Assessing the Threat: Autonomous Commercial Drones and its Potential for Mass Civilian Casualty Attacks

Conference Paper · April 2024

DOI: 10.13140/RG.2.2.14415.50088

1 author:

Vince Bernard Austria
STI College
7 PUBLICATIONS **1** CITATION

SEE PROFILE

8 - Page Research Manuscript
Used for Journal Publication

Paper Number:____

Assessing the Threat: Autonomous Commercial Drones and its Potential for Mass Civilian Casualty Attacks

Vince Bernard B. Austria[1]
First City Providential College

[1]vincebernard.austria@fcpc.com.ph

Abstract. The integration of commercial drones into contemporary warfare presents a grave threat of mass civilian attacks, These drones, constructed from off-the-shelf and 3D printed components, offer threat actors a readily available platform for malicious and grave intent. The incorporation of open-source UAV navigation software and AI systems enhances their autonomy, enabling them to operate independently and evade traditional countermeasures such as jamming. Moreover, the versatility of drone designs, ranging from fixed-wing to quadcopters, provides a multitude of attack vectors, including aerial bombings, mass, and targeted assassinations. Urgent action is needed to address these emerging threats, emphasizing the need for robust regulatory frameworks and technological solutions to safeguard against potential attacks. This paper underscores the critical importance of proactive measures to mitigate the risk of mass civilian casualty attacks perpetrated by commercial drones in modern warfare.

Keywords: Self-exploding drone, Improvised explosive device (IED), FPV drone, Asymmetric warfare, Autonomous navigation

1. Introduction

The ongoing conflict in Ukraine pushed commercial drones to the forefront of military operations. Unlike their larger, more sophisticated counterparts used in counterterrorism and peer-to-peer efforts, these smaller, commercially available drones play a distinct role. The war in Ukraine revealed the effectiveness of these drones. Primarily focused on antipersonnel role thousands of drones [1], loitering grenades, and suicide drones are proving their effectiveness without air superiority [2]. These lightweight, agile weapon systems operate effectively in contested environments, changing battlefield dynamics from lower airspace.

Security concerns surrounding drones extend beyond cyber-attacks. The hardware and software vulnerability and complexity of commercial drones raise possible security and privacy issues. Many existing drones lack security protocols such as intrusion detection systems (IDS) and Signal integrity systems. Additionally, the war in Ukraine has highlighted the importance of secure deployment. Ukraine's ability to acquire and crowdsource commercial drone technology, tactically modify drones based on real-time feedback, and alter tactics to defeat anti-drone systems has proved crucial to its war effort [3]. As commercial drones become more readily available, policymakers contend with regulatory frameworks to mitigate risks associated with their misuse.

The rise of commercial drones, coupled with AI advancements, demands an approach that fosters innovation while defending against unintended and malicious use. Commercial drones, far from being mere security nuisances, hold immense potential and pose challenges to local and global security.

2. Problem Statement

The increasing use of inexpensive commercial drones in warfare raises concerns. Particularly, the issue lies on the feasibility of mass casualty attacks made possible by these agile and accessible unmanned aerial vehicles. The potential consequences are devastating, as these drones can carry out targeted strikes with precision and speed. The rise of adoption of the following paved the way to the current threat of self-exploding drones:

Integration of Image Recognition and Autonomy:

- The fusion of image recognition technology with drone autonomy significantly amplifies their effectiveness. These drones can identify and track targets based on visual cues, making them formidable tools for both surveillance and offensive operations. [4]
- By leveraging real-time image analysis, drones can autonomously identify specific individuals, vehicles, or critical infrastructure. This integration enhances their chance of success in executing lethal attacks.
- The ability to recognize patterns, differentiate between friend and foe, without remote intervention adapt to changing scenarios allowed these drones to operate independently, even in complex and signal degraded environments.

Proliferation of Cheap FPV Drones and Improvised Explosives:

- First-person view (FPV) drones, initially designed for hobbyists, have been repurposed for combat. Their low cost and agility make them ideal platforms for carrying improvised explosives. [5]
- Despite their small size, FPV drones can reach speeds of up to 140 kilometers per hour and deliver payloads such as rocket-propelled grenades (RPGs) and improvised explosive devices (IED). [6]
- Particularly Ukraine, has become a testing ground for these modified drones. Adapted from consumer models, they challenge traditional warfare paradigms. The proliferation of such cheap and lethal drones demands urgent attention from the global security community.

