Criminal Justice Issues
Journal for Criminalistics, Criminology and Security Studies
Year XX, Issue 5, 2020, 43-56.
UDK 343.9
DOI 10.51235/kt.2020.20.5.43

DRONES AS A PERMANENT AND PRESENT DANGER

Review paper

Primljeno/Recieved: 08.11.2020.
Prihvaćeno/Accepted: 16.11.2020.

Zvonimir IVANOVIĆ
Valentina BAIĆ

Abstract

Reason(s) for writing and research problem(s): The lack of research on drone attacks in the West Balkans, but also within the European Union, has influenced our decision to conduct case study analysis of drone incidents occurring in the world, but also in our surrounding, in order to think how to prevent those in our own "backyard".
Aims of the paper (scientific and/or social): This article intends to present significant security and operational information on drone attacks from cases detected in various surroundings.
Methodology/Design: Methodology used in the paper includes case studies of drone attacks in certain countries, in order to evaluate these incidents from security and operational aspects.
Research/paper limitations: Limitations refer to possible unregistered activities in the form of new modus operandi of perpetrators involving drone attacks.
Results/Findings: The findings presented in this paper show a cross-section of attack vectors and modus operandi used by perpetrators, as well as vulnerabilities found at targeted institutions and objects. Those findings are to be considered for future prevention of perpetrators activities.
General conclusion: There is a real need to improve and modernize general security measures related to Unmanned Aerial Vehicles. This article points to such necessity at several different levels and aspects through the analysis of attack vectors, modus operandi, and the weaknesses of the attacked targets.
Research/paper validity: Findings presented in this article can be used to direct future research in this field, in order to strengthen and develop various measures to combat existing and persistent threats posed by drones.

Key words:
drones, attacks, law enforcement, prisons, prevention

1. INTRODUCTION

The existing drones threats are various, especially in this rapidly changing world of digital gadgets. Nowadays, drones pose a new threat to the security of prisons, within and outside of the prison walls. Through drones, organized crime and terror-related groups can deliver various items. Those items could represent strategic and tactical advantages for the prisoners both within and outside the walls of prisons. Items delivered by drones could be (but not an exhaustive list): SIM cards, mobile phones, drugs, explosives and weapons, different materials endangering people, objects and structures. Some of the new dangers arising from drones include drones disrupting critical infrastructure and other interfering with human-crewed aircraft. In January 2019, INTERPOL reported the emergence of this new risk highlighting that individuals or organized groups are using the Unmanned Aerial Systems (UAS) devices outside of the institutions to collude with an individual(s) inside the prison system to deliver the payload of contraband. These activities are achieved by attaching a payload to the device (Unmanned Aerial Vehicle – UAV, often referred as Unmanned Aerial Systems – UAS, and we consider it synonyms for drones), and they are scheduled to deliver the payload at a previously agreed location to be collected by a recipient inside the prison system (INTERPOL, 2019). Those include different actors – from the prisoners up to personnel of the correctional facility. Often the UAV devices used are small and difficult to spot through conventional means of surveillance, as they do not follow traditionally examined trajectories to deliver their payloads. Perpetrators of these activities are very covert in their activities, cognizant of different anti-drones' activities and measures. Perpetrators that successfully deliver illegal goods into a prison system require little knowledge or training on UAV equipment. This is due to the vast majority of the market overflow of different drones offered by Chinese and other Small medium enterprises (SMEs). The offender often utilizes inexpensive commercially available multi-copter UAV devices with GPS stabilization and pre-set trajectory programs to deliver payloads of contraband to their targets within the prisons. These widely available units can be purchased easily by the public, without registration or tracking systems.

