

A drónok szerepe a terrortámadásokban – A fenyegetés új dimenziója

Sabjanics István, Horváth Illés*

Belügyminisztérium, Tudománystratégiai és -koordinációs Főosztály, Budapest, Magyarország

*Levelező szerző, e-mail: illes.tamas.horvath@bm.gov.hu

Beérkezett: 2024. január 25.; elfogadva: 2024. február 22.

Összefoglalás

A dróntechnológia alapjainak katonai alkalmazása a II. világháború folyamán terjedt el, és hamarosan a koreai háború (1950–1953) kulcsfontosságú hírszerzési eszközévé vált. A 2000-es évekig az UAV-k (pilóta nélküli légi járművek) gyártásának és forgalmazásának monopóliuma kizárólag a hadiipar kezében volt, de a technológiában rejlő hatalmas lehetőségek gyorsan meghódították a civil szektort, és a gyártás önálló iparággá fejlődött. A piac robbanása alighanem forradalmasította a technológiát. Ennek következtében a drónok mérete csökkent, hatótávolságuk jelentősen megnövekedett. A piac által indukált technológiai fejlődés azonban nem csupán a laikus felhasználókat fogta meg, de az irreguláris, illetőleg a terrorista szervezetekre is komoly hatást gyakorolt. A technológiában rejlő potenciált hamar felismerték, így nemcsak integrálták, de kettős célok érdekében tovább is fejlesztették. 1990-től 2018-ig 14 olyan támadás történt, amelyben az elkövetők házilag, kereskedelmi forgalomban kapható alkatrészek felhasználásával készített UAV-t használtak. Jelen tanulmány célja, hogy megvilágítsa a drónok alkalmazásának lehetőségeit a terrorista csoportok körében, valamint, hogy rámutasson a lehetséges védelmi és biztonsági intézkedésekre.

Kulcsszavak: dróntechnológia, C-UAS, honvédelmi és civil felhasználás, jövőbeni támadások, terrorizmus

Role of Drones in Terrorist Attacks – The New Dimension of Threat

István Sabjanics, Illés Horváth

Ministry of Interior, Science Strategy and Coordination Department, Budapest, Hungary

Summary

The military application of the fundamentals of drone technology spread during World War II (1939-1945) and soon became a key intelligence tool in the Korean War (1950-1953). Until the 2000s, the monopoly over the production and marketing of UAVs (Unmanned Aerial Vehicles) was held exclusively by the military industry, but the enormous potential of the technology quickly conquered the civilian sector, and manufacturing developed into an industry in its own right. The explosion of the market revolutionised the technology. It significantly reduced their size, increased their power capacity and, although there was also a significant change in rotor size, their power and range increased exponentially. At the same time, advances have also had a very positive impact on control: the ability to follow a person or object without direct pilot intervention, the ability to program an autonomous flight path on the user interface, the ability to return to the pilot in the event of signal loss, the ability to avoid obstacles in complex environments thanks to advanced optical sensors, and the cameras on some models with facial recognition technology. The use of drone technology by irregular organisations or terrorists dates back to the 1990s, and by 2018 there had been 14 terrorist attacks in which the perpetrators had used a homemade UAV using commercially available parts. The aim of this study is to shed light on the motivation of extremist groups and the potential for the use of drones. In addition, take stock of the possible ways of protection.

Keywords: drone technology, C-UAS, military, civilian and extremist use, future attacks, terrorist

A dróntechnológia alapjainak harcászati alkalmazása a II. világháborúban (1939–1945) terjedt el, majd rövidesen a koreai háborúban (1950–1953) a hírszerzés egyik létfontosságú eszköze lett. A 2000-es évekig az UAV-k (*Unmanned Aerial Vehicle*) gyártása és forgalmazása felletti kizárólagos monopólium a hadi iparé volt. Csak-hogy a technológiában rejlő hatalmas potenciál gyorsan meghódította a civil szektort, így a gyártás önálló iparág-gá fejlődött. A piac robbanásszerű növekedése forradalmasította a technológiát. A drónok mérete szignifikánsan csökkent, energiakapacitásuk megnőtt, s habár a rotor méretében szintén jelentős változás állt be, a teljesítményük és hatótávolságuk exponenciálisan növekedett. A fejlődés igen kedvezően hatott a vezérlésre is; a pilóta közvetlen beavatkozása nélkül képesek lettek személyt vagy tárgyat követni, a felhasználói felületen már autonóm repülési útvonalat lehet beprogramozni, elvesztés esetén vissza tudnak térni a földi irányítóhoz, a fejlett optikai érzékelőknek köszönhetően komplex környezetben akadálykerülésre képesek, egyes modellek kamerái pedig arcfelismerő technológiával rendelkeznek. Így nem véletlen, hogy a technológiában rejlő jelentős potenciált már az 1990-es évek elejétől különböző irreguláris vagy terrorista szervezetek is alkalmazni kezdték. Igen figyelemfelkeltő adat, hogy 2018-ig legkevesebb 14 olyan terrortámadás vagy merényletkísérlet ismert, melyben az elkövetők legálisan, a kereskedelmi forgalomban is beszerezhető alkatrészek felhasználásával, saját kezűleg épített UAV-val terveztek merényletet (Bunker 2015). Jelen tanulmány célja, hogy megvilágítsa a drónok funkcióját a szélsőséges csoportok alkalmazásában, valamint rámutasson lehetséges védelmi és biztonsági intézkedések szükségességére.

Az első tervezett, ám meg nem valósult dróntámadás 1994-re datálható. A jelenleg is működő japán világvége várományos szekta, az *Aum Shinrikyo* terroristái több nagy forgalmú csomópont ellen tervezték ki támadást, hogy azzal később, az Egyesült Államokra fogva elősegítsék a III. világháború kirobbantását, mely elképzeléseik szerint megtisztította volna a világot. A támadásokat egy távirányítású helikopter segítségével hajtották volna végre, amely a tervek szerint szaringázzal árasztotta volna el a területet (Simons 2006). A szervezet előzetes tesztjei során a helikopter végül földhöz csapódott, ezért eltérő megoldást alkalmaztak a merényletek végrehajtására. Az 1994. június 27-én történt Matsumoto-konfliktus 8 civil életét követelte, s mintegy 200 további áldozat szenvedett kisebb-nagyobb sérüléseket. Az 1995. március 20-án elkövetett tokiói merényletben 13 ember halt meg, míg több ezren különféle sérüléseket szereztek (Jones 2008; Gunaratna 2018).

Az ezredfordulót követően a dróntechnológia alkalmazása robbanásszerűen terjedt el a szélsőséges csoportok körében. 2001-ben az al-Qa'ida tervezett támadást drónokra erősített IED-vel (*Improvised Explosive Device*) George Bush amerikai elnök és más nagyhatalmak vezetői ellen. Egy évvel később, 2002-ben anthraxszal töltött

drónt akartak bevetni a brit Képviselőház ellen (Miasnikov 2005). Az al-Qa'ida azt is tervezte, hogy bombákkal felszerelt drónnal kísérel meg terrortámadást a szigetország reptereivel és utasszállító repülőgépeivel szemben. Az iszlám szélsőségesek mintáit másolva állította fel flottáját a Kolumbia Forradalmi Fegyveres Erők (*Fuerzas Armadas Revolucionarias de Colombia = FARC*) gerilla-csoportja is, amely drónjait – hasonlóan a közel-keleti drónokhoz – IED-vel szerelte fel (Budai 2017). A távirányítású flotta célja az volt, hogy a gép testére szerelt robbanóanyaggal közvetlenül a kormányzati célpontokba belerrepülve mérjenek csapást. A politikusok és a kormányzati épületek mellett közvetlen célpontnak tekintették a kritikus infrastruktúra elemeit is, úgymint az olajfinomítókat és más állami ipari egységeket.

2002–2003-ban derült fény arra, hogy az amerikai Virginia államban a muszlim szélsőségesek egy csoportja, melyet leginkább *Virginia Jihad Network*ként szokás emlegetni, 1999-től 2003-ig a helyi mecset imámjával szerveződve folyamatos támogatást nyújtott a Lashkar-e-Taiba terrorszervezetnek. A csoport feladata az volt, hogy új technológiát és különböző eszközöket szerezzen a terrorszervezet számára. A csoport nemzetközi kiterjedtségét jól mutatja, hogy a nyomozó hatóság a szervezet több tagját Angliában érte tetten (The 9/11 Commission Report). Két évvel később Christopher Paul (Abdumalek Kenyatta) amerikai állampolgár került gyanúba, miszerint Boszniában részt vett a dzsihadisták támadásaiban, valamint távirányítású helikoptert és hajót fejlesztett az al-Qa'ida részére, amelyeket tömegpusztító fegyverként alkalmaztak a terroristák (*weapon of mass destruction = WMD*). Christopher Pault elítélték (Dífo 2010).

2002-ben a fenti technológiákat felhasználva épített flottát a Fatah al-Islam terrorszervezet is, ami Jeruzsálem zsidó negyede ellen készített elő támadást. A jelentések szerint megközelítőleg 100 drón állt a terrorszervezet szolgálatában, melyek tesztüzemmódban működtek. A következő években a palesztin al-Aqsa mártírjaiként ismert terrorszervezet is felfegyverezte magát harci drónokkal, amivel a gázai zsidó negyedek ellen készítettek elő támadásokat. A későbbi akcióba a Fatah IED-al felszerelt drónjai is részt vettek (Bunker 2015).

