A jövő nagy kihívása: kiberbiztonság és kiberhadviselés

A Magyar Természettudományi Társulat
és az
Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai
Mérnöki Kar
konferenciasorozata, 1-3. rész

szerkesztette
Rajnai Zoltán és Tardy János

A
Magyar Természettudományi Társulat
tanulmánykötetei

VII.

sorozatszerkesztő: Dr. Tardy János

Kiadja a Magyar Természettudományi Társulat
Budapest, 2023
Felelős kiadó Dr. Tardy János

Tipográfia és tördelés: Geobook Hungary Kiadó
Nyomta: Belovits-Print Kft.

ISBN 615 82104 5 4

A kötet megjelenését a Nemzeti Kulturális Alap Ismeretterjesztés és Környezetkultúra Kollégiuma és az Agrárminisztérium támogatta

A jövő nagy kihívása: kiberbiztonság és kiberhadviselés

A konferenciasorozatot szervezte és
a kötetet szerkesztette

Rajnai Zoltán és Tardy János

TARTALOM

Rajnai Zoltán – Tardy János: Előszó 7

Az I. konferencia programja 9

Kovács László: *Kiberműveletek a 21. század hibrid hadviselésében* 11

Haig Zsolt: *Elektronikai hadviselés a kibertérben* 33

Rajnai Zoltán: *A digitális hadszintér* 49

Farkas Tibor: *NATO-elvű infokommunikációs hálózatok katonai műveletekben* 63

A II. konferencia programja 67

Rajnai Zoltán: *Drónok alkalmazhatósága a védelmi szférában* 69

Czajlik Zoltán – Rupnik László: *A repülőgépes felderítéstől a drónos felmérésig. Régészeti célú légi fényképezés különböző platformokon* 81

Őszi Arnold: *A drónok veszélyei* 97

Nagy Balázs – Mészáros János: *Drónok a klímaváltozás vizsgálatában – térképezés magashegységi környezetben, Ojos del Salado, Chile* 108

Kovács Béla – Hajdinákné Vörös Fanni – Pál Márton: *Légből kapott képek elemzése. A drónok használata a térképészetben* 122

Gulyás Zoltán – Sillinger Fanni: *A drónok jelenlegi és jövőbeni alkalmazási lehetőségei a mezőgazdaságban* 141

Bíró György: *Drónok a természetvédelem szolgálatában* 154

Haramia Ákos: *Madáreltéritö telepítése drónnal* 160

Bertalan László – Szopos Noémi – Nagy Bálint – Szabó Gergely: *Kanyarulatfejlődés a drónok szemszögéből. Új módszerek a folyóvízi parterózió és a felszíni vízsebesség tanulmányozásában* 166

A III. konferencia programja 176

Rajnai Zoltán: *Mi a crypto-valuta, hogyan "bányásszák"?* 177

Ujváry Patrik Richárd: *Blokklánc és DeFi* 186

Nagy Attila: *Bitcoin-blockchain* 192

Előszó

A XIX. század utolsó évtizedeitől a közlekedés, a híradás, az energetika, a társadalmi élet gyors fejlődésének hozadékai elsősorban pozitív következmények előidézői. A világ nagyhatalmainak, koalícióinak a századfordulótól kiéleződött ellentétei miatt növekvő háborús veszély súlyos negatív hatásokkal járt az egyén, az elsődleges közösségek, de a nemzetek, népek, országok, régiók, világrészek, az egész világ biztonságérzetére egyaránt.

A XX. század közepétől a biztonság, ami a mind nagyobb számú pozitívan és negatívan ható tényező hatásrendszere miatt addig sem volt egyszerűen kezelhető, napjainkra egyre komplexebb „jelenséggé" vált. A gazdaság működtetéséhez nélkülözhetetlen technikai rendszerek (atomerőművek, vegyi üzemek, kőolajfinomítók, gázüzemek, gáztárolók és egyebek), a felgyorsult közlekedés, a tömeggyártást végző gyárak, tömegpusztító fegyverek, fegyverrendszerek megjelenése a biztonságot alapvetően befolyásolják, kockázati tényezőt jelentenek. Mindezek eredményeként a komfortosság érzelmi szintjének lebegése, a biztonság bizonytalansága egyre inkább érezhető lesz.

A XX. század utolsó évtizedében és az új évezredben a biztonság még ennél is komplexebben értelmezhető. A társadalmi élet minden területét átfogó, a korábbiaknál lényegesen gyorsabb – robbanásszerű – fejlődés, a háború, infláció, energiaínség, demográfiai bajok és mesterségesen gerjesztett válságok az egész világ, a földrészek, a régiók, a kis közösségek, de az egyén életét is gyökerestől megváltoztatják. A biztonságot legszámottevőbben befolyásoló tényezők: a terrorizmus, a környezetrombolás, a katasztrófák – köztük az ökológiai katasztrófa – veszélye az egész emberiség elpusztulásának veszélyét is magában hordozhatja. A világ ma egyidejűleg súlyos kihívások sorával néz szembe: biztonsági kockázatokkal, gazdasági recesszióval, energiaellátási válsággal.

A geopolitikai viharokhoz társul a technológia fejlődésével járó eszközök, módszerek és eljárások veszélye, vagy éppen azoknak a biztonság érdekében történő alkalmazása. Ezekre a technológiai újdonságokra, módszerekre, eszközökre és eljárásokra próbálja meg felhívni a figyelmet ez a konferenciasorozat, amelynek előadáskivonatait az olvasó a kezében tartja. A hadszíntér digitalizációja, a modern információs hadviselés, a drónok alkalmazásának különböző lehetőségei, vagy éppen a digitális pénz és az azt működtető technológia csak néhány szelet korunk kihívásaiból.

Ajánljuk ezt a kiadványt mindazoknak, akik jelen voltak az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar és a Magyar Természettudományi Társulat együttműködésében megvalósult, nagy érdeklődéssel kísért konferenciasorozat személyes vagy online előadásain, és azoknak is, akik azon nem tudtak részt venni, de érdekli őket a kiragadott témák sokasága, sokszínűsége.

Hasznos időtöltést kívánunk a publikációk olvasásához, és várjuk Önöket további rendezvényeinken is!

Prof. Dr. Rajnai Zoltán – Dr. Tardy János

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

A jövő nagy kihívása: kiberbiztonság és kiberhadviselés

Az Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
és a
Magyar Természettudományi Társulat
konferencia-sorozata – 1.

ELEKTRONIKAI HADVISELÉS A 21. SZÁZAD ELEJÉN

A konferencia-sorozat szervezői:
Prof. Dr. Rajnai Zoltán, PhD, dékán (Óbudai Egyetem)
és Dr. Tardy János, PhD, üv. elnök (MTT)

HELYSZÍN

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 1081 Budapest, Népszínház u. 8.

IDŐPONT

2020. február 6.,13:00-16:00 óra

PROGRAM

12:30-13:00 Érkezés, regisztráció, kávé, üdítő
13:00-13:15 Köszöntések
13:15-13:40 **Prof. Dr. Kovács László** dandártábornok, egyetemi tanár
(Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék)
Kiberműveletek a 21. század hibrid hadviselésében

13:40-14:05 **Prof. Dr. Haig Zsolt** ezredes, egyetemi tanár
(Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék)
Elektronikai hadviselés a kibertérben

14:05-14:15 Kérdések, hozzászólások

14:15-14:35 Kávészünet

14:35-15:00 **Prof. Dr. habil Rajnai Zoltán** egyetemi tanár, kutatóprofesszor, dékán (Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Biztonságtechnikai Intézeti Tanszék)

A digitális hadszíntér

15:00-15:25 **Dr. habil. Farkas Tibor** százados, egyetemi docens, (Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék)

NATO-elvű infokommunikációs hálózatok katonai műveletekben

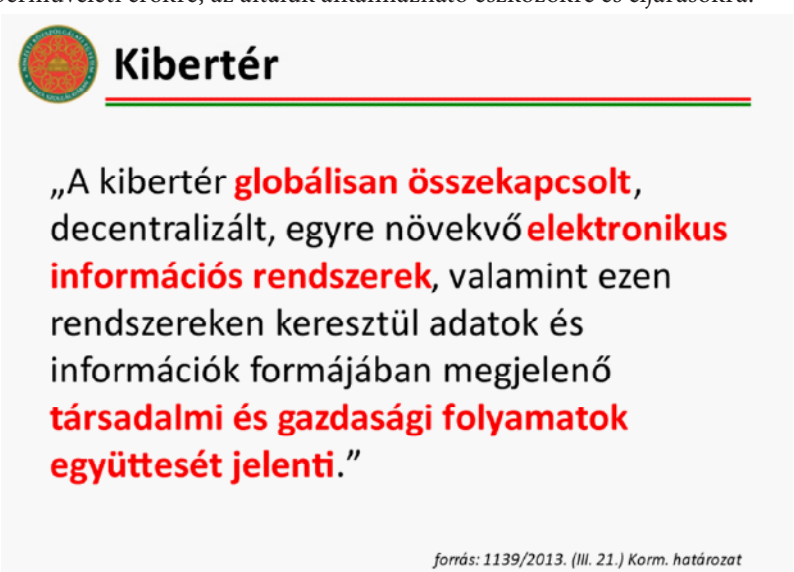
15:25-16:00 Kérdések, hozzászólások

Kiberműveletek a 21. század hibrid hadviselésében

(Hadmérnök • 16. évfolyam (2021) 3. szám alapján)

