VARSTVOSLOVJE
Journal of Criminal Justice and Security
year 23
no. 3
pp. 336–349

The Weaponisation of Drones – A Threat from Above Used for Terrorist Purposes

Ice Ilijevski, Zlate Dimovski, Kire Babanoski

Purpose:

The subject of this paper is to determine the threat of drones (unmanned aerial vehicles – UAVs), which are evolving rapidly and becoming more efficient, powerful, and easily weaponised, with regard to their use by terrorist organisations. Because of the precision, efficiency, and economy of drones, in the last decade terrorist organisations have used these to carry out attacks all over the world. The paper discusses the prevention and the countermeasures undertaken by national authorities, as well as the development of defensive tactics against drone strikes. The paper notes that the threat posed drones is even greater than many imagine, as they can be used to attack critical infrastructure.

Design/Methods/Approach:

The tactical ways in which terrorist organisations have made malicious use of drones are considered and described in the paper. In order to better understand the core of this problem, the methods and techniques of attack, the characteristics of the drones and the measures taken by the security and intelligence services in the fight against this threat are reviewed and assessed. All these questions were also addressed by theorists researching this field in semi-structured interviews conducted online.

Findings:

Because of the rapid development of the technology and progress in the area of drone production, as well as their low price and the availability, drones can be easily transformed into improvised explosive devices that are attractive to many terrorist organisations and individuals, producing a new type of asymmetrical threat. The threat coming from air that is posed by drones is very sophisticated and complex, and deserves more attention from national security authorities. Moreover, the development and introduction of protective and preventive approaches and mechanisms on an international level, and full implementation on a national level, is essential to prevent planned attacks with drones.

Originality/Value:

This topic is rarely discussed in security research and studies. The paper offers a solid overview of the problems and threats that drones are already causing to law enforcement agencies, and the challenges for national authorities with regard to preventing them.

Keywords: drone, unmanned aerial vehicle, terrorism, terrorist attack, threat.

UDC: 343.3+629.014.9

Brezpilotni letalniki kot orožje – grožnja od zgoraj, uporabljena v teroristične namene

Ice Ilijevski, Zlate Dimovski, Kire Babanoski

Namen

Predmet tega prispevka je ugotavljanje nevarnosti brezpilotnih letalnikov (dronov), ki se hitro razvijajo in postajajo učinkovitejši, zmogljivejši in jih je enostavno oborožiti, glede na njihovo uporabo terorističnih organizacij. Zaradi natančnosti, učinkovitosti in ekonomičnosti brezpilotnih letalnikov so jih teroristične organizacije v zadnjem desetletju uporabljale za izvajanje napadov po vsem svetu. Prispevek obravnava preprečevanje in protiukrepe, ki jih izvajajo nacionalni organi ter razvoj obrambnih taktik proti napadom z brezpilotnimi letalniki. Avtorji ugotavljajo, da je grožnja napadov z brezpilotnimi letalniki celo večja, kot si mnogi predstavljajo, saj jih je mogoče uporabiti za napad na kritično infrastrukturo.

Metode

V prispevku so obravnavani in opisani taktični načini zlonamerne uporabe brezpilotnih letalnikov, ki so jo uporabljale teroristične organizacije. Za boljše razumevanje bistva tega problema so predstavljene in ocenjene metode in tehnike napada, značilnosti brezpilotnih letalnikov ter ukrepi varnostnih in obveščevalnih služb v boju proti tej grožnji. Vsa ta vprašanja so avtorji naslovili tudi v polstrukturiranih intervjujih, opravljenih preko spleta.

Ugotovitve

Zaradi hitrega razvoja tehnologije in napredka na področju proizvodnje dronov ter njihove nizke cene in razpoložljivosti se ti zlahka spremenijo v improvizirane eksplozivne naprave, ki so privlačne za številne teroristične organizacije in posameznike, pri čemer nastane nov tip asimetrične grožnje. Grožnja iz zraka, ki jo predstavljajo brezpilotni letalniki, je zelo prefinjena in kompleksna ter si zasluži več pozornosti nacionalnih varnostnih organov. Poleg tega je razvoj in uvedba zaščitnih ter preventivnih pristopov in mehanizmov na mednarodni ravni ter njihova popolna implementacija na nacionalni ravni bistvenega pomena za preprečevanje načrtovanih napadov z brezpilotnimi letalniki.