Although there are different measures tried by many countries, for example Implementing boundaries in operating of UAVs – the pilot has to be licensed the and go through some training, and similar, but not with a lot of much. Moreover, drones can be used for cyber-surveillance, to leverage drones' proximity to prison premises to turn the UAV into a jumping-off point to illegally access networks and systems, thus creating a new category of infection vector of cybercrime. One of the most simplistic but very effective tactics for targeting different institutions is using drones as rogue Wi-Fi access points (Staniforth, 2012, February 13). Finally, drones are prone to the same type of hacks as laptops or smartphones. Some of the hacking techniques include password theft, Wireshark, Man-In-The-Middle (MITM) attacks, Trojan horse virus, Distributed denial of service (DDoS) attacks (Rani et al., 2015). Therefore, professional drones commonly used by government agencies and police forces can be remotely exploited by rogue hackers exploiting the vulnerabilities of their communication systems and protocols in case of the Internet controlled flights and point-to-point links.[1]

2. METHOD

The intention of the following case studies analysis was to determine which vectors were used by perpetrators in order to cause criminal activities, damages or abuses. Throughout carefully selected examples that are thoroughly examined in aspects of *modus operandi*, means and methods used regarding the offence, attack vectors and vulnerabilities targeted, we are trying to perceive the most exciting and most practical combination of those vectors. Examples analyzed in the case studies are those who are the most explored and researched, both by the press and authorities. Sources for research are not only publicized data and information released to the press by formal authorities, but also their public reports, as well as publicly available judgments. Cases were selected from different locations all over the world and in connections with different attacks vectors, from prison items delivered to war field engagement (especially different questions arise from different levels of engagement, that is, national, regional (EU level), and even the United Nations. The UN is not so thoroughly analyzed here but only mentioned. Therefore, war zone engagement is not the main focus of this paper, but engagement in the crime and criminal activities.

2.1 Case studies

Case study 1: (Case studies 1, 4-6 are extracts sourced from Markarian & Staniforth, 2020): Organized drug smuggling *via* drone into prisons (UK) - During 2017, eight members of an organized criminal gang that used drones to airlift and unlawfully deploy £500,000 (Great Britain Pounds Sterling) worth of drugs into prisons were sentenced on jail terms ranging from three to ten years. Over two years, drone pilots, drivers and lookouts had conspired with prisoners to smuggle drugs into seven jails,

[1] One of the biggest stories of the year related to drone threats happened when drones attacked the world's largest oil processing facility in Saudi Arabia. This attack exposed the fragility of a significant global critical infrastructure. The attacks knocked out about 5% of global oil production immediately. Twenty-five drones and missiles were used in the attack that forced the kingdom to shut down half of its oil production (Reid, 2019, September 20).

including Her Majesty's Prison and Probation Service (HMP) Birmingham (BBC News 1, 2018, October, 26) and HMP Liverpool. Remote-controlled drones, equipped with a fishing line and hooks, were flown to cell windows where inmates, in various communication contacts with the pilot, used tools such as extendable broom handles to retrieve smuggled items. During the investigation, eleven drones, including some which had crashed, were seized during police inquiries into flights that also targeted HMP Wymott in Lancashire, HMP Hewell in Worcestershire (Wirral Globe, 2018, October 26), HMP Risley in Cheshire, and HMP Oakwood and HMP Featherstone in Staffordshire. Craig Hickinbottom, a 35-year-old prison inmate at HMP Featherstone in Staffordshire, and later HMP Hewell in Worcestershire, directed the large-scale and persistent operation from behind bars, for which he was sentenced to seven years imprisonment after admitting four counts of conspiring to bring contraband into prison, and conspiracy to supply psychoactive substances. Drone-pilot Mervyn Foster received a sentence of six years and eight months for his part in the enterprise. At a later trial of a further 13 conspirators connected to the drone-enabled supply of drugs in prisons, they were sentenced to prison terms from six months to ten years. The prosecution case also provided evidence that the increase of illegal drugs and the unauthorized mobile phone use in prisons had caused heightened levels of violence, an increase in self-harm and deaths, as well as allowing witness intimidation and illegal financial transactions.