Prof. Dr. Kovács László, dandártábornok, egyetemi tanár
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar,
Elektronikai Hadviselés Tanszék, Budapest
kovacs.laszlo@uni-nke.hu

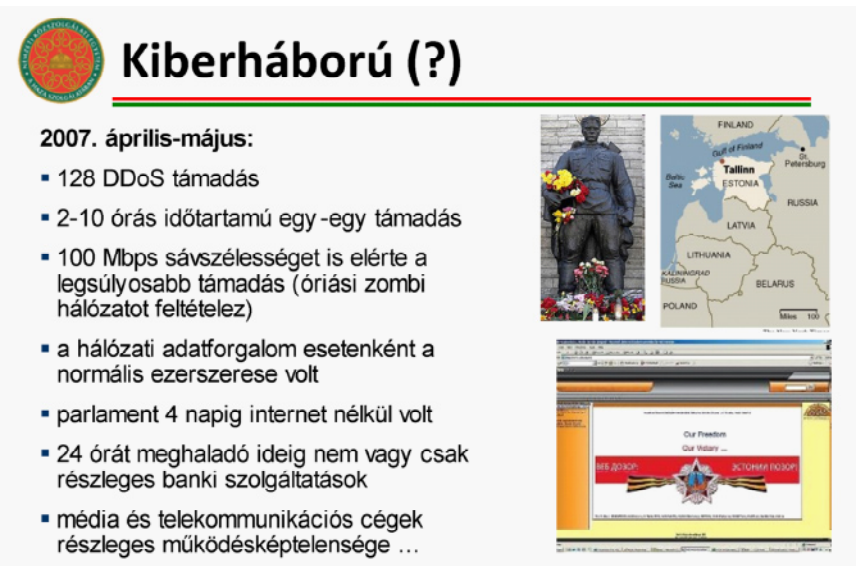
A kibertér biztonságának megteremtése számos tevékenység összehangolt megvalósítását igényli. A kiberbiztonság komplex rendszerében a szabályozási és eljárási kérdések mellett aktív kibervédelmi műveleteket is találunk. Ugyanakkor a védelmi célú kibertérműveletek önmagukban nem mindig elégségesek a teljes és átfogó kiberbiztonság megteremtéséhez. Így a védelmi kibertérműveletek mellett offenzív kiberműveletek végrehajtására is szükség lehet. Emellett az offenzív kibertér-műveletek, és az abban foglalt eszközök és eljárások természetszerűleg nemcsak a saját oldali rendszereink védelméhez járulnak hozzá, hanem az ellenérdekelt fél infokommunikációs rendszereinek lefogásával, azok működésének akadályozásával, vagy azokból információk kinyerésével más műveleti terekben végrehajtott tevékenységek támogatásához járulnak hozzá hatékony módon. Jelen tanulmány első része az offenzív kiberműveletek általános jellemzőit mutatja be, a második rész, azaz jelen írás az offenzív kiberműveleti képességek gyakorlati megvalósítását és alkalmazhatóságát elemzi, valamint kitér a kiberműveleti erőkre, az általuk alkalmazható eszközökre és eljárásokra.



Bevezetés

A kiberbiztonság és annak megteremtése jelen korunk egyik nagy kihívása. A 21. században általunk használt és alkalmazott ezernyi infokommunikációs eszköz, rendszer, megoldás és szolgáltatás olyannyira a mindennapjaink részévé vált, hogy azok valódi létfontosságú elemekké váltak életünkben. Így a biztonság megteremtése létkérdés ezen rendszerek esetében. A fentiekben megfogalmazottak azonban magukkal hozták a hadviselés változását is, hiszen egy ország elleni támadás ma már nem igényli fizikai határainak átlépését, a globális hálózatoknak köszönhetően a rosszindulatú beavatkozás egy-egy jól kiválasztott információs rendszerbe – jellemzően számítógép-hálózatba, vagy annak egyes elemeibe – gyakorlatilag a világon bárhonnan kivitelezhető, és abban komoly – akár a teljes működésképtelenséget is előidéző – kár okozható. A hadviselés tehát változik, mint az emberi történelem során eddig mindig. Ahogy a korábbi nagy technikai felfedezések, úgy a kibertérben használt infokommunikációs eszközök és rendszerek is változást eredményeznek a hadviselés eljárásaiban és a harcok megvívásának elveiben is. A kibertér jellemzői nagyban segítik azokat az eljárásokat, amelyekkel a hadviselést egyébként jellemezni szoktuk. A különböző támadásokhoz, az azok előkészületeihez szükséges információszerzéstől kezdve a rejtőzködésen át a nagy távolságból végrehajtott csapásokig a kibertér ideális terep a hadviselés számára. Természetszerűleg jelent meg tehát a hadviselés eddig is színes palettáján a kibertéri műveletek egész sora, amelyekkel a fenti támadások megvalósíthatók. A kérdés csak az, hogy szükséges-e egy adott ország számára kibertámadó, illetve a tágabb értelemben vett offenzív kiberképességeket kiépíteni, azokat fenntartani. A válasz már jelen tanulmány első részéből is körvonalazható volt. Ez a válasz pedig egyértelműen igen, szükséges ilyen képességekkel rendelkeznie egy országnak. Jelen tanulmány első része az offenzív képességek általános hátterét vizsgálta. Ennek során az olyan kérdések elemzését végeztük el, mint az offenzív kiberképességek összetevői és az offenzív kiberképességek stratégiai megfontolásai. Az írás első részében megvizsgált kérdések egy végső következtetés levonását indukálták, amely nem más, mint annak megállapítása, hogy a jövőben a kibertéri dominancia és a kibertér uralása elengedhetetlen lesz a győzelem kivívásához. Ezért a kibertéri fölény, illetve a kibertérben történő sikeres tevékenység offenzív a kibertéri képességeket is magában foglaló kibererők felállítását igényli. Ma már ezek a képességek elengedhetetlen részét képezik az adott ország biztonsági összetevőinek. Amennyiben a fentieket elfogadjuk, úgy egy másik, nem sokkal egyszerűbb kérdést, illetve kérdések egész sorát kell megválaszolnunk. Ez pedig nem más, mint az, hogy hogyan is nézzen ki az a szervezet, amely mindezeket a képességeket fel tudja mutatni. Egyáltalán milyen elvek mentén szükséges ezeket a képességeket kialakítani? Ki legyen a felelőse a képességek kialakításának? Milyen módszerek

és eljárások járulhatnak hozzá a kiberbiztonsági stratégiákban meghatározott kiberképességek kialakításához? Milyen szerepe van az egyes tagországoknak a NATO offenzív kiberképességének kialakításában? Ezernyi kérdés, amelyekre jelenleg nem, vagy csak nagyon nagy vonalakban tudunk válaszolni. Jelen írás ezekre a kérdésekre igyekszik – tudományos munka esetében eléggé el nem ítélhető módon a teljesség igénye nélkül – választ adni. A tanulmányban összegzett vizsgálatok irodalomkutatásra építenek, esetenként az összehasonlító elemzés, majd szintézis módszerének alkalmazásával kiegészítve. Az elvégzett vizsgálatokból levont következtetések a szerző sajátjai, azok nem feltétlenül esnek egybe sem a Nemzeti Közszolgálati Egyetem, sem a Magyar Honvédség hivatalos véleményével vagy álláspontjával.



