

NEW THREATS IN SECURITY

NOVÉ HROZBY V OBLASTI BEZPEČNOSTNEJ OCHRANY

Natália Kundráthová
Air Transport Department
University of Žilina
Univerzitná 8215/1
010 26 Žilina
nkundrathova@gmail.com

Karol Lysina
Air Transport Department
University of Žilina
Univerzitná 8215/1
010 26 Žilina
Karol.Lysina@nsat.sk

Abstract

The article is focused on modern threats in the department of security. The urge to address this issue is due to growing occurrence of unmanned aerial vehicles (UAV) all around the world. The operation of these vehicles is also closely linked to incidents that threaten security, but the most serious are increasing numbers of incidents connected to operation of UAV. For correct processing, it is very important to define the basic concepts and facts related to the topic of UAV. Safety and security in general, are inseparable parts of air transport. Taking into account the constant development of aviation technology, especially in the department of UAV, it is necessary to know the emerging threats and pitfalls associated with the operation of UAV. The following chapters define in more detail the causes of incidents. Later on, we get to know various methods of detection and protection connected to operation of UAV using the comparative method. Key part of our paper is being formed by the analysis of current regulatory framework at European and national level. The result is a proposal for new legislation that could and also should be implemented in national regulations. All things considered, such legislation must meet all attributes necessary for the safe operation of UAV and protection against their illegal use.

Keywords

UAV, threat, legislation

1. Úvod

Pojem *bezpilotný prostriedok*, *bezpilotné lietadlo* alebo *UAV* si za posledné desaťročie osvojilo mnoho ľudí po celom svete. Prostriedky, ktoré spájajú moderné princípy elektroniky a umelej inteligencie si našli svojich milovníkov, ale aj odporcov. Bezpilotné prostriedky, ktoré boli sprvu používané najmä na vojenské účely rýchlo uplatnili svoje využitie aj v civilných sférach. Jednoduchá dostupnosť týchto prostriedkov zvyšuje ich atraktivitu pre rôzne skupiny ľudí. Často je vybavenie takéhoto prostriedku kamerou najväčším lákadlom pre nadšencov, ale aj podniky. Významné postavenie majú bezpilotné lietadlá v službách polície a záchranných službách, ako aj službách činných v trestnom konaní. Vo všeobecnosti môžeme konštatovať, že za nárast výskytu bezpilotných prostriedkov môže práve ich schopnosť odpovedať na potreby ľudí. Nedávno sa však začalo čoraz viac objavovať škodlivé používanie dronov. Ich použitie viedlo k vzniku mnohých problémov v oblasti bezpečnosti, ochrany a súkromia, ktoré sa prejavili rôznymi kybernetickými útokmi, hrozbami a výzvami, ktoré sú uvedené a vysvetlené v tejto práci. Vzhľadom na fakt, že bezpilotné prostriedky sú súčasťou leteckej dopravy, podliehajú istým reguláciám a pri ich používaní je nutné dodržiavať stanovené pravidlá. Najväčšie riziko spojené s používaním bezpilotných prostriedkov vo vzdušnom priestore je ich stret s lietadlom. V tejto súvislosti boli navrhnuté rôzne bezpečnostné návrhy a odporúčania, aby sa zabezpečila ochrana pred UAV.

2. Bezpečnosť v letectve

Ak existuje odvetvie, ktoré má tendenciu ocitnúť sa na fronte globálnych bezpečnostných a kybernetických rizík, je to letectvo. Napriek tomu, že letecká doprava predstavuje najbezpečnejší spôsob cestovania, vďaka svojim rozsiahlym medzinárodným regulačným rámcom majú letecké udalosti mimoriadny vplyv na povedomie verejnosti. Od nedávnych útokov až po tie, ktoré siahajú do ďalekej minulosti, sú hrôzostrašné správy silnejšie ako upokojujúce štatistiky. Rozvíjajúce sa technológie, meniaci sa charakter vojny a rastúca závislosť na kybernetickom priemysle menia povahu hrozieb. Týmto spôsobom zároveň vytvárajú tlak na priemysel, aby zabezpečil udržanie svojej úrovne bezpečnosti, pričom sa predpokladá, že počet cestujúcich v leteckej doprave sa bude stále zvyšovať.

3. Bezpečnostné hrozby

Bezpečnostných hrozieb v letectve môže byť niekoľko. Druhý hrozieb pramenia z niekoľkých faktorov, ktoré si určite zaslúžia dôkladnú analýzu. Existuje veľa „chorobných príznakov“, ktoré hrozia prekazením akýchkoľvek pokusov o dosiahnutie globálnej bezpečnosti. Tieto príznaky predstavujú hrozby pre globálnu bezpečnosť a zahŕňajú širokú škálu trendov, medzi ktorými je medzinárodný terorizmus iba jedným z mnohých. Napriek zjavným prekážkam, ktoré hrozby a zraniteľnosti predstavujú, v súčasnosti existuje zásadnejší problém, ktorý vylučuje splnenie medzinárodnej bezpečnosti – neexistuje spôsob, ako dosiahnuť úplnú medzinárodnú bezpečnosť. Nové bezpečnostné hrozby

