Cybersecurity of Drone Operations in Public Space

TADEUSZ ZIELIŃSKI

Abstract Drones, have been the focus of business, military and public attention for several decades, showing potential in both civilian and military applications. The use of drones in the public domain may pose certain risks related to the safety of citizens and their property Particularly significant are the risks associated with taking control of the UAVs or the theft of data collected by drones through cyberattacks targeted at individual system components. The issue of ensuring the security of drone operations in public spaces requires a comprehensive approach. In this respect, it will be necessary to strengthen the cooperation between producers of UAV components, state administration authorities and services responsible for broadly defined security and public order.

Keywords: • cybersecurity • cyberattack • cyberthreat • drone • UAV • public space

CORRESPONDENCE ADDRESS: Tadeusz Zieliński, Ph.D., Associate Professor, War Studies University in Warsaw, Military Faculty, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: t-zielinski@akademia.mil.pl, ORCID 0000-0003-0605-7684, Researcher ID V-6001-2018.

https://doi.org/10.4335/2022.2.9 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Unmanned aerial vehicles (UAVs), commonly referred to as drones, have been the focus of business, military and public attention for several decades. They show potential in both civilian and military applications. Despite the fact that this technology was originally designed for the military – as yet another tool to be utilised in armed conflicts, offering an advantage over potential adversaries – it was very quickly adapted to civilian needs. Nowadays, drones can be regarded as "dual-use" technology.

It should be stressed that drones are used more and more extensively for civilian purposes. This is due to the emergence of new, transformative technologies that expand the capabilities offered by UAVs. In turn, more and more flexible legal regulations introduced at various levels, including global (i.e., the International Civil Aviation Organization, ICAO), regional (i.e., the European Aviation Safety Agency, EASA) and national, are making drones available to a wide range of users who often use them in innovative ways. As a consequence, drones increasingly appear not only in dedicated airspace but also in the public domain. This trend will grow and in the future, drones can be expected to be used in cities as aerial, automated or autonomous taxis, completing various deliveries or supporting certain law enforcement services. One can imagine that they will operate in airspace under similar rules as those applicable to other airspace users, performing various operations without exciting much interest from other users.

However, it should be remembered that UAVs are not capable of carrying out tasks entirely independently. Rather, they are part of a system composed, *inter alia*, of a control station, an operator, a communication link, and sensors – all of which enable UAV operations. Without these elements, drones cannot function properly and the safe performance of their operations is affected by the overall incidence of undesirable phenomena compromising the safety of individual system components. Particularly significant are the risks associated with taking control of the UAVs or the theft of data collected by drones through cyberattacks targeted at individual system components. It is easy to imagine the danger posed by terrorist or criminal groups taking unauthorised control of a drone to deploy it in public spaces, e.g., during a mass event or in a crowded city centre.

2 The potential use of drones for civilian purposes – examples

It is virtually impossible to list all the potential uses of drones for civilian purposes. The scope of their use is likely limited merely by human imagination, legal regulations and technological constraints. Nevertheless, the use of drones for civilian purposes can be divided into three main fields: a) support of services responsible for ensuring broadly defined security and public order; b) crisis management; and c) commercial use. It should be emphasised that this is not a closed list, but only some of the numerous potential use options. In addition, the use of drones will also depend on their capabilities and constraints resulting from the class they represent. Class I includes UAVs with a take-off