Izvirnost/pomembnost prispevka

O tej temi se v raziskavah in študijah s področja varnosti redko razpravlja. Prispevek ponuja dober pregled težav in groženj, ki jih brezpilotni letalniki že povzročajo organom pregona, ter izzivov za nacionalne organe pri njihovem preprečevanju.

Ključne besede: brezpilotni letalniki, droni, terorizem, teroristični napad, grožnja

UDK: 343.3+629.014.9

1 INTRODUCTION

In recent years there has been a significant increase in the use of unmanned aerial vehicles (UAVs, or drones) for various purposes. Drones give users the opportunity to obtain a bird's eye view of an area, and due to the fast activation method they can be used anywhere and at any time. Drones can be used for personal (i.e. recreational) and commercial goals, and can also be used by law enforcement agencies to support the implementation of the security tasks, such as monitoring state borders, carrying out reconnaissance, monitoring demonstrations, examining areas after natural disasters and catastrophes, and so on, and recently the international community has seen the use of drones in anti-terrorist operations.

However, we have also seen cases of drone misuse by criminal groups and terrorist organisations, because they are easy to control and can be used to carry out various attacks, with some of these briefly presented in the paper. One use of drones is as a new kind of improvised explosive device, which is attractive to many terrorist organisations and individuals due to the low price and wide availability of this technology. As such, the terrorist use of drones represents a new type of asymmetrical threat, and so it is essential to develop and introduction protective and preventive mechanisms to prevent such attacks.

Many countries, including the USA and those of the EU, have issued numerous warnings to drone owners urging all citizens to register the drones they own and apply for a license to use them, i.e. to obtain an official license from a civil aviation authority. This way, national authorities can know more about the current situation with regard to the number, types and owners of drones in their respective countries. If a person does not follow the rules for the use of drones, then they can be fined or even imprisoned.

In October 2014 (»Drone-flying Albanian arrested with guns ahead of Serbia match«, 2015) a drone with a flag was flying over the stadium that was hosting a football match between Serbia and Albania in Belgrade. The responsibility for this provocation was taken by an Albanian extremist. This event shows that a drone can easily be directed to fly over a certain location and to carry an item – in this case a flag, but it could be an explosive or even worse, some kind of weapon of mass destruction (chemical, biological or nuclear).

In December 2018 (»Gatwick Airport: Drones ground flights«, 2018) Gatwick Airport near London had to be temporarily closed due to reports that drones were flying near the runway. As a result, some 760 flights were cancelled, and more than 110,000 passengers were prevented from travelling. The Gatwick incident, which closed a key part of critical infrastructure for almost 48 hours, is another example of what can happen if drones are misused, again demonstrating the ability of drones to circumvent traditional security measures and at the same time the inability of security forces to counter such a threat.

A brief presentation and analysis of tactical and technical ways of using drones and their use by terrorist organisations will follow, with a special focus on their threat to critical infrastructure and national security. The issues raised, in addition to those related to a theoretical discussion of this problem, will then be explored with the views and opinions of experts with regard to the understanding the malicious use of drones and its prevention.

2 DRONE ARCHITECTURE, TACTICS AND TECHNIQUES OF USING DRONES BY TERRORISTS

The International Civil Aviation Organization (ICAO) (2011) defines an »unmanned aircraft« as an aircraft which is intended to operate with no pilot on board, while it defines an »unmanned aircraft system« as an aircraft and its associated elements which are operated with no pilot on board. It also uses the designation »remotely-piloted aircraft system«, which means a set of configurable elements consisting of a remotely-piloted aircraft, its associated remote pilot station(s), the required command and control links and any other system elements that may be required, at any point during flight operation.

