United States Coast Guard Academy

Department of Electrical Engineering

Small UAVs: A Threat to Economic Security

Impacts Paper

Ryan Von Brock, 1/c Cadet

Capstone Research

LCDR Jason Veara

15 April 2022

**Small UAVs: A Threat to Economic Security**

Recent years have brought about vast strides in unmanned aerial vehicle (UAV) technologies. Specifically, the cost of small UAVs has significantly decreased all while flight longevity, control capabilities, and availability have increased. For this paper, a “small” UAV is considered to have a footprint of no greater than two feet squared. The effects of these advancements have been appreciated by nearly every domain in which UAVs operate. Cinematography, disaster response, search and rescue, and even environmental management are only a handful of the many applications [1]. Nearly any person can monitor, search, or deliver cargo to previously unreachable areas. Unfortunately, not every application of small UAVs is good. These advancements have been equally advantageous for terrorism and other malicious uses. The decreased cost and increased availability of small UAVs have created a new threat vector with potentially devastating consequences [1]. Beyond the impacts to national security, the focus of this paper is the economic impact of low-cost, small UAVs as a force multiplier; specifically, when UAVs are used for malicious purposes.

The Predator drone is often the first to come to mind when thinking of UAVs and global affairs. It has seen great success in expanding the capabilities of unmanned missions while subsequently causing controversy. In opposition to what is often thought, though, is that these drones are not expendable. A single MQ-1 Predator—the smaller and cheaper model—is $4.5 million [2]. The sensors onboard cost nearly as much, if not more, than the airframe. While it remains true that no operator life is at risk, the financial investment had precluded them from being disposable assets [2]. The availability of small UAVs is changing the thought process warfare: an ELEV-8 drone, with a suggested retail price of $599, can carry a 2-pound payload and maintain flight for 15 minutes [3]. The missiles capable of destroying UAVs cost approximately $100,000: “it doesn’t take long to win a war when one is trading a $2,000-$20,000 UAV for a $100,000 missile” [2]. Since Major Abatti’s analysis was written in 2005, the cost of small UAVs has only continued to decrease. Those like the ELEV-8 are commercially available around the globe, and this has potential to exacerbate the economic disparity of defending against them.

The potential swarming—cooperative or coordinated flight between several vehicles—of UAVs depends on three factors: deploying the number of drones, making them autonomous to some extent, and coordinating them [4]. While an attack utilizing a swarm of small UAVs has not yet been seen, “this challenge is likely to meet solutions in a near future.” [4] Despite its inevitability, this method of attack threatens existing defense systems. Conventional air defense systems, which might involve shooting down targets, launching remote missiles, or even using experimental laser or microwave beams can become ineffective against large numbers of targets [4]. Due to their low cost, small UAVs can be sacrificed with the intent to overwhelm defense systems until other UAVs may circumvent them. Other methods of defending against drones include GPS spoofing or communication jamming [4]. However, as the research of this capstone group has shown, computer vision guided flight is achievable for small UAVs. Several alternative navigation methods exist and disrupting them all is not always feasible [4]. Thus, the technological advancements of small UAV research has necessitated a subsequent development of new defense systems: this must “has to become a component of any full-fledged military strategy [4].

The economic threat small UAVs pose to global security carries over to the safety of Coast Guard units. Major Coast Guard cutters, for example, are a potential target of bad actors acting against the United States. They are equipped with armament for their defense, sometimes including aerial defense like the Phalanx CIWS. Like the aforementioned defense systems, though, this is not adequate to defend against large numbers of UAVs. The Coast Guard must undertake additional research and development to mitigate this threat; however, budget constraints only increase this difficultly. When discussing the Coast Guard’s use of UAVs in March 2021, USCG Commandant ADM Schultz said “We look at commercial-off-the-shelf; following, you know, our other fellow services and seeing what they're doing. We have just got a finite amount of R&D (research and development) dollars… We just don't have a lot of that budgetary maneuver space to take high risks there” [5].