Case study 2: Italian critical events: *Secondigliano* – April 27, 2020, at about 22:00 at Secondigliano Prison (Naples), a suspicious buzzing was heard, and a staggering drone spotted that was about to crash into the courtyard of a prison ward. The drone was broken, and officers of the Penitentiary Police seized it the same evening. It carried six mobile phones, four of the micro type and two smartphones, all correctly functioning, some SIMs and chargers (Pupia TV, 2020, April 28).

Taranto – October 25 2018, a thirty-two-year-old convicted in Bari, then detained in Taranto, and his organized crime group had planned to carry psychoactive substances and cell phones inside the local prison. The plan failed because the drone got stuck in a nylon thread used to lay the underwear, carrying about 280 grams of hashish, 2.5 grams of cocaine, two tiny cell phones, and the USB cable to recharge them (Pipoli, 2018, October 25). The drone had been driven from surrounding terrain by a woman who, in an attempt to make it as invisible as possible, had deactivated the flashing optical sensors, and was driven to the place of delivery through the flame of a lighter that the prisoner had lit from the window of his prison chamber. Because of this, and due to a gust of wind, the woman had not noticed the cable that caused the drone to fall inside the prison yard. The contraband substance was contained in some sausages and, along with mobile phones, was directed to a room on the third floor of the surrounding house, in the maximum-security sector. Meanwhile, fireworks exploded in the area adjacent to the prison presumably to distract the attention of prison officers. All of the mentioned means were used to conceal and distract the attention of those looking so that the actual operation could succeed, and go unnoticed.

Venice – on July 2016, a tourist was trying to get aerial footage of the city, where drones are banned, but lost control of the mini aircraft, that accidentally landed near a group of police officers patrolling the area. Luckily, the 2kg drone fell in an area where there were not many people, and nobody was injured. Nevertheless, the perpetrator was prosecuted and fined for that activity (The Local, 2016, July 6).

Case study 3: Drone deliveries in Greek prisons - in Greece, on February 2, a small quadcopter drone sailed over a prison's high barbed wire fence, which is located at the city of Trikala, to make a delivery to prisoners. The prison's security personnel successfully intercepted the attempt to smuggle two packages/contraband containing mobile phones and related paraphernalia into Trikala prison using drones, Athens-Macedonian News Agency (ANA) sources revealed. The unknown perpetrators attempted to fly the drones over the prison and drop the packages during the night, but they were immediately discovered by prison staff. The items confiscated included phones, sim cards, chargers, illicit drugs. Prison staff subsequently also searched the prison cells, leading to the arrest of three inmates (The National Herald, 2020, March 2).

Case study 4: Mexican cartel drug smuggling border drone operations (United States) – During August 2017, US border patrol officers intercepted a drone-borne drug shipment when an agent in San Diego County heard the buzzing of a remotely-controlled aircraft coming over the border fence and contacted his fellow agents, who then found and arrested a 25-year-old man carrying 13 pounds of methamphetamine he had removed from the drone. Despite the best efforts of the United States law enforcement agencies to prevent the smuggling of drugs by drones through US-Mexico borders, which has included the establishment of specialized units to detect and combat all aerial drug smuggling, the use of drones as mules to transport illegal drugs continues to rise.

