Huszár Péter[1]

Drónok elleni fenyegetések a kibertérből
Threats against drones from cyberspace

Absztrakt
A publikáció azt a kérdést járja körül, hogy a manapság egyre nagyobb népszerűségnek örvendő, kereskedelmi forgalomban kapható, bárki által szabadon hozzáférhető pilóta nélküli légi járművek (köznyelvben elterjedten: drónok) mennyire vannak kitéve különböző, kibertérből származó fenyegetéseknek. Ehhez ismerteti a kibertér és a pilóta nélküli légijárműrendszer meghatározását, bemutatja egy ilyen rendszer általános felépítését és részegységeit, ezek alapján pedig rámutat a kettő közötti kapcsolatra. Ezt követően röviden ismerteti azokat a támadási felületeket és módszereket, amelyek már létező, kibertérből származó fenyegetést jelentenek a pilóta nélküli légi járművek számára. Végül a publikáció kitér arra is, hogy hogyan használhatók ezek a megoldások a pilóta nélküli légi járművekkel szembeni védekezés során.

Kulcsszavak: UAV, CUAV, drón, kibertér, drónok elleni védekezés

Abstract
The publication addresses the question whether commercially available unmanned aircraft (commonly known as drones), which are becoming increasingly popular today and are freely accessible to anyone, are exposed to various cyberspace threats or not. It describes the definition of cyberspace and the unmanned aerial vehicle system, presents the general structure and components of such a system and points out the relationship between the two. It then briefly describes the attack vectors and methods that pose an existing cyberspace threat to unmanned aerial vehicles. Finally, the publication also discusses how these solutions can be used in defense against unmanned aerial vehicles.

Keywords: UAV, CUAV, drone, cyberspace, protection against drones

1. Bevezetés

A számítástechnika töretlen fejlődésének eredményeképpen mára a legtöbb ember életében megkerülhetetlen szerepet töltenek be a különböző informatikai eszközök, szoftverek és az internet. A vezeték nélküli kommunikációs technológiák kifejlesztése és elterjedése e folyamat egyik kulcsfontosságú alappillére. Az IEEE 802.11 (elterjedt nevén: WiFi), a mobilhálózatok lefedettsége és a korszerű mobilinternet használati eszközeink milliárdjait kötik össze egymással világszerte szünet nélkül. Napjaink fejlett technológiája által nyújtott kényelemnek azonban megvan az ára. A hálózatos társadalomban számos új lehetőség kínálkozik egyének, szervezetek és nemzetek ellen irányuló támadás végrehajtására. Legyen szó akár rejtett információgyűjtésről, ipari létesítmények működésének befolyásolásáról vagy kiberhadviselésről. E világméretű hálózat végpontjai azonban nem csupán személyi számítógépek és mobiltelefonok lehetnek. Számos autonóm eszköz, szenzor és ipari berendezés is folyamatosan elérhető az interneten keresztül. Adódik viszont a kérdés, hogy a manapság egyre nagyobb népszerűségnek örvendő kisméretű pilóta nélküli légijárműrendszerek (sUAS - Small Unmanned Aircraft System), amelyek kisebb lokális vezeték nélküli hálózatok vagy akár, az internet, mint globális hálózat részei is lehetnek, tekinthetők-e a kibertér részeként? Alkalmazhatók-e velük szemben

[1] Doktorandusz, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola, e-mail: huszar.peter.92@gmail.com, ORCID: https://orcid.org/0000-0001-6169-3777

már létező kibertámadási módszerek? „Feltörhetők-e" távolról az operátor tudta nélkül klasszikus kibertámadási eljárásokkal? Ha igen, milyen és mekkora veszélyt jelentenek a megtámadott drónok? Végül fontos megvizsgálni azt is, ha erre van lehetőség, akkor hogyan lehet a nem kívánt, azonosítatlan, behatoló drónokkal szemben alkalmazni és így a velük szembeni védekezésre használni e módszereket.

