Autonomous Ghosts are Reshaping Irregular Warfare and Maritime Security

Description

This article is part of Project Maritime, which explores modern challenges and opportunities in the maritime dimension at the intersection of irregular warfare and strategic competition. We warmly invite your participation and engagement as we embark on this project. Please send submissions with the subject line â??Project Maritime Submissionâ?• and follow us on X (formerly Twitter) @proj_maritime.

Unmanned aerial vehicles may be the talk of the town, but aquatic drone developments of equal strategic magnitude are underway. This swell of seafaring phantoms**,** enhanced by other emerging disruptive technologies, will challenge traditional maritime force composition, subvert long-practiced naval missions and maneuvers, and complicate existing problems around attribution of maritime aggression. As facilitators and force multipliers, they will introduce yet-unseen asymmetries to the world of irregular warfare and might well redefine the rules of engagement at sea.

Commercial or military, no domain is sacredâ??â??and the proof is only accumulating. A pan-Nordic investigation in 2023 uncovered that Russian vessels were mapping critical underwater infrastructure across the North and Baltic Seas using unmanned maritime vehicles (UMVs). Nearby, UMVs surged in visibility when the Ukrainian Armed Forces launched high-profile autonomous strikes against Russiaâ??s Black Sea Fleet. Further south, Yemenâ??s Houthis deployed a variety of UMVs against ships transiting the Red Sea. In raising UMVsâ?? profiles, these incidents introduced fears of dual-use proliferation and adversaries equipping clients with autonomous proxy fleets. Together, they represent a lowered barrier to entry into military conflict.

https://irregularwarfareinsider.podbean.com/e/autonomous-ghosts-are-reshaping-irregular-warfare-and-maritime-security/

UMVsâ?? proposed advantagesâ??â??cheap, long-lasting, low-profile, low-human-riskâ??â??also diversify their applications to irregular warfare, which play off both unique and complementary missions to traditional vessels. Their spread amounts to an unfortunate marriage of legal, political, and operational problems, the core issue being how to simultaneously allow for desired advances in autonomous fleet integration at home while expecting and discouraging challengersâ?? parallel action. Gaps in maritime law and the oceanâ??s physical encumbrance, in particular, render UMV irregularity difficult to address, demanding technical and doctrinal innovation from the US Navy and bureaucratic

and regulatory reform around targets and perpetrators at home and abroad.

Ghost in the (Sea)Shell

Both state and non-state actors may covet surface and underwater UMVs due to their favorable cost-to-chaos ratio. According to RAND naval technology expert, Scott Savitz, UMVs offer the potential to deploy numerous non-lethal â??intermediate force capabilities,â?• like entangling propellers, ramming sonar domes, and creating obstacles.

One insidious opportunity for irregular UMV activity surrounds critical underwater infrastructure, a fundamental pillar supporting everyday life and national security. UMVs can surveil or interfere with it. Though UMVs threaten to disturb all types of port and offshore critical underwater infrastructure, zeroing in on fiber-optic cable sabotage exposes significant legal and operational problems. A coordinated UMV attack on exposed landing sites or underwater lines could stress a countryâ??s intelligence apparatus, financial flows, and communications, as these cables carry up to 95% of global internet traffic. Cable sabotage imperils the very presence of a digital information ecosystem, meaning that efficiently determining the who, what, where, when, why, and how of a cable attack is essential. Unfortunately, investigations are muddled as much by UMVsâ?? obscurity as they are by the flawed critical infrastructure legal regime.

A Specter Swims in No-Manâ??s-Land

The foremost complication regarding cable governance and interference is ownership. 99% of cables are privately owned, either by tech behemoths like Google and Microsoft, or by consortiums of private or state-owned entities. Companies harboring information on cablesâ?? construction and maintenance may obscure their intermittent and uncoordinated policing; even worse, they sometimes lack detailed knowledge of the cables they use or how cables support their services. The US government administers cables in an equally decentralized manner, with over twenty government bodies overseeing various elements of cable infrastructure. This disaggregation easily creates confusion during a natural disaster or military emergency. In the case of a serious outage, incomplete status data and scattered responsibilities make it hard to reroute essential traffic or organize repairs. Both the private and public sectors are therefore complicit in perpetuating a deficient protective regime.

