S. interests and U.S. forces are already under attack, and recent incidents should be viewed as an escalating cycle of experimentation by our adversaries. They should alert us to the fact that Iran and its proxy forces in the region are developing increasingly sophisticated platforms. This isn't so much a case of developing advanced technology as it is making existing technology more lethal and readily available. It is only a matter of time before the Houthis, or any one of a number of groups, are able to swarm multiple such platforms against U.S. targets. This is because the use of these drones en masse creates an offense-defense balance where the attacker has a distinct advantage in terms of cost and risk. And the more drones

that an attacker can employ simultaneously, the harder this becomes for the defender. Despite soothing assurances that short-range air defense systems are on their way, even the most sophisticated of such systems are unlikely to keep pace to counter the proliferation of expendable but increasingly sophisticated drones. The U.S. Army's Air and Missile Defense 2028 strategy itself warns that, "The most stressing threat is a complex, integrated attack incorporating multiple threat capabilities in a well-coordinated and synchronized attack."

It's a physical problem, but also a resource problem. Air defense projectiles, such as those launched by the Patriot and Iron Dome systems, are hugely expensive — as much as several million dollars apiece. By contrast, drones are cheap and expendable.

The prospect that Iranian proxies and other bad actors will soon be armed with systems that can penetrate even the most sophisticated air defense systems is not a future concern: Several countries are already ahead of Iran when it comes to drone technology and, even if all nations involved have only the best intentions, proliferation is inevitable.

The UAE has a fleet of Wing Loongs — a Chinese-made armed drone — that it used to devastating effect in Libya. But it is Turkey, with a defense budget a fraction of the U.S.'s, that has demonstrated how unmanned platforms have changed the nature of modern war, rendering even the most sophisticated air defense systems obsolete and handing the initiative to any attacker who understands how to best use them. It was Turkish drones that turned the tide against Khalifa Hifter's assault on Tripoli in Libya in 2019 and, more recently, halted the Tigrayan advance on Addis Ababa in Ethiopia in 2021.

But it was during the conflict in the disputed territory of Nagorno-Karabakh in the South Caucasus in 2020 that the drone really came into its own. The Azeris — equipped and guided by Turkish advisors — used drones in conjunction with loitering munitions to overwhelm an advanced integrated air defense system (IADS) and break the back of the Armenian military in just 44 days. The videos released every day by the Azeris to the world's media depicted a robotic ballet of precision carnage that undermined Armenian morale as much as it destroyed their ability to fight. The two systems that became the centerpiece of Azeri dominance were the Israeli Harop loitering munition — referred to in the media as a kamikaze drone — and the Turkish Bayraktar TB2 armed drone.

The TB2 is a "blue collar drone": inexpensive enough for mass production and thus expendable. Mass production gives it the capability to be employed in swarms designed to overwhelm the target acquisition process of any adversary. And yet, the TB2 is also remarkably sophisticated. In addition to providing identification and targeting data from high-resolution onboard systems that can include a signal's intelligence capability, the platform carries smart, micro-guided munitions that kill multiple targets autonomously and simultaneously.

The term "kill chain" is a military concept used to describe the process of an attack. It consists of initial target identification, a "fixing" phase that involves determining a target's location and other relevant details while preparing to strike, the final decision and order to attack, and the destruction of the target. The term is used for any method of attack, whether launched by drones, manned aircraft, artillery, or a ground force. It is also used to describe operations in the information or cyber environment.

The kill chain concept helps focus planning in three ways. First, the main objective for friendly kill chains (which, I admit, does sound like an oxymoron) is to "flatten" the process as much as possible, which means expediting its execution without incurring unacceptable operational, legal, or ethical risk. The second planning objective is to "harden" friendly kill chains — protecting them from enemy attack. Conversely, the third goal is to "break" or disrupt an opponent's kill chain as a method of defense or preemptive action.

These three objectives also help focus the technology and employment of drones. Counter-drone planning focuses on breaking the kill chain between the operator and the drone itself. This becomes harder to do as drones come closer to operating autonomously. The employment of TB2s and Harops in tandem is a step nearer to achieving this. However, a human is still in the loop; the find, fix, and finish functions are all performed in quick succession, close to the target, which expedites the process and makes it much harder to interdict. With an attack involving multiple drones, and thus providing redundancy, this becomes almost impossible.

In Nagorno-Karabakh, for example, the Azeris would flood an area with drones, which enabled rapid target acquisition and immediate precision engagement, either by direct delivery of the TB2's organic munitions or by vectoring in a loitering munition.

Photo above: A Bayraktar TB2 armed unmanned aerial vehicles lands at Gecitkale Airport Northern Cyprus on Dec.16, 2019. Photo by Muhammed Enes Yildirim/Anadolu Agency via Getty Images.