Az offenzív kiberképességek szükségessége

Az offenzív kiberképességek kialakításának egyik legfőbb indoka az, hogy a lehető legtávolabb tartsuk a potenciális támadó (szemben álló fél, ellenség) rosszindulatú kibertevékenységét a saját rendszereinktől. Ez akkor a leghatékonyabb, amennyiben még a rendszereink megtámadása előtt a potenciális támadót elrettentjük a támadás kivitelezésétől – például olyan védelmi rendszer kiépítésével, amely csak aránytalanul nagy energiabefektetéssel törhető át –, vagy olyan mértékben csökkentjük képességeit, amelyekkel már nem tud hatékony támadást indítani rendszereink ellen. Ez utóbbi esetben van szükség az offenzív kiberképességek meglétére. Az offenzív, és benne a kibertámadó képességek

kialakítása előtt azonban szükséges feltárni azokat a kihívásokat és veszélyeket, amelyek a kibertérben jelentkeznek. Ezek alapján lehet meghatározni az offenzív kiberképességek kialakításához szükséges feltételeket, eszközöket és módszereket. A kihívások és veszélyek feltárása mellett azonban szükség van a köztük lévő összefüggések, illetve azok hatásainak vizsgálatára is. Az okok között természetesen ott vannak azok a leggyakoribb kibertéri veszélyek, amelyek a technológia sérülékenységeit kihasználva jelentkeznek. Ezek vagy rosszindulatú programokban, vagy az azokra épülő olyan eljárásokban vannak jelen, amelyeket a támadók különböző célokkal alkalmaznak. Számos olyan infokommunikációs eszközt és rendszert használunk, amelyek vagy vegyes használatúak, azaz polgári és katonai célra egyaránt alkalmazzák őket vagy olyan rendszerek és eszközök, amelyek bár polgári rendszerek (például Commercial off the Shelves, COTS, azaz kereskedelmi forgalomban kaphatók), de mégis katonai célra is használjuk. Ebből következően az ezeket a rendszereket és eszközöket fenyegető veszélyeket is fel kell mérni. A csak katonai célú eszközök és rendszerek esetében a helyzet sok esetben furcsa mód sokkal nehezebb, mint a polgári célú eszközök esetében. Ennek oka elsősorban abban keresendő, hogy a csak katonai célra alkalmazott eszközök és rendszerek életciklusa – többek között azok bekerülési költsége miatt – sokkal hosszabb, mint ami a polgári rendszerek esetében megszokott. Ennek megfelelően azokat sokkal hosszabb ideig tartjuk rendszerben, így azok időközben napvilágra kerülő sérülékenységei is sokkal hosszabb ideig fennállhatnak. Ráadásul ez a hosszabb időtartam azt is jelenti, hogy a korszerűbb, a kibervédelmet szolgáló megoldások beépítése és alkalmazása egy-egy működő katonai rendszerbe csak lényegesen később és nagyobb energiabefektetéssel valósítható meg. Egy másik probléma az olyan, a polgári életben már nagy népszerűségnek örvendő és igen elterjedt szolgáltatásoknak a hadseregek életében történő megjelenése, mint amilyenek például a közösségimédia-platformok. Ezek nem önmagukban jelentenek kockázatot vagy veszélyt, hanem a nem tudatos használat révén. A katonák vagy a hadseregben dolgozó civil alkalmazottak meggondolatlan és sok esetben felelőtlen közösségimédia-jelenléte nagyon sokszor komoly információforrást jelent a szemben álló fél vagy a potenciális támadó számára. A kibertámadó képességek, illetve azok alkalmazásának okait vizsgálva számos közvetett okot is fel tudunk tárni. Ezek közül az első ok azonban rögtön egy komplex problémát takar. Egyrészt ma már számos olyan összetett infokommunikációs rendszert és -eszközt használunk, amelyek mind a civil, mind a katonai (védelmi) szféra működésében megtalálhatók. Sok esetben még ezek felhasználásának primer céljai is azonosak, hiszen alapvetően kommunikációra, adatfeldolgozásra és adattovábbításra használjuk ezeket az eszközöket és rendszereket. A legtöbb esetben még funkcionális értelemben is azonosak a célok, hiszen alapvetően a vezetés támogatása, illetve maga a veze-

tés megvalósítása az egyik legfontosabb célja ezeknek a rendszereknek. Ennek a problémának a komplexitását azonban az adja, hogy jelen korunk társadalma – és ez alól nem képez kivételt a kor modern hadserege sem – komoly függőséggel rendelkezik ezekkel az eszközökkel és rendszerekkel szemben. A függőség egyben sérülékenységet is jelent. Ráadásul az említett rendszerek komplexitása, a részrendszerek és elemek összekapcsoltsága és egymásra gyakorolt, a működést alapvetően befolyásoló hatása még inkább növeli ezt a sérülékenységet. Ez nyilvánvalóan azt a veszélyt is magában hordozza, hogy egy-egy részelem vagy részrendszer kiesése alapjaiban lehet negatív befolyással az egész rendszerre. Ez adott esetben a társadalom egy-egy funkciójának a teljes leállásához, vagy ezzel analóg módon egy-egy hadsereg valamely fontosabb funkciójának a leállásához vezethet. Mindezen okok miatt szükséges a lehető legtávolabb tartani a támadó felet a saját rendszereinktől, illetve a védelmi célú kiberműveletek alkalmazása mellett offenzív műveletekkel megfosztani a támadás lehetőségétől.

Katonai offenzív kiberműveleti képességek

A 21. századi korszerű hadseregek egyik jellemzője, hogy a katonai céllal készült infokommunikációs eszközök és rendszerek mellett számos civil megoldást is használnak. Ilyen megoldás például a kommunikáció és adatátviteli célokra használt civil mobil kommunikáció, a 4G vagy az 5G mobil technológia. Ennek több oka van, amelyek között az egyik legfontosabb az, hogy a civil eszközök és rendszerek a hadsereg részéről jelentkező bekerülési és fenntartási költségei jóval kisebbek vagy elenyészők a kimondottan saját katonai célú technológiafejlesztés költségeihez viszonyítva. Ugyanakkor ezek a technológiák egyfajta limitációt is jelentenek, hiszen értelemszerűen ezeket az eszközöket és rendszereket háborús körülmények között nem, vagy csak időszakosan tudja használni a hadsereg, mert ezek lesznek az ellenérdekelt fél részéről az elsődlegesen pusztítandó olyan célok, amelyek működésének gátlása a hadsereg vezetésének rombolását és így annak részleges működésképtelenségét is jelenti. Természetesen ez a polgári technológia esetén önmagában is igaz, hiszen minél több fejlett technológiát használ a civil társadalom, annál inkább nő annak a lehetősége, hogy ezeket támadva lehet – akár katonai – eredményeket is elérni. Itt vonatkoztassunk el attól, hogy ez a nemzetközi jogi szabályozásba ütközik-e vagy sem. Jelen tanulmány első része igyekezett a jogi, illetve nemzetközi jogi kérdéseket nagyon röviden felvillantani és részben megvizsgálni. Ugyanakkor a hivatkozott első részben azt kellett megállapítani, hogy ez ma a gyakorlatban még egyáltalán nem, vagy csak részben szabályozott terület. Ennek ellenére, vagy éppen emiatt jelenthetjük azt ki, hogy a civil infokommunikációs eszközök és rendszerek, ezeken keresztül pedig az adott ország fontos, ráadásul nagyértékű célpontok lesznek egy esetleges fegyveres konfliktusban, illetve az azzal párhu-

zamosan megjelenő kiberműveletekben. Természetesen az a tény, hogy a hadsereg civil infokommunikációs eszközöket és rendszereket alkalmaz, magával hozza azt is, hogy az ezekben meglévő vagy az ezekben a későbbiekben felfedezett sérülékenységekkel a hadseregnek is számolnia kell. A katonai kiberképességek egyik legfontosabb célja természetszerűleg a saját infokommunikációs rendszerek kibervédelmének a biztosítása. Emellett értelemszerűen azonban a hadsereg tevékenysége nem korlátozódik csak a saját rendszereinek védelmére. Ezeknek a képességeknek hozzá kell járulniuk az ország szuverenitásának védelme érdekében tett katonai tevékenységek komplexitásához. A magyar honvédelmi törvény által megfogalmazottak szerint műveleti területnek minősül „a műveleti tervben meghatározott és kijelölt földrajzi terület és a felette levő légtér, továbbá a kibertér". A hazai Nemzeti Biztonsági Stratégia (NBS) szintén rögzíti ezt a célt: „[H]aderőt úgy kell fejleszteni, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a kibertérben egyaránt."