This means that, typically, any drone or drone architecture consists of three main elements (Yaacoub et al., 2020): Unmanned Aircraft (UmA), Ground Control Station (GCS), and Communication Data-Link (CDL). These components, along with others, are briefly described as follows:

- Flight Controller: the drone's central processing unit;
- Ground Control Station: this is based on an On-Land Facility (OLF), which provides human operators with the necessary capabilities to control and/or monitor UAVs during their operations from a distance. GCSs differ depending on the size, type, and drone missions involved;
- Data Links: are wireless links used to control the information flow between the drone and the GCS. This depends on the operational range of UAVs and can be categorised based on their distance from the GCS:
    - Visual Line-of-sight (VLOS) Distance: allows control signals to be sent and received via the use of direct radio waves,
    - Beyond Visual Line-of-Sight (BVLOS) Distance: allows drones to be controlled via satellite communications.

According to their flying mechanisms, drones can be classified into three main types:

- Multi-Rotor Drones: these are also known as rotary-wing drones;
- Fixed-Wing Drones: these are more energy efficient than multi-rotor drones;
- Hybrid-Wing Drones: these are fixed/rotary wing drones that have recently entered the market.

The drones can be of different types and can have different characteristics and capabilities. Examples of additional equipment that can be installed include:

- Visual recording equipment;
- Detection equipment (optical-electronic sensors, infrared scanners, radars, etc.);
- Radio frequency equipment;
- Specific sensors for detection of nuclear, biological traces, chemicals, explosive devices, etc.

Drones can be used in many different ways, but these can be roughly divided into considerate or malicious use (Yaacoub et al., 2020). In the last few years, drones have been used in various civilian/commercial multi-purpose use cases, including search and rescue and disaster management (Altawy & Youssef, 2017). The police also use drones for traffic monitoring, tracking escapees, forensic search and rescue, as well as anti-rioting purposes (Straub, 2014). Drones are particularly appealing to the military, especially for intelligence and reconnaissance purposes in the fight against insurgencies and terrorism (Cook, 2007). However, as noted before, drones have also become to criminals and terrorists aiming to launch malicious attacks. Having drones in the wrong hands can lead to serious consequences (Ball, 2017), with Table 1 presenting some of the various ways terrorists can misuse drones.

Table 1: Some of the ways terrorists misude drones (source: Yaacoub et al., 2020)

Drone abuse	Biological, chemical, radiological and nuclear
	Propaganda
	Psychological
	Cyber-Attack
	Armed Use
	Surveillance
	Suicidal Drone

Experts have pointed to a set of advantages that may make UAVs attractive to terrorists (Miasnikov, 2005):

- The possibility to attack targets that are difficult to reach by land (by cars loaded with explosives or suicide bombers);
- The possibility of carrying out a large-scale (area) attack, aimed at inflicting the maximum death rate on a population (particularly through the use of chemical or biological weapons in cities);
- The covertness of attack preparation and flexibility in choice of a UAV launch site;
- The possibility of achieving long-range and acceptable accuracy with relatively inexpensive and increasingly available technology;
- The poor effectiveness of existing air defences against targets such as low-flying UAVs;
- The relative cost effectiveness of UAVs compared with ballistic missiles and manned airplanes;
- The possibility of achieving a strong psychological effect by scaring people and putting pressure on politicians.

Hezbollah and Hamas were early adopters of drone technology, and maintain an armed drone capability. In 2004, Hezbollah flew a military-grade drone, reportedly acquired from Iran, over Israeli airspace. The Lebanese militant group also conducted strikes in Syria in 2014 with an armed drone, and in 2016 with over-the-counter drones armed with small explosives (Axe, 2016).

The Houthi rebels in Yemen have also been actively using drones. In the first half of 2019, they attacked the Jizan and Abha airports in southern Saudi Arabia, as well as Saudi oil pipelines. Their multiple airport attacks have led to significant civilian injuries, and such activities do not show any signs of stopping in the near future (Bergen, 2019).