The focus of this capstone project, simply put, has been to design a low cost, open architecture, and autonomous quadcopter capable of autonomous flight. Specifically, one capable of computer vision guided flight. Over the course of a year, the group has designed a quadcopter capable of autonomously identifying a marker and landing on it. The landing is guided by an onboard camera and no operator input is needed. The cost of this prototype has remained below $1,000, and it includes all necessary hardware to communicate with other drones. While not intended, this prototype is capable of being used for malicious purposes. It is already capable of remotely delivering a payload, and the autonomous aspect of the computer vision enabled landing would increase the difficulty of leading the drone off target. The mesh communication network would lend to communicating with nearby drones, and the cost of less than $1,000 makes the platform easily obtainable. Moving forward, the security of the group’s drone must become a higher priority. Utilizing encryption for over-the-air communications would prohibit the hijacking of the platform and would serve as a first step for ensuring an ethical product.

**Source Review**

The first source is a broad overview of drone systems, published in September 2020. It begins with a summary of different unmanned aerial vehicles and establishes a sense of urgency by quantifying the vast number of private UAVs. This source provides a detailed list of UAV uses, both good and bad. It separates them into several domains, including criminal, terrorist, civilian, and military uses. Further, it details many common communication systems utilized by small UAVs their vulnerabilities. Finally, the article identifies the rise of small UAV centered threats and details many scenarios in which they are used for malicious purposes [1].

The second source is an unclassified report written by an Air Force Officer at the Air War College in 2005. It provides an in-depth analysis of Air Force strategies involving large UAVs and identifies small UAVs as a necessity for future warfare. Throughout the report, the author provides key details including the acquisition cost of large assets, such as the MQ-1 Predator, and different anti-UAV strategies. The author’s analysis of potential cost disparities between small UAVs and remote guided missiles provides a significant economic threat caused by small UAVs [2].

The third article focuses on the increased availability of small UAVs. It identifies many security and privacy concerns posed by the aircraft but, most significantly, includes a detailed analysis of off-the-shelf drones. This table includes retail costs, flight times, payload capabilities, as well as other pertinent information [3].

The fourth source focuses on the consequence of small UAV swarms. The paper compares drone swarms to those of locus. It outlines the difficulty of coordinating large swarms but acknowledges their inevitability in warfare based on the rate of UAV technological advancement. This source also provides a thorough analysis and explanation of UAV countermeasures and identifies several shortcomings of current technology [4].

The final source is a defense magazine article from the National Defense Industrial Association. It provides an overview of Coast Guard Unmanned Systems. Most relevant to this paper, the article contains quotes from ADM Schultz regarding the Coast Guard’s budgetary restrictions and reliance on off-the-shelf products [5].

**References**

[1] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations,” vol. 11, p. 100218, 2020, doi: 10.1016/j.iot.2020.100218. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/

[2] J. M. Abatti, “Small Power: The Role of Micro and Small UAVs in the Future,” Center for Strategy and Technology, Air War College, Air University, 2005 [Online]. Available: https://apps.dtic.mil/sti/citations/ADA463472

[3] Z. Liu, Z. Li, B. Liu, X. Fu, I. Raptis, and K. Ren, “Rise of Mini-Drones: Applications and Issues,” presented at the Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing, Hangzhou, China, 2015, pp. 7–12, doi: 10.1145/2757302.2757303 [Online]. Available: https://doi.org/10.1145/2757302.2757303

[4] M. J. Guitton, “Fighting the Locusts: Implementing Military Countermeasures Against Drones and Drone Swarms,” vol. 4, p. 26+, 2021 [Online]. Available: https://link.gale.com/apps/doc/A648260737/AONE?u=23266&sid=googleScholar&xid=6a01fed0

[5] J. Harper, “New Coast Guard Team to Flesh Out Unmanned Systems Requirements,” National Defense Magazine, NDIA’s Business & Technology Magazine, 2021 [Online]. https://www.nationaldefensemagazine.org/articles/2021/3/11/just-in-new-coast-guard-team-to-flesh-out-unmanned-systems-requirements