Mindezekből azt a következtetést kell levonnunk, hogy a katonai kibertérműveleti képességek, köztük az offenzív kiberképességekkel az ország kibervédelmi képességeinek szerves részét képezik. Ezek a képességek – az ország más kibervédelmi és kiberműveleti képességeivel együtt – hozzájárulnak az ország adaptív ellenállóképességéhez. Ugyanakkor számos egyéb kiberképesség szükséges egy adott ország kiberbiztonságának megteremtéséhez, fenntartásához, illetve a kibertéri szuverenitás biztosításához. Ezek a sok esetben civil képességösszetevők mintegy komplementer, azaz kiegészítő képességként teremtik meg a katonai kiberképességekkel együtt az ország megfelelő kibervédelmi képességét. Az ország megbízhatóan működni képes kibervédelmi rendszere a kibertéri tevékenységekért felelős szervezetek számára világos feladatrendszert, egyértelműen megfogalmazott hatás- és jogköröket kell, hogy jelentsen. Ugyanakkor ennek megteremtése során azt is figyelembe kell venni, hogy ez nem egy állandó, több évre vagy évtizedre meghatározott szisztéma, hanem a társadalmi, valamint a technikai és technológiai változásokat követni, azokhoz megfelelő módon alkalmazkodni képes rendszert szükséges kialakítani és fenntartani. Ennek egyik alapfeltétele az, hogy a kibervédelmi szereplők közel azonos módon lássák és értékeljék a kibertéri helyzetet. Ez már a nemzeti kiberbiztonsági stratégiában rögzített módon meg kell (vagy kellene), hogy jelenjen, hiszen annak felépítésével, azaz a változó kihívásokhoz alkalmazkodni képes stratégiai céloktól kezdődően a stratégia által meghatározott tevékenységeken át, a szintén a stratégia által meghatározott szervezeti struktúráig számos elemnek kell mindezt, vagyis az alkalmazkodásra és szükség esetén változásra való képesség elvét tükröznie. A katonai offenzív kiberműveletek szükségessége stratégiai szinten abból indul

ki, hogy az országnak joga van megvédenie a szuverenitását a kibertérben is, és joga van rosszindulatú kibertevékenységekkel szemben fellépni. A kibertéri védelem pedig sok esetben nem, vagy csak részlegesen működik kizárólag védelmi kiberműveletek alkalmazásával. Természetszerűleg az offenzív kiberműveletek alkalmazása során nagy jelentősége van a kiberműveletek életciklusának. Ebben – a már korábban bemutatott életcikluselemek mellett – az egyik legfontosabb tényező az, hogy minél kisebb teret engedjünk az ellenérdekelt fél tevékenységének, ugyanakkor a saját tevékenységeink mozgás- és cselekvési szabadságát biztosítsuk a kiber-, fizikai és információs térben egyaránt. A katonai offenzív kiberműveletek alkalmazása során számolni és tervezni kell a műveletek közvetlen és közvetett következményeivel is. Az offenzív kiberműveletek végrehajtásához számos feltételnek kell teljesülnie. Sok olyan előfeltétel megléte szükséges, amelyek mind jogilag, mind technikailag megalapozzák és lehetővé teszik e műveletek végrehajtását. Ugyanakkor az offenzív kiberképességek alkalmazása során számolni kell azok hatásaival. A hatások előrejelzése, különösen a járulékos, azaz a közvetett hatások felmérése sok esetben nem, vagy nem megfelelő mértékben lehetséges. Ennek oka a korábban már vizsgált infokommunikációs rendszerek intra- és interdependenciája, valamint azok egyéb – például kiberfizikai – rendszerekhez való összetett kapcsolódása. Ugyanakkor a katonai offenzív kiberműveleti képességek nem nélkülözhetik az ipari, a kis- és a közepes vállalatokkal, valamint az akadémiai szférával és a kutatóintézetekkel történő együttműködést, csakúgy, mint a nemzetközi kooperációt és kapcsolatokat sem.

Kibererők: példák és az azokból levonható következtetések

A katonai kibertéri feladatokat ellátó erők országonként eltérő módon épülnek fel. Ezt a felépítést az adott ország kibervédelméért, valamint a kiberműveletekért felelős szervezetek időbeni kialakítása, a civil és a katonai feladatok felosztása, valamint az adott ország politikai, kiberszakmai döntései és a kialakított jogszabályi háttér határozza meg. Nagyon röviden, nem tudományos alapossággal és csak a legfontosabb tényezőket felvillantva négy ország – az Amerikai Egyesült Államok, Németország, Lengyelország és Magyarország – kiberműveleti erőit tekintjük át, a katonai kibererőkre fókuszálva. A cél az azokban esetlegesen fellelhető azonos pontok feltárása, ezek mentén igyekszünk olyan általános érvényű következtetéseket levonni, amelyekből jól kivehetők a kiberműveleti erők legfontosabb jellemzői.

Szereplők

- **Országok (példák):**
  - ✓ Kína;
  - ✓ Oroszország;
  - ✓ Észak-Korea;
  - ✓ Irán;
- **Állami támogatású csoportok:**
  - ✓ pl.: APT 1, APT28
- **Nem állami szereplők;**
- **Gazdasági csoportok;**
- **Kiberbűnözői csoportok;**
- **Terrorszervezetek;**
- **Egyéni elkövetők.**

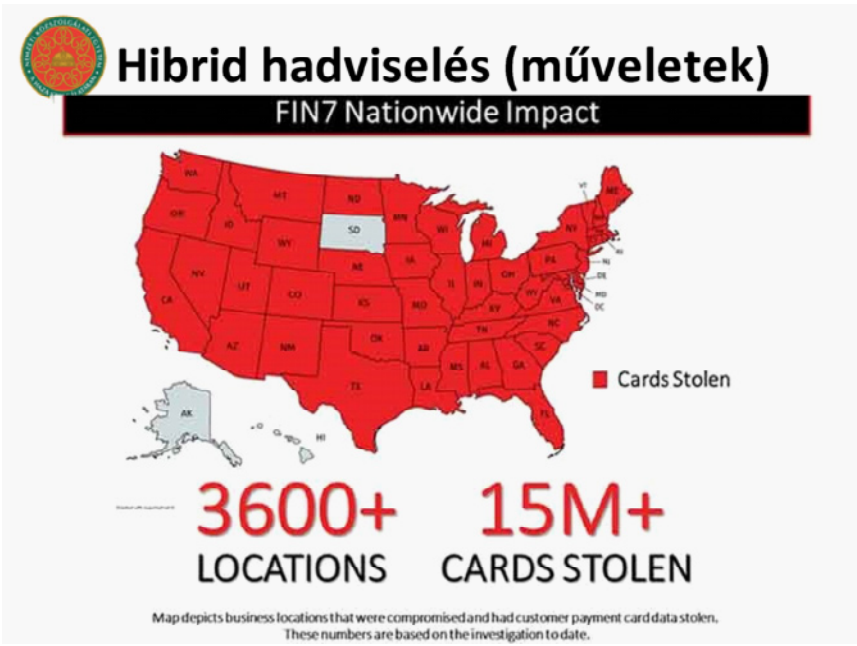
A nemzetközi jog

Kiberműveletek kategorizálása:

- békeidőben:
  - ✓ információszerzés;
  - ✓ befolyásolás;
  - ✓ kritikus infrastruktúrák támadása;
  - ✓ közigazgatás elleni támadások;
- különleges jogrendi időszakban:
  - ✓ katonai kibertámadások;

Amerikai Egyesült Államok

Az Egyesült Államokban a katonai kibererőket integráló szervezet az Egyesült Államok Kiberparancsnoksága, azaz a US Cyber Command. A szervezet 2009-ben jött létre az Egyesült Államok Stratégiai Parancsnokságának (US Strategic Command) alárendeltségében. Mint alárendelt parancsnokság a US Cyber Command 2010-ben érte el a műveleti készenlétet, és 2018-ban vált önálló komponens parancsnoksággá. Ugyanakkor a szervezet életében az egyik meghatározó mérföldkő ezt megelőzően az úgynevezett Cyber Mission Force, magyarul a Kiberműveleti Erő létrehozása volt 2013-ban, hiszen gyakorlatilag ez a US Cyber Command végrehajtó ereje. A US Cyber Command – *jelen tanulmány írásakor* – parancsnoka, Paul Nakasone tábornok, aki 2018 óta látja el ezt a tisztséget, és aki nem mellesleg egyben az Egyesült Államok Nemzeti Hírszerző Ügynökségének (National Security Agency, NSA) a vezetője is, a szervezet stratégiai jövőképét felvázoló kiadványában így foglalja össze a szervezet legfontosabb feladatát: „A USCYBERCOM hozzájárul a nemzeti stratégiai elrettentésünkhöz. Felkészítjük, működtetjük és együttműködünk a harcoló parancsnokságokkal, fegyvernemekkel, szövetségesekkel és az iparral annak érdekében, hogy folyamatosan akadályozzuk és megmérettessük az ellenséges kibertér szereplőit, bárhol is találjuk őket." Meg kell jegyezni, hogy az említett kiadványnak már a címe is rendkívül beszédes: „A kibertéri fölény elérése és fenntartása. Parancsnoki jövőkép az Egyesült Államok Kiberparancsnoksága számára" (angolul: Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command). A US Cyber Command 133 Cyber Mission Force (CMF), azaz 133 önálló kiberműveleti csoport kiképzését felügyeli. Ezek az egységek a különböző haderőnemek kiberparancsnokságai alárendeltségében működnek, ugyanakkor maguk a haderőnemi kiberparancsnokságok is a US Cyber Command szakmai felügyelete alá tartoznak. A CMF-ek egységes felkészítése és kiképzése óriási előnnyel jár abból a szempontból, amely az egységes terminológiai értelmezéstől kezdődően a kihívásokra adott egységes és koherens technikai válaszokig bezárólag jelentkezik. Meg kell jegyezni azonban, hogy a CMF-ek felkészítése és azok képességeinek magasabb szintre emelése nem megy mindig zökkenőmentesen. Ennek adott hangot az Egyesült Államok Számvevőszéke (Government Accountability Office, GAO), amikor kritikát fogalmazott meg ezzel kapcsolatban: „A Védelmi Minisztérium a CMF építéséről annak fejlesztésére helyezte át a hangsúlyt.