Boko Haram also uses drones in their attacks, presenting a serious security threat for Nigeria, and in 2018 the organisation attacked five military targets and caused serious damage (Xinhua, 2018).

The Islamic State has joined other terrorist organisations using drones to achieve their goals. The first case was reported in August 2014, near the northeastern Syrian province of Raqqa, where Islamic State militants sent a commercial DJI Phantom FC40 quad copter to spy on a Syrian air base, followed by a ground attack (Warrick, 2017). In addition to using drones for reconnaissance operations, which they used for propaganda purposes, the Islamic State also began using them for terrorist activities.

In 2015, Kurdish fighters in Syria shot down multiple small commercial drones laden with explosives, reportedly belonging to the Islamic State (Braun, 2020), while in September 2016 it bombed the Turkish military forces in the Vukuf region of northern Syria, wounding three Turkish soldiers (Serkan, 2017). In January 2018, a swarm of 13 homemade aerial drones attacked two Russian military bases in Syria (Pledger, 2021).

Most of Islamic State's drone attacks have involved lightweight military ordnance, such as grenades, rocket warheads, and bomblets from cluster bombs, occasionally modified to improve accuracy. Due to drones' limited carrying capacity, these strikes do not yield the same destructive power that mortar or heavier artillery fire could, but they allow for more precision than mortars or makeshift rocket launchers can provide (Wagner, 2019). When Iraqi troops captured drone facilities in Mosul, in 2017, they discovered scores of documents detailing an elaborate procurement system for purchasing the UAVs and parts, as well as extensive procedures for altering and testing the equipment. The records addressed the group's efforts to secure, modify, and enhance the range and performance of its drones. The documents showed Islamic State's efforts to acquire items like GoPro cameras, memory cards, GPS units, digital video recorders, and spare propeller blades. They also illustrated the group's efforts to secure, modify, and enhance the range and performance of its fleet of drones. To protect the transmission of their drone video feeds, members of the group wanted to acquire encrypted video transmitters and receivers. A long-range radio-controlled relay system was also included on a number of the group's 'acquisition' lists (to extend the range of its drones), as were various types of servo motors.

One recent study (Haugstvedt, 2020) concluded that various non-state actors choose targets carefully when using weaponised UAVs. Moreover, they tend not to cause mass casualties or injuries, and choose hard over soft targets. While it is true that some non-state actors, such as the Islamic Stata (also known as ISIS) and the Houthis, may aim to cause mass casualties, they currently do not attempt to do so by using weaponised UAVs. Nearly all incidents of the uses of drones by such groups (98.9% of the total) occurred between August 2016 and March 2020, making non-state actors' offensive use of UAVs a highly recent phenomenon in international conflict and warfare. Moreover, non-state actors' use of weaponised UAVs has been found almost exclusively in the Middle East (98.4% of cases), and mainly in Iraq, Syria, and Saudi Arabia (90.5% of cases). As such, we can say that non-state actors operating in the Middle East have adopted weaponised UAVs for their operations, that ISIS and the Houthis are responsible for the majority of cases, and that our findings are not necessarily transferable to other non-state actors in the region.

3 DRONES AS A THREAT TO CRITICAL INFRASTRUCTURE

The term »critical infrastructure« is not universally defined, but the need to ensure the vital functions of the state determines the significance and criticality of certain elements of a nation's infrastructure. It is thought that the term »critical infrastructure« dates back to the mid-1990s, and is closely related to energy security, telecommunications, energy systems, gas and oil pipelines, the economy, transportation, water supply and so on (Mitrevska et al., 2017). Critical infrastructure involves elements that are fundamental to the normal operations of society, and can be defined as referring to any asset, system or part thereof which is critical for the maintenance of vital societal functions, including the health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a very substantial impact as a result of the failure to maintain those functions (Ani et al., 2019). Critical infrastructure is exposed to many different types of dangers, and the most common are natural disasters, human errors, technical problems and criminal acts, the consequences of which can be huge. The provision of special protection against terrorist attacks is thus especially important with regard to this type of infrastructure, in order to maintain national security.