Case study 5: Critical national infrastructure rogue drone incursions in France (France 24, 2018, July 3). During 2014, France's state-run power firm Électricité de France (EDF) announced that unidentified drones had flown over seven nuclear powers plants during October, leading it to file a complaint with the police. EDF revealed that the uncrewed aircraft did not harm the safety or the operation of the power plants, stating that the first drone was spotted on October 5 above a plant in deconstruction in eastern Creys-Malville. More drone activity followed at other nuclear power sites across the country between October 13 and October 20, usually at night or early in the morning (The Guardian, 2014, October 30). Greenpeace, whose activists have in the past staged protests at nuclear plants in France, denied any involvement in the mysterious pilotless flight activity. However, the environmental group expressed concern at the apparent evidence of "a large-scale operation", noting that drone activity was detected at four sites on the same day on October 19 – at Bugey in the east, Gravelines and Chooz in the north and Nogent-sur-Seine in north-central France. During July 2018, a Superman-shaped drone crashed into the EDF's Bugey nuclear plant in Bugey, near Lyon. Greenpeace said it had flown the drone - piloted by one of its activists - into the no-fly zone around utility EDF's Bugey nuclear plant and then crashed it against the wall of the plant's spent-fuel pool building to demonstrate its vulnerability to outside attack. Greenpeace stated that action demonstrated: "The extreme vulnerability of French nuclear structures designed in the 70s and not equipped for external attacks."

Case study 6: Terrorist and insurgent use of drones as Improvised Explosive Devices (IEDs) (Iraq) Islamic State (IS) first used drones to film suicide car bomb attacks which militants posted online as part of their propaganda campaigns to raise awareness of their cause and to recruit and radicalize others to their ranks. As their use of drone technology advanced, American and Iraqi military commanders revealed that Islamic State drones were employed to support direct action on the battlefield (Hambling, 2016, December 9). Throughout the summer of 2016, American troops in Iraq and Syria reported seeing small drones hovering near their bases and around the front lines in northern Iraq. The commercially available drones were being deployed for surveillance and reconnaissance by IS who also called on their followers to implant small store-bought drones with grenades or other explosives, directing recruits to use them to launch attacks on crowded places at the Rio Olympic Games. During 2016, Kurdish forces seized dozens of drones used by IS. One captured drone was thought to be able to provide intelligence on IS drone operations. Nevertheless, as they were taking it apart, the small Improvised Explosive Device (IED) contained inside detonated, killing two Kurdish fighters in what is believed to be the first time IS has successfully used a drone with explosives to kill troops on the battlefield. The drone IED attack has been recently followed by further IS drone operations, prompting American commanders in Iraq to issue a warning to forces fighting the group to treat any type of small flying aircraft as a potential explosive device (Schmidt & Scmitt, 2016, October 11). For some American military analysts and drone experts, the incidents confirmed their view that military authorities were slow to anticipate the terrorist adaption of drones as weapons. Militants of illegal armed groups attempted to stage a drone attack on the Russian airbase at Syria's Hmeymim on 22.12.2019 (TASS, 2019, December, 12).

Several swarm drones were driven to attack airfield and war technologies – military warplanes and helicopters. In this area, it is crucial to acknowledge that there has been a wide variety of UAVs implementation in counter-terrorism and counter-smuggling area. Usage of drones – UAVs in monitoring armed groups and trafficking of arms and to evaluate environmental challenges, including assessing damages from natural disasters (Better World Campaign (2013).

Case study 7: Drone provocation on the football (soccer) match between Albania and Serbia in Tirana on Euro 2016 qualifier match held on October 2014 (BBC News 2, 2014, October, 15). This case is specific in the engagement of a few new tactics and techniques very resistant to police activities. It involved diplomatic services, untouchable due to diplomatic immunity, political influence, nationalistic background, as well as country and state agencies not being ready for such kind of attacks. Attacks were deliberately planned, and executed in order to create panic, riots and demonstrations. Carefully planning on the exploitation of rage instigated by drone bearing nationalistic and extremist symbols and maps and focusing on people mass hysteric reaction. In the end, it hit directly at the target – Serbian team was ruled out with defeat by official result 3:0 for Albania team, and the whole systematic activity was directed to produce that.