2. A kibertér és a pilóta nélküli légijárműrendszer

A kiberteret az évek során több különböző módon is meghatározták[2]. Ki-ki saját aspektusaiból. Abban azonban a legtöbb definíció egyetért, hogy hálózatba kapcsolt infokommunikációs eszközök felhasználásával, adatgyűjtésre, tárolásra és továbbításra létrehozott kapcsolatok összessége. A pilóta nélküli repülők szempontjából fontos, hogy nem csak vezetékes, de vezeték nélküli kapcsolatok is a kibertér részét képezik.
A UAS értelmezésére is, a kibertérhez hasonlóan, különböző definíciók születtek az évek során. A Szövetségi Légügyi Hatóság (Federal Aviation Administration – FAA), a Nemzetközi Polgári Repülési Szervezet (International Civil Aviation Organization – ICAO) és az Európai Repülésbiztonsági Ügynökség (European Aviation Safety Agency – EASA) definíciói is eltérnek némileg. Ez jól látható a Joint Authorities for Rulemaking on Unmanned Systems (JARUS) összefoglalójában[3], valamint más szakmai művekben is[4]. Az apró különbségek ellenére abban viszont mind egyetértenek, hogy az UAS része a pilóta nélküli légi jármű (UAV – Unmanned Aerial Vehicle) és annak földi irányító állomása (GCS – Ground Control Station), valamint a kettő közötti vezeték nélküli adatkapcsolat. Ez már a 2020-ban hatályba lépő Európai Uniós, a pilóta nélküli légi járművekkel végzett műveletekre vonatkozó rendeletben[5] is észrevehető.
A földi állomás jellemzően egy távirányítóból és/vagy egy kiegészítő számítógépből, mobiltelefonból épül fel. A kiegészítő számítógépen történik a repülési útvonal kijelölése és a beérkező adatok, élő videókép kijelzése, tárolása és kiértékelése. Ehhez kapcsolódhat még vezetékes vagy akár vezeték nélküli kapcsolat segítségével maga a távirányító. A távirányító és a drón között egy másik vezeték nélküli kapcsolat kerül kialakításra. Olyan, ami sokkal jobban megfelel a drónok irányítása által támasztott követelményeknek. Ez a későbbiekben kifejtésre kerül.
Méret szerinti csoportosítás szerint az UAS-ek egy alcsoportját képezik az sUAS-ek, amelyek esetében a pilóta nélküli légijárműrendszer részét képező UAV maximális felszálló tömege (MTOW – Maximum Take-off Weight) nem haladja meg a 25 kg-ot. Maximális repülési sebessége 160 km/h, repülési magassága pedig kevesebb, mint 400 láb AGL (Above Ground Level – talajszint feletti magasság).[6] Ebbe a csoportba tartoznak a legnépszerűbb kereskedelmi forgalomban, bárki által szabadon hozzáférhető drónok. Köztük megtalálhatók merevszárnyas (Fixed Wing UAV) modellek is, de az eladott modellek túlnyomó többsége valamilyen multirotoros, forgószárnyas (Rotary Wing UAV) kialakítású eszköz. Az említett kategóriába tartozik például a DJI egyik legújabb drónja. A 249 g felszálló tömeggel, 30 perces repülési idővel, 2 km-es hatótávolsággal és élő, nagy felbontású videó közvetítésre képes DJI Mavic Mini. Valamint szintén ide sorolható a cég másik terméke, a 24,5 kg maximális felszálló tömegű, nyolc rotoros permetező drón a DJI Agras MG1 is. Ebből látható, hogy e kategória rendkívül széles spektrumot ölel fel és az ide sorolható drónokkal elvégezhető feladatok is hasonlóan változatosak.