A minisztérium kidolgozta a CMF transzformációs tervét, amely az alapozó (második fázis8) képzési szakasz felelősségét átruházza a haderőnemekre. A szárazföldi haderőnek és a légierőnek azonban nincs elég időkerete az alapozó tanfolyamok CYBERCOM szabványoknak megfelelő érvényesítéséhez. Továbbá a haderőnemek tervei nem tartalmazzák a CMF összes képzési követelményét, például a kiképzésre szoruló létszámot. A CYBERCOM nem tervezi a szükséges független értékelők felállítását a kollektív (harmadik fázis) CMF-képzés következetességének biztosítása érdekében." A US Cyber Command részt vett az amerikai elnökválasztásba beavatkozni kívánó külföldi kibererők elleni tevékenységben, valamint egy 2018-ban, a Belbiztonsági Minisztérium (Department of Homeland Security, DHS) és a Védelmi Minisztérium (Department of Defense, DoD) között született megállapodás alapján a kritikus-infrastruktúra-védelemben is komoly szerepet kap. Azonban a US Cyber Command talán egyik leghíresebb művelete az úgynevezett Glowing Symphony művelet volt, amely során a Joint Task Force-Ares – a US Cyber Command által offenzív kiberműveletek végrehajtására dedikált egyik – csapat az ISIS nemzetközi terrorszervezet ellen mért célzott kibercsapásokkal az „ISIS média és online műveleteit célozta meg, megfosztva infrastruktúrájától, és megakadályozva az ISIS tagjait a propaganda kommunikációjában és közzétételében".

A fenti, 2016-ban végrehajtott offenzív kiberművelet, illetve műveletek együttese nagy vonalakban ma már tanulmányozható, hiszen számos olyan dokumentum titkosítását feloldotta az NSA, amilyenek például a támadásokról szóló jelentések voltak. Ugyanakkor ezek a ma már nem titkos minősítésű jelentések legtöbb részletükben kitakartak, így csak a legfontosabb történésekbe kapunk betekintést.

Németország

Németország meglehetősen egyedi utat választott a kibertérműveleti erők kialakítása során.2016 áprilisában Ursula von der Leyen, az akkori német szövetségi védelmi miniszter bejelentette, hogy Németország egy Kiber- és Információs Domain Parancsnokságot állít fel, amely közel 13.500 fő katona és civil szakembert foglal majd magában.

A szervezet a Bundeswehr alakulataként 2017 áprilisában létre is jött. Az új Kiber- és Információs Domain Parancsnokság számos korábbi alakulatot integrált, így kiterjedt feladatrendszerrel alakult meg. Ezek közül a feladatok közül – természetszerűleg a Bundeswehr saját információs rendszereinek a védelme és azok üzemeltetése mellett – a legfontosabbak a felderítés (hírszerzés, megfigyelés) a kibertérben és az elektromágneses spektrumban végzett aktív műveletek, valamint a geoinformációs szolgáltatások ellátása.

Ezek a feladatok magukban foglalják tehát a hadsereg infokommunikációs rendszereinek üzemeltetését, azok 24 órás felügyeletét, a szoftverfejlesztést, a szimulációs rendszerek IT- és geoinformációs támogatását. Az offenzív kiberműveleti feladatok mellett megjelenő elektronikai hadviselési tevékenységek jól jellemzik azt a tényt, hogy a német kibertér-értelmezés eltér a hagyományos kibertér-értelmezéstől, például attól, amit a NATO hivatalosan is követ, hiszen a NATO Kibertér Műveleti Doktrínája a kiberteret a következőképpen határozza meg: [Kibertér] „Globális tartomány, amely magába foglalja mindazon infokommunikációs és egyéb elektronikai rendszereket, hálózatokat és azok adatait, beleértve az elkülönült vagy független rendszereket, hálózatokat, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak."

Ezzel szemben, vagy talán ezt megerősítve a német kibertér-értelmezés szerint a kibertér tartalmazza az elektromágneses spektrumot és a kognitív dimenziót is. Ez magyarázhatja az elektronikai hadviselés és a kognitív dimenzióra ható információs domain integrálását is. A szervezet számos nemzeti és nemzetközi kapcsolatot tart fenn különböző kiberbiztonsági és kiberműveleti szervezetekkel, aminek során az egyik legfontosabb feladat az információcsere megvalósítása. Az alakulat felállítása és annak széles körű feladatai nagyon jól beleillenek abba a feladatrendszerbe, amelyet a német nemzetbiztonsági stra-

tégia 2016-ban meghatározott. (Németország fehér könyvként adja ki a nemzetbiztonsági stratégiáját, amely nemcsak a biztonságpolitikai célokat, hanem a hadsereg, azaz a Bundeswehr szerepét és stratégiai feladatait is meghatározza.).

Lengyelország

Lengyelországban a Védelmi Minisztérium égisze alatt alakították meg a Nemzeti Kiberbiztonsági Központot 2019-ben. A központ feladata a védelmi minisztérium és a lengyel hadsereg IT-üzemeltetési és -fejlesztési feladatain túl a nemzeti szintű kiberbiztonság koordinálása, valamint számos kriptográfiai tevékenység ellátása, továbbá a szervezet alárendeltségébe tartozik a katonai eseménykezelő központ (Computer Security Incident Response Team – Ministerstwa Obrony Narodowej, CSIRT-MON) is. A Központ egyik fontos szervezeti eleme a Kiberműveleti Központ, amely a „katonai műveletek teljes spektrumában hajt végre kibertéri műveleteket, olyan körülmények között is, amikor a hagyományos erők alkalmazása nem lehetséges vagy nem célszerű". A központ felállítása előtt a lengyel kiberbiztonsági rendszer sok elemből állt. Az eltérő közigazgatási szervezethez (például különböző minisztériumokhoz) tartozó kiberbiztonsági csoportok és feladataik megosztott helyzetet teremtettek, az abban megvalósuló koordináció, illetve annak nem kielégítő volta azonban sok kritikát kapott. Természetesen volt jól működő eleme is a rendszernek, például az eseménykezelés, amely folyamatosan jól teljesített. 2019-ben a védelmi minisztérium életre hívta az úgynevezett Cyber.Mil.Pl programot, amelynek két legfontosabb eleme a kibertérvédelmi erők létrehozásának támogatása, valamint a védelmi minisztérium kiberbiztonsági feladatainak az integrálása. A program stratégiai célja természetesen az ország kiberbiztonságának növelése. Ennek érdekében a programban olyan szervezetek is részt vesznek, mint a varsói Katonai Műszaki Egyetem, a lengyel Haditengerészeti Akadémia, a Katonai Kommunikációs Intézet, amely az 1950-es évek óta működő kutatóintézet, valamint szerepet kapnak a programban a lengyel területvédelmi erők is. 2020-ban adták át a Nemzeti Kiberbiztonsági Központ szakmai irányítása alá tartozó Kiberbiztonsági Képzési Kiválósági Központot (Cyber Training Centre of Excellence), amely újabb lépés lehet a szakmailag felkészült utánpótlás biztosítására a lengyel kibervédelmi és kiberműveleti erők számára.

Magyarország

Hazánk szintén sajátos utat jár be a kibererők építése során. A hazai kiberbiztonság megteremtése során az egyik legfontosabb állomás a 2013-ban megjelent információbiztonsági törvény, hivatalos megnevezéssel 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.), illetve annak 2015-ös jelentős módosítása. Ez azonban csak a kiberbiztonság civil szervezeti keretét határozta meg, és csak érintőlegesen tárgyalta a

