REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK
32. évfolyam (2020) 3. szám 135–141. • DOI: 10.32560/rk.2020.3.11

Dudás Zoltán[1] – Ujvári Bence[2]

A drónelhárítás módszerei és lehetőségei

A szerzők bemutatják a távirányítású repülőgépes rendszerek jogszerűtlen alkalmazásából eredő veszélyforrásokat. Valós példákon keresztül illusztrálják a drónok rosszindulatú használatának veszélyeit. A lehetséges védekezési módok önmagukban nem elegendőek az ilyen felhasználásból adódó kockázatok lecsökkentésére, ám a rendelkezésre álló technológiák kombinálásával funkció és hatás szerint tagolt hatékony védelmi struktúra hozható létre.

Kulcsszavak: *drón, drónelhárítás, veszélyforrás, UAS*[3]

Methods and Feasibilites of Drone Protection

The authors work on the hazards arising from the illegal use of remotely piloted aircraft systems. Through real-life examples they illustrate the perils caused by malicious use of drones. The possible protection methods alone are not sufficient to reduce the risks of such a use, but by combining the available technologies, an effective protection structure divided by function and effect can be built.

Keywords: *drone, drone protection, hazard, UAS*

1. Bevezetés

A távirányítású légi járművek alkalmazásának elterjedése nem csupán előnyökkel, hanem negatív következményekkel is jár. Az eszközök könnyű hozzáférhetősége és ellenőrizetlen felhasználása újszerű veszélyforrást jelent, amelyre számtalan példa hozható fel. Az egyik komoly kihívás mellett, amely az UAS-működésnek a hagyományos rendszerekbe történő biztonságos integrálása érdekében folyik, egye inkább előkerül a rosszindulatú felhasználással szembeni fellépés technikai, módszertani és alkalmazási vetületeinek vizsgálata.

[1] Adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Repülésirányító és Repülőhajózó Tanszék, e-mail: dudas.zoltan@uni-nke.hu, ORCID: https://orcid.org/0000-0002-8682-884X
[2] BSc-hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Repülésirányító és Repülő-hajózó Tanszék, Állami légijármű-vezető szakirány, e-mail: ujvari.b97@gmail.com, ORCID: https://orcid.org/0000-0002-5685-4393
[3] UAS: Unmanned Aircraft System – a pilóta nélküli légi járművön kívül a működését biztosító környezetet is magában foglalja.

2. A drónok rosszindulatú használatából adódó veszélyforrások

A drónok terjedése a világban újfajta veszélyforrások megjelenésével jár együtt. A távirányítású repülőgépek és helikopterek alkalmazása jó kézben hasznot hoz, rossz kézben pedig a biztonságunkra fenyegetést jelent. Ékes példája mindennek az az eset, amikor 2013 szeptemberében Angela Merkel német kancellár kampánysorozatának drezdai állomásán egy UAV átrepült a tömeg felett, és a kancellár lábai előtt csapódott a földbe.[4] 2015 januárjában pedig szintén egy távirányítású eszköz repült be és zuhant le a Fehér Ház területén. Mindez úgy történt, hogy a Fehér Ház radarja semmit nem jelzett a történtekből, mivel sokkal nagyobb méretű fenyegetések – repülőgépek, rakéták – észlelésére volt beállítva.[5] Drámaibb következményekkel járhatott volna az a támadás, amelynek során 2015 áprilisában a Sendai atomerőmű újraindítása ellen tiltakozó tüntető a japán miniszterelnök irodájának tetejére röptetett egy drónt, céziummal teli műanyag palackkal a fedélzetén.[6]

A fenti példák élesen mutatnak rá, mennyire sokrétű veszélyforrást jelenthetnek a szabálysértő, változatos konstrukcióban megjelenő UAV-k. Méretük változó, a legkisebb néhány centiméteres is lehet, a legnagyobb pedig a 40 m-es szárnyfesztávval rendelkező Northrop Grumman RQ-4 Global Hawk. Méretüktől függetlenül nagy felbontású, jó minőségű kamerákkal lehetnek felszerelve, ezáltal szinte észrevehetetlen módon képesek felvételeket készíteni. A pilóta nélküli légi járművek fénykép- és videókészítő képességét kihasználva, illetéktelenek akár személyi azonosítókhoz, jelszavakhoz, PIN-kódokhoz, bankszámla-információkhoz férhetnek hozzá.