weight of less than 150 kg, which can be further divided into micro, mini and small UAVs. This class does not require any certification standards. Such drones are generally equipped with mixed sensors (optoelectronic and infrared) and are characterised by relatively low logistic requirements. They operate at low altitudes not exceeding 1,600 m, and have a limited range and flight duration. Class II (with a maximum take-off weight of 150-600 kg) includes medium-sized UAVs which often use a catapult to take off, and which do not require robust logistic infrastructure. They operate at altitudes of up to 3,000 m. Their equipment includes optoelectronic and infrared sensors, and laser rangefinders. Class III drones (above 600 kg) are the largest UAVs, with the highest take-off weight, and have the longest range and mission duration. Usually they require prepared airfields (landing sites) to take off and land. They are capable of performing various missions thanks to special equipment, which may include radars, lasers and reconnaissance devices. Owing to satellite communication systems, they can carry out tasks in remote regions. They also require appropriate logistic backing. It should be stressed that Class I and II drones are the most common in the public domain, while Class III drones are primarily used by the military, although this is currently no longer a strict rule (The Joint Air Power Competence Centre, 2010: 8).

The main determinants of whether the use of UAVs will be considered possible are the characteristics described by both their benefits and limitations. Their ability to operate in the air for extended periods of time should be viewed as a key advantage associated with the use of UAVs. More specifically, contemporary unmanned aerial platforms are capable of operating in the air (depending on the class) for up to several dozen hours, and the introduction of solar propulsion will extend the UAV mission duration to weeks or even months. Other unquestionable advantages include the safety associated with the pilot (operator) staying outside of the UAV when performing tasks in a hostile environment (contamination, radiation, etc.) and operation flexibility thanks to the use of a wide range of loads (sensors). Due to all these features, one unmanned aerial platform can perform a wide spectrum of tasks.

The potential applications of unmanned aerial systems for civilian purposes may make them useful for two categories of users. The first are state authorities, mainly focused on Class II and III unmanned aerial platforms capable of performing long-term missions. However, under certain conditions, they will also use Class I drones, undoubtedly proving useful in crisis management and as a support in disaster prevention. For example, drones can be used to scrutinise, monitor and analyse a situation in the event of natural disasters such as fires, floods, earthquakes and weather anomalies, as well as to support search and rescue missions. Their role in the protection of critical infrastructure, for instance, in monitoring power plants, gas pipelines, oil pipelines, electricity transmission lines, airports and seaports, etc., is also quite significant, mainly for economic reasons. An important field of application will also be the use of drones providing support for civilian authorities in ensuring internal security: protecting the state border, monitoring mass events or traffic, or supporting police activities in various areas (Skrzypietz, 2012: 18).

The second category includes users of mainly Class I drones for service and commercial activities. In the civilian domain, this should be considered the fastest-developing area, creating new jobs and potential profits for companies using drone technology. This means an increase in the number of drones in public spaces and, by extension, potential security risks.

At present, drones can be used for civilian purposes across several areas related to commercial services. One of these is aerial filming and photography. Bird's eye view shots open up a new perspective and provide viewers with new experiences. The high quality of the recorded images, along with the wide availability of drones, offer substantial opportunities for both amateurs and professionals. Recordings of wedding ceremonies, advertising spots, news media reports, sports broadcasts, music videos, TV programmes or Oscar-winning movies are often shot using drones and they continue to enjoy ample popularity. Due to technological progress and with equipment decreasing in size, it is possible to take professional, high-quality pictures in the traditional 2D technique, and to obtain 3D images, as well as 360-degree pictures with modern technology. In other words, a photo or video camera installed on a drone has become a common working tool.

Virtual reality is another area where drones can be useful. Drones can be used to create spatial 3D scans for games or professional simulators, and not only flight simulators. Their mobility makes it possible to create spatial scans of objects of any height and of large areas. With UAVs, the analysis and documentation of inaccessible places with a large number of obstacles, posing a challenge for manned aircraft, are no longer an issue. Due to the high costs and limited capabilities of manned aviation, even 3D models of airports, which until recently were created using manned aviation, are now being made using drones. The material so acquired is used to create professional flight simulators for training pilots of manned aircraft.