---

[2] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018. ISBN 978-615-5945-05-2
[3] Julia Sanchez: *JARUS Glossary*. Edition 7. 2018. p. 83.
[4] Reg Austin: *Unmanned Aircraft Systems. UAVs Design, Developement and Deployment*. 2010. Wiley, ISBN: 978-0-470-05819-0, p. 3.
[5] EU 2019/947 Az Európai Bizottság végrehajtási rendelete a pilóta nélküli légi járművekkel végzett műveletekre vonatkozó szabályokról és eljárásokról, 2. cikk, 1. bekezdés
[6] Liling Ren et alii: *Small Unmanned Aircraft System (sUAS) Categorization Framework for Low Altitude Traffic Services.* IEEE AIAA 36th Digital Avionics Systems Conference, 2017. ISBN: 978-1-5386-0365-9/17

A rendszer következő fontos része az UAS működéséhez szükséges vezeték nélküli kommunikációs csatorna. Egy UAS több különböző vezeték nélküli kapcsolatot is használhat egy időben. E szempontból megkülönböztethető egy, az UAV vezérlésre és telemetriás adatok fogadására fenntartott csatorna (CNPC – Control and Non-Payload Communication) és egy másik, a hasznos teherrel történő kommunikációra használt csatorna (PC - Payload Communication). A kettő között az eltérő jellemzőik miatt kell különbséget tenni. Míg a CNPC-nek robosztusnak kell lennie minimális adatmennyiség átvitele mellett, magas rendelkezésre állással, addig a PC csatornán jóval nagyobb mennyiségű adatot kell eljuttatni az UAV-tól a GCS felé (pl.: nagy felbontású élő videó). A két kommunikációs csatorna gyakran különböző frekvenciatartományokban működik. Elterjedt megoldás, hogy a CNPC például 2,4 GHz-es, a PC pedig 5,8 GHz-es ISM[7] sávot használja. Az alacsonyabb frekvenciák kedvezőbbek a nagyobb távolságú rádiós összeköttetések létrehozására. Magasabb frekvenciákon viszont nagyobb adatátviteli sávszélesség alkalmazható, viszont előtérbe kerül az UAV és a GCS antennák közötti optikai rálátás biztosításának szükségessége. Az sUAS-ek esetében igen sokféle alkalmazott kommunikációs protokollal találkozhatunk, legyen az PC vagy CNPC csatorna. Használnak szabványos IEEE vezeték nélküli kommunikációs protokollokat (pl.: IEEE 802.15.4 ZigBee, IEEE 802.11 WiFi, IEEE 802.15.1 Bluetooth), RC[8] kommunikációs protokollokat (pl.: PCM[9], PPM[10], DSMX[11] stb.). Egyes gyártók saját fejlesztésű, szabadalmaztatott megoldásokat használnak (pl.: DJI Lightbridge 1 és 2, DJI OcuSync). Léteznek széles körben elterjedt nyílt forráskódú protokollok is (pl.: MAVLink 1 és 2).
Az előzőek alapján látható, hogy napjaink drónjai és az azokhoz tartozó kiegészítő eszközök, távirányítók, földi állomások számos olyan technológiát használnak, mint a mobiltelefonok, IoT eszközök és számítógépek. Ezek alapján és a korábban ismertetett definíciók alapján pedig megállapítható, hogy az sUAS-ek a kibertér részének tekinthetők.

3. Sebezhetőségek és támadási módszerek

Az sUAS-ekkel szemben alkalmazott kibertámadások fókuszában a rendszer bizalmasságának, integritásának és rendelkezésre állásának befolyásolása illetve lerontása áll, valamint az irányításának és felügyeletének az átvétele. A bizalmasság feltételezi, hogy a rendszerben kezelt információkhoz csak az arra jogosultak férnek hozzá. Ennek eredményeképpen az UAV és a GCS közti kommunikáció nem, vagy csak nehezen lehallgatható. Az integritás megléte biztosítja, hogy csak érvényes és eredeti információ kerül felhasználásra, ezzel biztosítva a megfelelő működést. A rendelkezésre állás pedig azt jelenti, hogy a pilóta nélküli légijárműrendszer folyamatosan megszakítás nélkül elérhető a névleges teljesítményén, amikor arra a felhasználónak szükség van.[12]
A SkyJack[13] és a DroneJack két olyan eszköz, amelyek kifejezetten WiFi kommunikációs protokollt használó COTS (Commercial off the Shelf – kereskedelmi forgalomban szabadon hozzáférhető) drónok irányításának átvételére lettek létrehozva. Mindkét megoldás WiFi hálózatok biztonságosságának tesztelésére és sebezhetőségeinek felfedésére használt szoftvercsomagokra