Such protection is even more necessary because critical infrastructure is very attractive to the criminals, and especially terrorists, for many different reasons (Ackerman, 2007), the main one being the strategic value that it has for society as a whole, especially in highly industrialised developed countries. Negative interventions in the functioning of critical infrastructure, which can then go on to have cascading effects, allow criminal groups to cause large-scale damage with a very small investment, and thus cause a degree of damage that may not be so easy to achieve by other means. For example, non-state entities (terrorist organisations) may attack power generation facilities, gas pipelines, oil pipelines, water systems, computer centres, etc., in order to interrupt the supply of basic resources and information and thus reveal the vulnerability of state institutions. Another possible motivation, related to the two previous ones, would be the desire to gain more publicity than would be possible by focusing on relatively low-profile targets.

The threats related to terrorism against the critical infrastructure have multiple dimensions depending on their nature (physical versus cyber-attacks), their origins (internal versus external attacks), and the context in which they occur (isolated or multiple-purpose) (United Nation Security Council Counter-Terrorism Committee Executive Directorate & United Nations Office of Counter-Terrorism, 2018).

It is important to emphasise that, given all the advantages of using drones set out above, when a terrorist organisation has all the necessary materials it is very difficult to prevent an attack. Indeed, any event held in the open is vulnerable to this type of attack, especially considering that these aircraft can travel long distances to a target. If we add that they have an electric motor that is very quiet and are usually not brightly coloured, then we can see that the possibility of detection is reduced, both visually and audibly, while their size and low flight paths make drones difficult to be detected by radar (Pejanovic et al., 2018).

4 RESULTS OF SEMI-STRUCTURED INTERVIEWS WITH EXPERTS: UNDERSTANDING THE THREAT OF DRONES

Given that this topic has not received a lot of attention from researchers, and thus the literature remains lacking, several experts dealing with the issues of terrorism, extremism, criminal tactics and techniques, security and safety systems were invited to take part in online interviews to examine and review their opinions and views. All interviewees who accepted the invitation are university staff/theorists who have been researching and/or publishing works related to this topic. The interviews were conducted during the months of April and May 2021. The interviews were semi-structured and composed of several questions related to three issues: (i) terrorist organisations' interests and motivations for using drones; (ii) purposes/types of activities in which they are using drones; and (iii) preventative approaches at the national level for stopping use of drones for terrorist purposes.

Firstly, the motivations and reasons why terrorist organisations are interested in using drones were discussed. All of interviewees agreed that drones have a number of critical qualities that make them attractive to such groups, and contribute to the evolving nature of these groups regarding their operational capacity or functionality. The characteristics of drones, their small size, low cost, ease of manoeuvre and maintenance, and relative difficulty with which they can be detected, make them very attractive devices for terrorists. The answers from the experts with regard to the motivations and reasons for terrorist groups using drones can be categorised as follows:

- **Economic reasons**: Due to their commercial availability, simple procurement (which is not an illegal activity), as well as their low price, armed non-state actors can now enjoy access to the aerial dimension with an ease that was previously unimaginable. Today such groups can acquire drones by several means (via state-support, off-the-shelf systems, legally purchased or even homemade) and that's why their use is becoming more common.

- **Easy to control remotely**: the control of a drone does not require special technical experience, the technology is easily accessible, and the operator can be at a safe distance from its target. Armed non-state actors consider drones of high value because they contribute to preserving their human resources and advancing their combat capabilities, as they are safe to use, remotely operated, easily cross boundaries, and can engage with a target without the need for in-person presence. This minimises the risk of a terrorist being caught or killed.
- **Lethality**: Although using drones by armed non-state actors does not constitute a »serious threat« given the primitive lethality of UAVs, the threat remains real, as drones can not only inflict severe damage, but can also kill.
- **Uncovered airspace**: The airspace is not fully monitored and is difficult to defend against external threats.
- **Attractiveness**: Drones can be easily re-configured for multiple purposes and missions. They can boost the prestige, status, and morale of these organisations when their missions are successful.