Land surveying is another major field for the commercial use of drones. Drones are capable of recording data for photogrammetric terrain models using "low-altitude" aerial photography. Until recently, photogrammetry and orthophoto maps were created using aerial photographs taken from a manned airplane or helicopter; this is referred to as "medium- and high-altitude" photogrammetry due to its moderate accuracy and high cost. This method is being gradually abandoned. The creation of orthophotos is the main land surveying task carried out using drones. Due to an automatic mission planning option, flight is very precise, saves surveyor's time, and the material so acquired is ready for further processing.

In many regions of the world, drones are already being used in agriculture as well. Modern agriculture is based on what is known as agrotechnology, which refers to all procedures used to cultivate land and plants with a view to producing high yield of the best quality that can be attained. In this field, unmanned aviation is perfect for tasks such as monitoring the vitality of plants, optimising fertilisation and the use of plant protection

products, and crop-dusting on valuable plants where the level of crop damage with traditional fertilisation methods is significant. In the case of any agricultural damage, the material obtained from the air can help to develop a reliable report making it easier to receive compensation for any damage.

Drones are also increasingly used in inspections and environmental protection. Using drones for conducting inspections of buildings, structures, ships, machinery and power lines, as well as performing thermal-imaging measurements of buildings or heat transmission networks, provides accuracy and is safer for people. And due to the high mobility and the ease of performing area observations, drones are also increasingly used for environmental protection. It becomes easier to control the population of forest animals, especially birds. General environmental contamination and the pollution of specific locations can be monitored from the air on an ongoing basis. Moreover, smog, which has become a significant problem in many cities, has prompted another application for drones. An increasing number of measuring devices are intended to be used and mounted on drones in order to monitor the environmental situation.

Also, one should not forget about the use of drones in the transport of various types of shipments. They can also be used to transport samples for analysis, as was the case during the COVID-19 pandemic, or to transport blood between hospitals or deliver medicines to people with impaired mobility. The use of drones for such purposes saves time, especially in crowded cities. In the future, they will also be used to transport people, with a suitably adapted urban infrastructure making this possible.

Drone use for civilian purposes, as discussed above, leads to the conclusion that their number in public spaces will grow significantly. This will raise concerns about the safety of operations performed by them in public spaces, along with related potential threats.

3 Cyber threats connected with the use of drones in public spaces

The use of drones in the public domain may pose certain risks related to the safety of citizens and their property. These can be categorised into several groups. First, technical problems beyond human control which may cause a drone to fall in a place where there are people or elements of their property (buildings, cars, urban infrastructure, etc.). Second, hazards related to human error, considered as non-deliberately contributing to the misuse of a drone or causing it to fail. Third, adverse environmental conditions increasing the likelihood of losing control of the drone, human error or technical failure. Fourth, unpredictable errors and failures which may occur within the infrastructure and any systems supporting UAV operation. Fifth, deliberate human action consisting of an attempt to take control of a drone and use it in an illegal manner. All these categories of hazards contribute to the loss of control of a drone and can consequently lead to the fatal injuries of people, or to property damage both on the ground and in the air (Tran, 2021).

The deliberate use of drones in an illegal manner by a variety of actors (e.g., terrorists or criminal groups) can include physical or cyber-attacks. These cause interference with citizens' privacy and threaten their physical safety. Such activities may include surveillance to track down specific individuals and private areas. The unintentional use of drones, especially over urban areas, can also lead to violations of the law, including the illegal collection of data on people and their property, which may be used for blackmail or fraud. Safety violations can also occur if a drone crashes and hits a built-up area, a parked car or civilians, resulting in property loss and/or damage and human casualties and/or death. What is more, drones are also used to attack guest Wi-Fi and/or short-range Wi-Fi connections, Bluetooth and other wireless devices such as keyboards connected via Bluetooth. Such connections are not protected under the current security measures which assume that nobody can get close enough to breach them or access internal networks using wireless signals. Such assumptions result in poor single-factor authentication and the use of typical passwords which can be easily cracked, especially in the absence of an encrypted connection. This facilitates the interception of information in both private buildings and public spaces (Lee, Eom, Park, & Lee, 2018).