A katonai szférában a haditechnikai eszközök állapotáról, mennyiségéről, típusokról, egységek elhelyezkedéséről, csapatmozgásokról, rejtett figyelők helyzetéről, védelmi rendszerek működéséről, járőrözési útvonalakról és eljárásokról szerezhetnek információkat, ez pedig komoly biztonsági kockázatot jelent. Erőszakos módon felhasználva őket – például polgári vagy katonai szállítógépekkel összeütköztetve – emberi életeket, haditechnikai eszközöket veszélyeztethetnek, veszélybe sodorva a műveletek sikerét. Lakott terület felett egy fegyvereket és robbanóanyagokat szállító katonai légi járművet érő dróntámadás a civil lakosság életére, a világörökség részét képező objektumokra és földrajzi nevezetességekre, valamint a növény- és állatvilágra jelent kockázatot. Mivel az állami célú légi közlekedés során katonai és állami vezetők szállítására is sor kerülhet, egy ilyen jellegű támadással az állam működésében kiemelt fontosságú személyek életüket veszthetik. A kritikus infrastruktúrák kiemelt célpontok lehetnek egy dróntámadás során. Példaként érdemes említenünk egy 2019 szeptemberében történt eseményt, amikor az Irán által támogatott húti felkelő hadsereg dróntámadásokat vezetett az Aramco olajvállalat olajmezői és feldolgozó üzeme ellen. A támadás következményeként a szaúdi olajtermelés napi 5 millió hordóval csökkent, amely a királyság olajtermelésének felét, azaz a világpiaci termelés 5%-át jelenti. A kőolaj árfolyama évtizedek óta nem látott mértékben emelkedett: a Brent árfolyama közel 20%-kal nőtt.[7] Az eset jól mutatja, hogy a drónok rosszindulatú alkalmazása milyen károkat képes okozni egy kiemelt

[4] Sean Gallagher: *German chancellor's drone "attack" shows the threat of weaponized UAVs.* Ars Technika, 2013.
[5] Michael D. Shear – Michael S. Schmidt: White House Drone Crash Described as a U.S. Worker's Drunken Lark. *The New York Times,* 2015.
[6] Will Ripley: *Drone with radioactive material found on Japanese Prime Minister's roof.* CNN, 2015.
[7] Michael Safi – Graeme Wearden: Everything you need to know about the Saudi Arabia oil attacks. *The Guardian,* 2019.

fontosságú létesítményben, közvetve pedig a világpiac működésében. Biztonsági szakértők az eset megtörténte előtt úgy gondolták, az ilyen kritikus infrastruktúrák védelme biztosítva van, azonban a támadás rámutatott, hogy a világ energiaellátó létesítményei sebezhetőbbek, mint hitték, és célpontnak tekinthetők.

Amint az alábbi példából kitűnik, nem feltétlenül szükséges a drónokat fegyverekkel felszerelni ahhoz, hogy kárt tudjanak okozni. Bizonyos esetekben, a légtérben való puszta jelenlétük is kockázatot jelent, amely képes megbénítani a teljes infrastruktúrát. 2018 decemberében több alkalommal hajtottak végre drónrepüléseket a londoni Gatwick repülőtér légterében, aminek következtében a légi forgalmat fel kellett függeszteni. A több mint 40 berepülés között akadt olyan eset, amikor a pilóta nélküli légi járművet 25–30 m távolságban reptették egy Airbus A320 típusú repülőgéptől, ezért annak vészhelyzeti kitérő manővert kellett végrehajtania.[8] Az incidens összesen megközelítőleg ezer járat törlését vagy átirányítását eredményezte, 140 ezer utast érintett, nagy veszteségeket okozva a légitársaságoknak, a repülőtérnek, valamint az utasoknak.[9]

A jogtalanul reptetett drónok nem csak a polgári repülést akadályozhatják, a katonai, rendvédelmi és mentőhelikopterek munkáját is képesek lassítani szabálysértő berepülésekkel. A 2010-es vörösiszap-katasztrófa során a Magyar Honvédség helikoptereinek és pilótáinak köszönhetik sokan az életüket. Ebben az esetben kritikus jelentőségű volt, hogy a pilóták időben kórházba tudták szállítani az érintetteket, végzetes kimenetele lehetett volna, ha drónokkal megzavarják a műveleteket. A nagy teljesítményű, professzionális pilóta nélküli eszközök képesek a helikopterekkel egy magasságon repülni. Ez kifejezetten egy vészhelyzet, katasztrófa, sebesültszállítás, bűnüldözési helyzet közben jelent komoly kockázatot. Emberi életek múlhatnak azon, hogy egy mentőhelikopternek útjába kerül-e egy drón, ezáltal késleltetve a helyszínre vagy a kórházba való érkezését. Erdőtüzek terjedhetnek tovább, ipari és természeti katasztrófák súlyossága nőhet, ha a katonai helikopterek nem tudják megfelelően ellátni feladataikat a zavarások miatt.