[7] ISM: Industrial Scientific and Medical – Ipari, tudományos és egészségügyi elektronikus berendezések működésére kijelölt frekvencia tartomány.
[8] RC: Radio Control – Rádió távirányítású modellekhez használt eszközök és technológiák összefoglaló neve.
[9] PCM: Pulse-code Modulation – Pulzus Kód Moduláció
[10] PPM: Pulse Position Modulation – Pulzus Pozíciós Moduláció
[11] DSMX: Digital Spectrum Modulation – Digitális Spektrum Moduláció
[12] Young-Min Kwon et alii: *Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles*, 2018. DOI: 10.1109/ACCESS.2018.2863237
[13] https://github.com/samyk/skyjack

épül (pl.: arcrack-ng[14] és airodump-ng[15]). Működésük során folyamatosan monitorozzák a hatótávolságon belüli WiFi hálózatokat és, ha találnak egy drónhoz köthető MAC[16] címet, a támadás automatikusan megkezdődik. A MAC címek és az azokat birtokló cégek nevei szabadon hozzáférhetőek internetes adatbázisokban[17]. A MAC címeket összehasonlítva ezekkel az adatbázisokkal, jó eséllyel eldönthető egy hálózati eszközről, hogy az egy drón vagy sem. A támadás következő lépéseként mindkét megoldás de-autentikációs csomagokat küldve megpróbálja megszakítani a GCS és az UAV közötti kapcsolatot. Amint ez sikerül a legtöbb drón aktiválja az ilyen esetekre előre definiált vészhelyzeti protokolljainak egyikét. Ez lehet például automatikus hazatérés (RTH - Return to Home) vagy egyhelyben lebegés (LOIT - Loiter). Közben az eszköz várakozik a kapcsolat helyreállására. Azonban, ha az előzőleg megszakadt kapcsolat nem védett például jelszóval, akkor mindkét megoldás el tudja foglalni a GCS helyét, ezzel átvéve az irányítást a drón felett. Ezt követően a DroneJack képes megadott GPS koordinátákra leszállítani a drónt, vagy visszaküldeni a felszállási helyére. Parrot drónok esetében a motorok azonnali leállítására is képes, mivel a gyártó implementálta ezt a lehetőséget is eszközeibe, mint vészhelyzeti protokollt. Míg a DroneJack néhány Raspberry Pi[18]-ből és egy internetes felhasználói felületből áll, addig a SkyJack egy légi platform. Az említett támadások csak egy részére képes, de azokat egy másik, támadó drón fedélzetéről indítja. Repülés közben képes felderíteni a környezetében lévő feltörhető drónokat és átvenni felettük az irányítást.[19] E két megoldás bizonyítottan működik és hatásos bizonyos típusú drónokkal szemben. Használatuk nem igényel különleges eszközöket és a szoftvercsomagok melyeken alapulnak sem kifejezetten drónok elleni használatra lettek létrehozva viszont erre az esetre is jól használhatónak bizonyultak. A támadási felület mindkét esetben a drón és a földi szegmens közötti WiFi kapcsolat. A sérülékeny drónok köre azonban szűk. Mindkét megoldás a Parrot cég AR és Bebop típusú drónjainak sebezhetőségét használja ki.