The main goal of terrorist organisations is to launch attacks against individuals (random or targeted), groups of people (random or targeted), and facilities or specific locations (random or targeted).

Interviewee 1[1] (interview conducted on 19. 04. 2021) stated that drones are used in a variety of ways by terrorist organisations, which can be as diverse as the imaginations and creativity of their users. However, their main function is to observe, photograph and record a certain area or space, as well as people of interest, in order to collect information that will be used to plan certain activities, which facilitates the preparation of the field and gaining full insight into the environment before carrying out a particular attack. So, for example, a group can observe the frequency of movement of people in a certain area and at what times of day this happens, where there are any members of the security services present, the lighting of the area, whether the area is under video surveillance, the layout and position of buildings, accessibility to buildings, positions from which it is easiest to carry out an attack, and so on.

Although drones were initially designed as surveillance and info-gathering systems, they have evolved over time and improved their features and performance, thus changing the things they are used for. Today, drones are potentially more lethal than ever, so their deadly nature is their most notable feature in the context of the current study. Armed non-state actors are interested in this, because they can easily create a "threat from above" using a drone.

Interviewee 2[2] (interview conducted on 21. 04. 2021) explained that terrorist organisations often use drones in the following types of activities (armed and/or non-armed):

[1] *Dr. Marija Popovic Mancevic, Professor at University of Criminal Investigation and Police Studies, Belgrade, Serbia.*

[2] *Dr. Ali Chehab, Professor of ECE, American University of Beirut, Lebanon.*

- When fighting against legitimate armed forces, terrorist organisations use them for surveillance of the territories around them and to identify targets for attacks. Drones can then be used to launch attacks against some of these targets, as well as guide any shelling that is carried out, and to record the attacks for intelligence or propaganda purposes.
- For assassination missions aimed at the leaders or key figures in a country.
- With the intent to terrorize a population by launching attacks on it, the infrastructure, or government agencies. In addition to regular explosives, terrorists could arm a drone with a chemical agent, and thus cause even greater damage and fear.
- A drone does not need to carry explosives to carry out an attack, as it can also be used as an access point to activate and detonate a bomb that is already placed at a target.
- Smuggling drugs, phones, and even weapons to prisoners.
- To setup a fake mobile Wi-Fi network or a rogue access point to intercept smartphone traffic, or to hijack other drones.

Interviewee 3[3] (interview conducted on 06. 05. 2021) put such activities into three major domains:

- Intel-operations – info gathering, surveillance;
- Combat – used as flying bombs or for dropping bombs;
- Trafficking – various criminal activities related to smuggling.

He mentioned that there are two above-regional non-state actors which are known to use armed drones, Hezbollah and ISIS, noting that these are not the only groups to use drones, just the most famous ones. In the last few years, the Iran-backed Houthi militia in Yemen has used drones extensively as flying missiles with relatively precise targeting, and probably top the list worldwide with regard to this, while the Kurdish PKK can be classified as an emerging actor in the field of drones.

The last subject discussed in the interview was the approach that countries around the world should take to prevent the use of drones for terrorist purposes.

Interviewee 4[4] (interview conducted on 21. 04. 2021) considered that no administrative bans on the use of drones would be effective given their widespread commercial availability, so it is difficult to track who owns each drone and for what purpose. He said that states should instead develop effective anti-aircraft formations that are able to recognise a drone at a sufficient distance to act operatively, i.e. to disable it, but also to prevent it from flying in a predetermined area. In this regard, it is especially important when developing such technology to take into account the disabling of drones without endangering the people of property underneath them. Interviewee 1 also agreed with this approach to anti-drone systems.