3. FINDINGS

Within these case studies, specificities could be observed through attack vectors, specialities' and targeted, exploited or attacked vulnerabilities. The intention is to present in one line all concerns, attack vectors and vulnerabilities that should be observed when thinking about proactive actions and preventive activities. Although these case studies did not have the same cultural, micro-social and linguistic similarities, and not even the same object of targeting; still, they have adequate similarities that can be used in abstracting the vectors while thinking about preventive countermeasures. The list of those is as follows:

Table 1. *Attack vectors - MOs – Vulnerabilities*

Attack vectors	Specialities'	Vulnerabilities attacked
Prison attack	Drugs smuggling, phone smuggling,	Inability to prevent drone attack, inability to detect and track drone, inability to intercept and engage with the drone in a manner to dismantle it or interrupt the attack

Prison attack	Drugs smuggling, phone smuggling, phone accessories smuggling, using detection avoidance techniques and measures, flashlight guidance to the target, concealing items in sausages, usage of fireworks in order to distract the attention of the authorities.	Inability to prevent drone attack, inability to detect and track drone, inability to intercept and engage with the drone in a manner to dismantle it or interrupt the attack, inability to detect and intercept various anti-detection techniques and activities,
Prison attack	Drugs smuggling, phone smuggling, SIM cards smuggling, phone accessories smuggling,	Anti-drone measures not present
Prison attack	Mobile driven UAV	Anti-drone utilities and measures absent
Cross border smuggling	Over the fence hovering, drop-off activity,	International Multi – agencies measures taken (creation of specialized units to detect and combat all aerial drug smuggling) but also exploited in order to probe the strength of those and find the weak links.
Nuclear power plant attack	Flying in the no-fly zone around utility EDF's Bugey nuclear plant and deliberately crashing against the wall of the building of spent nuclear fuel	Exploiting protective measures – in order to show their extreme vulnerabilities.
Terrorist and insurgent's usage	Support in direct action on the battlefield, Improvised Explosive Devices (IEDs) even as booby-trapped devices, drone operations	Using warfare tactics and exploiting not readiness of the targets, military authorities were slow to anticipate the terrorist adaption of drones as weapons.
Sports activity	Diplomatic services, untouchable for diplomatic immunity, political influence, nationalistic background, targeted	

	national pride, xenophobic line of people reactions	

The above listed provides possibilities to think about different perpetrators and their thoughts on perpetrating a crime. Regarding the prisons – **most often attacked** are inner premises and means of defending the inner circle of the prison, and prisoners. Cross border smuggling is very similar in attack vectors with prison attacks in a manner of attack – the target is to cross a particular position in order to drop-off or deliver something. The following attack vectors are more warfare oriented. They are discussed here because of their inventive and already experienced attacks, and they should be further researched because of their possible future implementation in the real criminal surrounding. Nuclear power plant attack is very similar to the terrorist and insurgent exploits – in those the primary purpose is achieving some damage which could have a significant impact on the panic, terrorizing much more audiences than targeted aims. Cyber-attacks are oriented on the network intrusions, enabled by the drones, industrial exploitation. **Ways of attack – MOs**, used in the attacks are following: various means and methods of smuggling, detection avoidance techniques, flashlight guidance, means of concealment, means of distracting defences, over the fence hovering, different drop-off activities, flying in a no-fly zone of a nuclear power plant, crashing on the facility of spent nuclear fuel – nuclear waste facility, support at the warzone for the direct action on the battlefield, usage of improvised explosive devices, booby-traps for those investigating it, network intrusion exploits, new categories of cybercrime infection vectors, rogue access points, and infectious carriers of malware, remote exploits of different devices, swiping of targets data. Specific MOs also include diplomatic services that are untouchable because of diplomatic immunity, political influence, nationalistic background, targeted national pride, xenophobic line of people reactions. **Targeted vulnerabilities** are mostly as following: anti-drone measures and utilities with an inability to prevent drone attack, and to detect and track drone, or to intercept and engage with the drone in a manner to dismantle it or interrupt the attack, and inability to detect and intercept various anti-detection techniques and activities. The very interesting vulnerability addressed is multi-agency deployed measures exploitation in order to test their strength and find weak links; this is followed with deliberately probing of defence capabilities of a nuclear power plant by international non-governmental organizations, in order to expose extreme vulnerabilities. Warfare activities more than other best show the vulnerabilities in fighting different opponents with significant ingeniousness, and also a weakness of preventive measures taken. Cybercrime infection vectors are attacking insufficient security measures, confidence in employees and employers, BYOD (Bring Your Own Device) trust exploiting, Bluetooth wireless and other protocols, software, zero-day software and control vulnerabilities.