Ezt követően nem telt el sok idő, hogy a Hezbollah is felfegyverkezzen. 2004-ben egy Libanonból indított iráni fejlesztésű UAV-val derítette fel az izraeli légierő védelmi képességét (Krajnc 2018). Némely esetben előfordult, hogy kínai fejlesztésű drónokat vetettek be (Bunker 2015).

A dróntechnológia terrorszervezetek általi alkalmazásának eszkalációja a II. Libanoni háború idejében következett be (OCHA, Situation Report 1-38. Lebanon Response). 2006. augusztus 13-án a Hezbollah három iráni gyártmányú, egyenként 40 kg robbanófejjel ellátott *Ababil* drónt indított Izrael ellen, amit az izraeli légierő F-16-os vadászgépei semmisítettek meg Haifa mellett. Ugyanebben az időben az al-Qa'ida igyekezett globális

szinten is bevetni drónjait. A legismertebb Rezwan Ferdaus tálib fizikus esete, aki 2011 szeptemberében került letartóztatásra. Az FBI fedett nyomozója leleplezte, hogy a tálib fizikus titokban egy F-86-os mintájára merevszárnyú drónt épített, amelyre C4 robbanószert szerelt azzal a céllal, hogy megtámadja a Capitoliumot és a Pentagont annak reményében, hogy tette majd felkelti az Egyesült Államokban élő muszlim szélsőségeseknek a figyelmét és hozzá hasonlóan támadásokat hajtanak végre (Mueller 2014).

Egy évvel később Cengiz Yalçın török állampolgár és két csecsen társa, Mohammed Ankari Adamov, valamint Eldar Magomedov tervezett támadást a londoni olimpia ideje alatt egy gibraltári bevásárlóközpont ellen. Mind a három személy kapcsolatban állt az al-Qā'idával, egyikük pedig ismert bombakészítő volt. A spanyol hatóságok időben elfogták a merénylőket. A Cengiz Yalçinnél folytatott házkutatás során robbanóanyagra utaló nyomok kerültek elő, melyek egészen a ház garázsához vezettek. A kutatás során a nyomozók találtak egy videofelvételt, amelyen egy UAV volt látható. A nyomozás során igazolást nyert, hogy a terroristák a fenti eszközzel kíséreltek volna támadást végrehajtani. A szakértői vizsgálatok szerint a drón közel 1 kilogramm robbanóanyag szállítására is képes lehetett (Rassler 2016).

2013 nyarán a német hatóságoknak sikerült feltérképezni két terrorista sejtet, melyek UAV-val terveztek terroristátámadásokat végrehajtani. A merénylők tunéziai állampolgárok voltak, akik felsőfokú tanulmányaikat a Stuttgarter Egyetem Repüléstudomány szakán folytatták. A jelentések alapján a gyanúsítottak többnyire Stuttgart, München és Dachau, Baden-Württemberg területén éltek. A terroristák olyan drónt fejlesztettek, amely már rakéta hordozására is képes volt. A német hatóságok fellépésének köszönhetően a csoport valamennyi tagját még a merénylet előtt sikerült elfogni. A házkutatás során előkerült a drón, valamint több bombakészítéshez használatos anyag (Dunn 2013).

2014-ben a közel-keleti események alapjaiban változtatták meg a drónhadviselés formáit. Július 14-én a Hamász kísérelt meg dróntámadást Izrael ellen. Noha önmagában a tény, hogy egy közel-keleti terrorista szervezet megtámadja Izraelt, nem tekinthető újdonságnak, az viszont kétségtelenül *novum*nak tekinthető, hogy ezt olyan eszközzel tette, amely már több föld-levegő rakéta (*air-to-ground rockets*) hordozására és pontos kilövésére is alkalmas volt. A támadás jól mutatta, hogy a terror-szervezetek rendkívül rövid idő alatt hatalmas előrelépést tettek a dróntechnológia alkalmazásában (Rassler 2016).

Ugyanebben az évben egy új terrorszervezet, az Iszlám Állam (*ad-Dawlah al-Islamiyyah*) létrejöttével a hadviselés egy új korszaka köszöntött be, melyben a technológia minden eddiginél központibb szerephez jutott. 2014. augusztus 23-án az Iszlám Állam fegyveresei még a kereskedelmi forgalomban elérhető kínai DJI Phantom FC40-es eszközökkel rögzítették a szíriai

Er-Rakka kormányzóság 93-as bázisának ostromát, majd szeptemberben Kobani városának ostroma során már kettős céllal, propaganda-film-készítés és földi célpontok elleni támadások végrehajtására kezdték alkalmazni, egyfajta virtuális mártírként (*virtual martyr unit*). A drónok különösen alkalmasnak bizonyultak arra, hogy a szélsőségesen értelmezett rejtőzködést, lelepleződést (*taqiyyah*) a földi irányító minden tekintetben fenntartsa, ugyanakkor – ahogy a fenti *terminus technicus* is jól mutatja – a technológia újradefiniálta a fundamentalista alapon értelmezett dzsihádot (Dévényi 2017). A kezdeti sikerek hatására az Iszlám Állam rendkívüli gyorsasággal építette fel saját drónprogramját, amelynek következtében két önálló műhelyt hozott létre. Irakban és Szíriában. Az év végére már teljesen önálló flottát üzemeltettek. 2015-re a kurd hatóságok jelentései alapján ismertté vált, hogy az Iszlám Állam már a Skywalker X8-as mintájára saját önálló egységet hozott létre. A következő évben pedig már IED, valamint rakéta szállítására és kilövésére alkalmas drónt fejlesztettek. Abu Bakr al-Baghdadi vezetése alatt olyan drónokat is fejleszteni kezdtek, melyek ideggázzal töltve alkalmasak lettek volna nyugati vezetők meggyilkolására is (Rassler 2016).

A gyors technikai fejlődés alapvetően növelte a pilóták repülési kompetenciáit is, aminek következtében különböző támadási stratégiák és módok alakultak ki. A *single* és a *group fly* mellett megjelentek az úgynevezett UAV rajok (*swarm attack*), amelyekkel a földi irányító automata üzemmódban, több mint 8 drónnal is képes egyszerre csapást mérni egy adott célpontra vagy célpontokra.

Az UAS-okkal elkövetett támadások tipológiáját tekintve alapvetően öt kategóriát különböztethetünk meg:

(I.) Felderítés (*Surveil Objectives*)

Az UAS-ok terrorszervezetek általi felhasználásának legelterjedtebb fajtája a légifelderítés. Az amerikai, orosz, valamint a kurd hadsereg közel-keleti tapasztalataiból jól ismert, hogy az ISIS harcosai gyakran márdártávlatból (*bird's eye view of battle*) mérték fel az egyes célpontok közvetlen környezetét, lakó-, tartózkodási és munkahelyét, valamint a támadás lehetséges formáira tekintettel gyakran a szokványos útvonalát. A célpont vagy célszemély körüli viszonyok előzetes felmérése lehetőséget kínált arra, hogy a tervezett művelet sikerének érdekében, szükség esetén további légi támogatást vonjanak be az akcióba. Különösen fontos szempont, hogy a rejtőzködő terrorista csoportok nem csupán a küldetést veszélyeztető tényezőket derítették fel, hanem gyakran saját biztonságuk érdekében rejtékhelyük környezetét is folyamatosan monitorozták. A legújabb katonai és titkosszolgálati jelentések szerint, az utóbbi időben a felderítés egy eddig nem ismert, rendkívül kezdetleges formája az úgynevezett kiberfelderítés (*cyber-surveillance*) is egyfajta potenciális fenyegetéssé vált (Altawy–Youssef 2016; Yancoub et al. 2020; Pyzynski–Balcerzak 2021). A terroristák igen

gyakran UAV-k segítségével próbálják megszerezni a nem megfelelően titkosított helyi elektronikus kommunikáció adatállományát (*Dahm 2020*), és nem egyedi eset, hogy bankkártyaadatokat tulajdonítanak el (*Hartmann–Giles 2016*) (*Elint Capability, Email, Instant Messaging, Video Conferencing, Social Media, Text Messaging, File Transfer Protocol*) (*Rassler 2016; Almohammad–Speckhard 2017*).