A nyíltforrású UAV és GCS közti kommunikációs célra kifejlesztett protokollok egyik legjobb példája a 2009-óta elérhető és azóta egyre nagyobb népszerűségnek örvendő MAVLink (Micro Air Vehicle Link). Nagyobb drónrobotpilóta-gyártók és nyílt forráskódú repülésszabályzók (FCU – Flight Control Unit), mint például a népszerű Pixhawk és az ArduPilot is ezt használják. A MAVLink egy üzenet alapú, kétirányú, titkosítatlan protokoll. Az egyes üzenetek felépítését pontosan meg lehet ismerni szabadon hozzáférhető dokumentumok alapján. Szintén ISM frekvenciasávokon használják, de gyakran 1 GHz alatt is, mint például a 433 MHz-es sáv. A DroneCode Project[20] része. Szüntelen tesztelésnek és fejlesztésnek van kitéve a felhasználók által a szabad hozzáférhetőségből adódóan, ezért folyamatosan és változatos módszerekkel próbálják feltörni.

Egy másik tanulmány[21] például azt mutatja be, hogy úgynevezett protokoll fuzzing[22] technikát alkalmazva, hogyan lehet kihasználni a MAVLink egyik sérülékenységét. A módszer lényege az ismert, szabadon hozzáférhető, titkosítatlan kommunikációs protokollból fakad. A támadó

---

[14] https://www.aircrack-ng.org/

[15] https://www.aircrack-ng.org/doku.php?id=airodump-ng

[16] MAC: Media Access Control - Hálózati eszközök egyedi azonosítója.

[17] Az IEEE regisztrációs hatóságától megvásárolt egyedi szervezeti azonosítói tartományok adatbázisa (OUI – Organizationally Unique Identifier): http://standards-oui.ieee.org/oui/oui.txt

[18] Bankkártya méretű egykártyás számítógép.

[19] Guillaume Fournier et alii: *DroneJack: Kiss your drones goodbye!* SSTIC 2017-Symposium sur la sécurité des technologies de l'information et des communications, Rennes, France, 2017; Kamkar, Samy: SkyJack project GitHub page.

[20] Egy nyílt forráskódú UAV platform megalkotásán és szabványosításán dolgozó munkacsoport. Tagjai között számos nagy technológiai vállalat megtalálható. https://www.dronecode.org/

[21] Karel Domin et alii: *Security Analysis of the Drone Communicatoion Protocol: Fuzzing the MAVLink protocol*, 2016. Brussels, Belgium,

[22] A protokoll fuzzing egy szoftver tesztelési eljárás, amely során különböző algoritmusok hibakezelési és hibatűrési képességeit vizsgálják nem várt, érvénytelen és szélsőséges bemeneti értékek felhasználásával.

eszköz a kommunikáció átvételét követően a protokollnak minden tekintetben megfelelő és a korábbiakkal megegyező kommunikációs csomagokat küld a drón számára. Viszont a bennük lévő adatmezőket úgy állítja elő, hogy a fogadó drón fedélzeti számítógépében futó, MAVLink csomagokat feldolgozó algoritmusoknak szélsőséges értékeket kelljen feldolgozni és hibaállapotokat kelljen folyamatosan kezelni. Ha minden feldolgozó algoritmus minden lehetséges hibás bejövő érték kezelésére tökéletesen fel lenne készítve, akkor ez nem jelentene problémát. A valóságban azonban ez nem így van. A kutatóknak az egyik teszt során sikerült is a drón fedélzeti számítógépében olyan kritikus hibát okozni, hogy az, ha csak nem SITL (Software in the Loop) szimulátor lett volna, hanem egy valódi eszköz, feltehetően azonnal lezuhan.
Az előző módszerek az úgynevezett beékelődéses (MITM – Man in the Middle) támadásnak tekinthetők. Ilyenkor a támadónak fizikálisan is a létrejött kapcsolat közelében, valahol a két végpont között kell elhelyezkednie. Ekkor lehetőség nyílik az adatfolyam vételére és dekriptálására is, ha erre van egyáltalán szükség. A MAVLink például egyáltalán nem használ semmilyen titkosítást egyelőre, bár a nyílt forráskódúságnak köszönhetően több kutató is megvizsgálta a titkosításának lehetőségeit az utóbbi években.[23] A WiFi-n kommunikáló drónok esetében pedig a felhasználó döntheti el, hogy szeretné-e jelszóval védeni az sUAS hálózatát vagy sem. A sikeres beékelődést követően további támadásokra nyílik lehetőség. A kommunikáció lehallgatása kézenfekvő lehet ezen a ponton. Ez az adatkapcsolat bizalmassága ellen irányuló támadás. Az ismert kommunikációs protokoll esetén a támadó fél hamis csomagokat küldhet magának a drónnak vagy a földi szegmensnek, ahogy azt az előzőekben a fuzzing módszernél láthattuk. Ez a kapcsolat integritását és elérhetőségét befolyásolja. A következő lépés lehet egy szolgáltatás megtagadásos (DoS - Denial of Service) támadás. Ekkor a támadó a beékelődést követően kisajátítja a kommunikációs csatornát annak túlterhelésével. A bemutatott SkyJack és DroneJack is képes folyamatos deautentikációs csomagok küldésével telíteni és túlterhelni a sérülékeny drónt. Ezzel csökkentve az UAS rendelkezésre állását. Ezek a támadások kifejezetten problémásak a MAVLink esetében a nyíltforráskódúság és titkosítatlanság miatt.