Interviewee 3 concluded that preventing armed non-state actors from acquiring drones might be a »mission impossible«, and this is why states should give more attention to developing effective countermeasures. Despite the progress

[3] *Dr. Ali Bakir, Research Assistant Professor, Ibn Khaldon Center at Qatar University.*

[4] *Dr. Josip Pavlichek, Professor, Police College Zagreb, Croatia.*

achieved in this regard in the last few years, efforts to create anti-drone platforms and systems lag behind the evolution of drones, and appear to be random, less cost-effective, and reactive. Efforts to produce effective anti-drone solutions should utilise the growing potential of artificial intelligence and follow a two-path track to provide advanced, pre-emptive, and cost-effective »hard kill« and »soft kill solutions«.

Interviewee 2 gave some concrete proposals for the approaches that countries around the world should introduce to prevent terrorists from using drones, as follows:

- Countries should have very strict policies related to selling drones or selling the essential parts that are used to build them.
- Strict policies should govern the activities of drones when taking images or recording videos of people and property, which should only be done with the correct authorisation.
- A strong security system should be put in place to minimise the risk of terrorists compromising a legitimate drone and gaining access to it. There must be a strong authentication protocol to enable the legitimate owner to operate a drone.
- Governments should have regulations in place and awareness campaigns related to the safe practices and features of drones to ensure their proper integration into the national airspace domain.
- Countries should force drone manufacturers to equip their drones with some type of intrusion detection system to prevent terrorists from taking control of legitimate drones.
- Countries should put in place drone detection systems, especially in sensitive locations likely to attract terrorist interest.

5 CONCLUDING CONSIDERATIONS

Drones (or UAVs) are remotely controlled aircraft that can be equipped with a variety of technical equipment, including deadly weapons for attacking targets.

From the analysis presented above, it is evident that terrorist organisations have access to drones and often decide to use them to strengthen their ability to attack targets in both war zones and beyond. As such, it can be assumed that drones will become a standard tool for terrorist organisations. Since low-flying drones cannot be detected by radar, and so can carry deadly cargo without being noticed by state authorities, security and military technologists must develop and refine effective countermeasures for detecting and preventing their malicious use. At present, however, there are not many practical solutions or concrete measures to counter this threat.

It is therefore necessary for national security services to be better prepared to counter the new risks and have responses ready in advance. Concrete practical measures should be taken immediately to establish preventive actions to counter the misuse of this new technology and develop strategies to combat the threat of drones, such as drone detection measures and techniques. The security services must be reorganised and well-equipped, and their personnel well-trained and adapted to this emerging threat in order to effectively protect their countries and citizens from such attacks.

However, the aim is not to stop developing new technologies or enjoying their benefits, or to ban the civil/commercial use of drones. Drones are not the problem, the problem is their use and application, especially if they are used for malicious purposes. Understanding this threat, where it comes from and how it works, is key to effectively stopping attacks before they happen. Therefore, any misuse of drones should be identified at a very early stage and effective measures should be undertaken to prevent the potential danger they pose.

That said, because of the reasons set out in this study, such as the low cost of drones, their easy remote control and lethality, as well as unprotected airspace and the possibility to carry out multiple simultaneous attacks, at low cost and considerable distance, these vehicles may soon become the primary tool in terrorist attacks.

REFERENCES

Ackerman, G. (2007). *Assessing terrorist motivations for attacking critical infrastructures*. Centre for Nonproliferation Studies, Monterey Institute of International Studies. https://e-reports-ext.llnl.gov/pdf/341566.pdf

Altawy, R., & Youssef, A. M. (2017). Security, privacy, and safety aspects of civilian drones: a survey. *ACM Transactions on Cyber-Physical Systems, 1*(2), 1–25.