vznikajú zo dňa na deň. Existuje však jedna oblasť medzinárodnej bezpečnosti, v ktorej hrozby, zraniteľnosti a procesy prevencie boli katalogizované, a tou je bezpečnostná ochrana civilného letectva. V dvadsiatom storočí došlo k exponenciálnemu tempu technologických zmien. Ľudia, ktorí disponujú takouto technológiou naďalej osídľujú planétu spôsobmi, ktoré vytvárajú nové a zvyšujú existujúce demografické tlaky. Našu kolektívnu budúcnosť budú čoraz viac formovať naše kroky a postoje v súčasnosti. Všetky tieto príznaky zmeny sa opierajú o súčasnú éru. Pokus o dôsledné a statické vymedzenie pojmov ako je terorizmus, nie je v takom dynamickom prostredí úplne bezproblémový. Podľa Paula Wilkinsona je terorizmus „osobitnou formou politického násillia, nie politickou filozofiou alebo hnutím. Je to vopred dané a jeho cieľom je vytvoriť atmosféru extrémneho strachu. Je zameraná na širšie publikum alebo cieľ než na bezprostredné obete násillia. A to neodmysliteľne zahŕňa útoky na náhodné a symbolické ciele vrátane civilného obyvateľstva, a preto terorizmus predstavuje útok na ľudské práva.“[1]

Na základe záznamov z histórie bezpečnostnej ochrany letectva možno konštatovať, že pri mnohých príležitostiach boli pokusy o sabotáž úspešné, čo zdôrazňuje mylnosť existujúcich bezpečnostných systémov leteckých spoločností. Napriek rôznym protiopatreniam stále existuje potenciál úspešnej sabotáže, a zároveň existuje veľa spôsobov ako preniknúť do bezpečnostného systému leteckej spoločnosti. Aj keď je hrozba teroristického útoku pre civilné letectvo relatívne nízka, sabotáž lietadla vo vzduchu predstavuje najtraumatickejšiu a najviditeľnejšiu tvár medzinárodného terorizmu. Tento samotný aspekt by mal byť dostatočným stimulom na zabezpečenie úplného vykonávania akýchkoľvek medzinárodných právnych predpisov. Letecké predpisy radu L predstavujú implementáciu štandardov a odporúčaných postupov Medzinárodnej organizácie civilného letectva – ICAO. Zmluvné štáty organizácie ICAO sa zaväzujú plniť štandardy/opporúčania pre štát. Ak sa členské štáty rozhodnú plniť tieto odporúčania, je potrebné plniť ich v plnom rozsahu. V prípade, že sa rozhodnú neplniť nich, musia oznámiť ICAO-u odchýlku. Najrozšírenejšie druhy bezpečnostných hrozieb.

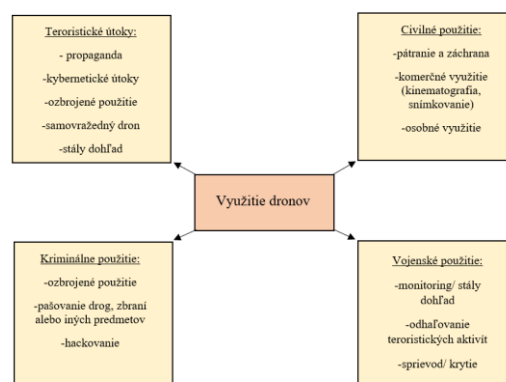
4. Hrozby 21. storočia

Svet bol nedávno svedkom významného nárastu počtu použitých UAV a globálnym neustálym nárastom dopytu po ich viacúčelových aplikáciách. Prenikavý aspekt týchto dronov je spôsobený ich schopnosťou odpovedať na potreby ľudí. UAV poskytujú používateľom *vtáčie oko*, ktoré je možné aktivovať a používať takmer kedykoľvek a kdekoľvek. Nedávno sa však medzi zločincami aj kybernetickými zločincami začalo objavovať škodlivé používanie UAV. Pravdepodobnosť a frekvencia takýchto útokov je veľmi vysoká a ich dopad môže byť veľmi nebezpečný, nakoľko má ničivé účinky. Preto je veľmi nevyhnutná potreba detekčných, ochranných a preventívnych opatrení. „Zločinci“ využívajú UAV na dosiahnutie svojich škodlivých cieľov. Technologický pokrok umožňuje ľahkú manipuláciu s týmito zariadeniami a dajú sa tak použiť na rôzne útoky. Vďaka bezdrôtovej komunikácii sú UAV zraniteľné voči rôznym útokom, vrátane únosov UAV. Tieto útoky môžu mať drastické účinky, najmä obchodné a nekomerčné straty. Od skorého zavedenia bezpilotných prostriedkov sa na UAV hľadí ako na zariadenia spojené s hlavnými bezpečnostnými problémami, čo z nich robí legitímne ciele, ktoré sú náchylné na

rôzne typy útokov. Ďalej ich možno použiť ako potenciálny vektor útoku pre používateľov so zlými úmyslami. Zvyšuje sa tak šanca na nový asymetrický typ vojny.