Miért vonzó lehetőség a drónok jogtalan alkalmazása? Jevgenyij Mjasznyikov összefoglalta az UAV-k terroristák számára nyújtott előnyeit:

- Szárazföldről nehezen elérhető célpontok támadásának lehetősége.
- Nagy kiterjedésű területek támadásának lehetősége, a maximális halálozási arány elérésével (kifejezetten biológiai és vegyi fegyverek városi alkalmazásával).
- A támadások előkészítésének fedettsége, valamint az UAV indítási pontjának flexibilis megválaszthatósága.
- Nagy hatótávolság elérése megfelelő pontossággal, relatív olcsón és egyre széleskörűbben elérhető technológiával.
- A légvédelmi eszközök gyenge hatékonysága az alacsonyan repülő UAV-k ellen.
- Költséghatékonyság a repülőgépekkel és ballisztikus rakétákkal szemben.
- Komoly pszichológiai hatás elérésének lehetősége az emberek megfélemlítésével és a politikusokra gyakorolt nyomással.[10]

[8] PA Media: Passenger plane in near-miss with drone at Gatwick airport. *The Guardian,* 2019.
[9] Airportal.hu: *Drónok miatt bénult meg a légiforgalom a London–Gatwick repülőtéren.* 2018.
[10] Eugene Miasnikov: *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects.* Moscow, Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology, 2015.

Patrick Stevens, az Interpol terrorelhárításért felelős igazgatója szerint a kritikus infrastruktúrákat és könnyű célpontokat drónnal támadó terroristacsoportok jelentette növekvő fenyegetés szükségessé teszi a rendvédelmi szervek közösségén belüli globális információ- és tapasztalatcseréjét a drónok elleni védekezésben. Ugyanakkor a drónok a bűnüldözésben való alkalmazása számos előnnyel is jár, hiszen információkkal (sebesség, magasság, GPS-adatok, ujjlenyomat, DNS) és bizonyítékokkal szolgálnak a bűnözőkről.[11] A 2018-as Formula 1-es évad silverstone-i versenyén a DJI cég AeroScope nevű dróndetektáló eszköze a verseny kvalifikációs szakaszában sikeresen detektált egy illetéktelen drónt a pálya határain belül. A rendezvény biztonságáért felelős személyzet információt kapott a drónt irányító személy valós idejű helyzetéről, akik ezáltal képesek voltak megtenni a verseny biztosításához szükséges ellenlépéseket.[12] A példa jól mutatja, egy C-UAS[13]-rendszer felderítő képessége mennyire hatékony tud lenni a bűnüldözésben. Ezt a lehetőséget integrálva a helyi rendvédelmi szervek, terrorelhárítási egységek bűnmegelőzési rendszerébe még hatékonyabb munkát, valamint jövőbe mutató elemzéseket lehet elérni.

2.1. Lehetséges ellentevékenységek

A drónelhárító rendszereket angolul Counter-UAS vagy C-UAS-rendszereknek nevezzük. Napjainkban megoszlani látszik az iparág, egyes gyártó cégek az UAV-k blokkolását rádiófrekvenciás (RF) zavarókkal, jelhamisítással *(spoofing)* és elektronikai interferenciával képzelik, mások azonban a drónok mechanikus semlegesítésében látják a megoldást.[14]

A C-UAS-rendszerek piaca növekszik, jelenleg 235 termék van bejegyezve 155 cégtől, 33 különböző országból. Ezek közül néhány már használatban van, mások még fejlesztés alatt állnak. A 235 termékből 88 csak felderítésre, 80 csak semlegesítésre alkalmas, 67 pedig mindkettő feladatot képes ellátni. A rendszerek nagy része földi telepítésű, emellett vannak kézből alkalmazhatók és olyanok is, amelyek egy drónplatformról üzemelnek. Természetesen ezek kombinációi is léteznek. A legnépszerűbb detektálási módszerek a radar, rádiófrekvenciás (RF-) eszköz, elektrooptikai (EO-) és infravörös (IR-) szenzorok használata. Semlegesítés terén a legelterjedtebb az RF vagy GNSS[15] zavarás *(jamming)*.[16]