The category of threats associated with deliberately taking control of a drone includes one of the more serious risks associated with drones used in public spaces involving cyber-attacks on specific drone components. This stems from the fact that a drone is only one of the three basic components of the entire system that ensures its functioning (Best, Schmid, Tierney et al., 2020: 15). More specifically, the UAV components include an unmanned aircraft, a ground controller and a communication link. The drone, as an unmanned aircraft, is itself a complex electronic system containing, *inter alia*, a flight controller and navigation devices based on global positioning systems (GPS). The control station provides communication between the ground controller and the station itself, while the communication link ensures communication between the control station and the drone (control and data transfer) (Abid, Austin, Fox, & Hussain, 2014). In other words, an unmanned aerial system can be viewed as an advanced computer containing a wide range of electronic components, a GPS module and communication systems, which may be vulnerable, to a varying extent, to threats involving cyber-attacks. Special attention should be paid to the vulnerability of drone systems to:

a) spoofing: pretending to act as, or disrupting the operation of, the global positioning system (GPS). The lack of encrypted telecommunications links makes it easy for hackers to pretend to act as, jam or disrupt GPS signals. Jamming or disrupting the GPS signal occurs when the hacker is able to generate a stronger signal on the same communication frequency as the one used by a civilian GPS satellite; the drone cannot then receive GPS location information. In consequence, the drone loses its orientation in the air and uses a false location, which may lead to its crashing on the ground (Seo, Lee, Im, Jee, 2015);
b) malware infection. The communication protocols used in drones allow users to pilot them wirelessly using smartphones, tablets or laptops. Nonetheless, this poses the threat of these devices being infected with malware, which may in consequence lead

to taking control of the drone or stealing data collected by the UAV (Kim, Wamper, Goppert, Hwang, Aldridge, 2012: 2438);

c) data interference and interception. Telemetry channels are used to monitor an UAV and to facilitate the transmission of information through open and unsecured wireless transmission, making it vulnerable to various threats. This can result in the interception of data, the implantation of false data and the alteration of pre-established drone airways (Abdallah, Ali, .Mišic´, Mišic´, 2019:43). Moreover, installing or transmitting a number of infected digital files (videos and images) from the drone to the ground station is also possible.
d) manipulation. Since drones generally cover pre-programmed and pre-defined routes, high-value cargo may be exposed to theft, and drones may be diverted to other locations in order to use explosives, biological weapons or other dangerous cargo. All this may happen due to taking control of the drone by, *inter alia*, taking control of or disrupting the GPS signal (Ramon Soria, Bevec, Arrue, Ude Ollero, 2016:700);
e) technical issues. Drones are technical devices which can be vulnerable to all kinds of failures, including application errors such as a loss of connection between the user's control device and the drone, resulting in the drone crashing or being lost. Problems related to the lack of a stable connection, especially under challenging terrain conditions, as well as to battery life, resulting in a very limited flight duration, are also likely to be encountered (Tomislav, Andrija, Jurica, 2018);
f) Wi-Fi jamming. Drones can also be taken over by means of a de-authentication process between the access point and the drone's control device, which can be implemented as a temporary or permanent action, for example, by jamming the drone's operating frequency and redirecting it to the hacker's Wi-Fi connection (Westerlund, Asif, 2019).

The methods presented above involve taking control of the drone or obtaining unauthorised access to data acquired by an UAV. This poses a real danger to people and property in the public domain. Depending on the intentions of the adversary, a drone can be used as a tool for a terrorist attack in a crowded urban area or during a mass event, which may, in consequence, result in a large number of fatalities. A drone can also be used to collect private and sensitive data on specific individuals, which can then be used for blackmail or fraud purposes (Yaacoub, Noura, Salman, Chehab, 2020). As the increasing number of drones in public spaces involves a real danger of unauthorised use, there is a need to counter such incidents.