5. Zneužívanie UAV na protiprávne činy

Drony môžu nájsť svoje všestranné využitie v rôznych doménach. Napriek tomu, že vieme tieto zariadenia použiť v náš prospech, úmerne vzrastá popularita zneužívania týchto prostriedkov na vykonávanie kriminálnych alebo teroristických aktivít. V súlade so vzrastajúcou popularitou využívania dronov práve na tieto účely existujú nové výzvy spojené s niekoľkými otázkami bezpečnosti a bezpečnostnej ochrany.



Obrázok 1: Využitie dronov. Zdroj Vlastné spracovanie podľa Jean-Paul, et al., *Security analysis of drones systems: Attacks, limitations, and recommendations*, in Elsevier Public Health Emergency Collection 2020, doi: 10.1016/j.iot.2020.100218]

6. UAV verzus letecká doprava

Je nevyhnutné, aby sme skonštatovali, že počet incidentov medzi UAV a lietadlami má stúpajúcu tendenciu. V tomto prípade je nevyhnutné riešiť porušenia bezpečnosti a súkromia na najvyššej vnútroštátnej úrovni. To zahŕňa prijatie veľmi prísnych postupov, ktoré obmedzujú schopnosť dronu zhromažďovať obrázky a nahrávať videá ľudí a nehnuteľností bez povoleného súhlasu.

Hlavné existujúce obmedzenia z hľadiska bezpečnosti dronov:

1. Dostupnosť na trhu – dostupnosť dronov na všetkých trhoch z nich urobila vhodnú voľbu pre teroristov a zločincov na vykonávanie nelegálnych aktivít. Potrebne sú ďalšie bezpečnostné kontroly a inšpekčné požiadavky, najmä pre majiteľov pokročilých typov dronov.
2. Slabé zabezpečenie – výrobcovia by mali brať bezpečnosť ako kľúčovú súčasť pri vývoji ľubovoľného firmvéru, hardvéru a aplikácií. Osvedčeným postupom na prevenciu väčšiny bezpečnostných útokov je preto zabezpečenie už „od plienok“.
3. Videnie/vyhnutie sa – operátori dronov majú obmedzené zobrazenie vzdušného priestoru, pri ovládaní dronu z obrazovky (napríklad počítača) je náročné spozorovať okolité lietadlá, prípadne zabrániť ich stretu.

4. Oneskorené reakcie – pokiaľ nie je dron riadený plne autonómne, kontrola zariadenia je závislá na signáloch prenášaných z riadiacej stanice.
5. Slabé politiky – prijatie politik autorizácie a autentifikácie by malo byť prísne, aby sa zabránilo neoprávneným subjektom v prístupe do systému dronu, a taktiež aby sa zabránilo možným vnútorným hrozbám.
6. Izolácia v reálnom čase – vo veľkej miere sa prijíma a používa implementácia mechanizmov, ktoré okamžite odpoja/vypnú dron, akonáhle sa zistí bezpečnostná hrozba. Takto sa minimalizujú možné škody a zabráni sa zraneniam alebo úmrtiam. Rovnako dôležitá je potreba mať na akomkoľvek drone nainštalovaný príkazový čip návratu na základňu.
7. Fáza obmedzeného testovania – drony musia prejsť dôkladným testovaním, aby vyhodnotili zodpovedajúcu úroveň ohrozenia, keď sa dostanú do nesprávnych rúk. Preto aplikácie ovládajúce drony musia byť testované – aby sa zabránilo akejkoľvek bezpečnostnej chybe, ktorú by mohli útočníci zneužiť vo svoj prospech.
8. Obmedzené možnosti forenzej činnosti – napriek tomu, že forenzné drony nie sú v súčasnosti prioritou, účinné a ľahké forenzné nástroje sú potrebné pri zisťovaní, lokalizácii, hľadaní a uchovávaní digitálnych dôkazov spolu s ich odpovedajúcimi zdrojmi.
9. Slabá úroveň ochrany – systémy ochrany dronov by mali obsahovať tri hlavné fázy (detekcia, oprava a ochrana).
10. Slabá schéma autentifikácie – boli odhalené spôsoby ako možno drony ľahko uniesť a zachytiť prostredníctvom procesu narušenia autentifikácie. Preto sa na vylepšenie tohto nedostatku odporúča vylepšiť viacfaktorovú autentifikačnú schému.