4. DISCUSSION

In the literature, most of the Serbian researchers are addressing the issues of drone use from the point of observing the manner of their use, but not from a perspective of the protection from the drone attacks. In the regional context, many of our colleagues are researching the issue of UAS (even under the term drones) (Boštjan, 2016) and in the majority of cases, they are considering measures that should be taken within law enforcement agencies and their usability. The world literature review is tackling the issue of their societal and technological role (see Crotty, 2014; Finn & Wright, 2012; Perritt & Sprague, 2015; Sandbrook, 2015; Završnik, 2016a, 2016b on multiple roles that drones have in contemporary life), and further there is research on the law enforcement agencies roles and anti-forensic activities in the area of UAV implementation.

Forensic and intelligence aspects are also areas of a vast variety of research and elaboration (John & Maguire, 2007; Newburn & Reiner, 2012), but not much research is provided regarding the anti-forensic and counter-intelligence aspects. In an attempt to think about these measures and activities, it should be acknowledged that the use of UAVs by law enforcement agencies is intended to substantially enhance prevention by increasing their visibility and decreasing reaction time. Therefore, increasing prevention considers the visible presence of the UAVs in the area, but does not consider counter-drone (UAVs) capabilities. From that point of view, the following aspects should be taken into account (Skylock 2020; AARTOS, 2020): anti-drone jammers for countering any UAV threat, and drone detection systems deployed to detect and prepare for any UAV related threat and counter – UAV systems deployed to detect, prepare for and mitigate threats posed by unauthorized UAVs (like Skyforce or Dronelock – from Skylock or AARTOS Generation 6). This is important because of the displayed attack vectors and vulnerabilities attacked, and they were mentioned within presented case studies. Those can be targeted, and risk can be mitigated through the deployment of counter-drone measures and systems in order to prevent drone attacks by criminals. However, this is not the only aspect of risk mitigation measures. For correctional or penitentiary facilities (prisons) or other kinds of defended or guarded facilities or objects, it is of great importance to use existing systems – like security systems, or systems of physical security measures already deployed on the site and connect them with newest ones. In that way, mitigation measures will provide a compact and uniform system in order to counteract UAVs.

From the other aspect of the problem, there is a need to address anti-forensic activities of criminals and forensic activities of the state agencies in order to gather, secure and preserve the evidence existing in and on UAVs, since they represent digital crime scene with enormous digital capabilities – GPS tracking evidence, photos, images, videos gathered, source code of firmware but also DIY devices source code. Anti-forensic activities used by criminals to counter forensic investigations include various online available tools, and they are not limited only to software leaning tools, even hardware tools are used. The latest and most severe anti-forensic tool includes hardware booby trapping of the UAV with explosive, in order to attack forensic staff or to destroy evidence (UAV). Therefore, the aspect of organizing effective and efficient defence from those attack vectors, and defending and solving of vulnerabilities must be discussed in the area of deployment of such system that is capable of countering all threats efficiently and effectively. That means that it must include a not only area of coverage, but must do it efficiently with countermeasures such as signals intelligence (SIGINT), communications intelligence (COMINT) and human intelligence (HUMINT) (Rohde &Schwarz, 2020; Steele, 2010). This should be done in a manner that creates a robust system capable of detecting and repelling such attacks and uses activities in order to gather evidence and prosecute masterminds and activists behind them. In that context, there are numerous commercial solutions available online, as well as in defence industries, and that should be considered when deciding how and what to deploy in countering such attacks. Areas of application should not be only limited to prison and penitentiary facilities, objects guarded and secured. Nevertheless, they should be further expanded on state agencies objects and facilities, and even human capacities in the field. This is very justifiable because of the presented attack vectors and vulnerabilities that can be exploited by perpetrators in order to attack law enforcement agencies.