4 Counteracting threats involving the unauthorised use of drones in public spaces

The issue of ensuring the security of drone operations in public spaces requires a comprehensive approach. It should include the following: a) relevant legal regulations; b) prevention; c) the readiness of dedicated services and resources to counter threats; d)

the detection, identification and neutralisation of drones posing threats; and e) gathering experience.

Legal regulations provide the basis for the appropriate and lawful use of drones in public spaces. Current legislation allows drones to be used in urban areas under certain conditions. Drone users must hold the required licences, and drones should be registered so that they can be identified and, when necessary, that those who use UAVs in violation of the law can be held liable. The second component, i.e., prevention, should focus on raising awareness among drone users of the risks associated with their use. This entails the need for drone users to obtain specific authorisations, acquired through training, along with appropriate licences authorising them to use drones. In addition, it is necessary to hold responsible any persons who deliberately use drones in an unlawful manner. The inevitability of punishment, including the confiscation of equipment or the suspension or revocation of licences for life, should make users aware of the real risks associated with drones used in public spaces. Information campaigns for both drone users and society at large that should be aware of the dangers associated with the operation of drones in public spaces should constitute an important element of the aspect in question. This also involves the need for decision-makers to have social acceptance for drone operations conducted in public spaces. Only then will it be possible to develop drone technology for economic and social needs. The third component concerns the readiness to use appropriate force and resources to prevent any threats connected with drones used in public spaces. This readiness should be based on the developed risk scenarios and risk prevention procedures for UAVs (Majeed, Abdullah, Mushtaq, Kazmi, 2021). Furthermore, exercises of crisis management teams should be conducted, and these should be based on scenarios taking into account the risk of using drones in an illegal manner in the public domain. Well-prepared services should also have technologies to respond appropriately to a given situation. Another aspect involves activities aimed at physically responding to the threats connected with the unauthorised use of drones in public spaces. It includes detecting, identifying and possibly neutralising drones that are used in public spaces in an illegal manner. Detection may include the use of multiple technologies to track down a drone in airspace. These technologies are: radars, passive radio frequency identification systems, optoelectronic systems, active optical systems, magnetic detection and acoustic detection systems, as well as watchers. The best outcomes are achieved by combining several drone detection methods. Identification, in turn, should ensure the confirmation that a drone being used in an illegal manner has been detected and the specific risk has been defined. Another aspect is the neutralisation of drones posing threats in public spaces. The neutralisation can be either passive or active. Passive neutralisation may include the use of barriers, nets or physical fences in selected public spaces. Geofencing should also be used, which is a limiting feature within a drone, preventing it from going beyond pre-defined zones in public spaces. In the future, dynamic geofencing will also be used, making it possible to react, in real time, to drones penetrating prohibited areas within the public domain. Active neutralisation, by contrast, involves the physical neutralisation of drones in public spaces. This may consist in jamming radio links, taking control of a drone, intercepting it and, as the last-case scenario, shooting it down. Such neutralisation

requires the provision of security measures for people and property within the impact zone. The comprehensive approach to counteracting threats related to the use of drones in an unauthorised manner ends with "lessons learned" – conclusions to be gathered and incorporated in relevant legal regulations and procedures.

This comprehensive approach also includes the use of cyber defence technologies in relation to drones posing threats in public spaces. These operations are implemented in an identical manner as those undertaken by people intending to use drones in an unlawful manner, the only difference being that such measures are carried out by the relevant services acting in accordance with the law. However, the tools that are used in cyber defence are virtually the same.