Jamming, azaz zavarás alatt azt az ellentevékenységet értjük, amikor a drón és az operátora közötti kommunikációt blokkolva akadályozzuk az UAV további működését. Egyes drónok ilyen esetekben visszatérnek az utolsó koordinátára, ahol még kaptak jelet, esetleg egészen vissza a kiindulási pontig, másfajta drónok a földre zuhannak. A spoofing módszer abban tér el az előzőtől, hogy az eljárás során egy harmadik félnek is lehetősége van átvenni az irányítást a drón fölött. Tim Bean, a Fortem Technologies vezérigazgatója szerint ezek az eljárások azonban csak bizonyos körülmények között alkalmazhatók. Szerinte a drónpilóták 30–40%-a már nem rádiófrekvencia alapján irányítja az eszközöket, hanem útvonalpontok használatával.

[11] Interpol: *Drone technology: security threats and benefits for police focus of Interpol forum.* 2018.
[12] COPTRZ: *COPTRZ DDaaS – Drone Detection as a Service.* 2019.
[13] C-UAS: Counter-Unmanned Aircraft System – olyan rendszerek megnevezése, melyek a pilóta nélküli légi járművek detektálására és feltartóztatására lettek kifejlesztve.
[14] Talal Husseini: *When drones are used maliciously, can anyone stop them?* Airforce Technology, 2019.
[15] GNSS: Global Navigation Satellite System – globális műholdas navigációs rendszer.
[16] Arthur Holland Michel: *Counter-Drone Systems.* Center for the Study of the Drone at Bard College, 2018.

Ebben az esetben az RF-zavarók hatástalanok.[17] Ilyenkor továbbra is alkalmazhatók a GNSS-zavarók, továbbá a mechanikus hatástalanítás elvén működő rendszerek.

A fentieken túl a drón fizikai megsemmisítése is szóba jöhet. Egyes C-UAS-rendszerek nagy erejű lézersugarat használnak, mások földről kivetett hálóval kapják el a drónokat, illetve léteznek olyanok is, amelyek egy másik drónt lőnek ki nagy sebességgel, ami a levegőből támad egy hálócsapdát alkalmazva. Ezeknek a rendszereknek azonban sok esetben az államok jogszabályi háttere jelent akadályt. Ilyen esetre példa a Rafael Advanced Defense Systems Ltd. által gyártott rendszer, amelyből a brit szabályozás alapján el kellett távolítani a lézeres megsemmisítő képességet, ezáltal pedig jelentősen csökkent annak hatékonysága.[18]

A drónelhárításra további megoldást jelenthetnek a „geofencing" eljárások. Ezek szoftveres biztonsági rendszerek, amelyek GPS- és egyéb műholdas jelek alkalmazásával akadályozzák meg a drónokat, hogy olyan szenzitív létesítményekhez közel repüljenek, mint a repülőterek, börtönök, atomerőművek és kiemelt fontosságú rendezvények.[19] Ezeket a rendszereket egyelőre csak kevés gyártó alkalmazza, és gyenge pontjuk, hogy bizonyos engedélyek megszerzésével feloldhatók a korlátozások, amelyek visszaélésekhez vezethetnek.

2.2. A védelmi rendszerektől elvárható képességek

Egy hatékony drónelhárító rendszer sokrétű, több komponensű technológiákat integrál magában. Elsősorban rendelkeznie kell a rendeltetésének megfelelő hatótávolságú felderítő berendezéssel. Fix telepítésű rendszerek esetében a több tíz kilométeres hatótávolság elvárható teljesítmény, valamint ellenállónak kell lennie az időjárás viszontagságainak. Olyan alapvető információkat kell azonosítania a szabálysértő drónról, mint a típus, azonosítási szám, pillanatnyi helyzet, magasság, sebesség, továbbá, ha a felszállási helyét és az operátor tartózkodási helyét is képes meghatározni, nagyban hozzájárulhat a rendvédelmi erők munkájához. Mobilisan telepíthető egységek esetében az antennák kisebb teljesítményét figyelembe véve a hatótávolság természetesen lecsökken. Az észlelés akkor hatékony, ha a rendszer együttesen képes több radar- és rádiófrekvenciás eszközt, elektrooptikai, valamint infravörös szenzorokat integrálni, kiküszöbölve a hibalehetőségeket, valamint lefedve a drónok rosszindulatú alkalmazási lehetőségeinek teljes spektrumát.