In engagements over Syria and Libya, as well as the one in Nagorno-Karabakh, the TB2 alone demonstrated the ability to successfully challenge the most advanced IADS that nations can muster. Systems such as the S-300PS, Buk-M2, Tor-M2, and Pantsir-S1 — used in conjunction with electronic warfare systems such as the Avtobaza-M, Repellent-1, Borisoglebsk 2, and Groza-S — are designed to deny airspace to the latest generation of Western strike aircraft. None of these systems proved capable of stopping the TB2 — a revelation that Russian manufacturers still try to deny, even when their claims are refuted by high-resolution full-motion video from no less than three conflicts. The fact that a relatively light and inexpensive drone can not only evade but actively search out and destroy such systems while incurring few losses represents an evolutionary leap in the employment of air power and a tectonic shift in the conduct of modern war.

In the aftermath of the Nagorno-Karabakh conflict, the TB2 became a hot item on the international market, with multiple countries seeking to vaunt their status by joining the exclusive club of states with armed drone technology. Again, it's only a matter of time before this technology falls into the wrong hands.

Sadly, at a time when the Department of Defense (DoD) could really use help from the commercial technology sector in solving these problems, the gulf between the two has never been wider. The schism has its roots in a cultural distrust that many employees of the big tech companies have for the U.S. military — Google's withdrawal from Project Maven, a DoD AI initiative, is just one such example. Aside from ethical concerns, the DoD fails to make the prospect of partnership appealing for such companies. DoD contracting processes are cumbersome, opaque, and ill-suited for the world of commercial technology. Last year's cancelation of a $10 billion contract to help DoD develop an enterprise-scale cloud-computing capability, for instance, left the two competitors, Amazon and Microsoft, frustrated and disillusioned. Instead of reaching across this divide in a transparent effort to explain why the United States needs this technology and to assuage the ethical concerns of Silicon Valley's workforce, the DoD continues to function within its procurement comfort zone — with the handful of large

Photo above: A partial view of the Musaffah industrial district in Abu Dhabi on Jan. 17, 2022. Three people were killed in a suspected drone attack that set off a blast and a fire in the city. Photo by AFP via Getty Images.

defense contractors whose forte is to manufacture increasingly exquisite but obsolete platforms. As with cloud computing, AI, and a host of other technological problems faced by DOD, the counter-drone problem is more likely to be solved in the whimsical workspaces of Silicon Valley than in the cubicle warrens of Lockheed or Raytheon.

So, what can be done? First, we have to address this particular problem at its source by finding an effective way to counter Iran's malign influence in the region — notably its use of proxies to launch attacks on U.S. personnel, partners, and interests. We must preempt this escalation by taking action now in three areas:

1. **Impose costs directly on Iran.** To date, they hold the cards in this asymmetric contest. They use proxies to destructive effect at little cost to themselves. After the attack on the Jan. 24, there was talk of striking back at the Houthis. This may well be necessary, but it's not going to be enough. We must impose direct costs on Iran by putting Iranian personnel and interests at risk. The strike on Qassem Soleimani, head of the Islamic Revolutionary Guard Corps – Quds Force, two years ago in Baghdad would have been a good example had it been part of a wider strategy backed by a coherent messaging campaign. This time, our messaging must be unequivocal and backed by action: There can be no more unconsummated talk of redlines. This will take resolve and consistency at the policy level.

2. **We must work closely with our partners in the region to preempt these attacks, but defensive measures will not be enough.** We must go after the networks — the personnel, infrastructure, and supply chains — that enable these attacks. Only the U.S. has the regional expertise and geopolitical influence to bring together disparate governments in the region, including Israel, to work together to solve this problem. This step is not a giant leap. We already have a number of bilateral fusion cells scattered throughout the region, focused on the threat from Sunni extremist groups. And when it comes to interdicting the

supply chain, the problem is relatively simple. All shipments must pass through one of a small group of Iranian ports and either move overland across Oman or parallel to the coast. Intercepting shipments is not a problem of resources or intelligence assets — it's one of political will.

3. **We must dedicate our acquisition process to find technical solutions and methods of employment that will mitigate the threat of swarmed attack.** Iranian proxies are not our only enemies in the region capable of attacks such as those I have described.

   The U.S. military's current acquisition process is too lockstep, platform-centric, and mired by parochialism to find such a solution. The DoD needs to engage with tech companies outside the defense industry to make it worthwhile for them to do so.

   Defense reform is, of course, a political challenge not just a bureaucratic one — and will require a concerted political effort focused on a clearly defined roadmap in order to bring about real change. However, the enormity of this task shouldn't preclude the DoD from taking steps in the meantime to solicit wholehearted support from the technology sector, while making such collaboration worthwhile. Holding high prize competitions in which companies compete to provide the best solution to specific problems is just one method of doing so.

Winston Churchill once commented that the U.S. "can always be relied upon to do the right thing, after exhausting all alternatives." We may yet again be in just such a situation — and the time to find a solution is now.

Andrew Milburn retired from the Marine Corps in 2019 as the Deputy Commander of Special Operations Command Central, the headquarters responsible for all US special operations in the Middle East. Since retiring, he has written a critically acclaimed memoir, When the Tempest Gathers, and articles for a number of publications. He is on the Adjunct Faculty of the Joint Special Operations University, a co-host of the Modern War Institute's Irregular War Podcast and Irregular War Initiative, and a Non-Resident Senior Fellow with MEI's Defense and Security Program. The views expressed in this piece are his own.