3. Objectives

3.1 Assessing Potential Threats:

Investigating the feasibility of successful mass casualty drone attacks, these threats comes from various sources:

- **Terrorism**: Extremist groups exploit commercial drone availability and ease of conversion and use for targeted attacks, bypassing traditional security surveillance measures. The agility and accessibility of drones make them potent tools for asymmetric warfare.
- **Opposing Nations**: State-sponsored actors deploy drones for reconnaissance, surveillance, and offensive operations specially against civilian population this brings tactical and morale consequences as the ability to strike with precision using inexpensive drones challenges existing defense systems [7].
- **Civilian Crime**: Misuse by individuals for criminal purposes such as targeted murder or conducting unauthorized surveillance poses a significant risk to public safety.

3.2 Analyzing Material Availability:

Understanding the ease of acquiring drone components sheds light on the threat landscape:

- **Bill of Materials** (BOM): This includes components such as the FPV drone chassis, motors, ESCs, batteries, and Raspberry Pi Zero for image recognition are readily accessible. Online platforms offer these components without stringent checks, enabling the assembly of modified drones. [8]
- **Explosive Fillers**: Explosive agent from fireworks, nails, and other materials for shrapnel creation are available at hardware stores and can be combine with FPV drones to create self-exploding drone. The combination of these readily available components poses grave risk.

3.3 Proposing Enhanced Security Measures:

Traditional jamming techniques are ineffective against autonomous self-exploding drones. As such strategies must shift to physical countermeasures and deterrence:

- **Nets and Obstacles**: Deploying physical barriers can disrupt drone operations. Nets can capture drones mid-flight, while obstacles limit their maneuverability.
- **Anti-Drone Systems**: Developing and deploying specialized anti-drone technologies is crucial. These systems can detect, track, and neutralize rogue drones. [9]

Proactive measures are essential to balance technological advancements with responsible safeguards. By addressing threats, material availability, and security strategies, we can mitigate risks associated with drone misuse and enhance global safety.

4. Methodology

4.1 Data Collection:

Widespread availability of FPV drone components from well known e-commerce websites, coupled with advancements in autonomous software, opens up opportunity for better integration in manufacturing and deployment of such drones. The need for enhanced vigilance and implementation of better security protocols to effectively address this dynamic and potentially hazardous dangers of commercial drone technology in warfare.

1. Surveillance of drone materials market: Browsing top three e-commerce website in the Philippines namely Amazon, Lazada and Shopee reveals that there's wide availability of FPV drone parts and accessories including compute units such as Raspberry Pi zero/Orange Pi Zero 3. Allows for easier assembly and nearly a one stop shop solution in manufacturing such drones. [10]

2. Autonomous software framework: This includes integration of internal navigation suites such as lateral and vertical sensor data processing, visual information from colored camera and active comparison through pretrained imagery, handling of computational bulk of human and crowd recognition and finally hardware communication of payload trigger mechanism. Achievement of such software is relatively doable in shorter timescale through architectural specialization and modification of current autopilot software such as Ardupilot and PX4.

3. Drone related security lapses:

Jordan Drone Attack (January 2024) Three US Army soldiers were killed, and more than 30 service members were injured in a drone attack overnight on a small US outpost in Jordan near the border with Syria. This marked the first time US troops were killed by enemy fire in the Middle East since the beginning of the Gaza war. The drone was fired by Iran-backed militants and appeared to come from Syria. [11]

Ukraine Drone Attacks (March 2024) Amid the ongoing Russo-Ukrainian War, Ukraine launched a new massive wave of drone attacks. These attacks occurred as Russians cast ballots on the final day of a presidential vote set to extend President Vladimir Putin's rule for another six years. Drones have become a critical tool in Ukraine's military strategy, demonstrating their effectiveness in warfare. [12]

The convergence of image recognition, autonomy, and the availability of affordable FPV drones creates dangerous and volatile landscape.

4.2 Assessing Drone Capabilities:

Assessment of drone flight patterns through the simulation of given scenario. Assessment of this flight trajectories, insights are gained into potential attack routes and vulnerabilities.

4.2.1 Simulating flight scenario:

Simulating flight scenarios allows for the visualization of potential attack routes, taking into account factors such as altitude, speed, and maneuverability. By analyzing how drones navigate through various environments, attackers can identify optimal paths to reach their intended targets.