(II.) Stratégiai kommunikáció (*External Comms or strategic messaging*)

Alighanem 2014-ben az Iszlám Állam volt az első olyan irreguláris katonai haderő, amely propaganda-filmjeinek leforgatásához, terjesztéséhez drónokat kezdett használni. Az egyes célpontok elleni merényleteket, hadműveletet vagy az útjukba kerülő műemlékek lerombolását nagy gonddal, teátrális módon dokumentálták és terjesztették a Twitteren és a Telegramon, mely közösségi platformok különösen alkalmasnak bizonyultak arra is, hogy további követőket szerezzenek (*Singer 2015; Magdy–Darwish–Weber 2016; Maggioni–Magri 2015; Gambhir 2016; Fisher 2015; Berger–Morgan 2015*). 2016. október 9. és 2018. december 30. között 524 képet tölthettek fel különböző közösségi oldalakra drónműveletekről. Ebből mintegy 208 fájl merénylet volt (*Archambault–Veilleux-Lepage 2020; Grossman 2018*). A drónnal készített propaganda adathalmaz a következőkből állt: (1) Dróncsapások: RPA (*Remotely Piloted Aircraft*) felhasználása, a célpont elpusztítása, a merénylet vagy a pusztítás utóhatása; (2) VBIED (*Vehicle Born Improvised Explosive Device*), vagy más jellegű „mártírhálál” rögzítése; (3) Felderítés. Katonai felügyelet alá tartozó terület bemutatása, ellenséges erők láthatóvá tétele; (4) Flotta bemutatása; (5) Drónok harci képességeinek prezentálása (*Cohen 1960; Kaczowski 2019; Bloom–Horgan–Winter 2016*). Ezenfelül különösen gyakoriak voltak az olyan propagandafilmek, amelyekben csak a tájat, vagy a katonai ellenőrzés alatt álló területet rögzítették. Ez utóbbi célja egyértelműen a terület feletti totális ellenőrzés, valamint hegemonia reprezentálása volt.

(III.) Csempészség, szállítás (*Smuggle, Courier*)

Az UAV-k talán legáltalánosabb alkalmazási lehetősége a csempészet. A védett vagy jól őrzött területeket – különös tekintettel a nemzetközi határookra – meglepő gyakorisággal lépik át pilóta nélküli légijárművel, melynek aljára a földi irányítók fegyvert, pénzt, kábítószert vagy mobiltelefont erősítenek (*Bunker–Sullivan 2021*). E cselekményekben leginkább a börtönök, valamint az intenzív menekülthullámnak kitett országhatárok, mint például az Egyesült Államok déli, Magyarország déli, illetve Törökország szintén déli határszakasza érintett. Az Egyesült Államok déli határszakaszán a mexikói drokartellek építettek UAV flottát, hogy a hatóságok figyelmét elkerülve csempésze-

nek drogot az Egyesült Államokba. Külön figyelmet érdemelnek a büntetés-végrehajtási intézetek, amelyek az UAV piac szélesedésével egyre inkább érintetté válnak a csempészetben (*Montanari et al. 2022; Gooch–Treadwell 2021*). A jelentések alapján a rabok hozzátartozói, barátai vagy korábbi bandatagjai nagyrészt mobiltelefonokkal, SIM-kártyákkal, marihuánával, úgynevezett elektromos cigarettával (*Disposable Vape Penekkel*), és más dohányipari termékekkel, hasissal, nyugtatókkal, különböző kábító hatású gyógyszer-alapanyagokkal, ragasztókkal, öngyújtókkal, pornográf felvételekkel, szteroidokkal, rágógumival, illetve különféle higiénias eszközökkel kísérik meg ellátni az elítéltet (*Chavez–Swed 2020*). Az Egyesült Királyság börtöneinek közelében 2019 és 2021 között megközelítőleg 504 dróndetektálás történt. 2022 májusában a hatóságok egy 35 000 GBP értékű csomagot találtak, amelyben többségében mobiltelefonok, illetve kábítószer volt. Ennek hatására a brit kormány úgy határozott, hogy a börtönök 400 méteres környezetét *no-fly zónának* nyilvánítja, mely intézkedés várhatóan jelentősen csökkenti a jövőben a börtönök, különösen pedig az állomány kiszolgáltatottságát (*Air Navigation Order 2016 No. 765.*).

(IV.) Zavarás (*Disrupt or Sabotage*)

Egy rendezvény drónokkal való zavarása különösen kedvelt formája a szélsőséges csoportoknak. 2013. szeptember 15-én Drezdában a Német Kalózpárt pilótája által irányított drón zavarta meg Angela Merkel szövetségi kancellár választási kampánygyűlését, amely 2 méterre közelítette meg a kancellárt, majd végül a színpadnak csapódott (*Strauss 2013*). Az incidenst egy tréfával elütötték, de számos biztonsági kérdést vetett fel. Például mi lett volna, ha az eszköz fegyverrel vagy bombával van felszerelve (*Rottler 2018*)?

2014 októberében a Szerbia–Albánia Európa-bajnoki mérkőzés 42. percében egy drón jelent meg a pálya felett, amely egy albán zászlót húzott maga után. Az incidens hatására a játékvezető félbeszakította a mérkőzést (*Kovačević 2020*).

(V.) Fegyver, fegyverkezés (*Weaponize*)

Az UAS-ok fegyverrel való felszerelése alighanem az egyik legveszélyesebb kategóriának tekinthető. A szélsőséges csoportok legtöbbször robbanóanyagot erősítenek a pilóta nélküli légijárműre, amelyet közvetlen a célpont közelébe navigálva szinte láthatatlanul elhelyeznek, majd a megfelelő időpontban élesítik a robbanóanyagot. 2018. augusztus 4-én két, egyenként 1 kg plastikkal felszerelt drónnal kísérelték meg Nicola Maduro venezuelai elnököt meggyilkolni. Az eset kétségtelenül új korszakot indított a terrorizmus történetében (*Clarke 2018*).

2015-től az Iszlám Állam Irakban már több ízben használt kifejezetten a földi járművek elpusztítására kialakított kamikaze drónokat, melyek funkciója alapve-

tően kettős volt. Egyrészt úgy kerültek kialakításra, hogy az alapvető operatív funkciókat betöltsék, a műveletek megtervezéséhez képesek legyenek ellátni a felderítést szolgáló célokat, másrészt felismerve azt a tényt, hogy egy mozgó járműre nehéz robbanószert ejteni, az UAV-re erősített robbanóanyaggal a földi irányító direktbe repült a gépjárműbe (*suicide car bombers*). 2015 és 2017 között az Iszlám Állam nagyszabású drónprogramot indított, ami a hibrid hadviselés (AJP-01 Allied Joint Doctrine, NATO) egy új, eddig ismeretlen formájának, valamint terrorfenyegetésnek nyitott utat (Rassler 2018a). A terror első automatizált, rajban is repülni képes flottája jelent meg. Hasonlóan, mint a kamikaze drónok esetében, a harci drónok testére improvizált robbanószerkezetet, tömegpusztító fegyvert vagy löfegyvert szereltek (Snell-Keusenkothen 1995; Renchan 1997). Az UAS-re erősített robbanószerkezet leejtését egy kioldószerkezet biztosította. A célpont fölé repülve a drónok szinte láthatatlanul, hang nélkül tudtak bombát dobni a célszemélyekre és különböző objektumokra. Igen gyakori volt, hogy a nagyobb távolságban található célpontok elérésének érdekében merevszárnyú UAS-eket vetettek be, és hasonlóan, mint a multirotoros drónok esetében, a légijármű aljára kioldószerkezetet erősítettek, amely a robbanóanyagot tartotta, majd a cél fölött kioldották a házilag készített bombát. A bombák többsége 40 mm-es házilag átalakított gránát, *Shell*, *White Shell*, *Leaflets*, és egy eddig azonosíthatatlan, a szíriai Raqqah városa ellen használt bombatípus volt (Balkan 2017). 2015 és 2017 között az Iszlám Állam a drónokra szerelt bombák, löfegyverek, lángszórók mellett kémiai és biológiai fegyvereket is (*Chemical or Biological Weapons = CBW*) (Bhushan 2022; Marturano et al. 2021; Rabajczyk et al. 2020) alkalmazott védelmi stratégiájában (Hummel 2016; Strack 2017). A fenti időszakban 48 támadást Irakban, míg 28-at Szíriában követek el. Az eddigi vizsgálatok alapján megállapítható, hogy a vizsgált időszakban 17 alkalommal mustár-, 28 alkalommal klórgázt vetettek be. 31 további merényletet a mai napig nem sikerült kategorizálniuk a hatóságoknak. A támadásokat bizonyíthatóan távvezérelt quadcopterekkel hajtották végre (Blair 2013). E tekintetben a gyárilag permetszer kibocsájtására alkalmas mezőgazdasági drónok használatát a jövőben rendkívül nagy figyelemmel szükséges kísérni.

Minden bizonnyal idővel új kategóriaként kell majd ide sorolni a légiközlekedés résztvevőinek zavarását vagy veszélyeztetését. 2018. december 19-én több drón berepült az Egyesült Királyság London-Gatwick repülőtérre, melynek következtében leállították a légiforgalmat. A szándékos zavarás okozta fennakadás közel 110 000 utast érintett. Miután a légikikötő akkor még nem rendelkezett detektáló és elhárító berendezéssel, a hadsereg hajtotta végre a szükséges védelmi és biztonsági intézke-

déseket. Az átmeneti zárlat alatt csaknem 40-50 drónnal való illetéktelen berepülést érzékelték (Shelley 2020). A légiforgalom a fejlett izraeli *Drone Dome C-UAS Anti-aircraft System* telepítése után indulhatott újra (Tomkins 2018; Holland 2019). A reptér védelmére felszerelt drónkupola nemcsak detektálni képes a tiltott légtérben megjelenő UAV-eket, de még az elhárításban is kiválóan jeleskedik, hiszen alkalmas arra, hogy az egyes dróntípusok és működtetőjük között megszakítsa a rádiókapcsolatot, ezáltal pedig biztonságos helyen leszállásra kényszerítse az eszközt. 2023 májusában a reptér irányítása ismét gyanús drónt érzékelt a tiltott légtérben, ám ezúttal nem 33 órára, hanem a nyomozás idejére, mindössze 1 órára zárták le a kifutópályát. Hasonló incidens a Hungaro-Control Zrt. jelentése szerint a Budapest Liszt Ferenc Nemzetközi Repülőtérén is több ízben előfordult. 2018-ban több mint egy tucat repülő személyzete jelezte a légiforgalom-irányításnak, hogy drónt láttak a légtérben, 2019 októberében két alkalommal is rövid időre, de fel kellett függeszteni a reptér légiforgalmát repülésbiztonsági kockázatok elhárítása végett, míg a dróntevékenység teljes bizonyossággal meg nem szűnt.