honvédelmi ágazatot, illetve a hadsereg szerepét a kiberbiztonság megteremtésében. Ennek megfelelően, Magyarországon a kiberbiztonság civil szervezetei közül az egyik legfontosabb elem a Belügyminisztérium irányítása alatt működő Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NKI). Az NKI magában foglalja a nemzeti információbiztonsági hatóságot, a kormányzati hálózat- és eseménykezelő központot, illetve a sérülékenységvizsgálatot végző szervezeti elemet. Ebből következően az NKI elsősorban az eseménykezelésre, az elektronikus információbiztonság hatósági feladataira és a sérülékenységvizsgálatra, valamint nem utolsósorban a biztonságtudatosság növelésére fókuszál. Ugyanakkor sem a civil kiberbiztonsági szervezetek, sem az NKI nem rendelkezik a jelen tanulmányban megfogalmazott kritériumoknak megfelelő kiberműveleti erővel és offenzív kiberképességekkel. A honvédelmi ágazaton belül két kiberműveleti szervezet alakult meg az elmúlt években. A Katonai Nemzetbiztonsági Szolgálatnál (KNBSZ) 2017-ben létrejött a Kibervédelmi Központ, amely 2021-től új néven, mint KNBSZ Kibertér Műveleti Központ látja el az ágazati elektronikus információbiztonsági eseménykezelés feladatait, valamint e szervezet egyik eleme a honvédelmi ágazati elektronikus információbiztonsági hatóság is. A honvédelmi ágazat másik kiberszervezete a Magyar Honvédség (MH) Parancsnoksága (MHP) alárendeltségében 2019-ben megalakult Kibervédelmi Haderőnemi Szemlélőség, illetve annak szakmai vezetésével várhatóan létrejövő Magyar Honvédség Katonai Kibertér Műveleti Központ (MH KKMK). A Szemlélőség fő feladata, hogy stratégiai szinten felügyelje és irányítsa az MH katonai kibertér műveleti erőinek kialakítását, fejlesztését, majd azok működtetését. A Szemlélőség szakirányítási feladatköre kiterjed a kiberszakterületet érintő valamennyi haderőfejlesztési és -fenntartási programra. A kiberszakterületen „szakmai felelős" jog- és hatáskörrel rendelkezik. A Szemlélőség határozza meg az MH kibervédelmi és kiberműveleti szakterülete vezetéséhez szükséges szervezeti kialakítás alappilléreit, valamint a kialakítandó kibervédelmi szervezetek struktúráját. Természetszerűleg a Szemlélőség szorosan együttműködik az MHP Infokommunikációs és Információvédelmi Csoportfőnökséggel, amely szervezet a honvédség IT-rendszereinek üzemeltetéséért és elektronikus információbiztonságáért felelős. A Szemlélőség szakmai irányításával megkezdődött az MH Katonai Kibertér Műveleti Központ kialakítása, amely a következő években várható folyamatos fejlődése során a katonai kibervédelem és a kiberműveletek szervezeti hátterét is nyújtja majd. Ez azt is jelenti, hogy a szervezet a kiberműveletek tervezéséhez és végrehajtásához szükséges adat- és információfeldolgozó képességgel, valamint offenzív kiberműveleti képességekkel és azok hatásait elemezni képes szervezeti elemekkel is fog rendelkezni. Az MH KKMK magában foglalja a már korábban, 2019-ben megalakult kiberképzési központot (Kiberakadémia) is.

A katonai kiberműveleti képességek kialakításáról a már említett új Nemzeti Biztonsági Stratégia rendelkezik. A stratégia az offenzív kiberműveleti képességeket is magába foglaló katonai fejlesztést és képességépítést a következő módon határozza meg: „A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit." Az NBS által meghatározott katonai kiberműveleti képességek alkalmazására a honvédelmi törvény ad felhatalmazást, illetve szab feladatot a 2020. január 1-jével a törvénybe bekerült katonai kibertérműveleti erőkre vonatkozó szabályokkal. Ezek többek között tartalmazzák, hogy az MH katonai kibertérműveleti erői folyamatosan ellátják „a honvédelmi szervezetek, gyakorlatok, műveletek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét, az arra történő felkészülést és a kapcsolódó biztonsági feladatokat", „a folyamatban lévő, kibertérből érkező támadás megszakításához szükséges intézkedések végrehajtását, vagy annak kezdeményezését", valamint „külön döntés szerint a Magyarország biztonságát, honvédelmi érdekeit, vagy szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai kibertérműveleti fellépést". Mindezek a katonai kibertérműveleti erők alkalmazásához szükséges, de nem elégséges feltételek, ugyanis számos egyéb olyan tényező is szükséges ezen erők alkalmazásához, mint amilyenek például a fenti – honvédelmi törvényből idézett – „külön döntés alapján" kitételek. Ez többek között a Kormány döntését jelenti, amely a törvény meghatározása alapján más elemek fennállása – például különleges jogrendi helyzet – esetén szükséges egy-egy támadó jellegű kibertérművelet végrehajtásához.

A felvázolt kibererők elemzéséből levonható következtetések

Már a fentiekben bemutatott néhány kiberműveletekért felelős szervezet vizsgálata alapján is azonosítani tudunk olyan általános jellemzőket, amelyek a legtöbb ország kibertérműveleti szervezetei esetében igazak. Ezek a szervezetek – természetszerűleg a fentiekben megfogalmazottaknak megfelelően országonként eltérő módon, de mégis jól azonosíthatóan – három nagy területre koncentrálnak. Ezek a területek, amelyeket jelen tanulmány első részében részletesen is bemutattam, az információszerző, célkiválasztó, célazonosító és célkövetési, valamint szimulációs képesség, a kibertámadás képessége és a hatások értékelésének képessége területek. Bár a fent bemutatott kibervédelmi és kiberműveleti szervezetek országonként eltérő feladatrendszerrel rendelkeznek, de többnyire ezek mégis a kibertérre és esetenként az információs dimenzióra vonatkozó feladatokat is jelentenek. Az azonban a többé-kevésbé eltérő feladatrendszer ellenére is világosan látszik, hogy minden ország a katonai kibererőitől az adott

ország teljes kibervédelmi képességeinek a növelését várja, illetve ezekben az erőkben látja ennek garanciáját. A katonai feladatok mellett esetenként megjelenik az adott ország kritikus infrastruktúrája védelmének feladata is. Természetszerűleg az Egyesült Államok katonai kiberműveleti erői sok esetben olyan feladatokat is ellátnak, amelyek egy-egy európai ország katonai kiberműveleti erői esetében békeidőben nem feladatok (például a politikai választások informatikai rendszereinek a védelme, vagy aktív hírszerző/felderítő tevékenység).A bemutatott katonai kiberműveleti erők elemzése azt is világossá teszi, hogy ezeknek a szervezeteknek a kialakítása, majd felkészítése és aktív, offenzív műveletek végrehajtására is kész képesség birtokába hozása hosszú időt vesz igénybe, ami 3-4 évet, de a teljes készenlét elérése akár 10 évet is jelenthet. Ugyanakkor fontos hangsúlyozni, hogy egy katonai kibertérműveletek ellátására alkalmas szervezetről sosem jelenthető ki, hogy az kész van, hiszen időről-időre újabb és újabb kibertéri kihívásokkal kell szembenézni, ami megköveteli a szervezet és/vagy annak képességbeli változását. Ugyanez igaz a személyi állományára is, hiszen az ő felkészítésük nem ér véget egy-egy tanfolyam vagy képzés elvégzésével. A különböző műveletek végrehajtása során felhalmozott tapasztalat és annak átadása szintén hozzájárul az állomány folyamatos fejlesztéséhez. Itt azonban egy problémát szükséges jelezni. Ez pedig a szakértő kiberműveleti állomány megtartása. Megfelelő bérezés, megfelelő munkakörülmények és nem utolsósorban megfelelő és inspiráló szakmai kihívások azok a tényezők, amelyek megtartó erőként szolgálhatnak. Egy ideig. Ugyanis a jól képzett, gyakorlott, megfelelő szakmai és nem utolsósorban műveleti tapasztalattal rendelkező kiberműveleti szakember értéke a munkaerőpiacon évről évre exponenciálisan nő. A civil – főleg a multinacionális – cégek által nyújtott fizetési és egyéb juttatásokkal a közszféra, így a katonai terület sem tud versenyezni. Ez még az Egyesült Államokra is igaz. Egy másik, bár meglehetősen triviális megállapítás a fentiek alapján, hogy minden ország rendkívül fontosnak tartja a szakemberek utánpótlásának folyamatos biztosítását. Ez már a középiskolák és az ott tanuló diákok képzésében és toborzásában is megjelenik. Ezt teszi a US Cyber Command. A parancsnokság létrehozta a Cyber Patriot STEM (Science, Technology, Engineering, and Mathematics, STEM, magyarul mérnöki és matematikatudományi) programot, amely keretében helyi középiskolákkal folytat együttműködést, illetve több mint 50 egyetemmel végez közös munkát, amely egyrészt közös kutatás-fejlesztést, másrészt tehetséges jövőbeni munkavállalók felkutatását és kiválasztását is jelenti. Hasonló programot indított a lengyel Nemzeti Kibervédelmi Központ is, amely az úgynevezett Cyber.Mil.Pl program keretében a varsói Katonai Műszaki Egyetem támogatásával kiberbiztonsági tematikájú középiskolai osztályt, illetve e mellett kiberbiztonsági egyetemi mesterképzést is indított 2019 őszén.