7. Incidenty

Od roku 2015 sa na celom svete dramaticky zvýšil počet incidentov UAV týkajúcich sa bezpečnosti a bezpečnostnej ochrany (v blízkosti letísk alebo lietadiel samotných). Hlavným problémom dronov operujúcich v blízkosti letísk a vo vzdušnom priestore je nebezpečenstvo kolízie medzi lietadlami s letovou posádkou a UAV. Napriek tomu, že niektoré lacnejšie verzie UAV nie sú schopné vykonávať dlhý let, sofistikovanejšie modely takýchto zariadení sú schopné stráviť vo vzduchu aj niekoľko hodín. To znamená, že keď sa v blízkosti letiska alebo jeho zariadení objaví dron, môže byť z bezpečnostných dôvodov letisko uzavreté. Najväčšie riziko, ktoré bezpilotné lietadlá predstavujú pre lietadlá s letovou posádkou, je ich nasatie do motorov, ktorého účinky majú devastačný charakter. To samozrejme predstavuje ďalšie náklady, prípadné meškania letov, „poškodenie mena“ letiska a podobne. Práve z tohto dôvodu sme sa rozhodli spomenúť v tejto práci niekoľko závažných incidentov, ktoré sa stali za posledné roky. Jedná sa o incidenty, ktoré mali vážny dopad na bezpečnosť.

8. „Anti-drone“/ „counter-drone“ systémy

Zvyšujúci sa počet výskytu dronov v zakázaných oblastiach, v blízkosti letísk, a samozrejme, aj neustále sa zvyšujúci počet incidentov „vo vzduchu“ viedol k narastajúcim obavám o

bezpečnosť a bezpečnostnú ochranu. Práve z tohto dôvodu vznikli technológie Anti-Drone/Counter-Drone (C-UAS). Takéto technológie sa môžu používať na letiskách. Spravidla sú rozdelené do troch hlavných kategórií: preventívne opatrenia, detekčné senzory a technológie a protipatrenia na zmiernenie protiprávnych činov.

9. Útoky UAV na kritické infraštruktúry letísk

Špionážne letecké telekomunikačné systémy zamerané na zhromažďovanie informácií sú prvým krokom pri prieskume pri príprave útoku. Operátor môže špehovať akýkoľvek cieľ bez toho, aby bol detegovaný – vďaka schopnosti manévrovať a zhromažďovať informácie na veľkú vzdialenosť. Pripojená kamera UAV je schopná snímať údaje, získavať vysokokvalitný materiál (fotografie, video) a naspäť odosielať zhromaždené informácie s cieľom pripraviť útok [2]. Niekoľko štúdií [3, 4] dokázalo, že drony vybavené rádiovými vysielačmi/prijímačmi sa dajú použiť na získavanie nezašifrovaných informácií z rádiových prenosov alebo dokonca na vytvorenie vysokofrekvenčného šumu alebo telekomunikačného rušenia. Okrem toho môžu drony spôsobiť značné škody napríklad na dislokovaných alebo personálom neobsadených zariadeniach, ktoré podporujú letecké telekomunikačné systémy alebo inú kritickú infraštruktúru [2]. Najviac dotknutými takýmito útokmi sú CNS (Communication, Navigation and Surveillance) systémy. Tieto systémy zahŕňajú: letecké telekomunikačné systémy, navigačné systémy a prehľadové systémy. Systémy CNS môžu pri napadnutí stratiť integritu a svoju prevádzkovú účinnosť. To má zároveň za následok spomalenie toku premávky a služieb ATM. Navyše sa môžu vyskytnúť meškania alebo dokonca zrušené lety. Zároveň môže dôjsť k strate materiálu/neposkytnutiu služieb a to predstavuje vyvodenie právnej zodpovednosti voči iným poskytovateľom/letiskovým zariadeniam. Ďalším z mnohých populárnych útokov je útok na bezdrôtové siete a IT infraštruktúru letiska. Práve operačné stredisko letiska, ktoré je podporované centrálnou informačnou sieťou, slúži ako interakčný bod pre všetky zainteresované strany letiska. Riadi procesy od prevádzkových častí letiska, systémov riadenia letu až po operácie na zemi a systémy pozemnej obsluhy [5]. Operačné stredisko riadi všetku výmenu údajov a zdieľanie informácií, ktoré sa získavajú zo senzorov a iných inteligentných zariadení, a kvôli rozšíreným hraniciam letiska komunikujú prostredníctvom bezdrôtových sietí LAN alebo bezdrôtových sietí s rozsiahlymi oblasťami. Drony vybavené bezdrôtovými anténami a softvérom môžu využívať výhody komunikácie prístupového bodu, a takýmto spôsobom vystopovať a zachytávať dáta odoslané medzi bezdrôtovo pripojenými zariadeniami.

Aj keď existuje množstvo technologických riešení C-UAS, neexistujú žiadne medzinárodné štandardy pre správny návrh a používanie takýchto systémov práve na letiskách a ich kritických infraštruktúrach. Podľa FAA (Federal Aviation Administration) by letiská usilujúce sa o nasadenie detekčných systémov UAS mali poznať riziká spojené s nasadením týchto systémov [6]. Vzdušný priestor by mal byť primerane chránený. Najmä v koncových riadených oblastiach a riadených okrskoch letiska je nevyhnutné vylúčiť akékoľvek rušenie iných dôležitých rádiových signálov – systémy pre pristátie podľa prístrojov (ILS), prehľadové radary, samotná rádiová komunikácia a podobne. Rušenie je navyše v mnohých krajinách nezákonné, a rušenie ako také nemôže byť na mnohých letiskách použité, a to najmä z bezpečnostných

dôvodov. Rovnako rušenie GPS/GLONASS signálov v blízkosti letiska sa považuje za nebezpečné aj pre civilné letectvo, pretože mnohé lietadlá sa v súčasnosti pri vzlete a pristátí spoliehajú práve na satelitnú navigáciu.