4. Kibertámadáson alapuló drón elhárítás

Tanulmányok és híradások alapján tudjuk, hogy a kereskedelmi forgalomban kapható drónokat, egyszerűen és olcsón át lehet alakítani akár bűnelkövetési célokra is.[24] Repülési hatótávolságuk növelhető nagynyereségű antennák és követő antenna platform használatával.[25] Működésük erősen függ a globális helymeghatározási rendszerek rendelkezésre állásától, melyek vétele szintén befolyásolható.[26] Azonban nem feltétlen kell egy drónt átalakítani ahhoz, hogy valaki kárt tudjon okozni vele. Elegendő azt megzavarni, kommunikációját lehallgatni, esetleg átvenni felette az irányítást és pusztán nekivezetni egy célpnak, ami lehet akár egy személy vagy egy utasszállító repülőgép is. Az előzőek alapján látható, hogy mindezekre van lehetőség és eszköz, ráadásul a drónokhoz hasonlóan többségében olcsók és szabadon hozzáférhetők. A drónok elleni védekezés képességének kialakítására, többek között azok kiberbiztonsági problémái miatt több szempontból is szükség lehet. Az egyik, amikor a drónt egy támadó direkt módon olyan tevékenységre használja, ami tiltott, veszélyes vagy kárt akar azzal okozni. A másik aspektus,

---

[23] Azza Allouch et al.: *MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems*. 2019.
[24] Don Rassler: „*The islamic state and drones: supply scale and future threats",* 2018; Krajnc Zoltán: *Drónok, hibrid fenyegetés, terrorizmus a légtérből: a légi hadviselés privatizálása*. Hadmérnök, XIII. 4. 2018. 358-369; Huszár Péter: *Ukrajna közösségi finanszírozású, katonai célokat szolgáló oktokoptereinek elemzése*. Hadmérnök, XIV. 2. 2019. 34-43
[25] Huszár Péter: *UAV és földi szegmense közötti kommunikáció hatékonyságának javítása,* Repüléstudományi Közlemények, XXXI. 1. 2019. 167-182
[26] Wührl Tibor: *GPS navigációs problémák UAV alkalmazásokban*, Hadmérnök, 6. Robothadviselés Tudományos Szakmai Konferencia különszám, 2006.