Ani, U. D., Watson, J. D. McK., Nurse, J. R. C., Cook, A., & Maple, C. (2019). *A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape.* PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT. https://arxiv.org/ftp/arxiv/papers/1904/1904.01551.pdf

Axe, D. (2016). *Hezbollah drone is a warning to the U.S.* Daily Beast. https://www.thedailybeast.com/hezbollah-drone-is-a-warning-to-the-us

Ball, R. J. (2017). *The proliferation of unmanned aerial vehicles: Terrorist use, capability, and strategic implications*. Lawrence Livermore National Lab. https://doi.org/10.2172/1410035

Bergen, P. (2019). *Global terrorism: Threats to the homeland, Part 1*. House Committee on Homeland Security. https://congress.gov/116/meeting/house/109886/witnesses/HHRG-116-HM00-Wstate-BergenP-20190910.pdf

Braun, T. (14. 9. 2020). Miniature menace: The threat of weaponized drone use by violent non-state actors. *Wild Blue Yonder*. https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2344151/miniature-menace-the-threat-of-weaponized-drone-use-by-violent-non-state-actors/

Cook, K. L. (2007). The silent force multiplier: the history and role of uavs in warfare. *2007 IEEE Aerospace Conference*. https://ieeexplore.ieee.org/document/4161584

Decree on the conditions under which an unmanned aircraft can fly in the Macedonian airspace. (2017). *Official Gazette of the Republic of Macedonia,* (no. 187 of 20. 12. 2017).

Drone-flying Albanian arrested with guns ahead of Serbia match. (2015). *BeSoccer*.

https://www.besoccer.com/new/15967

Gatwick Airport: Drones ground flights. (20. 12. 2018). *BBC*. https://www.bbc.com/news/uk-england-sussex-46623754

Haugstvedt, H., & Otto Jacobsen, J. (2020). Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors' Use of Weaponized Unmanned Aerial Vehicles (UAVs - 'Drones'). *Perspectives on Terrorism, 14*(5), 26–40. https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2020/issue-5/haugstvedt-and-jacobsen.pdf

International Civil Aviation Organization. (2011). *Unmanned Aircraft Systems (UAS)*. https://www.icao.int/meetings/uas/documents/circular%20328_en.pdf

Miasnikov, E. (2005). *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects*. Center for Arms Control, Energy and Environmental Studies at Moscow Institute of Physics and Technology.

Mitrevska, M., & Mikac, R. (2017). *Handbook on Critical infrastructure protection*. Chamber of Republic of Macedonia for Private Security.

Pejanovic, L., Vrkatic, L., & Milenkovic, M. (2018). Upotreba bespilotnih letelica u teroristicke svrhe. *Vojno delo, 69*(3), 356–369

Pledger, T. (2021). *The role of drones in future terrorist attack*. Association of the US Army. https://www.ausa.org/publications/role-drones-future-terrorist-attacks

Serkan, B. (2017). *Daesh's drone strategy technology and the rise of innovative terrorism*. SETA publication. https://setav.org/en/assets/uploads/2017/08/Report88.pdf

Straub, J. (2014). Unmanned aerial systems: consideration of the use of force for law enforcement applications. *Technology in Society, 39*, 100–109.

United Nation Security Council Counter-Terrorism Committee Executive Directorate & United Nations Office of Counter-Terrorism. (2018). *The protection of critical infrastructures against terrorist attacks: Compendium of good practices*. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

Wagner, D. (17. 9. 2019). Terrorists and the Weaponization of Drones. *International policy digest*. https://intpolicydigest.org/terrorists-and-the-weaponization-of-drones/

Warrick, J. (21. 2. 2017). Use of Weaponized Drones by ISIS Spurs Terrorism Fears. *Washington Post*. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

Xinhua. (2018). *Nigeria says Boko Haram now uses drones, mercenaries against military*. http://www.xinhuanet.com/english/2018-11/30/c_137642456.htm

Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020) Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things, 11*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/

About the Authors:

Ice Ilijevski, PhD, is an Associate Professor at the Law Faculty in Kichevo, University St. Clement of Ohrid in Bitola, North Macedonia. E-mail: iilijevski@uklo.edu.mk

Zlate Dimovski, PhD, is a Full Professor at the Faculty of Security in Skopje, University St. Clement of Ohrid in Bitola, North Macedonia. E-mail: zlate.dimovski@uklo.edu.mk

Kire Babanoski, PhD, holds a PhD in the field of security and is an independent researcher. E-mail: kbabanoski@gmail.com