10. Právne predpisy v Európskej únii

Pre zabezpečenie efektívnej a bezpečnej prevádzky vo vzdušnom priestore je nutné, aby boli vytvorené predpisy a postupy, ktoré sú schopné regulovať všetky oprávnenia a zákazy spojené s prevádzkou bezpilotných prostriedkov. Európska únia zriadila Agentúru Európskej únie pre bezpečnosť letectva - *European Union Aviation Safety Agency* (EASA), ktorej primárnym cieľom je koordinovať postup štátov Európskej únie v oblasti civilného letectva. Na žiadosť Európskej komisie, členských štátov Európskej únie a ďalších zainteresovaných strán, vypracovala agentúra EASA dokument, ktorý definuje tri kategórie bezpečnostných požiadaviek na UAV, a to konkrétne: otvorená kategória, špecifická kategória a certifikovaná kategória.

V roku 2019 bolo vydané vykonávacie nariadenie Komisie (EÚ) 2019/947 o pravidlách a postupoch prevádzky bezpilotných lietadiel. Toto nariadenie komplexne zjednocuje pravidlá používania UAS v celej Európskej únii. S účinnosťou od 1. januára 2021 EASA štandardizovala predpisy týkajúce sa UAV vo všetkých svojich členských štátoch. Nový regulačný rámec nahrádza existujúce nariadenia, ktoré predtým prijali jednotlivé členské štáty. Okrem 28 členských štátov prijali nové predpisy o bezpilotných lietadlách aj Island, Švajčiarsko, Lichtenštajnsko a Nórsko.

Zodpovednosť za hybridné hrozby prevzala aj Európska únia. Aby si mohla plniť úlohu poskytovateľa bezpečnosti, mala by sa zamerať najmä na vzájomnú prepojenosť medzi vonkajšou a vnútornou bezpečnosťou. Definície hybridných hrozieb sú rôzne, a aby bolo možné reagovať na premenlivú povahu týchto hrozieb, musia zostať flexibilné. Pod pojmom hybridná hrozba si môžeme predstaviť akúkoľvek činnosť, ktorá je vykonávaná so zámerom poškodiť cieľ ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni (napríklad ovplyvňovanie verejnej mienky v kybernetickom priestore). Nástrojmi týchto hrozieb môžu byť masívne dezinformačné kampane a využívanie sociálnych sietí na propagandu alebo radikalizáciu/nábor/priame ovládanie priaznivcov. Hlavnú zodpovednosť za hybridné hrozby nesú samotné členské štáty, pretože jednotlivé slabiny sú väčšinou špecifické pre jednotlivé krajiny. Mnoho členských štátov Európskej únie sa však stretáva aj so spoločnými hrozbami, ktorých cieľom môžu byť aj cezhraničné siete alebo infraštruktúry.

11. Právne predpisy na Slovensku

Pravidlá lietania s bezpilotnými prostriedkami na území Slovenskej republiky sú vymedzené v zákone č. 143/1998 Z. z. o civilnom letectve (letecký zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, podľa ktorého *lietadlá spôsobilé lietať bez pilota môžu vykonávať lety vo vzdušnom priestore len za podmienok, ktoré prihlasujú na bezpečnosť letu a ktoré určí rozhodnutím Dopravný úrad po dohode s ministerstvom obrany*. [53]. Letecký zákon však bližšie nešpecifikuje prevádzku bezpilotných prostriedkov, preto bolo

Dopravným úradom vydané Rozhodnutie č. 2/2019 zo dňa 14. novembra 2019, ktorým sa určujú podmienky vykonania letu lietadlom spôsobilým lietať bez pilota a vyhlasuje zákaz vykonania určených kategórií lietadiel vo vzdušnom priestore Slovenskej republiky [7].

Na základe tohto rozhodnutia je prevádzka bezpilotných prostriedkov rozdelená do dvoch skupín (označenie A a B). Dovoľená minimálna vzdialenosť od vzťažného bodu letiska, v ktorej je možné vykonať let s takýmto bezpilotným lietadlom, je 5,6 km v maximálnej dovolenej výške od zeme 30 metrov. Pre hmotnostné kategórie C0- C2 je dovoľená minimálna vzdialenosť od vzťažného bodu letiska 3,7 km v maximálnej dovolenej výške od zeme 30 metrov. Pokiaľ je let vykonávaný v riadenom vzdušnom priestore, je potrebné vyplniť žiadosť a kontaktovať riadenie letovej prevádzky, najneskôr 24 hodín pred vykonaním letu. V žiadosti o povolenie na vykonanie letu bezpilotným prostriedkom v riadenom okrsku letiska (CTR) je operátor povinný uviesť základné informácie týkajúce sa plánovaného letu. Operátor je zároveň povinný oboznámiť príslušné stanovište riadenia letovej prevádzky o vykonaní letu s časovým predstihom minimálne 15 minút. Riadenie letovej prevádzky je oprávnené vykonávať zmeny týkajúce sa plánovania letu - určenie iného priestoru pre vykonanie letu, určenie maximálnej výšky letu, určenie času vzletu a pristátia. V prípade ukončenia letu lietadla schopného lietať bez pilota je povinnosťou operátora oboznámiť o prerušení/ukončení letu príslušné stanovište riadenia letovej prevádzky [7]. Na základe nariadenia Komisie (EÚ) 2019/947 . existujú aj výnimky, ktoré si môžu členské štáty upraviť samostatne. Ide konkrétne o minimálny vek pre lietanie s UAS, či pravidlá pre lietanie v riadenom vzdušnom priestore.