Stealthy UMVs are poised to exploit these vulnerabilities at the domestic *and* supranational echelons. International law has no agreed-upon definition of cables, meaning that multilateral institutions operating under a patchwork architecture of the United Nations Convention on the Law of the Sea

(UNCLOS) and regional maritime agreements have few avenues to hold a malicious party accountable in international waters and contested territory.

Insufficient response mechanisms become egregious given the range of where critical underwater infrastructure damage may fall on the kinetic spectrum, risking escalation to conventional conflict. That is, can anything less than a penetrating blow to a military asset be considered an act of war? Currently, maritime law does not bar states from viewing undersea cables as legitimate military wartime targets. This issue is aggravated by UNCLOSâ?? provisional deficit regarding covert damage and theftâ??â??punitive thresholds are too high for risky commercial activities. It also poorly defines which proactive policy prescriptions adhere to international law.

As long as a malicious actor targets nodes in the high seas, or even its own exclusive economic zone, injured states are unable to bring those responsible to justice. While Article 113 offers criminal sanctions for willful or negligent injury of underwater cables, a state may actualize these punishments only after passing legislation implementing said Article, which few nations have accomplished. *Willful* is the operative word here, and UMVs could affect plausible deniability and causal ambiguityâ??â??i.e., obscure â??whodunit.â?• Outright repudiations of obvious interference constitute what Savitz terms *im* plausible deniability, but frequent *accidental* damage, usually created by commercial vesselsâ?? nets and wayward anchors, is increasingly employed as a legal disguise when circumstantial evidence points to a culprit. It is not hard to imagine how a well-executed operation using nimble UMVs may render identification impossible.

Creeping the Deep

These governance gaps give even short-term reasons to worry; intentional attacks against American partners and allies are already occurring. For example, in 2023, a Chinese fishing vessel and a cargo ship cut two cables connecting Taiwan to the Matsu Islands, which virtually terminated internet access and stalled the islandsâ?? online economy for almost two months. Taiwanâ??s lack of cable-repair resources exacerbated the damage, leaving the islands to rely on in-demand international restorative ships. As of early 2023, similar cuts had occurred over two dozen times in the preceding several years. It is a near-certainty that Beijing could use UMVs to execute a larger, coordinated attack to cut most or all of Taiwanâ??s international cables in the event of A2/AD, a strategy that limits an opponentâ??s operations in a given area. Similarly, Russia has also been suspected of several cable-cutting and other infrastructure sabotage incidents around the Shetland Islands, Norway, and, though thrown into fresh debate, the Nord Stream pipelines in the Baltic Sea. Reports suggest that select Russian espionage ships already carry small unmanned underwater vessels (UUVs) to sever or tap cables, often focusing on remote but critical cables that are difficult to maintain.

There is also some evidence of Sino-Russian coordination. The two statesâ?? cable activity collided in 2023, when a Chinese cargo ship and accompanying Russian vessel were tied to both pipeline and cable damage in the Baltic Sea. A flagrant example of critical underwater infrastructure abuse, the awkward legal chase that followed demonstrated that intercepting *manned* vessels is already difficultâ??â??UMVs could be even trickier. Moscow and Beijing are far from the only actors interested in wedding autonomy and sabotage, but these alleged interferences and consequent know-how imply that they may seek to exploit irregular UMV applications with purpose.

To Chase or Embrace

UMVs exemplify the occasional imperative to fight fire with fire. That is, develop a robust domestic unmanned capability to expose and fend off adversarial UMVsâ??â??providing a conventional deterrent effect, a blockade in the case of attack, or an amplification of traditional assetsâ?? surveillance matrix. In the case of critical underwater infrastructure, this might mean deploying UMVs as coastal or chokepoint surveyors, to say nothing of the myriad missions offered independent of defense. But developing UMVs to prevent, react to, and *perform* critical underwater infrastructure sabotage is rife with technical challenges, especially surrounding reliable autonomy. UMVs must address many contingencies, from underwater terrain to marine life and other collision avoidance. According to Savitz, better autonomy requires large test sites, enhanced communication methods beyond low-bandwidth acoustics, and more prolific data provided by rapidly improving sensors. But meager funding and specialized applications hinder progress compared to many commercial autonomous vehicles. While hacking a UUV can be difficult due to escaping the electromagnetic spectrum when submerged, electronic warfare can disrupt or manipulate data and algorithms when surfaced. These hazards demand that operators protect the physical integrity, trust the navigational acuity, and correctly assess the data accuracy of UMVs. Without human confidence in a vesselâ??s total autonomy or remote controls, UMVs canâ??t execute delicate defensive *or offensive* missions. So, while critical underwater infrastructure interference is inevitable, we remain far from replacing divers or meandering anchors with robots.

