www.usni.org /magazines/proceedings/2020/may/how-drones-could-mission-kill-us-destroyer

How Drones Could Mission Kill a U.S. Destroyer

Lieutenant (J.G.) Artem Sherbinin, U.S. Navy ⋮ 9-11 minutes ⋮ 5/4/2020

By Lieutenant (J.G.) Artem Sherbinin, U.S. Navy, and First Lieutenant Richard Kuzma, U.S. Army

“Navy Destroyer Attacked!” was the headline of every U.S. newspaper and morning talk show on 12 October 2020, the 20-year anniversary of the al Qaeda attack on the USS Cole *(DDG-67). A terrorist group used a swarm of drones carrying explosives to cripple the radars and weapon systems of the USS* John Basilone *(DDG-122) only months before she was due to deploy with her carrier strike group. The* John Basilone *was moored at Naval Weapons Station Seal Beach and in the process of onloading missiles and ammunition.*

The drone threat has been around for years, but the Navy has yet to prioritize defending against these easily acquired weapons. Amid preparations for a high-end fight, the Navy still is vulnerable to an adversary trading thousand-dollar drones for billion-dollar warships.

How It Could Happen

The Islamic State first used explosive-carrying drones in 2016, and a do-it-yourself drone swarm attack was reported in Syria in 2018. Terrorist groups can purchase high-end commercially available hobbyist drones for around $2,000, masking the money trail by purchasing drones over time from multiple brick-and-mortar stores or by using cryptocurrencies at online retailers.

A top-of-the-line consumer drone such as the DJI Mavic Pro 2 has a range of up to ten nautical miles, a maximum speed of 40 knots, a small payload capacity, and the ability to fly via waypoints. Speed and range would be degraded were the drone equipped with an explosive payload, but range would not necessarily be a limiting factor.

Figuring out when a ship will deploy is not difficult either. Most aircraft carrier strike groups follow predictable deployment schedules to maintain a U.S. naval presence in the western Pacific and the Middle East, and all ships go through a work-up period prior to a deployment that includes short underways, readiness checks, and weapons onloads—making it clear which ships are nearing their deployment dates. Terrorists also could use social media to dig deeper: following the public Facebook pages of warships or infiltrating sailor family and friends Facebook groups and befriending group members to probe for information on ships’ upcoming movements.

To know how to strike the ship, the terrorists could study open-source images of the *Arleigh Burke*–class guided missile destroyers to determine the locations of key weapon and communications systems. This expensive electronics equipment is vulnerable to drone-carried explosive devices or kamikaze-style attacks. Hobbyists with coding skills have shown they can reprogram drones to track people. Building on this knowledge base, the terrorists could program drones to focus on communications antennas, weapon systems, or radar arrays.

After flying to the waypoint of a target ship, the drones would not need to emit a radio signal to a controller if their final approach were made using electro-optical sensors—their camera eyes—paired with software that tells each drone when and where to strike. Such an approach would make the drones impervious to antidrone systems that jam radio transmissions between the controller and the drone. The drones could strike the SPY radar arrays, half a dozen satellite communications antennas, or the intakes and exhausts of the destroyer’s main engines. Sprinkling these key systems with shrapnel from exploding drones would cause millions of dollars of damage, take months of unplanned maintenance to repair, and leave a destroyer unable to perform its mission.

Warships are most vulnerable when they have limited ability to maneuver—such as in the Suez Canal, Bosphorus Strait, and Panama Canal. But a warship trapped inside Seal Beach’s Anaheim Bay (or any other pier), saddled by cranes onloading thousands of pounds of explosive ammunition, also presents an exposed target. Warships are also vulnerable at sea, because their advanced air defense radars are calibrated for traditional air threats: missiles and tactical aircraft flying hundreds of miles per hour, tens of thousands of feet in the air. Drones flying at lower speed and altitude are difficult to detect if a warship isn’t actively looking for them.

The Way Ahead

The fragility of weapon systems, radars, and antennas on modern U.S. warships means that even small attacks could yield significant damage. This vulnerability, combined with the small-investment-for-a-large-payoff incentive for U.S. adversaries, make drone attacks a serious risk to the Navy's operational schedule. This threat must be mitigated, but the current state of drone defense is lacking.

Traditional antiterrorism and force protection measures are not sufficient. Expecting sailors who shoot shotguns, rifles, or machine guns twice a year on a range to be able to engage multiple small, fast-moving targets is unreasonable. Even if a few sailors were expert shooters capable of shooting down drones, it likely would take a few minutes from the first report of a potential drone to identify the drone, raise the alarm, and bring key weapons and associated ammunition to bear against the threat—time the ship might not have.

Since current kinetic methods are generally ineffective against drones, the Navy has turned to electronic counters. Shipboard electronic attack capabilities and counter-unmanned aerial system (UAS) systems supplied by traditional defense contractors are supposed to defeat drones with a "soft kill." However, these means quickly lose their effectiveness against large swarms of drones or when the drones do not rely on a transmitted radio signal for control. Future counter-drone technologies such as lasers are still too early in development. The first U.S. guided-missile destroyer to deploy with a functioning laser will not sail until 2021, meaning it will take a decade to roll-out this capability to the rest of the fleet.

Even soft kills are not a guarantee. In counter-drone warfare in Ukraine, just 10 percent of drones have been destroyed by electronic measures. Many of these defeated drones were focused on image collection, loitering over the battlefield, making them easy targets.

Cheap commercially available hard-counters to drones offer the best near-term prospects. Antidrone nets placed around critical communications equipment, or even counter-UAS drones, are readily available technologies that should join the Navy's arsenal immediately. As witnessed in the anti–improvised explosive device campaign of the past decade—which pioneered the rapid procurement of everything from mine-resistant vehicles to portable counter-radio frequency systems—the Defense Department is able to quickly roll out new technologies to counter irregular threats.

The best way to counter the advent of commercial weapon systems is to leverage the nation's own world-class technology sector, but defense technology spending still is centered on traditional contractors. These firms are critical for national security procurement, but they typically are neither the most agile nor the most technologically progressive companies, and they are just one arrow in the defense acquisition quiver.

The counter-drone market is expected to grow to $2.25 billion in 2024. This financial draw means smaller startups will be entering the market and worth consideration. Black Dart 2019, a drone exercise featuring 16 counter-UAS venture-backed technology companies, is an example of Department of Defense (DoD) reaching out to nontraditional defense contractors for difficult technology solutions. The Navy must be willing to be more of a player in the nontraditional commercial technology space, using DoD technology conduits such as the Defense Innovation Unit, while continuing to leverage large defense contractors, traditional service laboratories, and the Defense Advanced Research Projects Agency.

Put Money on the Table

Drones and artificial intelligence no longer are the technologies of science-fiction books and research labs. They are commoditized and democratized and can be used by anyone with a few thousand dollars and some technical know-how—including malevolent actors with the intent to do harm.

The Navy used to worry only about threats from nation-states in waters far from U.S. shores, but this technology means ships may be vulnerable even in their homeports. Conversations about advanced threats to ships cannot happen only inside the Beltway; tactical-level leaders must talk with their sailors about the dangers of drone attacks, prepare to defend against them, and apply pressure up the chain of command to acquire state-of-the-art technology solutions.

The Navy has been slow in responding to the drone threat, and this is just the beginning. Drones are only one of the myriad novel technologies—think cryptocurrency, social media manipulation, and the like—that national security leaders will encounter this decade. To counter these threats, the Navy must adapt its mind-set toward acquiring and deploying technology.