Németország is hasonló lépéseket tett, hiszen a müncheni Bundeswehr Egyetemen kiberbiztonsági mesterképzést indított. Hazánk is komoly lépéseket tett az oktatás és az utánpótlás területén. Számos egyetemen indult el az informatikai szakokon kiberbiztonsági témájú tárgy oktatása, illetve a Nemzeti Közszolgálati Egyetem elindította a Kiberbiztonság nevű kétéves mesterképzési szakját is. A vizsgált országok mindegyikében kiemelt szerepet kap a kutatás-fejlesztés a kiberbiztonság és a kiberműveletek területén. A kibertéri erők ehhez sok esetben igénytámasztóként jelennek meg, de természetszerűleg maguk is kell, hogy rendelkezzenek K+F képességekkel, amelyek a kevésbé energia- és időigényes fejlesztési feladatokat látják el. Ugyanakkor az akadémiai szférával – például egyetemekkel, kutatóintézetekkel –, valamint a civil IT-szektorban és/vagy a kiberbiztonsági iparban dolgozó és kutató vállalatokkal történő kapcsolattartás és szoros együttműködés szintén elengedhetetlen. A jól működő K + F hosszú távú folyamat, amely azokra az igényekre ad gyakorlatban is használható választ (eredményt), amelyek a potenciális szemben álló fél polgári és/vagy katonai rendszereinek védelméhez, illetve támadásához szükségesek. A kutatás-fejlesztés egyik nagyon jó példája, és ha tetszik, reklámja is az amerikai Dreamport kezdeményezés, amelyben azok a legújabb kutatás-fejlesztési és innovációs projektek és azok eredményei kapnak helyet, amelyeket a kormányzati szervezetek – mint például a US Cyber Command –, az akadémiai szféra és az ipari szereplők közösen végeznek és érnek el. Németország a haderő támogatásával egy kiberbiztonsági kutatóintézetet alapított Berlinben, amely szintén ellát K + F feladatokat.

Hazánkban a Nemzeti Közszolgálati Egyetemen alakítottak meg egy Kiberbiztonsági Kutatóintézetet, amely alkalmas lehet a jövőben a kiberterület tudományos alapjainak megteremtése és kutatása mellett K + F feladatok elvégzésére, illetve azok akadémiai szférán belüli koordinálására.

Az offenzív kiberképességek és a NATO

A NATO nagy utat tett meg azóta, hogy 2016-ban a Varsói Csúcsértekezleten a negyedik műveleti térré minősítette a kiberteret. A kibertér műveleti térré nyilvánításával egy időben a tagországok egyöntetűen állást foglaltak abban, hogy kibervédelmi képességeiket fejlesztik. Ez az úgynevezett Cyber Pledge, azaz Kibervállalás, amelyet azóta is évente nagyon következetes módon a NATO ellenőriz. Ennek során nemcsak az ellenőrzésen van a hangsúly, hanem a szervezet tanácsokat és segítséget is nyújt a kibertéri képességek kialakításában, illetve fejlesztésében. A Cyber Pledge esetében is igaz az a tény, amelyet a nemzeti kibervédelmi képességek során már megállapítottunk. Nevezetesen, hogy ez nem csak katonai, hanem össztársadalmi feladat. Ezt támasztja alá a NATO hivatalos közleménye is, amely a Cyber Pledge-dzsel kapcsolatosan a következőket jelenti

ki: „A Pledge-et a washingtoni szerződés 3. cikkével összefüggésben fogadták el, amely kimondja, hogy »a szövetségesek fenntartják és fejlesztik egyéni és kollektív képességüket a fegyveres támadások ellen.« Mivel ebben a térben lehetetlen teljesen szétválasztani a katonai, polgári és ipari kérdéseket, a NATO-nak komoly érdeke fűződik a Szövetségen kívüli szervezetek kibervédelmi képességeinek javításához." A NATO-nak önmagának nincsenek offenzív kiberképességei. Ilyen képességekkel a tagországok rendelkeznek, de mivel nem minden tagország mutatja be vagy vállalja fel nyilvánosan e képességeit, ezért pontos számot vagy képességet csak becsülni lehet. Néhány ország ezeket a képességeit felajánlotta a NATO számára, így róluk biztosan tudhatjuk, hogy rendelkeznek offenzív kiberképességekkel. A tagállamok által önkéntesen felajánlott offenzív kiberképességekre a NATO egy sajátos terminológiát is alkotott, amelyet az angol kifejezésből származtatott mozaikszóval SCEPVA-nak (Sovereign Cyber Effects Provided Voluntarily by Allies, azaz a Szövetségesek Önkéntes Hozzájárulásán Alapuló Kiberhatások) neveznek. Ennek fontosságát hangsúlyozza Libicki egy tanulmányában: „Bár a NATO-nak nincs saját támadó kiberképessége, de a kiberműveletek növekvő jelentősége a NATO hatékony kollektív védelme és elrettentése szempontjából megköveteli annak alapos megértését, hogy a kiberképességek kihasználása hogyan befolyásolhatja a konfliktusok dinamikáját." Németország az egyik olyan ország, amely felajánlotta kiberképességeit a Szövetségnek. Az akkori német védelmi miniszter, a már említett Ursula von der Leyen nem részletezte a felajánlott kiberképességek mibenlétét, de úgy fogalmazott: „Ahogy a szárazföldi haderőkkel, a légierővel és a haditengerészeti erőkkel támogatjuk a NATO-t, most abban a helyzetben vagyunk, hogy a rendelkezésünkre álló nemzeti és jogi keretek között biztosítsuk a NATO képességeit kiberügyekben." Mindezeket a tagországi felajánlásokat is koordinálja a NATO Kibertér Műveleti Központja (Cyberspace Operation Center, CyOc), amit a NATO parancsnoki struktúrájának részeként állítottak fel. A CyOc a SHAPE, a NATO Európai Erők Főparancsnokságán (Supreme Headquarters Allied Powers Europe, SHAPE) J6 besorolású, azaz az infokommunikációs főnökség része. Dedikáltan ez a – 2017-es felállítását követő három évben magyar tábornok, Vass Sándor által vezetett – szervezet lehet az egyik legfontosabb szereplője a kibertámadások összehangolásának a Szövetségen belül. Ugyanakkor a kiberműveletek területén a NATO egyik legnagyobb kérdése, ha tetszik legfontosabb problémája a tagországok eltérő kibervédelmi fejlettsége. Ez részben igaz az offenzív kiberképességek területére is. Azért csak részben, mert ezen a területen egyéb kérdések is felmerülnek. Az első ilyen kérdés az, hogy abban az esetben, ha egy tagország felajánlja kibertámadó képességeit a NATO-nak, és azt alkalmazzák, akkor a nemzet vagy a Szövetség lesz-e a felelős a művelet végrehajtásáért, illetve azok esetleges következményeiért? A fentiek mellett a NATO még egy hatalmas

problémával küzd, amely nem más, mint a háborús küszöbszint alatt tartott kiberkonfliktusok problémája. Korábban már említettük, hogy ez a helyzet talán a „még nincs háború, de már nem beszélhetünk békéről" kifejezéssel jellemezhető. Ez az időszak óriási kihívás elé állítja a kiberbiztonság területén dolgozó szakembereket. Az ilyen módon alkalmazott offenzív kiberműveletek nem elsősorban technikai értelemben vett kihívást, sokkal inkább politikai, jogi és diplomáciai problémát jelentenek. Ezeknek a kérdéseknek a kutatása kiemelten fontos. Itt ki kell emelni a NATO Kibervédelmi Kiválósági Központjának (Cooperative Cyber Defence Centre of Excellence, CCDCOE) munkáját. A 2008-ban alakult kutatóközpont a NATO-hoz hasonlóan önmaga is hatalmas utat járt be a kiberbiztonság kutatásának területén, és mára az egyik meghatározó szereplőjévé vált a témának. A stratégiai kérdésektől és az azokban a tagországoknak nyújtott segítségtől kezdődően, a kiberbiztonság területén végzett különböző kutatásokig elmenően hatalmas oktatási, képzési munkát is végez a központ. A szervezet által készített és rendszeresen publikált tanulmányokban nem csak a NATO-tagországokból származó kutatók a fenti kérdésekre keresik a választ.

Ezeknek a kérdéseknek a korántsem egyértelmű megítéléséről így ír Libicki és társa a CCDCOE-nek, a NATO-val szembeni kiberfenyegetéseket 2030-as idősíkon elemző kötetében: „A kibertérben véget nem érő konfrontációk ellenére a stratégiai kiberháború azon lehetősége, hogy komoly károkat okozzon a modern gazdaságban, továbbra is vita tárgya [...] Minél nehezebb előre kitalálni a [kiberháború] hatását, annál nagyobb a nézeteltérés annak megítélésében, hogy az ilyen műveletek elkezdődnek-e."