A modern C-UAS-rendszerek szükségszerűen több, egymástól eltérő elven működő hatástalanító eszközzel rendelkeznek, amelyek valamilyen kombinációját (*soft kill* és *hard kill*) képesek hatékonyan bevetni, amikor a szabálysértő drón eléri a semlegesítési zónát. A védelmi rendszerek jellemzően az elektronikai ellentevékenységeket részesítik előnyben, végső védelmi eszközként pedig a fizikai válaszcsapás is szóba jöhet. A védelmi rendszerek elektronikai egységei zavarják az ellenséges eszköz és az operátor közötti adatátvitelt, ugyanakkor képesek destabilizálni azokat az RC vezérlőjéből kiadott jelek és parancsok, a VHF és UHF dróncsatornák, valamint az eszköz GNSS jelének blokkolása útján. A jelzavarás következményeként a legtöbb esetben az eszköz földbe csapódik, kivételes esetben visszatér a vezérlőhöz. Az ellenséges drón irányítatlan lezuhanása természetesen további kockázatot jelent, hiszen energiatartalmánál

[17] Husseini (2019) i. m.
[18] Yuval Azulai: *Rafael to sell 6 anti-drone systems to UK for $20m.* Globes, 2018.
[19] DJI: *DJI Improves Geofencing To Enhance Protection of European Airports and Facilities.* 2019.

fogva jelentős károkat okozhat. Amennyiben a fedélzetén biológiai, vegyi fegyverek, robbanótöltetek, sugárzó anyaggal felszerelt eszközök is előfordulnak, az okozott kár és a hatás még drámaibb lehet. A drón „elhárítása" nem érné el a célját. Az ilyenfajta kockázat csökkentésére a *spoofing* módszer ad lehetőséget. Ez a drón feletti irányítás átvételét jelenti, ami lehetővé teszi a fenyegető eszköz biztonságos leszállítását anélkül, hogy a rászerelt fegyverek, anyagok kifejthetnék hatásukat. Repülőterek, atomerőművek, kormányzati létesítmények és egyéb kritikus infrastruktúrák környezetében a biztonság további növelése érdekében földbe mélyített leszállító helyek kiépítését is érdemes volna fontolóra venni, ha a felfegyverzett drónt más módon nem lehetne biztonságosan leszállítani. A földbe vájt leszállító helyen az ellenséges eszközöket biztonságosan el lehet különíteni.

A drónvédelmi struktúrát hagymahéjszerűen, szakaszosan célszerű kialakítani, ahol minden védelmi vonalnak megfelelő funkciója és változatos észlelő és ellentevékenységet biztosító eszközrendszere van. Abban az esetben, ha a támadó drón túljut az elsődleges védelmi vonalakon, a C-UAS-rendszer „hard kill" eszközei kerülnek előtérbe, immár fizikai megsemmisítéssel semlegesítve a fenyegetést jelentő eszközt. Véleményünk szerint erre a feladatra a nagy erejű lézersugár, valamint az elfogóháló a legalkalmasabb, azonban figyelembe kell venni, hogy alkalmazásukra az adott állam szabályozásaival összhangban van lehetőség. Az elfogóhálós módszer alkalmazásakor érdemes figyelembe venni a tényt, hogy ezt a feladatot az autonóm rendszerek nagyobb pontossággal és hatékonysággal tudják végrehajtani, mintha emberi irányítással próbálnánk az ellenséges drónra való rávezetést megvalósítani, ami az Egyesült Államok Hadseregében szolgáló drónspecialisták tapasztalatai alapján a legtöbb esetben nem jár sikerrel.[20]

Az elhárító rendszerek mellett, azokat támogatva célszerű *geofencing* módszereket is alkalmazni, amelyek leginkább a szabályokat betartó felhasználók segítésére valók, de használatukkal elkerülhetők a véletlenszerű, illetve a tájékozatlanságból adódó szabálysértések, amelyek így kockázatot jelenthetnek. Véleményünk szerint egyértelműen nem tekinthetünk védelmi eszközként ezekre a szoftverekre, mivel bennük módosítások eszközölhetők (a megfelelő engedély megszerzése után feloldhatók például a korlátozott zónák paraméterei) ez pedig magában hordozza a visszaélés lehetőségét. Ha egy rendszer hozzáférhető kód segítségével semlegesíthető, akkor könnyű célpontot jelent a rosszindulatú hackerek számára. Mindenesetre e lehetőség segítheti és könnyebbé teheti a szabályos drónhasználatot, növelheti az operátorok tájékozottságát.