In this simulated scenario the aggressor opt to target a large social gathering on the enclosed court. This posses challenges such as improbability of drone dropped munition attack and various obstacles such as roof purlins and support. As such, the aggressor deploys a self-exploding drone (figure 1) that incorporates fixed explosive filler rather than projectile or gravity drop munitions. This way, the attack can be precisely positioned at the optimal height to maximize the effective kill radius.

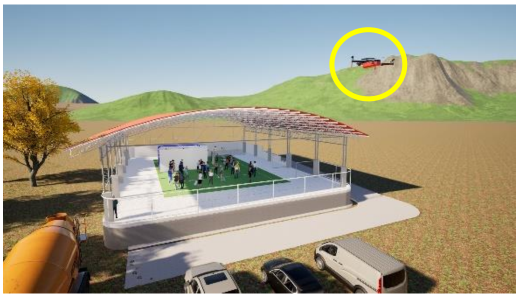


Fig 1: Social gathering on covered court

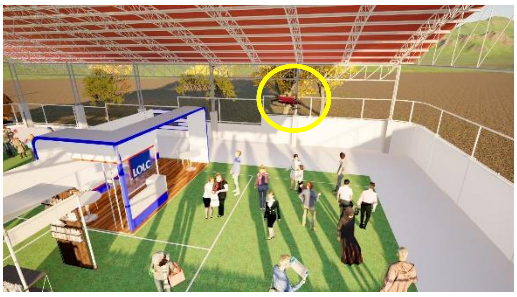


Fig 2: Self-exploding drone sneaking above group of people (encircled)

The simulated attack would proceed as follows, the attacking drone would be delivered by either the deployment drone (which is a fixed-wing UAV that carries multiple self-exploding drones that are controlled by the aggressor or the built-in daylight image-matching system and Inertial Navigation System) or guided manually by the operator up to the vicinity of the target area. Then, the attacking drone would switch to autonomous mode that will provide last-hop delivery. The guidance software aboard the single board computer decides on the optimal altitude and path to clear covered court obstacles and finally triggers the explosive filler mechanism when the image recognition software detects the specified threshold of group of individuals is reached in close proximity.

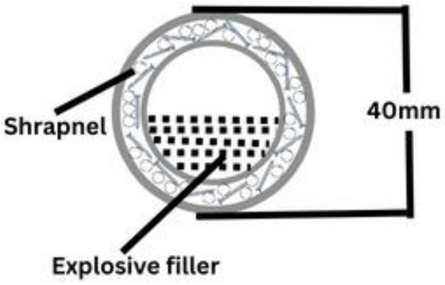
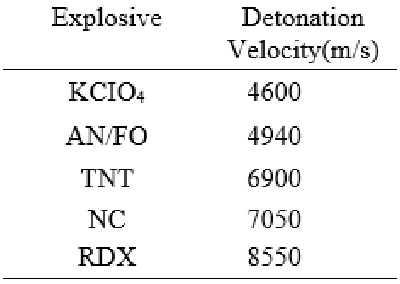


Fig 3: Basic pipe based explosive design



Explosive	Detonation Velocity(m/s)
$KClO_4$	4600
AN/FO	4940
TNT	6900
NC	7050
RDX	8550

Fig 4: Detonation velocity of various explosive fillers

Furthermore, attacks might opt to design a basic pipe explosion device as not only on its simple construction but also due to the easy acquisition of components. In which the passive components such as the metal steel pipe (which acts as chassis) and shrapnel (that delivers the most bodily harm) are available in hardware stores. While explosive filler can be bought on firecracker dealers for extraction with differing detonation velocity. (figure 4) Additionally, the electronic triggering mechanism can be designed in such a way to produce high temperature when detonation signal is received from the single board computer. This can be made either by opening a short to ground with bare wire in series or by designing a high voltage generator circuit. Which would provide the high temperature needed for the explosive filler to ignite.[13]

5. Results

5.1 Feasibility Assessment

Due to the widespread availability of the materials to build and deploy autonomous self exploding drones, the risk of carrying out such an attack against a civilian population is greater than ever. This also includes various sources of information that allow an individual or a group of people to pool their resources and carry out such heinous attacks. Information that is presented in this paper presents the simple yet lethal effectiveness of such weapons from existing. Challenges such as integration of traditional autopilot software to image recognition systems may exist now but this doesn't stop the threat from materializing as any software developer can fork these open-source projects and modify and integrate them to suit the self-exploding drone mission profile. In physical feasibility, the open nature of covered courts and other places of gathering venues posed a very significant threat as this opens up multiple areas of ingress and advantageous points of detonations. Whilst, the open and free nature of satellite-based imagery such as Google Earth and Maps provides quality training data on visual-based autonomous navigation of both deployment drones and self-exploding drones.[14]

