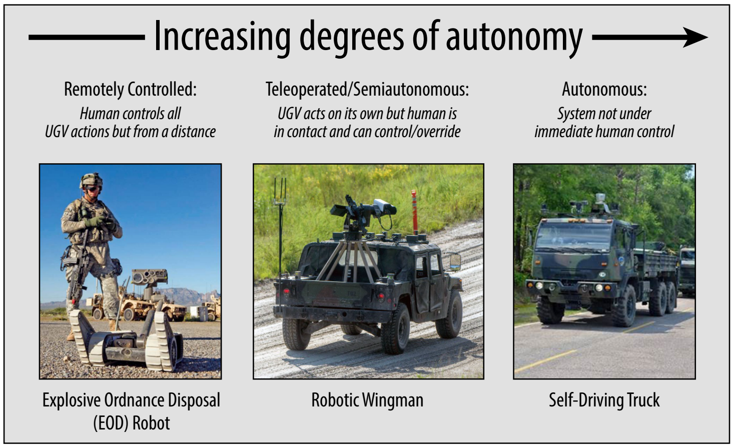
IDA | Research Insights

January 2019

# Countering Unmanned Vehicles

Eric A. Adelizzi (eadelizz@ida.org) and Geoffrey M. Koretsky (gkoretsk@ida.org)

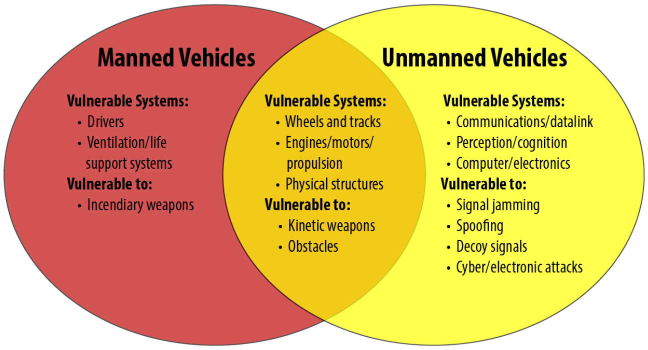
Russia and China are among the foreign countries that have made substantial investments over the past decade to develop unmanned aerial vehicles (UAVs), unmanned maritime surface vehicles (USVs), unmanned underwater vehicles (UUVs), and unmanned ground vehicles (UGVs). Such vehicles, collectively known as unmanned vehicles (UxVs), transport payloads such as sensors, weapon systems, communication nodes, supplies, or personnel. UxVs are distinguished from manned vehicles by the fact that their command and control is either remote, artificial, or something in between (below).


Increasing degrees of autonomy
Remotely Controlled:
Human controls all UGV actions but from a distance
Teleoperated/Semiautonomous:
UGV acts on its own but human is in contact and can control/override
Autonomous:
System not under immediate human control
Explosive Ordnance Disposal (EOD) Robot
Robotic Wingman
Self-Driving Truck

Range of autonomy in unmanned ground vehicles

**Potential U.S. adversaries may choose unmanned over manned vehicles because of lower cost, reduced signatures, and longer endurance.** Because they are unmanned, UxVs also offer greater obedience, non-attribution, immunity to psychological effects, and employability in harsh physiological conditions. On the other hand, UxVs depend either on remote operators who may lack situational awareness or on artificial intelligence that may be maladapted to dynamic situations, or both. UxVs are also likely to have thinner armor and weaker self-defenses than manned vehicles. Still, as UxVs have become more affordable and readily available, their potential use by small countries and non-state actors increases. In the long term, state actors operating UxVs pose the greater threat to the U.S., but the more likely and immediate threat is from non-state actors. UxVs' commercial availability and non-attribution potential make them particularly attractive for purposes of terrorism and hybrid warfare.

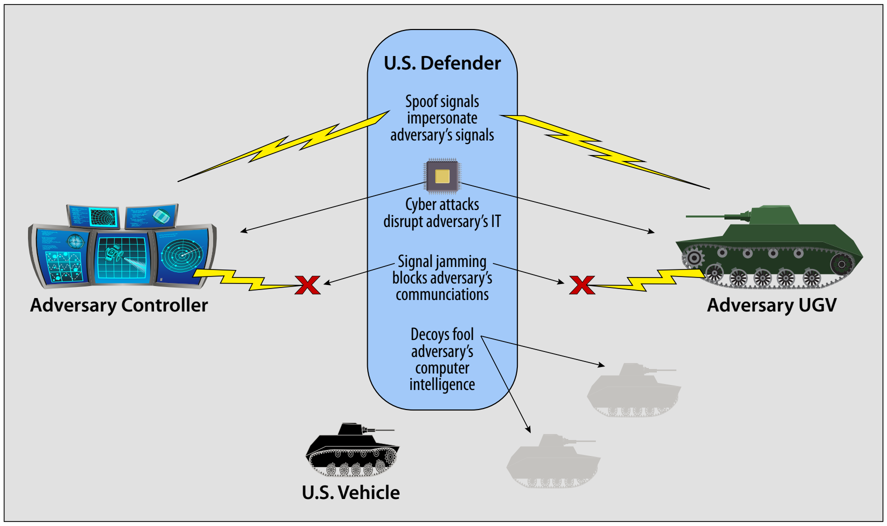
**IDA researchers have developed insight into ways of countering the threat posed by proliferation of UxVs by examining the vulnerabilities of current UxVs, developing credible scenarios for their employment by potential adversaries, and determining how they might best be countered.** Unmanned vehicles have more exploitable vulnerabilities than do manned vehicles (left). Although any vehicle that relies on computer systems to operate is vulnerable to cyber and electronic attacks, UxVs' computer systems are especially vulnerable because they rely entirely on computers to accomplish tasks that would, in a manned vehicle, be performed by a person. Further, teleoperated UxVs are vulnerable to jamming, spoofing, and, sometimes, decoys, whereas autonomous UxVs are generally vulnerable to anything that targets their autonomous perception and cognition.