amikor a támadó célja egy szabályosan működő drón eltérítése, megzavarása esetleg a kommunikációjának lehallgatása. Ez utóbbinak kiemelt jelentősége lehet állami célú drónüzemeltetés terén. Látható, hogy van arra technikai lehetőség, hogy drónokkal szemben olyan elhárítási módszerek és rendszerek kerüljenek alkalmazásra, amelyek az UAS kommunikációs hálózatainak sebezhetőségeit használják ki és a fenti megoldások egyikét a védelem javára fordítsák. A bemutatott SkyJack és DroneJack megoldások pontosan erre lettek létrehozva. Alapvetően mindkettő egy kezdetleges drónelhárító, illetve semlegesítő rendszer néhány elemét valósítja meg. Működésük során képesek észlelni, követni és befolyásolni egy ellenőrzött területre behatoló drónt. Ugyanakkor az is egyértelmű, hogy pusztán kibertámadási módszerek nem lehet hatékonyan védekezni drónokkal szemben. Az előre beprogramozott, autonóm módon működő eszközök végrehajthatják feladataikat akár vezeték nélküli kommunikáció nélkül is. A gyűjtött adatokat tárolhatják fedélzeti memóriában, amiből azok kinyerhetők a visszatérésüket követően. További hiányosságuk, hogy a drón rajokkal szemben tehetetlenek. A behatoló drónokat csak egyesével képesek kezelni. Manapság ez még lehet, hogy elégséges, de a közeljövőben biztosan nem lesz az. Az egymással hatékonyan együttműködni képes, egyetlen operátort igénylő, több tíz akár több száz drónból álló rajokra már most is lehet példákat találni. Gondoljunk csak a 2018. évi phjongcsangi téli olimpia megnyitójára, ahol nyolcszáz drónból álló raj segítségével tartottak látványos bemutatót.

5. Összegzés

Egy UAS működése során létrehozott vezeték nélküli kapcsolatok hasonló sebezhetőségekkel rendelkeznek, mint bármelyik hétköznapi számítógép hálózat. A MAVLink sérülékenységeivel és támadási lehetőségeivel az itt bemutatottakon kívül több tanulmány is foglalkozik. A közös mindegyikben, hogy abból indulnak ki, hogy ismert a protokoll és egyelőre titkosítatlan. A nem nyíltforrású drón kommunikációs technológiák közül pedig azok a sebezhetőbbek, amelyek szabványos WiFi protokollt használnak. Gond nélkül használhatók azok a már létező támadási módok, eszközök és szoftverek, amelyek nem kifejezetten pilóta nélküli repülőrendszerek támadására lettek létrehozva, de a megegyező technológia miatt kézenfekvő megoldásnak bizonyulnak. A különböző hálózatos támadások veszélyeztetik az UAS, mint eszköz rendszer integritását, rendelkezésre állását és a rajta keresztül áramló adatok bizalmasságát. A hálózat adatfolyama lehallgatható, a benne résztvevő kommunikációs végpontok pedig félrevezethetők egyedi kommunikációs csomagok injektálásával vagy adott csomagok rögzítésével és folyamatos visszajátszásával. A kommunikációs csatornák telíthetők ezzel szolgáltatás kiesést okozva és így csökkentve a rendszer rendelkezésre állását.
Bár a látóhatáron túli (BVLOS - Beyond Line of Sight) repülések egyelőre inkább a katonai alkalmazásokban terjedtek el, a polgári felhasználási irányok és az azt kiszolgáló ipar fejlődése afelé mutat, hogy a közeljövőben a civil alkalmazásokban is nagy jelentőséggel fog bírni ez a felhasználási terület. Itt fontos megjegyezni azt is, hogy a jelenlegi technológia már most is lehetővé teszi a látóhatáron túli drónrepülések kivitelezését. Sokkal inkább jogi akadályai vannak a széleskörű elterjedésének. E jogi akadály elhárításának pedig kritériuma, hogy a drónok még tovább integrálódjanak a kibertérbe. A mobil technológiák drónkommunikációs célokra történő felhasználásával pedig a drónok a mobiltelefonokhoz hasonlóan, szinte folyamatosan hálózati eszközökként működnek majd. Azok nem csak saját, de más földi állomásokkal és más drónokkal is kommunikálni fognak. Ez már jelenleg is felvet számos kiberbiztonsági és adatvédelmi problémát, viszont a jövőben ez csak tovább fog erősödni. A drónok kiberbiztonsági problémáira növekvő hangsúlyt kell fektetni úgy az iparnak, mint a témával foglalkozó kutatóknak.