5 Summary

The use of drones in public spaces can undoubtedly be expected to increase in the near future. The potential of drones, on the one hand, cannot be overestimated when it comes to the functioning of many spheres of social and economic life. On the other hand, their operation in public spaces poses threats to the safety of people and property. Therefore, the first thing to do should be to develop a map of threats to specific public spaces within which drones will perform operations in the future and to establish an effective plan to neutralise any identified risks. The identification of security gaps in the components used for drone production, as well as in software used for their operation, is another aspect that should be taken into consideration. This requires the constant monitoring of the UAVs systems and keeping pace with technological development. It is no less important to invest in regular equipment tests as part of cross-sectoral cooperation (involving the state, private companies, laboratories, research centres, etc.), as in this way, it is possible to develop universal safety and security protocols which could be implemented on a wider scale. It also seems indispensable to ensure coordinated and constantly updated monitoring and intervention systems, as even cutting-edge solutions do not offer full immunity against all cyber-attacks. In this respect, it will be necessary to strengthen the cooperation between producers of UAV components, state administration authorities and services responsible for broadly defined security and public order.

References:

Abdallah, A., Ali, M.Z., Mišic,´ J. & Mišic´, V.B. (2019) Efficient security scheme for disaster surveillance uav communication networks, *Information*, 10(2), pp. 1-22.

Abid, M.E, Austin, T., Fox, D. & Hussain, S.S. (2014) *Drones, uavs, and rpas: an analysis of a modern technology* (Worcester, Massachusetts: Worcester Polytech. Inst.).

Best, K.L., Schmid, J., Tierney, S., Awan, J., Beyene, N.M., Holliday, M.A., Khan, R. & Lee, K. (2020) *How to Analyze the Cyber Threat from Drones* (Santa Monica: RAND Corporation).

Kim, A., Wampler, B., Goppert, J., Hwang, I. & Aldridge, H. (2012) Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, *Infotech@ Aerospace*, 2012, pp 1-30.

Lee, H., Eom, S., Park, J. & Lee, I. (2018) Uav-aided secure communications with cooperative jamming, *IEEE Transactions on Vehicular Technology*, 67(10), pp. 9385–9392.

Majeed, R., Abdullah, N.A., Mushtaq, M.F. & Kazmi, R. (2021) Drone Security: Issues and Challenges, *International Journal of Advanced Computer Science and Applications*, 12(5), pp. 720-729, https://doi.org/10.14569/IJACSA.2021.0120584.

Ramon Soria, P., Bevec, R., Arrue, B., Ude, A. & Ollero, A. (2016) Extracting objects for aerial manipulation on uavs using low-cost stereo sensors, *Sensors*, 16(5), pp. 1-19.

Seo, S.-H., Lee, B.-H., Im, S.-H. & Jee, G.-I (2015) Effect of spoofing on unmanned aerial vehicle using counterfeited gps signal, *Journal of Positioning, Navigation, and Timing*, 4(2), pp. 57–65.

Skrzypietz, T. (2012) Unmanned Aircraft Systems for Civilian Missions, *Policy Paper*, (1) (Potsdam: Brandenburg Institute for Society and Security).

The Joint Air Power Competence Centre (2010) *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO* (Kalkar: NATO).

Tomislav, R., Andrija, V., Jurica, I. & Bo, W. (2018) Challenges and solutions for urban uav operations, *International Scientific Conference "Science and Traffic Development"(ZIRP 2018)*, available at: https://www.bib.irb.hr/938317/download/938317.Radii_Vidovi_Ivoevi_Wang_Challenges_and_Solutions_For_Urban_UAV_Operations.pdf (August 31, 2022).

Tran, T.D. (2021) *Cybersecurity risk assessment for Unmanned Aircraft Systems*, available at: https://hal.archives-ouvertes.fr/tel-03200719v2 (August 30, 2022).

Westerlund, O. & Asif, R. (2019) Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things, *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, (IEEE), pp. 1-10.

Yaacoub, J.P., Noura, H., Salman, O. & Chehab, A. (2020) Security analysis of drone systems: Attacks, limitations, and recommendations, *Internet of Things*, 11, pp. 1-39, https://doi.org/10.1016/j.iot.2020.100218.