11.1. Súčasná situácia v Slovenskej republike

Všeobecné podmienky pre prevádzku bezpilotných prostriedkov sú jasne vymedzené a každý prevádzkovateľ by ich mal ovládať. Okrem rôznych rozdelení a technických vymedzení je však nevyhnutné dbať pri prevádzke na základné práva. V rozhodnutí Dopravného úradu č. 2/2019 zo 14. novembra 2019 je dané: „Let bezpilotným lietadlom sa vykoná tak, aby nebola ohrozená bezpečnosť iných lietadiel, osôb a majetku na zemi a aby sa zabezpečila ochrana životného prostredia pred hlukom a emisiami zo znečisťujúcich látok z bezpilotného lietadla.“ Neodmysliteľnou súčasťou prevádzky s bezpilotnými prostriedkami je ochrana súkromia. Dodržiavanie pravidiel ochrany osobných údajov, ktoré sú stanovené v smernici 95/46/ES o ochrane údajov alebo v rámcovom rozhodnutí č. 2008/977, sú nevyhnutné. Ďalšou oblasťou je ochrana osôb a majetku. Majetkové právo upravuje rôzne formy vlastníctva nehnuteľností a osobných vecí. Pod pojmom majetok možno rozumieť osobné vlastníctvo, vrátane duševného. Súčasná legislatívna úprava Slovenskej republiky však nijak bližšie nešpecifikuje následné kroky, ktoré možno podniknúť pri ohrození bezpečnosti iných lietadiel, osôb alebo majetku na zemi, spôsobené prevádzkou bezpilotných prostriedkov.

11.2. Oprávnenie bezpečnostných zložiek

Čo súčasná legislatíva špecifikuje, je zásah bezpečnostných zložiek, konkrétne Vojenskej polície, pokiaľ sa jedná o zabezpečenie obrany a bezpečnosti štátu. Zakázaná je činnosť bezpilotného prostriedku v chránenom vojenskom

objekte, a to do výšky 120 metrov nad zemou, ktorý je označený zákazom fotografovania. Operátor bezpilotného prostriedku sa pri porušení takéhoto zákazu dopúšťa priestupku. V ustanovení § 20d zákona č. 124/1992 Zb. o Vojenskej polícii v znení neskorších predpisov je uvedené, cit.: „vojenský policajt je pri zaistovaní ochrany chráneného vojenského objektu oprávnený prerušiť činnosť lietadla spôsobilého lietať bez pilota na mieste, kde je to zakázané“. Zároveň „o použití donucovacieho prostriedku prerušenia činnosti lietadla spôsobilého lietať bez pilota rozhoduje vojenský policajt podľa konkrétnej situácie tak, aby použitý donucovací prostriedok a intenzita jeho použitia neboli zjavne neprimerané zakázanej činnosti. Vojenský policajt upustí od použitia donucovacieho prostriedku, ak by prerušením činnosti lietadla spôsobilého lietať bez pilota mohlo dôjsť k ohrozeniu života alebo zdravia“ [8]. Vojenský policajt je oprávnený použiť zbraň iba ak nie je možné prerušiť činnosť bezpilotného prostriedku na mieste, kde je takáto činnosť zakázaná, iným spôsobom. Pod pojmom zbraň sa rozumie strelná zbraň, bodná zbraň alebo zbraň hromadnej účinnosti. Použitíu zbrane však predchádza výzva vojenského policajta od upustenia vykonávania protiprávneho činu s výstrahou, že bude použitá zbraň. Zároveň je policajt povinný vykonať varovný výstrel. Výstraha a varovný výstrel môže absentovať len ak je vojenský policajt napadnutý alebo ak je ohrozený život alebo zdravie inej osoby/vec neznesie odklad. Poslednou výnimkou je situácia, kedy vojenský policajt nie je schopný lokalizovať osobu, ktorá ovláda bezpilotný prostriedok a ide o použitie zbrane podľa oseku 1 písm. i).