A bemutatott felderítési és megelőzési módszerek, az ellentevékenységek dokumentálása, valamint a visszakereshetőség is fontos tényező, leginkább a tapasztalatgyűjtés és nem utolsósorban a felelősségre vonás lehetőségének biztosítása érdekében.

3. Összegzés

A drónok rosszindulatú felhasználása ellen ma már számos technikai eszköz áll rendelkezésre. Ezek helyes megválasztásával és konfigurálásával a távirányítású eszközök jelentette fenyegetés kezelhető, a rosszindulatú alkalmazás kockázata csökkenthető. Az ellentevékenység sikere alapvetően azon múlik, hogy olyan rendszert állítsunk elő, amely képes megfelelni

[20] Husseini (2019) i. m.

a kihívásoknak. Egy ilyen mélységben tagolt rendszerrel sikerülhet a drónokat jogszerűtlenül alkalmazók „előtt járni" technikai szempontból, valamint a kihívásokhoz való alkalmazkodóképesség szempontjából is.

Felhasznált irodalom

Airportal.hu: *Drónok miatt bénult meg a légiforgalom a London–Gatwick repülőtéren.* 2018. Online: https://airportal.hu/dronok-miatt-benult-meg-a-legiforgalom-a-london-gatwick-repuloteren/

Azulai, Yuval: *Rafael to sell 6 anti-drone systems to UK for $20m.* Globes, 2018. Online: https://en.globes.co.il/en/article-rafael-to-sell-6-anti-drone-systems-to-uk-1001250393

COPTRZ: *COPTRZ DDaaS – Drone Detection as a Service.* 2019. Online: www.coptrz.com/aeroscope-dji-drone-detection-system/

DJI: *DJI Improves Geofencing To Enhance Protection of European Airports and Facilities.* 2019. Online: www.dji.com/ae/newsroom/news/dji-improves-geofencing-to-enhance-protection-of-european-airports-and-facilities

Gallagher, Sean: *German chancellor's drone "attack" shows the threat of weaponized UAVs.* Ars Technika, 2013. Online: https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/

Holland Michel, Arthur: *Counter-Drone Systems.* Center for the Study of the Drone at Bard College, 2018. Online: http://dronecenter.bard.edu/counter-drone-systems/

Husseini, Talal: *When drones are used maliciously, can anyone stop them?* Airforce Technology, 2019. Online: www.airforce-technology.com/features/threats-from-small-drones/

Interpol: *Drone technology: security threats and benefits for police focus of INTERPOL forum.* 2018. Online: www.interpol.int/en/News-and-Events/News/2018/Drone-technology-security-threats-and-benefits-for-police-focus-of-INTERPOL-forum

Miasnikov, Eugene: *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects.* Moscow, Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology, 2005. Online: www.armscontrol.ru/UAV/UAV-report.pdf

PA Media: Passenger plane in near-miss with drone at Gatwick airport. *The Guardian,* 2019. Online: www.theguardian.com/uk-news/2019/aug/28/passenger-plane-near-miss-drone-gatwick-airport

Ripley, Will: *Drone with radioactive material found on Japanese Prime Minister's roof.* CNN, 2015. Online: https://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone

Safi, Michael – Graeme Wearden: Everything you need to know about the Saudi Arabia oil attacks. *The Guardian,* 2019. Online: www.theguardian.com/world/2019/sep/16/saudi-arabia-oil-attacks-everything-you-need-to-know?fbclid=IwAR1Jnh3IDtR-Zn3_Hp3yYQWnoKmp8248E7W2lEIfNt2CghBm4zgxkwIqqoI

Shear, Michael D. – Michael S. Schmidt: White House Drone Crash Described as a U.S. Worker's Drunken Lark. *The New York Times,* 2015. Online: www.nytimes.com/2015/01/28/us/white-house-drone.html?_r=0