A légikikötők zavarása mellett sokkal súlyosabb fenyegetést jelent magának a légiforgalomnak a zavarása. 2014 júliusában az Egyesült Királyság Heathrow repterén egy Airbus A320 típusú repülőgép 700 láb magasságban kis híján összeütközött egy drónnal. Az esetet követően a *Civil Aviation Authority* közleményében hívta fel a figyelmet az UAS-ek szerepére a légiközlekedés veszélyeztetésében (Abbot et al. 2016). 2018 júliusában Mauritius szigetén egy drónpilóta a Sir Seewoosagur Ramgoolam Nemzetközi Repülőtér közelébe reptette a Parrot Anafi drónját, és közvetlen közlőről rögzítette a mellette elhaladó Airbus A380 típusú repülőgépet, mely alighanem katasztrófához is vezethetett volna. A megszaporodó esetek tekintetében talán nem véletlen, hogy ugyanebben az időben történtek az első drón-balesetek is. 2018 februárjában az egyesült államokbeli Dél-Karolina államban történt, hogy egy Robinson R22 kétszemélyes könnyű helikopter előtt váratlanul egy DJI Phantom típusú drón tűnt fel, melynek hatására a pilóta kitérő manőverrel próbálkozott, hogy elkerülje az ütközést, azonban a gép a földhöz csapódott. Személyi sérülés nem történt.

2023. augusztus 18-án az Emirates Légitársaság Dubai Nemzetközi Reptéréről a franciaországi Nizza Côte d'Azur Repülőtérre tartó Airbus 380 típusú utasszállítójának a szárnya sérült meg egy drónnal való ütközés során. A fenti példák jól látható, hogy a légiforgalom UAV-ekkel való blokkolása, zavarása és veszélyeztetése a jövőben minden bizonnyal a szélsőséges csoportok homlokterébe kerül majd.

A támadások kockázatát nyilvánvalóan nehéz megbecsülni, azonban a megvalósíthatóságot nem. Az elmúlt években a Közel-Keleten, Kelet-Európában és Észak-Afrikában többször érte támadás a kritikus infrastruktúrát. A Húti-mozgalom vagy más néven az *Ansar Allah Qasf Samad* drónokat (Voskuyl-Dekkers 2020) vetett be

a szaúdi célpontok ellen, többek között a Saudi Aramco olajipari társaság szivattyúi, illetve Abha és Jizan nemzetközi repülőterek ellen (Voskuyl–Dekkers 2020). 2018-ban január 5-én az Iszlám Állam indított támadást harci drónjaival az oroszok által ellenőrzött Khmeimim és Taurus légitámaszpontok ellen. A korábbi támadásokkal ellentétben a terrorszervezet már a jelentősebb, nagyobb hatótávolságú merevszárnyú drónjait vetette be, amelyek testére, illetve szárnyára bombákat, és kisebb, közvetlen az eszközről indítható rakétákat erősítettek (Urcosta 2020; Cafarella et al. 2020). A támadás alighanem egy újabb UAV hadviselési forradalmat indított meg a Közel-Keleten. E forradalom pedig nem csupán a felderítés és a támadás szempontjait írta felül, hanem a védelmi-biztonsági stratégia terén is megfontolásra intette Oroszországot és a NATO tagállamait, különösen a személy-, objektum- és a kritikus infrastruktúra védelmének szempontjából.

Az UAV-k elleni küzdelemhez alkalmas eszközök kifejlesztése rendkívül nagy kihívást jelent. A kereskedelmi szempontok és a fogyasztói igények által vezérelt technikai fejlesztések folyamatos lépéshátrányban tartják az elhárítórendszer (C-UAS) fejlesztőit. Alkalmasint azt is mondhatjuk, hogy gyakran a védelmi-biztonsági szempontokat a piac akarva-akaratlanul maga mögé utasítja. Ugyanakkor a technikai változásokkal való lépéstartást még a magánélet védelmére vonatkozó törvények, a kereskedelmi szabályozás, illetve a hatályos jogi normák is sok esetben akaratlanul hátráltathatják (Huijgen–Janssen 2021). Mint az ismert, korábban a drónok csak a világ technológiailag legfejlettebb, jól finanszírozott hadseregeire vagy a távirányítású repülőgépek (RC) szerelmeseinek viszonylag szűk közösségére korlátozódtak. Az elmúlt tizenöt évben azonban a repülésvezérlők, az autopiloták, a globális navigációs műholdrendszerek (GNSS) és a szoftveres rádiók terén bekövetkezett ugrásszerű technológiai fejlődés lehetővé tette, hogy az egyén a törvényes piaci körülmények között megvásárolja, vagy saját maga építsen drónt. A technológia (fedélzeti kamerák és akadályelkerülő érzékelők) ugrásszerű fejlődése és a kereskedelmi forgalomban kapható quadcopterekbe történő integrálása forradalmasította az RC repülőgépipart, és népszerűsége az egekbe szökött. Az erős vásárlói kereslet viszont új vállalkozásokat hozott az iparágba, ami felgyorsította a fejlesztések ütemét. Az UAV-k relatív könnyű irányítása, valamint az eszköz hadászatba átvihető kettős alkalmazási lehetősége miatt az irreguláris hadseregek és terrorszervezetek könnyen adaptálták a dróntechnológiát. Ismert, hogy az Ansar Allah nagyobb drónjaiban ugyanolyan katonai minőségű repülésvezérlőket használ, mint az iráni hadsereg (Final report of the Panel of Experts on Yemen, S/2020). A kisebb, felderítő drónjai esetében elsősorban kereskedelmi forgalomban is kapható vezérlőket használ, mint amilyeneket az Arduino is kínál (Voskuyl–Dekkers 2020). Az online térben ma már több olyan fórum is fellelhető, amely bemutatja, hogy a fenti vállalat alapanyagaiból

hogyan lehet létrehozni mindössze 370 USD költségvetésből olyan UAV-kat, melyek ellen a *geofencing* (Shu 2017) teljesen hatástalan.

Védekezés szempontjából kiváló *exemplum*ként szolgálhatnak a szaúdi, az emírségek és az oroszok közel-keleti tapasztalatai. Az UAV-technológia jelenlegi ismeretei alapján, tekintettel arra, hogy a terrorista csoportok milyen gyakorlati megfontolások alapján terveznek dróntámadást, európai szinten bizonyos, hogy a szélsőséges csoportok a közel-keleti típusoktól eltérő megoldásokat alkalmaznák, amit a kritikus pontok közötti kisebb távolság is indokol. Bizonyos, hogy emiatt a légijárművek valószínűleg kisebbek lennének, mint azok, amelyeket az Arab-félszigeten lévő repülőterek ellen használnak. A Qasfek és Samadok, amelyekkel az Ansar Allah is repül, nagyok; súlyuk megközelíti a hetven kilogrammot, és szárnyfesztávolságuk majdnem három méter. A műveletek megtervezéséhez jelentős anyagi, valamint logisztikai támogatásra van szükség, ugyanakkor szükséges egy biztonságos rejtékhely is. Míg az Arab-félszigeten leginkább a katonai létesítmények, repülőterek, valamint kikötők a kiemelt célpontok, úgy Európában mindezek mellett sokkal valószínűbb az üzemanyag, víz-, gáz-, földgáztárolók, csővezetékek, áramelosztók, élelmiszerellátási helyek, illetve kórházak és kormányzati objektumok, rendezvények elleni támadások eshetősége (Crino 2020; Haugstvedt–Jacobsen 2020).

A Közel-Keleten kívüli célpontok esetében a kisebb méretű, multirotorral rendelkező UAV alkalmazásának nagy a valószínűsége, azonban alternatív megoldásként egy terrorista csoport dönthet úgy, hogy fix szárnyú UAS-t használ a multirotor helyett. Ebben az esetben a kereskedelemben kapható EPO-habból (Sutthison–Wongkamchang–Sukuprakarn 2022) készült hobbikészletek széles választéka létezik, amelyekből meg lehet építeni a testet, ugyanakkor a *frame* már 3D nyomtatással is pillanatok alatt elkészíthető (Bunker, R. J. (2015). Európai viszonylatban a vezérléshez nélkülözhetetlen elektronikai egységek (*brushless motors, mounting accesories, UbEC ESCs, power distribution board with XT-60 con., battery, propellor, microcontroller, GPS Shield, Wi-Fi Transceiver, Channel Trasmitter, Gyro, USB A to B male to male adapter cord.*) könnyebben beszerezhetők (Santos–Oliveira 2019). Ezáltal a logisztika gyorsabb és kevesebb időt vesz igénybe, mint a keleti partvidéken.