5.2 Material Availability

The hobby nature of FPV drones allows anyone to acquire such components to build self-exploding drones. While the rise of 3D printing paved the way for the untraceable fabrication of drone chassis. The tradition of firecracker use in the Philippines enables anyone to acquire low explosive fillers that are sensitive and powerful enough to cause serious bodily harm, particularly to the head as self-exploding drones are meant to detonate in height proximity rather than direct contact. Different items, such as nails, bearings, plastic pellets, glass [15], and others, can be inserted between the explosive filler and pressure housing. These objects can serve as shrapnel, causing localized damage upon impact to the intended group of individuals.

6. Discussion

The emergence of inexpensive commercial drones has sizeable impact on conventional warfare, particularly evident in the ongoing conflict in Ukraine. These drones, ranging from scouts to loitering grenades and suicide drones, challenge conventional military strategies by operating effectively in contested environments. The asymmetrical nature of their impact underscores the need for a reevaluation of traditional warfare paradigms [16]. Security concerns surrounding commercial drones extend beyond their physical capabilities. The vulnerabilities inherent in their hardware and software, coupled with the accessibility of these systems, raise significant security and privacy issues. The ability of actors in the conflict, such as Ukraine, to crowdsource and tactically modify drones based on real-time feedback highlights the evolving nature of warfare in the digital age [17]. The convergence of commercial drones with advancements in artificial intelligence presents both opportunities and challenges for global security. While these drones offer tactical benefits, their potential for misuse in the form of mass casualty attacks is a growing concern. As such, there is a pressing need for regulatory frameworks to mitigate risks associated with their proliferation. [18]

5.1 Proposed Security Changes

Enhancing drone security requires a multifaceted approach, combining physical barriers and technological innovations. This section explores proposed changes to mitigate risks associated with self-exploding drones. Addressing both practical and technical aspects, the aim is to promote safe and responsible drone use while preventing and deterring attacks. A comprehensive approach to enhancing drone security, considering both physical barriers and technological advancements

1. **Physical Barriers**: The deployment of physical barriers in open spaces is essential to deter autonomous self-exploding drones. This includes the designation of obstacle zones in architectural

plans around critical infrastructure, public events, and sensitive areas. These zones can be marked by physical barriers such as fences, netting, or natural features. These Obstacles disrupt drone flight paths, preventing unauthorized access and reducing the risk of self-exploding drones reaching their targets. Additionally, the deployment of Anti-Drone Nets in strategic locations allows them to capture drones mid-flight, rendering them ineffective.

2. **Technological Countermeasures**: Advancements in drone detection and neutralization technologies remain crucial. Such as the utilization of Anti-Drone Systems this specialized anti-drone systems capable of detecting rogue drones. These systems can use radar, lidar, and optical sensors to identify unauthorized aerial vehicles. Neutralization of self-exploding drones can include automated radar-guided low caliber guns such as shotgun rounds are proven effective against drones particularly buck and bird shot variants [19]

CONCLUSION

The rise of commercially available drones in conventional warfare, particularly evident in conflicts like Ukraine, poses significant security challenges. These drones, ranging from loitering grenades to suicide drones, have proven effective in contested environments, changing the dynamics of warfare. However, the proliferation of these drones also raises concerns about mass casualty civilian attacks using self-exploding drones. Integration of image recognition with drone autonomy has enhanced their effectiveness, allowing them to autonomously identify and track targets. Additionally, the accessibility of inexpensive FPV drones and improvised explosives makes it easier for malicious actors to acquire the necessary components for such attacks.

To address these threats, a multifaceted approach to drone security is essential. This includes implementing physical barriers and technological countermeasures. Physical barriers, such as obstacle zones and anti-drone nets, can disrupt drone flight paths and prevent unauthorized access to sensitive areas. Meanwhile, technological innovations, like specialized anti-drone systems equipped with radar and optical sensors, are crucial for detecting and neutralizing rogue drones. By balancing innovation with responsible safeguards, we can mitigate the risks associated with drone misuse and enhance civilian safety.

References

[1] Skove S. UK, Latvia launch effort to send thousands of FPV drones to Ukraine [Internet]. Defense One. 2024. Available from: https://www.defenseone.com/threats/2024/02/uk-latvia-launch-effort-send-thousands-fpv-drones-ukraine/394238/

[2] Drones have boots: Learning from Russia’s war in Ukraine. https://www.tandfonline.com/doi/full/10.1080/13523260.2023.2262792.