Köszönetnyilvánítás:

AZ INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM ÚNKP-19-3-I-NKE-69 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.

Hivatkozások

Allouch, Azza. et al.: *MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems.* 2019, url.: https://arxiv.org/pdf/1905.00265.pdf (Megtekintés: 2020. 02. 24.)

Austin, Reg: *Unmanned Aircraft Systems. UAVs Design, Developement and Deployment*. 2010. Wiley, ISBN:978-0-470-05819-0, p. 3.

Domin, Karel. et alii: *Security Analysis of the Drone Communicatoion Protocol: Fuzzing the MAVLink protocol*, 2016. url.: https://www.esat.kuleuven.be/cosic/publications/article-2667.pdf (Megtekintés: 2020. 02. 23.)

EU 2019/947 Az Európai Bizottság végrehajtási rendelete a pilóta nélküli légi járművekkel végzett műveletekre vonatkozó szabályokról és eljárásokról (2019. 05. 24.) 2. cikk, 1. bekezdés url.: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0947&from=EN (Megtekintés: 2020. 02. 24.)

Fournier, Guillaume et alii: *DroneJack: Kiss your drones goodbye!*. SSTIC 2017-Symposium sur la sécurité des technologies de l'information et des communications, Rennes, France, url.: https://hal.inria.fr/hal-01635125/document (Megtekintés: 2020. 02. 24.)

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018. ISBN 978-615-5945-05-2 Budapest, url.: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf;jsessionid=2EE93F6A71126B0827915CE804D3B7D2?sequence=1 (Megtekintés: 2020. 02. 23.)

Huszár Péter: *UAV és földi szegmense közötti kommunikáció hatékonyságának javítása,* Repüléstudományi Közlemények, XXXI. 1. 2019. 167-182, url.: http://journals.uni-nke.hu/index.php/reptudkoz/article/view/276/43 (Megtekintés: 2020. 02. 23.)

Huszár Péter: *Ukrajna közösségi finanszírozású, katonai célokat szolgáló oktokoptereinek elemzése*. Hadmérnök, XIV. 2. 2019. 34-43, url.: http://www.hadmernok.hu/192_03_huszar.pdf (Megtekintés: 2020. 02. 23.)

Kamkar, Samy: SkyJack project GitHub page. url.: https://github.com/samyk/skyjack (Megtekintés: 2020. 02. 23.)

Krajnc Zoltán: *Drónok, hibrid fenyegetés, terrorizmus a légtérből: a légi hadviselés privatizálása*. Hadmérnök, XIII. 4. 2018. 358-369, url.: http://hadmernok.hu/184_29_kranjc.pdf (Megtekintés: 2020. 02. 23.)

Kwon, Young-Min et alii: *Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles*, 2018. DOI: 10.1109/ACCESS.2018.2863237 url.: https://csi.dgist.ac.kr/uploads/Publications/2018-Access.pdf (Megtekintés: 2020. 02. 23.)

Rassler, Don: „*The islamic state and drones: supply scale and future threats",* 2018. url.: https://ctc.usma.edu/app/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf (Megtekintés: 2020. 02. 23.)

Ren, Liling. et alii: *Small Unmanned Aircraft System (sUAS) Categorization Framework for Low Altitude Traffic Services.* IEEE AIAA 36th Digital Avionics Systems Conference, 2017. ISBN: 978-1-5386-0365-9/17, url.: https://utm.arc.nasa.gov/docs/2017-Ren_DASC17.pdf (Megtekintés: 2020. 02. 24.)

Sanchez, Julia: *JARUS Glossary*. Edition 7. 2018. p.83. url.: http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_del_jarus_glossary_v0.7_0.pdf (Letöltve: 2020. 02. 23.)

Wührl Tibor: *GPS navigációs problémák UAV alkalmazásokban*, Hadmérnök, 6. Robothadviselés Tudományos Szakmai Konferencia különszám, 2006. url.: http://hadmernok.hu/kulonszamok/robothadviseles6/wuhrl_rw6.html (Letöltve: 2020. 02. 23.)