A házilag elkészített drónra rendszerint heveder kerül felhelyezésre, amelynek a hasznos teher rögzítése mellett egy kioldó mechanizmus is része. A hasznos teher kvázi bármilyen robbanószer lehet, amelyet a célpont fölé repülve arra ráejtenek. Alternatív megoldásként egy bombát helyezhetnek a repülőgép testébe, és egy GPS-koordináta alapján a célhoz érve robbanásra állítják be. Ezenkívül gyakori megoldásnak számít az alacsony költségvetésű, kevésbé fejlett kamikaze drón alkalmazása is (Rassler 2018b).

Különösen fenyegetők a már megjelenő turbinás, sugárhajtású drónok (Cwojdzinski 2014). A fűvókákat álta-

lában készletekből és kereskedelmi forgalomban kapható repülési alkatrészekből állítják össze. A turbinás meghajtású repülőgépek kialakítása hatékony gyújtófegyverré teszi őket anélkül, hogy további hasznos teherre lenne szükség, hiszen amikor egy turbina nekiütközik egy felületnek, a motor hője meggyújtja az üzemanyagot, ami robbanást okoz. Bár a turbinás sugárhajtású technológia fegyverekhez való alkalmazása nagyrészt törekvés, a jövőben mégis életképes fenyegetésnek kell tekinteni (Ghazafi 2022; Wessley–Chauhan 2018).

A drónok által okozott fenyegetéssel szembeni semlegesítésre egy vagy több különböző elemből álló, összehangolt elhárítórendszer kialakítása szükséges. A C-UAS rendszerek alapvetően több létfontosságú komponensből tevődnek össze: (a) érzékelő és detektáló rendszer, amely érzékeli, nyomon követi és azonosítja a légijárművet, (b) légijármű mitigációjára vagy semlegesítésére szolgáló ellenintézkedési rendszer, (c) kommunikációs és információs rendszerek, amelyek lehetővé teszik az érzékelők és az ellenintézkedések hatékony együttműködését. Az érzékelőket általában az általuk felismert jelenségek szerint rendezik: rádiófrekvenciás érzékelők (RF), radar, elektrooptikai/infravörös (EO/IR) kamerák és akusztikus érzékelők (Basakand–Scheers 2018; Kaplan et al. 2021; Rozenbeek 2020).

Az RF érzékelők érzékelik a jelátvitelt az UAS és a távirányítója között. Az RF detektorok az RF spektrum egy meghatározott terét pásztázzák, keresve azokat a jeleket, amelyeket összehasonlítanak adatbázisukkal. Pozitív korreláció esetén az érzékelő talált vagy detektált valamit. Míg az egyes rádiófrekvenciás érzékelők érzékelési tartománya jellemzően a 3-5 kilométeres tartományban van, több érzékelő is elhelyezhető egy hálózatban a rendszer lefedettségének növelése érdekében. A rádiófrekvenciás érzékelők számára kihívást jelent a frekvenciaugratásos kiterjesztett spektrum (*Frequency Hopping Spread Spectrum* = FHSS) technológia terén a közelmúltban elért fejlődés (Basakand–Scheers 2018; Kaplan et al. 2021; Rozenbeek 2020). Az FHSS javítja a jelkapcsolat megbízhatóságát a repülőgép és vezérlője között, gyorsabban tud átugrani a csatornák között az ISM sávokon (*Industrial, Scientific and Medical*) belül, ami még a legnépszerűbb drónmodellek észlelésében is gondot okoz (Popovski–Yomo–Prasad 2006; Ma–Yan 2016).

A radarok az UAS elleni rendszerek másik kritikus összetevői. A radarrendszerek hatótávolsága segít túllépni az RF detektorok hatótávolságán, és áthidalhatja a rádiófrekvenciás lefedettség hiányosságait. Sőt, a radarok által kínált kibővített hatótávolság megnöveli a válaszidőt, ami jelentősen javíthatja az esélyeket. Az RF detektorokhoz hasonlóan azonban a radarrendszernek is megvan a maga korlátai. A legtöbb kereskedelmi forgalomban kapható UAS kis mérete, valamint a test összetétele, az UAS burkolatának, bevonatának egyszerű módosítása jelentősen nehezíti az észlelést. Különösképpen, ha a dróntechnológiát a biomimikri technológiával ötvözik (Tanaka et al. 2022; Nagai et al. 2021). A biomimikri

lényege, hogy a drón testét durva szén- és üvegszálborítás helyett szintetikus tollakkal vonják be, ezáltal az UAS lényegesen könnyebb lesz. Az eltérő burkolat miatt, különösen, ha a drón képes utánozni az állatok mozgását, lényegesen megnehezíti a detektálást (Pledger 2021).

A kisebb méretű UAS-ek érzékelése a legnehezebb feladat. Integrált, többszintű védelmi rendszer kialakítását igényli, melyet igazítani kell a védett terület egyedi működési környezetéhez is. Különböző, egymást átfedő érzékelőrendszerekre van szükség, melyek képesek a veszélyt a földön, vízen és levegőben időben elhárítani. Fontos kiemelni, hogy egy viszonylag lassú multirotoros UAS 65 km/h sebességgel tud repülni, ami azt jelenti, hogy egy perc alatt több mint egy km távolságot tesz meg. Így nem ritka, hogy az érzékelésre már hatótávolságon belül kerül sor. A fenti helyzetben az ellenintézkedések megtételére szinte csak másodpercnyi reakcióidő áll rendelkezésre. A kezelőszemélyzetnek azonban nemcsak a kritikus döntés meghozataláról kell döntenie, hanem ezzel egy időben a rendvédelmi szerveket is értesítenie kell, hiszen egy jól működő rendszer felfedheti a pilóta pontos helyét, akinek elfogása a bűnüldözési érdek.

Az elhárítás egy lehetséges formája az irányított energiájú fegyverek, mint a mikrohullámú vagy a lézer fegyverek használata. Előnyük, hogy biztonságos és megbízható eszköznek számítanak a drónelhárításban, ugyanis rendkívül gyorsak, pontosak, és nagy hatótávolságba lehet velük tüzelni. Azonban rendkívül magas az energiaigényük (3/5 Kw). Az olyan légijárművek, amelyek fényvisszaverő burkolattal vannak ellátva, jelentősen csökkentik hatékonyságukat, ugyanakkor potenciális veszélyt jelentenek a földi egységek és az infrastruktúra számára. Ezért a nagy energiájú mikrohullámú (*High Power Microwave* = HPM) fegyverek jobb választásnak bizonyulhatnak. A HPM-alapú fegyverek elsősorban elektromágneses hullámot használnak a drónok belső elektronikájának megsemmisítésére. A HPM-fegyverek előtt még megoldásra váró kihívás áll a hatótáv kiterjesztése, valamint a civil lakosságra jelentő potenciális kockázatok felmérése kapcsán.

A drónelhárítás eszközeinek tekintetében külön kategóriát képviselnek az RF, valamint GNSS *disruptorok* vagy *jammerek*, melyek lényege, hogy elektronikusan zavarják vagy megszakítják a légijármű és a földi irányító közti kapcsolatot. Jelen eszközök valójában csak akkor hatékonyak, ha az UAS és a pilóta között RF kapcsolat áll fenn. Az eddigi tapasztalatok alapján elmondható, hogy a zavarás legvalószínűbb következménye, ha a drón visszatér a kiindulóponttra (Kozic et al. 2018; Borio et al. 2015; Xiufang et al. 2018; Kuusniemi et al. 2012). E védekezési forma azonban alapvetően hatástalannak bizonyul a házilag készített, támadó UAS-ekkel szemben. Ezek ellen elsősorban bizonyos fokig a „hard kill” módszerek, mint a háló, vagy a manapság konzervatívnak számító, de intelligens célzó technológiával felszerelt löfőfegyverek bizonyulnak meggyőzőnek (Morrow et al.

2021). A gatwicki incidenst követően a C-UAS védelmi rendszer fejlesztői arra a következtetésre jutottak, hogy a hálózatos rendszereket különösen hatékonyan lehetne használni az elhárításban. A védekezési mód lényege, hogy az észlelést követően egy sűrített levegővel töltött, precíziós célzórendszerrel felszerelt *launcher* egy hálót lő ki a támadó egység felé. Ha a vető eltalálja az UAS-t, akkor a rotor vagy a multirotor rendszer ösztönösen felteker, ezáltal a drón végül letilt és lezuhan (Yu et al. 2022). A nagyobb biztonság érdekében megfontolandó egy elfogó, vagy úgynevezett vadász (*hunter*) drón alkalmazása, mely szintén hálózatos, valamint precíz célzó és kioldószerkezettel van ellátva. A holland Delft Dynamics *DroneCatcherje* vagy a Fortem Technologies *Sky-Dome* rendszere, valamint a *DroneHunter 700-as* elfogója nemcsak a multirotoros egységeket, de még a merevszárnyú támadókat is képes hatástalanítani. Az elfogók védelmi-biztonsági alkalmazása több szempontból is megfontolandó. Egyrészt, ha a kellően fejlett detektáló rendszer rendelkezésre áll, a flotta könnyen megelőzhet egy támadást. Másrészt rendkívül mobilis, ugyanakkor a kritikus infrastruktúrától több kilométerre képes a veszélyt elhárítani. E védelmi rendszer azonban nemcsak a kritikus infrastruktúra védelmében játszhat fontos szerepet, hanem személy- és objektumvédelmi funkciókat is kiválóan elláthat.