Zároveň zákon č. 4/2001 Z. z. o Zbore väzenskej a justičnej stráže v znení neskorších predpisov hovorí, že v objektoch, ktoré sú chránené zborom, je zakázaná činnosť bezpilotných prostriedkov, ak nebola takáto činnosť vopred písomne odsúhlasená generálnym riaditeľom. Taktiež tento zákon oprávňuje príslušníka zboru vykonať potrebné úkony na zabránenie činnosti takéhoto prostriedku, ak by jeho činnosťou mohol byť zmarený alebo inak ohrozený účel výkonu väzby, účel výkonu trestu odňatia slobody, účel výkonu detencie¹¹ alebo bezpečnosť chránených objektov. Podľa ustanovenia § 13c je príslušník zboru oprávnený vykonať tieto úkony najmä rušičkou, špeciálnymi donucovacími prostriedkami alebo strelnou zbraňou [9] [12].

Na základe zistených informácií a analýzy zákonov platných v Slovenskej republike môžeme konštatovať, že súčasná legislatívna úprava týkajúca sa oprávnenia prerušiť činnosť bezpilotných prostriedkov oprávňuje na vykonanie takéhoto aktu len dve vyššie spomenuté bezpečnostné zložky, a to konkrétne Vojenskú políciu a príslušníkov Zboru väzenskej a justičnej stráže. Toto oprávnenie samozrejme podlieha rôznym podmienkam, ktoré je nutné splniť.

12. Návrh

Legislatíva v oblasti civilného letectva si vyžaduje neustálu zmenu a aktualizáciu. Letecká doprava predstavuje dynamické odvetvie, preto je veľmi často nutné okrem zmien dopĺňať aj právne predpisy o nové oblasti a požiadavky. Samotné UAV už dávno nie sú vo vzdušnom priestore ničím výnimočným. Práve naopak, vo veľkej miere sú UAV súčasťou vzdušného priestoru, a je na čase, aby sa orgány začali zaoberať tým, ako ich prevádzka ovplyvňuje bezpečnosť, bezpečnostnú ochranu a riadenie letovej prevádzky. Vzhľadom na fakt, že technológia v

oblasti bezpilotných prostriedkov napreduje raketovým tempom, treba predpokladať, že nové hrozby budú taktiež rásť raketovým tempom. Mnoho krajín už podniká veľké kroky v implementácii a obrane proti bezpilotným lietadlám (USA, Spojené kráľovstvo, Belgicko, Bulharsko, Poľsko a mnoho ďalších). Na spomínané letiská boli nainštalované špičkové detekčné systémy s cieľom zvýšiť bezpečnosť a bezpečnostnú ochranu v oblasti letiska, a zároveň „bojovať“ proti neoprávnenej činnosti UAV. Podľa mnohých odborníkov je však akýkoľvek úmyselný útok schopný tieto detekčné systémy obísť. Najdôležitejšia otázka, ktorú si však treba položiť, znie: Stačí sa riadiť tým, čo nám hovorí Ústava? Naozaj „Každý môže konať čo nie je zákonom zakázané, a nikoho nemožno nútiť, aby konal niečo, čo zákon neukladá? [10]“. Stačí sa riadiť tým, že prevádzkovateľ môže konať všetko, čo mu zákon nezakazuje, alebo je potrebná reaktívna činnosť a riešenie problematiky aktívnej ochrany letísk?

Pokiaľ by Slovenská republika nasledovala vzor zo zahraničia a implementovala by na letiská detekčné systémy, ktoré sú schopné nie len detegovať, ale aj zneškodniť bezpilotné prostriedky, bude musieť vytvoriť k tomuto zákroku príslušnú legislatívnu úpravu - prevádzkovatelia civilných letísk nie sú policajno-bezpečnostné zložky, ktoré majú takéto oprávnenie, ale právnické osoby alebo fyzické osoby. Nie na všetkých letiskách je, ani medzinárodných, stála prítomnosť príslušníkov Policajného zboru, pričom ide o príslušníkov hraničnej a cudzineckej polície. Zamestnanci ochrany letiska sú držiteľmi preukazu odbornej spôsobilosti podľa zákona č. 473/2005 o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti) v znení neskorších predpisov, pričom konajú na základe oprávnení vymedzených najmä v tomto a leteckom zákone.

Neraz sa stretávame s rôznymi názormi, ktoré sú spojené so zneškodňovaním bezpilotných prostriedkov napríklad v oblasti letiska. Predstavuje ohrozenie širšej verejnosti v dôsledku zneškodnenia bezpilotného prostriedku správne riešenie? Neohrozuje takáto činnosť ľudí viac ako samotné UAV? Ideálne by bolo, keby sa podarilo UAV eliminovať už na hranici priestoru letiska. Pre zločincov je rovnako ako vzdušný priestor atraktívny aj priestor letiska samotného (letová časť, terminál, a podobne). Páchatelia sa na tieto miesta zameriavajú z dôvodu veľkej koncentrácie prítomných ľudí – ich cieľom je spôsobiť čo najväčšie škody na životoch a majetku. Uplatnením jednoduchého princípu - keď raz niečo vzlietlo na oblohu, musí z nej aj dopadnúť naspäť na zem – sa nám vynára ďalšia otázka. Je horšie, ak zostrelené UAV dopadne na zem a pri páde poškodí lietadlo, alebo fakt, že výbušné zariadenie pripevnené na bezpilotnom prostriedku môže zabiť celú posádku lietadla? Riskujeme, že vystrelené náboje doletia na rôzne miesta, no nie je to „menšie zlo“, než nechať vyhodiť do vzduchu celé lietadlo s niekoľkými osobami na palube, resp. dopustiť zrážku drona (nasatie do motora) s lietadlom najmä pri vzlete?