Manned and unmanned system vulnerabilities

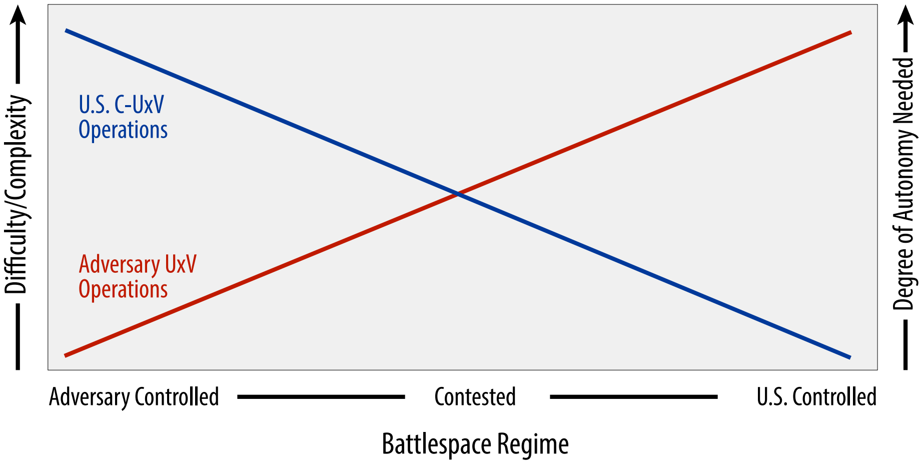
*(continued)*

© Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882
ida.org


U.S. Defender
Spoof signals impersonate adversary's signals
Cyber attacks disrupt adversary's IT
Signal jamming blocks adversary's communications
Decoys fool adversary's computer intelligence
Adversary Controller
Adversary UGV
U.S. Vehicle

Non-kinetic options for countering unmanned systems

**In terms of countering UxVs, U.S. forces may be able to quickly respond using kinetic weapons that deliver deadly force if the absence of a human operator in an adversary's UxV allows for less restrictive rules of engagement.** A direct kinetic attack would likely require detection and geolocation of a UxV target, but detection may be difficult for several reasons: (1) a small UAV or UGV also has a small signature that may preclude detection until it is too late to attack; (2) a well-camouflaged USV may be difficult for remote sensors to distinguish from surrounding surface waves; and (3) acoustic detection of even a large UUV is challenging at great distances. On the other hand, non-kinetic counter-UxV methods (depicted above) would not necessarily require detection and geolocation. Broad-area jamming of signals between a UxV that is not fully autonomous and its teleoperator could defeat a mission that requires data transmission. Another counter-UxV method involves broadcasting spoofed signals that direct the vehicle to behave in undesired ways or send false data to the vehicle's remote operator. In addition, decoys or cyber attacks may be used to fool a UxV's artificial intelligence. Exquisite intelligence about how the UxVs function would benefit many of these non-kinetic attack mechanisms. For instance, ability to spoof a signal depends on clear understanding of the UxV's signal format.



Relative advantage given battle space regime

**The difficulty and complexity of countering UxVs depend on the battlespace in which they are employed (left).** Adversaries operating UAVs over their own territory or UUVs in their own waters may rely on use of pre-built infrastructure, robust communications, and pre-surveyed areas in a known environment. U.S. counter-UxV operations in these scenarios would be conducted in unfamiliar environments that may be difficult for U.S. forces to navigate. Further, whether U.S. counter-UxV systems are manned or unmanned, they may need to operate without guaranteed communications. On the other hand, adversaries would find it difficult to fly UAVs over U.S. soil or attack a U.S. port with a USV or UUV. In this situation, adversaries would require a high degree of autonomy in their systems since the U.S. could jam their communications, detect or spoof their systems, create obstacles, or even mount kinetic attacks. In contested battlespaces—along the forward line of ground troops, within an occupied city, or around a carrier battle group in international waters—operating UxVs would be moderately challenging for an adversary and defeating them, moderately challenging for the U.S.

Based on several IDA projects sponsored by the Office of the Under Secretary of Defense for Research and Engineering. For more information, contact Eric Adelizzi (eadelizz@ida.org) or Geoff Koretsky (gkoretsk@ida.org).