5. CONCLUSION

Law enforcement agencies need to be prepared, equipped and fitted for actual threats of drone attacks. Whether it is an object that is protected, object area or subjects within the object, there is evident need to have a system for protection, early warning and reconning system. This system is capable of detection, apprehension, neutralization of the threat, and forensic system covering the evidence gathering. These systems have to fulfil all security and forensically sound standards. This means that they need to interconnect digital, security, and forensic measures in order to protect, repel and neutralize all threats covered by attack vectors, MOs of perpetrators and vulnerabilities targeted that are presented in our case studies. An essential part of these systems is a human factor, and these systems need to include various sensors and devices (including anti-AUV device) that cover and analyze signals in the filed.

Furthermore, the whole system should be cyber resilient to the attack vectors described earlier in the text. To be regionally friendly, we could say that it is a matter of science fiction to think about such a system to be engaged in the area of Balkans. There are few reasons for this, such as its price for purchase and application, dependency to the different manufacturers and "spheres of influence" excluding NATO countries on the Balkans. Therefore, in a manner of covering real vulnerabilities and attack vectors, in our opinion, the objective approach must consider real capabilities of the countries in the Balkan region. Finally, bearing in mind findings from our case studies analysis, that means that particular, sectoral and partial approach should be deployed.

REFERENCES

1. AARTOS (2020). Systems and versions. https://drone-detection-system.com/aartos-dds/systems-versions/
2. BBC News 1 (2018, October, 26). Gang who flew drones carrying drugs in prison jailed. https://www.bbc.com/news/uk-england-45980560
3. BBC News 2 (2014, October, 15). Serbia condemns drone flag stunt at Albania match. https://www.bbc.com/news/world-europe-29627615
4. Better World Campaign (2013). The UN's use of Unmanned Aerial Vehicles in the Democratic Republic of the Congo: US Support and Potential Foreign Policy Advantages. http://betterworldcampaign.org/assets/pdf/bwc-white-paper-the-uns-use-of-uavs-in-th-drc-may-2013.pdf
5. Boštjan, S. (2016). Drones in (Slovene) criminal investigation. Criminalistic Theory and Practice, 3(5), 7-25.
6. Clarke, R. (2014). Understanding the drone epidemic. Computer Law & Security Review, 30(3), 230–246.
7. Crotty, S. (2014). The aerial dragnet: A drone-ing need for fourth amendment change. Valparaiso University Law Review, 49(1), 219– 265.
8. Cvijic, S. Klingenberg, L. Goxho, D. Knight, E. (2019). Armed drones in Europe. Editor Ros Taylor. Open Society, European Policy Institute, Open Society Foundations.
9. Finn, R. L., & Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. Computer Law & Security Review, 28(2), 184–194.
10. France 24 (2018, July, 3). Greenpeace activists 'crash' drone into french nuclear plant. https://www.france24.com/en/20180703-greenpeace-activists-crash-drone-french-nuclear-plant
11. Hambling, D. (2016, December 9). How Islamic State is using consumer drones. BBC [Online] https://www.bbc.com/future/article/20161208-how-is-is-using-consumer-drones