Práve kvôli týmto nezodpovedaným otázkam by legislatívna úprava nemala upravovať „len“ oprávnenie zneškodniť bezpilotný prostriedok, ale mala by zároveň vyriešiť túto „morálnu dilemu“. Ako sme už v práci spomenuli, súčasná platná legislatíva nám špecifikuje zásah bezpečnostných zložiek, a to konkrétne Vojenskú políciu a Zboru väzenskej a justičnej stráže, pokiaľ sa jedná o zabezpečenie obrany a bezpečnosti štátu. Podľa nášho názoru je potrebné takto oprávniť aj iné osoby, ktoré síce nepredstavujú bezpečnostné zložky SR, ale z

rovnakých dôvodov (zabezpečenie obrany a bezpečnosti štátu alebo ochrany zdravia a života osôb) takéto oprávnenie potrebujú.

Kľúčovým riešením problematiky hrozieb spojených s používaním bezpilotných prostriedkov je byť vždy o krok vpred. Rýchlo rozvíjajúce sa možnosti zneužívania bezpilotných prostriedkov nemôžu predbehnúť príslušné orgány v možnostiach reagovať.

13. Záver

Predmetom tohto článku bola analýza novodobých hrozieb v oblasti bezpečnostnej ochrany [11]. Po tom, ako sme si predstavili hrozby, ktoré sú v súčasnej modernej spoločnosti najvýznamnejšie, sme sa zamerali práve na bezpilotné prostriedky. Bepilotné prostriedky sa tešia obrovskej popularite, no zároveň predstavujú pre leteckú dopravu obrovskú hrozbu, pokiaľ nie sú používané správne, respektíve s dobrým úmyslom. Nárast incidentov stúpa priamoúmerne s nárastom výskytu týchto zariadení vo vzduchu. Ako sme sa mohli v článku dozvedieť, v súčasnosti existuje mnoho účinných systémov a zariadení, ktoré sú schopné detegovať bezpilotné prostriedky. Čo však absentuje, je právna úprava, ktorá by oprávňovala prevádzkovateľov letísk na zásah voči bezpilotným prostriedkom, ktoré ohrozujú bezpečnosť alebo sa nachádzajú v zakázaných zónach. Je veľmi dôležité, aby orgány s normotvornou právomocou v oblasti civilného letectva reflektovali na súčasnú situáciu a dynamický charakter tejto oblasti a reagovali potrebnou zmenou a doplnením príslušných právnych predpisov.

Referencie

- [1] WILKINSON, P.: How to combat the reign of terror, New Statesman 2.august 1996, s.12
- [2] Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies [online]. Dostupné na internete: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349857/#B38-sensors-20-03537>
- [3] Security, Privacy, and Safety Aspects of Civilian Drones: A Survey [online]. Dostupné na internete: https://www.researchgate.net/publication/313329204_Security_Privacy_and_Safety_Aspects_of_Civilian_Drones_A_Survey
- [4] Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls [online]. Dostupné na internete: <https://www.mdpi.com/1424-8220/19/1/19>
- [5] Addressing airport cyber- security (Final report) [online]. Dostupné na internete: https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber_security_Full_0.pdf
- [6] FAA Letter from FAA Office of Airports on Guidance on Use of Counter UAS Systems at Airports [online]. Dostupné na internete: https://www.faa.gov/airports/airport_safety/media/attachment-1-counter-uas-airport-sponsor-letter-july-2018.pdf
- [7] Dopravný úrad. *Rozhodnutie č. 2/2019 ktorým sa určujú podmienky vykonania letu lietadlom spôsobilým lietať bez pilota a vyhlasuje zákaz vykonania určených kategórií lietadiel vo vzdušnom priestore Slovenskej republiky* 2019. [online]. Dostupné na internete: <http://nsat.sk/wp-content/uploads/2019/11/R2-2019.pdf>
- [8] Zákon č. 124/1992 Zb. o Vojenskej polícii [online]. Dostupné na internete: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/124/>
- [9] Zákon 4/2001 Z. z. Zákon o Zbore väzenskej a justičnej stráže [online]. Dostupné na internete: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/4/>
- [10] 460/1992 Zb. Ústava Slovenskej republiky [online]. Dostupné na internete: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/460/>
- [11] Galierikova, A., Materna, M., Sosedova, J. 2018. Analysis of risks in aviation. Transport Means - Proceedings of the International Conference, 2018, 2018-October, pp. 1427–1431.
- [12] Novák Sedlačková, A., Kandra, B. 2015. Medzinárodnoprávna úprava ochrany civilného letectva pred činmi protiprávneho zasahovania. Bratislava : DOLIS, 2015. - 132 s., ilustr. - ISBN 978-80-8181-028-2.