A nyugati rendszerek tekintetében védelmi szempontból egyre nagyobb törekvés mutatkozik arra, hogy a potenciális veszélyt jelentő UAS-ek detektálását, valamint elhárítását egy önálló, országos hatáskörrel rendelkező szerv végezze, melyben a katonai nemzetbiztonság, a polgári nemzetbiztonság, valamint a rendészeti feladatok ellátásával megbízott szervek is szakterületenként képviseltetik magukat. Ugyanakkor az elhárítás tekintetében, figyelembe véve, hogy jelenleg a multirotoros vagy merevszárnyú UAV-k percnként egy km/h, vagy ennél gyorsabb sebességre is képesek, önálló döntési jogkörrel kell felruházni az elhárításért felelős szolgálatot. Fontos, hogy a jogos vagy jogellenes repülések adatvagyonának tárolására, valós időben való megfigyelésére és elemzésére elkészüljön egy adattár, amelyet szenzitivitása miatt jogosultságokon alapuló szakrendszerre szükséges fejleszteni, különösen, ha a technológia lehetővé teszi a kibertfelderítést, valamint a WAMI, vagyis a *wild-area motion imagery* alkalmazását.

Mint az a fenti példákból kitűnt, az irreguláris katonai erők, valamint terrorista csoportok rendkívül gyorsan adoptálták a dróntechnológiában rejlő potenciális lehetőségeket, ezáltal már az 1990-es évek elejétől igen széles körben a lehető legkülönbözőbb célokkal kezdték alkalmazni, különösen tervezett merényleteik eszközeként. A dróntechnológia jelentős lépéselőnyt biztosít a nevezett szélsőséges csoportok számára, hiszen a légifelderítéstől kezdve, a propagandafelvétel elkészítésén át, egészen a zavarásig, csempészésig mind olyan logisztikai szükségletet biztosít, amelyet egyes rejtőzködő elemek nem, vagy csak nagyon nehezen tudnának megoldani.

A támadások tekintetében látható, hogy a sejtek nem a mainstream gyártók által értékesített eszközöket választják, hanem többnyire legális úton a kereskedelmi forgalomban beszerezhető elemekből építik meg saját drónjaikat. Fontos kiemelni, hogy az eddigi támadások tekintetében az improvizált robbanószerkezetek, rakéták használata mellett, gyakorta terveznek és hajtanak végre támadást olyan drónokkal, melyek alkalmasak arra, hogy bizonyos vegyifegyvert, idegmérget, többek között szaringázt permetezzenek szét. A merénylettekkel szemben a nyugati példákat követve szükséges egy hatékony detektáló és elhárító rendszer kidolgozása, illetve kiépítése, mely összehangolt érzékelőkre, fenyegetés esetén pedig hibrid (*soft* és *hard kill*) megoldással a lehető legkevesebb kárt okozva a földre kényszeríti az UAV-t. A védelmi rendszer kiépítését a United States Cybersecurity & Infrastructure Security Agency által meghatározott pontokon szükséges kialakítani. Ugyanakkor a rendezvények alkalmával a lakosság biztonságának érdekében mobil detektáló és elhárító rendszert szükséges telepíteni.

Irodalomjegyzék

- Abbot, C., Donnellan, C., Clarke, M., Hathorn, S., & Hickie, S. (eds) (2016) *Hostile Drones: The Hostile Use of Drones by Non-State Actors*. Oxford Research Group. Remote Control Project, 2016
- Adam P. W., Anderson, M. L., & Westfall, J. T. (2021) *Countering Malicious small Unmanned Aerial System: Understanding the Problem for Border Security*. United States Air Force Academy. AIAA Scitech Conference, Colorado Springs. 2021. 01. 21. Virtual Event. https://www.researchgate.net/publication/348257974_Countering_Malicious_Small_Unmanned_Aerial_Systems_Understanding_the_Problem_for_Border_Security [Letöltve: 2023. 10. 27.]
- Almohammad, A., & Speckhard, A. (2017) *ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics*. International Center for the Study of Violent Extremism. <http://www.icsve.org/research-reports/isis-drones-evolution-leadership-bases-operations-and-logistics/> [Letöltve: 2024. 01. 05.]
- Al-Obaidi, A. S. M., Phang, S. K., & How, Y. G. (2019) *Improving aerodynamic efficiency of a Skywalker drone*. 13th International Engineering Research Conference (13th EURECA 2019). https://www.researchgate.net/publication/341171260_Improving_aerodynamic_efficiency_of_a_Skywalker_drone [Letöltve: 2023. 10. 29.]
- Altawy, R., & Youssef, A. M. (2016) *Security, privacy, and safety aspects of civilian drones a survey*. ACM Transaction on Cyber-Physical Systems, Vol. 1. No. 2. pp. 1–25.
- Archambault, E., & Veilleux-Lepage, Y. (2020) *Drone imagery in Islamic State propaganda: flying like a state*. International Affairs, Vol. 96. No. 4. 955–973.
- Balkan, S. (2017) *Daesh's drone strategy. Technology and the rise of innovative terrorism*. SETA, <https://www.seta.org/en/daeshs-drone-strategy-technology-and-the-rise-of-innovative-terrorism/> [Letöltve: 2023. 10. 27.]
- Basakand, S., Scheers, B. (2018) *Passive radiosystem for realtime drone detection and DoA estimation*. International Conference on Military Communications and Information System (ICMCIS), May 2018. pp.1–6.
- Berger, J. M., & Morgan, J. (2015) *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*. Brookings Institution. <https://www.brookings.edu/articles/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/> [Letöltve: 2024. 01. 05.]