[3] Kunertova D. The war in Ukraine shows the game-changing effect of drones depends on the game. Bulletin of the Atomic Scientists [Journal]. 2023 Mar 4;79(2):95–102. Available from: https://doi.org/10.1080/00963402.2023.2178180

[4] Pradelle O, Chaine R, Wendland D, Digne J. Computer vision and image understanding. Social Science Research Network [Internet]. 2022 Jan 1; Available from: https://doi.org/10.2139/ssrn.4313787

[5] Burgess A. Why Ukraine’s kamikaze racing drones are causing a buzz on and off the battlefield. ABC News [Internet]. 2023 Mar 31; Available from: https://www.abc.net.au/news/2023-04-01/fpv-racing-drone-kamikaze-attacks-ukraine-russia-war/102155702

[6] Horton A, Korolchuk S. In Ukraine, explosive DIY drones give an intimate view of killing. Washington Post [Internet]. 2023 Oct 15; Available from: https://www.washingtonpost.com/world/2023/10/04/fpv-drone-ukraine-russia/

[7] Yaacoub JP, Noura H, Salman O, Chehab A. Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things. 2020;11:100218. doi:10.1016/j.iot.2020.100218

[8] Defensebridge. Where to Buy Drone Parts: A Comprehensive List of Online Stores. Defensebridge [Internet]. 2023 May 19; Available from: https://defensebridge.com/article/where-to-buy-drone-parts-a-comprehensive-list-of-online-stores.html

[9] Cybersecurity and drones: How to address the security threats [Internet]. Tripwire. Available from: https://www.tripwire.com/state-of-security/cybersecurity-and-drones-how-to-address-the-security-threats

[10] Amazon.com: 6inch RC Drone 250mm Omnibus Quadcopter Drone [Internet]. Available from: https://amazon.com/dp/B0BRW6WMPX

[11] U.S. Department of Defense. 3 U.S. service members killed, others injured in Jordan following dron [Internet]. U.S. Department of Defense. Available from: https://www.defense.gov/News/News-Stories/Article/Article/3659809/3-us-service-members-killed-others-injured-in-jordan-following-drone-attack/

[12] KATIE MARIE DAVIES Associated Press, ABC News. Russia says Ukraine launched far-ranging drone attacks on final day of Russia's presidential vote. ABC News [Internet]. 2024 Mar 18; Available from: https://abcnews.go.com/International/wireStory/ukraine-launches-ranging-drone-attacks-final-day-russias-108197056

[13] Mehta, Neha, et al. "Primary explosives." Zeitschrift für anorganische und allgemeine Chemie 640.7 (2014): 1309-1313

[14] Supervised classification [Internet]. Google for Developers. Available from: https://developers.google.com/earth-engine/guides/classification

[15] Weapons Primarily Injuring by Non-Detectable Fragments [Internet]. International Humanitarian Law Databases. [cited 2024 Mar 20]. Available from: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule79#Fn_23247C9_00001

[16] Kunertova D. The war in Ukraine shows the game-changing effect of drones depends on the game. Bulletin of the Atomic Scientists [Internet]. 2023 Mar 4;79(2):95–102. Available from: https://doi.org/10.1080/00963402.2023.2178180

[17] Omolara AE, Alawida M, Abiodun OI. Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey. Neural Computing and Applications [Journal]. 2023 Aug 31;35(31):23063–101. Available from: https://doi.org/10.1007/s00521-023-08857-7

[18] Al-Nabhan N. Security, safety and privacy issues of unmanned aerial vehicle systems. In: Communications in computer and information science [Internet]. 2020. p. 28–39. Available from: https://doi.org/10.1007/978-981-15-7530-3_3

[19]Pemčák, I., Skala, J., & Bača, J. (2022). SUITABILITY OF USING DIFFERENT TYPES OF SHOTGUN SHELLS IN DEFENCE AGAINST LOW-SLOW-SMALL UAV. Science & Military Journal, 17(2).

8 - Page Research Manuscript
Used for Journal Publication

Authors’ background

Your Name	Title*	Research Field	Personal website
Vince Bernard B. Austria		College of Computer Studies	https://github.com/elsaversailles

*This form helps us to understand your paper better; the form itself will not be published. Please delete it in the final paper.

*Title can be chosen from master student, PhD candidate, assistant professor, lecturer, senior lecture, associate professor, full professor