12. INTERPOL (2019). Modus Operandi, Illegal delivery of contraband to prison systems using unmanned aerial systems (UAS). Fine No. 2019 / 15826-1.
13. John, T., & Maguire, M. (2007). Criminal intelligence and the National Intelligence Model. In: T. Newburn, T. Williamson, & A. Wright (Eds.), Handbook of Criminal Investigation (pp. 199–225). Willan Publishing Ltd.
14. Markarian, G., & Staniforth, A. (2020). Counter-Unmanned Aerial Vehicle Handbook. Artech House.
15. Newburn, T., & Reiner, R. (2012). Policing and the Police. In: M. Maguire, R. Morgan, & R. Reiner (Eds.), The Oxford handbook of criminology (pp. 806–837). Oxford University Press.
16. Perritt Jr., H. H., & Sprague, E. O. (2015). Drones. Vanderbilt Journal of Entertainment & Technology Law, 17(3), 673–749.
17. Pipoli, R. (2018, October 25). Italy police: Drone tried to deliver 2 phones, drugs to prisoner. UPI. https://www.upi.com/Top_News/World-News/2018/10/25/Italy-police-Drone-tried-to-deliver-2-phones-drugs-to-prisoner/8171540485684/
18. Pupia TV (2020, April 28). Napoli, intercettato drone su carcere Secondigliano con sei cellulari per detenuti. https://www.pupia.tv/2020/04/canali/cronaca/napoli-intercettato-drone-su-carcere-secondigliano-con-sei-cellulari-per-detenuti/471936
19. Rani, C., Modares, H., Sriram, R., Mikluski, D. & Lewis, F. L. (2015). Security of unmanned aerial vehicle systems against cyber-physical attacks. Journal of Defense Modeling & Simulation 13(3), 1-12.
20. Reid, D. (2019, September 20). Saudi Armaco reveals attack damage at oil production plants. CNBC. https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html
21. Rohde & Schwarz (2020). Wide area reconnaissance (COMINT). https://www.rohde-schwarz.com/hu/solutions/aerospace-defense-security/defense/signal-intelligence-electronic-warfare/strategic-sigint/wide-area-reconnaissance-comint-/wide-area-reconnaissance-comint-overview_233130.html
22. Sandbrook, C. (2015). The social implications of using drones for biodiversity conservation. Ambio, 44(S4), 636–647.
23. Schmidt, M. S. & Scmitt, E. (2016, October 11). Pentagon confronts a new threat from ISIS: Exploding drones. New York Times [Online] https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html?_.
24. Skylock (2020). Comprehensive anti-drone systems. https://www.skylock1.com/

25. Staniforth, A. (2012, February 13). Countering-Drones: A global challenge. Defence IQ. https://www.defenceiq.com/cyber-defence-and-security/articles/countering-drones-an-evolving-cybersecurity-requirement
26. Steele, R. D. (2010). Advancing Strategic Thought Series- Human Intelligence: All humans, all minds, all the time. https://permanent.access.gpo.gov/lps122746/PDF%20version/PUB991.pdf
27. TASS (2019, December 12). Militants attempt drone attack on Russian airbase at Syria's Hmeymim. https://tass.com/world/1102767
28. The National Herald (2020, March, 2). Drones used in attempt to smuggle phones into Greek prison. https://www.thenationalherald.com/archive_general_news_greece/arthro/drones_used_in_attempt_to_smuggle_phones_into_greek_prison-256165/
29. The Guardian (2014, October 30). Drones spotted over seven French nuclear sites, says EDF. https://www.theguardian.com/environment/2014/oct/30/drones-spotted-over-seven-french-nuclear-sites-says-edf
30. The Local (2016, July 6). Tourist fines after drone crashes in St. Mark's Square. https://www.thelocal.it/20160706/tourist-fined-after-drone-crashes-in-st-marks-square-venice
31. Wirral Globe (2018, October 26). Seven jailed for using drones to airlift drugs into prison. https://www.wirralglobe.co.uk/news/national/17010190.seven-jailed-using-drones-airlift-drugs-prisons/

About the authors

Zvonimir Ivanović, associate professor at the University of Criminal Investigation and Police Studies in Belgrade.
E-mail: zvonimir.ivanovic@kpu.edu.rs.
Valentina Baić, associate professor at the University of Criminal Investigation and Police Studies in Belgrade.
E-mail: valentina.baic@kpu.edu.rs.