World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:05, 2023

Dual-use UAVs in Armed Conflicts: Opportunities and Risks for Cyber and Electronic Warfare

Authors : Piret Pernik

Abstract : Based on strategic, operational, and technical analysis of the ongoing armed conflict in Ukraine, this paper will examine the opportunities and risks of using small commercial drones (dual-use unmanned aerial vehicles, UAV) for military purposes. The paper discusses the opportunities and risks in the information domain, encompassing both cyber and electromagnetic interference and attacks. The paper will draw conclusions on a possible strategic impact to the battlefield outcomes in the modern armed conflicts by the widespread use of dual-use UAVs. This article will contribute to filling the gap in the literature by examining based on empirical data cyberattacks and electromagnetic interference. Today, more than one hundred states and non-state actors possess UAVs ranging from low cost commodity models, widely are dual-use, available and affordable to anyone, to high-cost combat UAVs (UCAV) with lethal kinetic strike capabilities, which can be enhanced with Artificial Intelligence (AI) and Machine Learning (ML). Dual-use UAVs have been used by various actors for intelligence, reconnaissance, surveillance, situational awareness, geolocation, and kinetic targeting. Thus they function as force multipliers enabling kinetic and electronic warfare attacks and provide comparative and asymmetric operational and tactical advances. Some go as far as argue that automated (or semi-automated) systems can change the character of warfare, while others observe that the use of small drones has not changed the balance of power or battlefield outcomes. UAVs give considerable opportunities for commanders, for example, because they can be operated without GPS navigation, makes them less vulnerable and dependent on satellite communications. They can and have been used to conduct cyberattacks, electromagnetic interference, and kinetic attacks. However, they are highly vulnerable to those attacks themselves. So far, strategic studies, literature, and expert commentary have overlooked cybersecurity and electronic interference dimension of the use of dual use UAVs. The studies that link technical analysis of opportunities and risks with strategic battlefield outcomes is missing. It is expected that dual use commercial UAV proliferation in armed and hybrid conflicts will continue and accelerate in the future. Therefore, it is important to understand specific opportunities and risks related to the crowdsourced use of dual-use UAVs, which can have kinetic effects. Technical countermeasures to protect UAVs differ depending on a type of UAV (small, midsize, large, stealth combat), and this paper will offer a unique analysis of small UAVs both from the view of opportunities and risks for commanders and other actors in armed conflict.

Keywords : dual-use technology, cyber attacks, electromagnetic warfare, case studies of cyberattacks in armed conflicts
Conference Title : ICCWS 2023 : International Conference on Cyber Warfare and Security
Conference Location : Barcelona, Spain
Conference Dates : May 22-23, 2023