- Bhushan, M. (2022) Biological and Chemical Threats and UAV Delivery System. A Lethal Combination. *Journal of Defence Studies*, Vol. 16. No. 4. 2022. pp. 159–179.
- Blair D. (2013) Iraq arrests five in 'al-Qaeda chemical weapons plot'. *Telegraph*, June 2, 2013. <https://www.telegraph.co.uk/news/worldnews/al-qaeda/10094187/Iraq-arrests-five-in-al-Qaeda-chemical-weapons-plot.html> [Letöltve: 2023. 10. 27.]
- Bloom, M., Horgan, J., & Winter, C. (2016). Depictions of children and youth in the Islamic State's martyrdom propaganda. *CTC Sentinel*, Vol. 9 No. 2. pp. 29–32.
- Borio, D., Gioia, C., Dimc, F., Bazec, M., Fortuny, J., Baldini, G., & Basso, M. (2015) An Experimental Evaluation of the GNSS Jamming Threat. 24th Electrotechnical and Computer Conference, Erk, Portorož, Slovenija. pp. 269–272.
- Budai Á. (2017) A Kolumbiai Forradalmi Fegyveres Erők (FARC): múlt, jelent, jövő. *Nemzet és Biztonság*, No. 2. pp. 68–94.
- Bunker, J., & Sullivan J. P. (eds) (2021) *Criminal Drone Evolution: Cartel Weaponization of Aerial IEDs*. XLibris US
- Bunker, R. J. (2015) Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications. *Strategic Studies Institute, US Army War College*. pp. 1–55.
- Cafarella, J., Dunford, J., Land, M., & Wallace, B. (2020) Turkey Commits to Idlib. *Institute for the Study of War*, 18 March 2020. <https://understandingwar.org/backgrounders/turkey-commits-idlib> [Letöltve: 2023. 10. 29.]
- Chavez, K., & Swed, O. (2020) Off the Shelf: The Violent Nonstate Actor Drone Threat. *Air & Space Power Journal*, Vol. 34. No. 3. pp. 29–43.
- Civil Aviation Authority Air Navigation Order 2016. No. 765. <https://www.legislation.gov.uk/ukxi/2016/765/data.xht?view=snippet&wrap=true> [Letöltve: 2024. 01. 22.]
- Clarke, C. P. (2018) Approaching a "New Normal": What the Drone Attack in Venezuela Portends. August 13, 2018. *National Security Program. Foreign Policy Research Institute*. <https://www.fpri.org/article/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela-portends/> [Letöltve: 2023. 10. 27.]
- Cohen, J. (1960) A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, Vol. 20. No. 1. pp. 37–46.
- Corfield, G. (2017) Drone Maker DJI Quietly Made Large Chunks of Iraq, Syria No-Fly Zones. *The Register*, 26 April 2017. https://www.theregister.com/2017/04/26/dji_drone_geofencing_iraq_syria/ [Letöltve: 2023. 11. 14.]
- Criminal Complaint: Affi-davit, United States vs. Rezwan Ferdaus. September 28, 2011. https://www.investigativeproject.org/documents/case_docs/1702.pdf [Letöltve: 2024. 01. 05.]
- Crino, S., & Dreby, C. (2020) Drone Attacks Against Critical Infrastructure: A Real and Present Threat. *Atlantic Council*. May 1. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/drone-attacks-against-critical-infrastructure-a-real-and-present-threat/> [Letöltve: 2023. 10. 27.]
- Cwojdzinski, M. A., & Admaski, M. (2014) Power units and power supply systems in UAV. *Aviation*, Vol. 18. No. 1. pp. 1–8.
- Dahm, J. M. (2020) *Electric Warfare and Signals Intelligence*. Johns Hopkins Applied Physics Laboratory LLC. pp. 2–24.
- Dévényi K. (2017) A dzsihád az iszlámban. *Világtörténet*, Vol. 39. No. 2. pp. 297–324.
- Difo G. (2010) Ordinary Measures, Extraordinary Results: An Assessment of Foiled Plots Science 9/11. *American Security Project*. 1–29. <https://www.jstor.org/stable/resrep06002> [Letöltve: 2024. 01. 05.]
- Diplomatic, Informational, Military, Economic. AJP-01 Allied Joint Doctrine. NATO Standardization Office, 2017. https://www.coe-med.org/files/stanags/01_AJP/AJP-01_EDE_V1_E_2437.pdf [Letöltve: 2023. 10. 27.]
- Dunn, D. H. (2013) Drones: disembodied aerial warfare and the unarticulated threat. *International Affairs*, Vol. 89. No. 5. pp. 1237–1246.
- Enav, P. (2014) Hamas Boasts New Level of Sophistication, Releasing Video Showing One of Its Drones for First Time. *National Post*, July 14, 2014. www.news.nationalpost.com/news/israel-says-it-shot-down-hamas-launched-drone-four-palestinians-killed-in-separate-airstrike [Letöltve: 2024. 01. 05.]
- Engel, J., Sturm, J., Cremers, D. (2012) Camera-based navigation of a low-cost quadcopter. *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 2815–2821.
- Final report of the Panel of Expertson Yemen. United Nations Security Council, S/2020/326, 28 April 2020, 82–84. <https://www.un.org/securitycouncil/sanctions/2140/panel-of-experts/work-and-mandate/reports> [Letöltve: 2023. 10. 29.]
- Fish, F. E. (2020) Bio-inspired aquatic drones. *Bioinspiration & Biomimetics*, Vol. 15. No. 6. DOI: 10.1088/1748-3190/abb002
- Fisher, A. (2015) Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence. *Perspectives on Terrorism*, Vol. 9. No. 3. pp. 3–20.
- Foulkes, C. H. (2001) "Gas!" The story of the special brigade. Uckfield, U.K.: Naval & Military Press
- Gambhir, H. (2016) *The Virtual Caliphate: ISIS's Information Warfare*. Institute for the Study of War, Wahington
- Ghazafi, S. M. (2022) Study on the Evolution of Drone Engine and the Future of Drone Propulsion. *International Journal of I.C. Engines and Gas Turbines*, Vol. 8. No. 1. 10–19.
- Gooch, K., & Treadwell, J. (2021) It doesn't stop at the Prison Gate: Understanding Organised Crime in Prison. *Prison Service Journal*, Vol. 252. pp. 15–30.
- Grossman, N. (2018) *Drones and terrorism: asymmetric warfare and the threat to global security*. London and New York: I. B. Tauris
- Gunaratna, R. (2018) Aum Shinrikyo's Rise, Fall and Revival. *Counter Terrorist Trends and Analyses*, Vol. 10. No. 8. pp. 1–6.
- Hartmann, K., & Giles, K. (2016) UAV Exploitation: A New Domain for Cyber Power. 2016 8th International Conference on Cyber Conflict. https://www.researchgate.net/publication/305871943_UAV_exploitation_A_new_domain_for_cyber_power [Letöltve: 2024. 01. 05.]
- Haugstvedt, H., & Jacobsen, J. O. (2020) Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors' Use of Weaponized Unmanned Aerial Vehicles (UAVs—'Drones'). *Perspectives on Terrorism*, Vol. 14. No. 5. (October 2020) pp. 26–40.
- Holland, A. M. (2019) *Counter-Drone Systems*. Center for the Study of the Drone at Bard College
- Huijgen, H., & Janssens, L. (2021) The Juridical Landscape of Countering Unmanned Aircraft System. In: Willis, C. M., Haider, A., Teletin, D. C., Wagner, D. (eds) *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. The Joint Air Power Competence Center, Kalkar. pp. 395–414.
- Hummel, S. (2016) The Islamic State and WMD: Assessing the Future Threat. *CTC Sentinel*, Vol. 9. No. 1. pp. 18–21.
- Jims, G., Wessley, J., & Chauhan, S. (2018) Parametric analysis of a down-scaled turbo jet engine suitable for drone and UAV propulsion. *International Conference on Electrical, Electronics, Materials and Applied Science*. https://www.researchgate.net/publication/324754398_Parametric_analysis_of_a_down-scaled_turbo_jet_engine_suitable_for_drone_and_UAV_propulsion [Letöltve: 2023. 10. 27.]
- Johnson, N. F., Zheng, M., Vorobyeva, Y., Gabriel, A., Qi, H., Velasquez, N., Manrique, P., Johnson, D., Restrepo, E.M., Song, C., & Wuchty, S. (2016) New Online Ecology of Adversarial Aggregates: ISIS and beyond. *Science*, Vol. 352. pp. 1459–1463.
- Jones, J. W. (2008) *Blood That Cries Out From The Earth: The Psychology of Religious Terrorism*. Oxford, Oxford University Press, 2008. pp. 71–87.
- Kaczkowski, W. (2019) Qualitative content analysis of images of children in Islamic State's Dabiq and Rumiya magazines. *Contemporary Voices: St Andrews Journal of International Relations*, Vol. 1. No. 2. pp. 26–38.