Despite these hurdles, adversaries nonetheless understand that these nimble, adaptable machines can outsource interventionist, resource-sapping missions from precious conventional vessels. Likewise, the US Navy could compartmentalize the capabilities it wants from huge, survivable assets like attack submarines or carriers and redistribute the remaining capabilities between numerous UMVs. Complementary autonomy wonâ??t require reinventing the wheel; per Savitz, UMV mechanics are subject to the â??same operational and physical phenomena that apply to any other vessel.â?• Significant technical and procedural continuity in acquisition and operation is essential to convincing military figures that UMVs are a worthwhile investment. Gradual progress in this regard is also valuable

for both effective expenditure and scientific development; avoiding buying all the most advanced iterations of a vehicleâ??s parts at once, for example, can reduce obsolescence later and better tune tactics and procedures. The bottom line is that the United States must keep offensive and defensive pace by leaning on autonomy where feasible.

Moreover, amid competing priorities and naval industrial base struggles, Washington should provide cheap, scalable UMVs to partners like Taiwan to engage in and defend against irregular instruments (and vice versa), in addition to expensive, limited, and slow-to-produce assets. UMVs can protect alliesâ?? cables by searching for evidence of manipulation and even hardwiring sensors, though it remains to be seen if they can manage cascading failures from multi-cable damage. Even so, insufficient legal provisions over increasing state and private UMVs and the impossibility of policing every open-sea cable mean authorities are likely to focus on responses over prevention.

Cooperation and exchange should also be as prevalent at home as abroad. Within the military, the Navy is far more advanced in UMV development and deployment in comparison to the Coast Guard, for instance, which suffers from lean funding and depends on hand-me-downs. Given how adversarial UMVs may proliferate around the United Statesâ?? shorelines and ports, this should raise eyebrows among those occupied with coastal security. This isnâ??t only a Pentagon effort, either. While recomposing forces will keep military leaders occupied for decades to come, diplomats and lawyers have just as urgent a call: reduce risk through more robust permitting and other regulations around UMVs, response vessels, and likely perpetrating vessels, advocate for less fragmented maritime legal architectures, discourage dual-use component proliferation through export controls, facilitate multilateral preemptive training, and help fortify the fleets and processes undergirding domestic and supranational response and repair mechanisms. In other words, this mess requires a whole-of-government cleanup.

Rising Tides

Critical infrastructure interference is one of a plethora of irregular UMV opportunities. Because cable damage fundamentally constitutes a communications crisis, actors may prey on weak repair resources, capitalize on ambiguous intent, or exploit ineffectual enforcement of maritime law to distort information. Irregular maritime activity counter-initiatives are therefore imperative. Adversaries are already enthusiastic about UMV integration, meaning the US Navy and other Western maritime forces should expect to defend against and acquire their own hybrid fleets. Doing so merits background domestic and multinational regulatory reform around both UMVs and the cable protection regime. As sure offenders and potential guardians, UMVs will not *replace* traditional vessels anytime soon. However, their clandestine weaponization will compound by virtue of their obscurity, versatility, and multiplicity.

These are the new poltergeists of the sea.

Laurel Baker is the 2024 Rising Expert on Geostrategy in the Rising Experts Program at Young Professionals in Foreign Policy. Currently working for Pacific Northwest National Laboratory (PNNL) as a National Nuclear Security Administration Graduate Fellow, she previously conducted research at a variety of think tanks and NGOs, including the Hoover Institution, Institute for the Study of War, The Arctic Institute, the Wilson Center, and the National Academy of Sciences. Laurel holds an MA in Russian, East European, and Eurasian Studies from Stanford University. Laurelâ??s views are her own and do not represent those of PNNL or the US Government.

The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

Main Image: Hammerhead sharks (Image by baechi from Pixabay)

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Date Created
2024/09/12