- Kaplan, B., Kahraman, I., Yarkan S., Ekti, A. R., & Cirpan, H. A. (2018) Detection Identification and Direction of Arrival Estimation of Drone FHSS Signals With Uniform Linear Antenna Array. *IEEE*. Vol. 8. pp. 27–69.
- Kishor, V., & Singh, S. (2015) Design and Development of Arduino Uno based Quadcopter. *International Journal of Engineering and Manufacturing Science*, Vol. 7. No. 1. pp. 14–19.
- Kovačević, I. (2020) Keče i dron. Modeli političke ekspresije na fudbalskim utakmicama albanske reprezentacije u Beogradu. *Етноантрополошки проблеми*, н. с. Vol. 15. No. 2. pp. 489–505.
- Kovacina, M. A., Palmer, D., Yang, G., & Vaidyanathan, R. (2002) Multi-agent Control Algorithms for Chemical Cloud Detection and Mapping using Unmanned Air Vehicles. *International Conference on Intelligent Robots and System*, Vol. 3. pp. 2782–2788.
- Kozić, N., Čančarević, A., Brusin, R., & Pokrajac, I. (2018) Jamming of GNSS signals. *Scientific Technical Review*, Vol. 68. No. 3. pp. 18–24.
- Krajnc Z. (2018) Drónok, hibrid fenyegetés, terrorizmus a légtérből: A légi hadviselés privatizálása. *Hadmérnök*, Vol. 13. No. 4. pp. 359–363.
- Kuusniemi, H., Airos, E., Zahidul, M., Bhuiyan, H., & Kroger, T. (2012) Effect of GNSS jammers on consumer grade satellite navigation receivers, *Proceedings of the European Navigation Conference (ENC)*, Gdansk, Poland pp. 1–14.
- Li, Y., Yonezawa, K., Xu, R., & Liu, H. (2021) A Biomimetic Rotor-configuration Design for Optimal Aerodynamic Performance in Quadrotor Drone. *Journal of Bionic Engineering*, Vol. 18. pp. 824–839.
- Lu, Y., Macias, D., Dean, Z. S., Kreger, N. R., & Wong, P. K. (2015) A UAV-Mounted Whole Cell Biosensor System for Environmental Monitoring Applications, *IEEE Trans. Nanobioscience*, Vol. 14, pp. 811–817.
- Ma, Y., & Yan, Y. (2016) Blind detection and parameter estimation of single frequency-hopping signal in complex electromagnetic environment. In *2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control. (IMCCC)*. pp. 370–374.
- Magdy, W., Darwish, K., & Weber, I. (2016) #FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support. <https://aaai.org/papers/12695-12695-failedrevolutions-using-twitter-to-study-the-antecedents-of-isis-support/> [Letöltve: 2024. 01. 05.]
- Maggioni, M., & Magri, P. (eds) (2015) *Twitter and Jihad: The Communication Strategy of ISIS*. Italian Institute for International Political Studies, Milan
- Marturano, F., Martelluci, L., Chierici, A., Malizia, A., Giovanni D. D., d'Errico, F., Gaudio, P., & Jean-Francois, C. (2021) Numerical Fluid Dynamics Simulation for Drones' Chemical Detection'. *Drones*, Vol. 5. No. 3. https://www.researchgate.net/publication/353579484_Numerical_Fluid_Dynamics_Simulation_for_Drones_Chemical_Detection [Letöltve: 2023. 10. 27.]
- McElroy, D. (2014) ISIS storms Saddam-era chemical weapons complex in Iraq. *Telegraph*, June 19, 2014. <https://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10913275/Isis-storms-Saddam-era-chemical-weapons-complex-in-Iraq.html> [Letöltve: 2023. 10. 27.]
- Miasnikov, E. (2005) *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects*, Moscow, Russia: Center for Arms Control, Energy and Environmental Studies Moscow Institute of Physics and Technology, 2005. pp. 3–26.
- Montanari, L., Royuela, L., Hasselberg, I., & Vandam, L. (eds) (2022) *Prison and drugs in Europe. Current and future challenges*. European Monitoring Centre for Drugs and Drug Addiction 25. Luxembourg, 2022
- Morrow, A., Pitsky, P., Samani, A., & Haider, A. (2021) Protection of Critical Infrastructure. <https://www.japcc.org/chapters/c-uas-protection-of-critical-infrastructure/> [Letöltve: 2023. 10. 30.]
- Mueller, J. (2014) Case 46: Model Planes. In: John Mueller (ed.) *Terrorism Since 9/11: The American Cases* (Washington, D.C.: Cato Institute, March 16, 2014). Decision on the Government's Motion for Detention, United States vs. Rezwan Ferdaus. November 28, 2011. <https://politicalscience.osu.edu/faculty/jmueller/46MODL7.pdf> [Letöltve: 2024. 01. 05.]
- Nagai, H., Nakamura, K., Fujita, K., Tanaka, I., Nagasaki, S., Kinjo, Y., Kuwazono, S., & Murozono, M. (2021) Development of Tailless Two-winged Flapping Drone with Gravity Center Position Control. *Sensors and Materials*, Vol. 33. No. 3. pp. 859–872.
- National Institute of Justice: Addressing Contraband in Prisons and Jails as the Threat of Drone Deliveries Grows. June 2, 2023, <https://nij.ojp.gov/topics/articles/addressing-contraband-prisons-and-jails-threat-drone-deliveries-grows>. [Letöltve: 2023. 10. 27.]
- Pledger, T. G. (2021) The Role of Drones in Future Terrorist Attack. *Land Warfare Paper*, No. 137. pp. 1–7.
- Popovski, P., Yomo, H., & Prasad, R. (2006) Strategies for adaptive frequency hopping in the unlicensed bands. *IEEE Wireless Communications*, Vol. 13. No. 6. pp. 60–67.
- Pyzynski, M., & Balcerzak, T. (2021) Cybersecurity of the Unmanned Aircraft System (UAS). *Journal of Intelligent & Robotic Systems*, Vol. 102. No. 2. pp. 1–13.
- Rabajczyk, A., Zboina, J., Zielecka, M., & Fellner, R. (2020) Monitoring of Selected CBRN Threats in the Air in Industrial Areas with the Use of Unmanned Aerial Vehicles. *Atmosphere*, Vol. 11. No. 12. https://www.researchgate.net/publication/347788031_Monitoring_of_Selected_CBRN_Threats_in_the_Air_in_Industrial_Areas_with_the_Use_of_Unmanned_Aerial_Vehicles [Letöltve: 2023. 11. 03.]
- Rassler, D. (2016) Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology. *Combating Terrorism Center*, No. October. <https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/> [Letöltve: 2024. 01. 05.]
- Rassler, D. (2018a) Drone Games, Terror Drone Diffusion, and Near-Term Threats. *The Islamic State and Drones: Supply, Scale, and Future Threats*. <https://www.jstor.org/stable/resrep21486.7> [Letöltés ideje: 2023. 10. 27.]
- Rassler, D. (2018b) *The Islamic State Drones. Supply, Scale, and Future Threats*. Combating Terrorism Center at West Point
- Renahan, J. N. (1997) *Unmanned Aerial Vehicles and Weapons of Mass Destruction. A Lethal Combination*. Air University Press. Maxwell Air Force Base, Alabama
- Rottler V. (2018) A drónhasználat jogi szabályozásának nemzetközi trendjei és hazai helyzete. *Magyar Rendészet*, No. 4. pp. 157–171.
- Rozenbeek, D. J. (2020) Evaluation of drone neutralization methods using radio jamming and spoofing techniques. *School of Electrical Engineering and Computer Science, KTH, Stockholm, Sweden, Tech. Rep.*
- Santos, A. C. S., & Oliveira, J. C. S. (2019) Arduino Applicability Model for the Construction of Flight Controller for Drones. *International Journal of Advanced Engineering Research and Science (IJAERS)*. Vol. 6. No. 4. 138–146.
- Shelley, A. (2020) *Essays in the Regulation of Drones and Counter-Drone System*. Victoria University of Wellington, 2020. pp. 147–149.
- Shu, C. (2017) DJI Adds Much of Iraq and Syria to Its List of No-Fly Zones for Its Drones. *TechCrunch*, 27 April 2017. https://consent.yahoo.com/v2/collectConsent?sessionId=3_cc-session_7ec8321e-3c5f-4919-8371-33fa43629393 [Letöltve: 2023. 10. 29.]
- Simons, E. (2006) Faith, Fanaticism, and Fear: Aum Shinrikyo – The Birth and Death of a Terrorist Organization. *Forensic Examiner*, Vol. 15. No. 1. pp. 37–45.
- Singer, P. W. (2015) Terror On Twitter: How ISIS Is Taking War To Social Media. *Popular Science*, Vol. 11. No. December. <https://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media/> [Letöltve: 2024. 01. 05.]

- Snell, A. E., & Keusenkothen, E. J. (1995) Mass Destruction Weapons Enter Arsenal of Terrorists. *National Defense*, January 1995. pp. 20–25.
- Strack, C. (2017) Islamic State's Chemical Weapons Efforts. *CTC Sentinel*, Vol. 10. No. 9. <https://ctc.westpoint.edu/the-evolution-of-the-islamic-states-chemical-weapons-efforts/> [Letöltve: 2023. 11. 03.]
- Strauss, M. J. (2013) Boundaries in the Sky and a Theory of Three-Dimensional States. *Journal of Borderlands Studies*, Vol. 28. No. 3. pp. 369–382.
- Sutthithon, D., Wongkamchang, P., & Sukuprakarn, N. (2021) Aerodynamic Studies of Small Box-Wing Unmanned Aerial Vehicle Using CFD. The 12th Asia Conference on Mechanical and Aerospace Engineering (ACMAE 2021). *Journal of Physics: Conference Series*, No. 3.
- Tabrizi, A. B., & Bronk, J. (2018) Armed Drones in the Middle East Proliferation and Norms in the Region. *Royal United Services Institute for Defence and Security Studies*. London
- Tanaka, S., Asignacion, A., Nakata, T., Suzuki, S., & Liu, H. (2022) Review of Biomimetic Approches for Drones. *Drones*, Vol. 6. No. 11. 2022. https://www.researchgate.net/publication/364761994_Review_of_Biomimetic_Approaches_for_Drones [Letöltve: 2024. 01. 05.]
- Terrorism 2002–2005. U.S. Department of Justice. Federal Bureau of Investigation. Counterterrorism Division. https://www.fbi.gov/file-repository/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view [Letöltve: 2024. 01. 05.]
- Tipl, A. H., Wadhel, V. B., Sawant, H. S., Sawant, T. T., & Sawant, S. S. (2019) Design of Surveillance Based Quadcopter using Arduino. *SSRG International Journal of Electrical and Electronics Engineering (SSRG - IJEEE)*. Vol. 6. No. 3. pp. 1–4.
- Tomkins, R. (2018) Rafael Unveils Drone Dome Anti-Drone System. *United Press International (UPI)*, 23 June 2018. <https://www.upi.com/Defense-News/2017/06/23/Rafael-unveils-Drone-Dome-anti-drone-system/9161498239207/> [Letöltve: 2023. 10. 27.]
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA). Situation Report 1-38. Lebanon Response. <https://www.unocha.org/publications/report/israel/lebanon-response-ocha-situation-report-no-38> [Letöltve: 2024. 01. 05.]
- Urcosta, R. B. (2020) The Revolution in Drone Warfare. The Lessons from the Idlih De-Escalation Zone. *Journal of European, Middle Eastern, & African Affairs*, Vol. 2. No. 3. pp. 50–65.
- Voskuijl, M., Dekkers, T., Savelsberg, R. (2020) Performance Analysis of the Samad Attack Drones Operated by Houthis Armed Forces. *Science & Global Security*, Vol. 28. No. 3. pp. 1–22.
- Xiufang, S., Chaoqun, Y., Weige, X., Chao, L., Zhiguo, S., & Jiming, C. (2018) Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges. *IEEE Communication Magazine*, Vol. 56. No. 4. pp. 68–74.
- Yaacoub, J-P., Noura, H., Salman, O., & Chehab, A. (2020) Security analysis of drones systems: Attack, liminations, and recommendations. *Internet of Things*, Vol. 11. September. <https://www.sciencedirect.com/science/article/pii/S2542660519302112> [Letöltve: 2024. 01. 05.]
- Yu, D., Judasz, A., Zheng, M., & Botta, E. M. (2022) Design and Testing of a Net-Launch Device for Drone Capture. *AIAA SC-ITECH 2022 Forum*. pp. 1–15.