Összefoglalás, következtetések:

Az ma már nem kérdés, hogy a kibertér és annak biztonsága az egyik legfontosabb biztonság- és védelempolitikai és ezzel együtt katonai kérdés is egyben. Az új műveleti tér a hadviselés változásával, és nem utolsósorban az ehhez a térhez (is) történő adaptációjával új típusú katonai szervezetek létrehozását is indukálta világszerte. A jelen írásban bemutatott néhány ország, köztük hazánk kiberműveleti képességeiből számos következtetés vonható le, amelyek közül az egyik az, hogy e képességek egyre növekvő mértékben tartalmazzák az offenzív kiberműveleti képességeket. Az offenzív kiberképességek megjelenését leginkább az indokolja, hogy ezzel a képességgel, annak akár aktív alkalmazásával, akár csak egyszerű deklarálásával (amely mögött azonban a korábban említett valódi képességeknek meg kell lenniük) a saját rendszereinktől, legyenek azok katonai vagy civil rendszerek, a lehető legtávolabb tartsuk a potenciális rosszindulatú kibertevékenységeket. Ez jelenthet egyfajta elrettentést is, de jelentheti azt is, hogy olyan mértékben csökkentjük az ellenérdekelt fél (kiber)képességeit, amelyek-

kel már nem tud hatékony támadást indítani az információs rendszereink ellen. A katonai kibertérműveleti képességek azonban nem csak, és nem elsősorban katonai célokat szolgálnak. Ezek a képességek az ország kibervédelmi képességeihez alapvető módon járulnak hozzá, annak szerves részét képezik. A katonai kiberképességek, az ország civil kibervédelmi és kiberműveleti képességeivel együtt jelentik az ország adaptív ellenállóképességének egyik igen fontos elemét. A tanulmányban bemutatott négy ország kiberműveleti erőinek elemzéséből levonható következtetések is mutatják, hogy a katonai kibertéri feladatokat ellátó erőket országonként eltérő módon alakították ki és részben eltérő feladatokat is látnak el. Ugyanakkor – szervezeti kialakítástól függetlenül – megállapíthatók az azonos feladatok és felelősségi területek. Az információszerző, célkiválasztó, célazonosító és célkövetési, valamint szimulációs képesség, a kibertámadás képessége és a hatások értékelésének képessége területek a bemutatott országok katonai kiberműveleti erői esetében is fellelhetők. A helyenként eltérő feladatrendszer ellenére is világosan látszik, hogy minden országban a katonai kiberműveleti erők az adott ország teljes kibervédelmi képességeinek a növeléséhez szignifikáns módon járulnak hozzá.

A bemutatott katonai kiberműveleti erők elemzése során látható, hogy ezeknek a szervezeteknek a kialakítása, felkészítése és aktív, offenzív műveletek végrehajtására is kész, egységes szemlélettel rendelkező, ütőképes erővé való fejlesztése minimum 3-4 évet, de azok teljes műveleti készenlétének elérése akár 10 évet is igénybe vehet. Az elemzésekből levonható további markáns következtetés, hogy a technikai fejlesztéseken kívül a szakemberek utánpótlásának biztosítása, illetve a szakemberek megtartása kiemelten fontos kérdés. Az ezeket a kérdéseket kezelni képes oktatási és továbbképzési rendszer, a szakembereknek a szintén elengedhetetlen kutatás-fejlesztés feladataiba való – minél korábban történő – bevonására is komplex módon ki kell terjedjen. A NATO-t kiberműveleti szempontból röviden megvizsgálva kijelenthető, hogy a Szövetségnek önmagának nincsenek offenzív kiberképességei. Ilyen képességekkel csak a tagországok rendelkeznek, amelyeket önkéntes alapon ajánlanak fel a szervezetnek. Ezek a felajánlott képességek, illetve azok alkalmazásai, bár hozzájárulnak a NATO elrettentési politikájához, mégis számos – elsősorban jogi és felelősségi – kérdést vetnek fel, amelyekre jelenleg számos tudományos kutatás keresi a választ. A fentiekben idézett Libicki-gondolat is rávilágít arra, hogy sem a NATO, sem a nagyhatalmak, sem a kisebb országok nem lehetnek teljesen biztosak a kibertér, illetve az abban folytatott műveletek jövőbeni szerepében. Ennek megfelelően szükséges akár a Szövetség, akár az egyes országok kiberképességeit a védelmi képességek mellett az offenzív képességeket is magában foglaló módon építeni.

Hibrid hadviselés (műveletek)

- A hibrid hadviselésnek nincs általánosan elfogadott meghatározása
- A NATO walesi csúcstalálkozója alapján: „a hibrid fenyegetés széles körű nyílt és fedett katonai, félkatonai és nem katonai eszközök és eljárások alkalmazása egy szorosan integrált műveleti terv mentén.”

forrás: Kiss Álmos Péter: A hibrid hadviselés természetrajza. https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf

Hibrid hadviselés (műveletek)

- **EU meghatározása szerint:**
  - kényszerítő és felforgató tevékenységek;
  - hagyományos és nem hagyományos módszerek együttese:
    - katonai, diplomáciai, gazdasági, technológia;
    - social media, félretájékoztatás, befolyásolás;
  - állami vagy nem állami szereplők összehangolt akciói;
  - döntéshozatal befolyásolása;
  - a deklarált hadviselés szintjét el nem érő módon.

forrás: Kiss Álmos Péter: A hibrid hadviselés természetrajza. https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf

Felhasznált irodalom

AFP: Germany to Let NATO Use its Cyber Skills. Security Week, 2019. február 14. Online: www.securityweek.com/germany-let-nato-use-its-cyber-skillsAJP-3.20

Allied Joint Doctrine for Cyber Space Operations Edition A Version 1, 2020.Brent, Laura: NATO's role in cyberspace. NATO, 2019. február 12. Online: www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Bundeswehr: Kommando Cyber- und Informationsraum. (é. n.). Online: www.bundes-wehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraumBundeswehr: The Cyber and Information Domain Service. (é. n.). Online: www.bundes-wehr.de/en/organization/the-cyber-and-information-domain-serviceBundeswehr: Zentrum für Cyber-Sicherheit der Bundeswehr. (é. n.). Online: www.bun-deswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-orga-nisation-cir/kommando-informationstechnik-der-bundeswehr/zentrum-fuer-cy-ber-sicherheit-der-bundeswehr

CSIRT-MON: Ministerstwa Obrony Narodowej. (2021). Online: https://csirt-mon.wp.mil.pl/pl/

Cyber.Mil.PL: Cyber Operations Center. (2021). Online: Cyber Security Training Centre of Excellence: What we do. (é. n.). Online: https://cstcoe.mil.pl/en/pages/what-we-do/

Ertan, A. – K. Floyd – P. Pernik – T. Stevens (szerk.): Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDOE, 2020. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Ana-lysis.pdf

Kovács László: Offenzív kiberműveletek I.: Az offenzív kiberműveletek természete. Hadmérnök, 16. (2021), 2. 187–204. Online: https://doi.org/10.32567/hm. 2021.2.13

Kovács László: Kiberbiztonság és -stratégia. Budapest, Dialóg Campus, 2018. Online: http://kovacsx.hu/download/books/KovacsLaszlo_A_kiberbiztonsag_es_strategia.pdf

Leinhos, Ludwig: Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr. Connections: The Quarterly Journal, 19. (2019), 1. 9–19. Online: https://doi.org/10.11610/Connections.19.1.02

Leinhos, Ludwig: The German Cyber and Information Domain Service as a Key Part of National Security Policy. Ethics and Armed Forces, (2019), 1. Online: www.ethikundmilitaer.de/en/full-issues/20191-conflict-zone-cyberspace/leinhos-the-german-cy-ber-and-information-domain-service-as-a-key-part-of-national-security-policy/

Libicki, Martin C. – Olesya Tkacheva: Cyberspace Escalation: Ladders or Lattices? In A. Ertan – K. Floyd – P. Pernik – T. Stevens (szerk..): Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDOE, 2020. 60–73. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scan-ning-and-Analysis.pdf

National Security Archive: USCYBERCOM 30-Day Assessment of Operation Glowing Symphony. (2016. december 13.). Online: https://nsarchive.gwu.edu/dc.html?-doc=6655596-National-Security-Archive-5-USCYBERCOM

Nemzeti Közszolgálati Egyetem: Kiberbiztonsági mesterképzési szak. (é. n.). Online: https://antk.uni-nke.hu/oktatas/mesterkepzes/kiberbiztonsagi-mesterkepzesi-szak

Pomerleau, Mark: What Cyber Command's ISIS operations means for the future of information warfare. C4ISRNet, 2020. június 18. Online: www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-me-ans-for-the-future-of-information-warfare/

Świątkowska, Joanna – Izabela Albrycht – Dominik Skokowski: National Cyber Security Organisation: POLAND. Tallinn, NATO CCDCOE, 2017. Online: https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf

United States Government Accountability Office: DOD TRAINING. U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force.(2019. március). Online: www.gao.gov/assets/gao-19-362.pdfUniversität der Bundeswehr München: Studiengang Master Cyber-Sicherheit. (é. n.). Online: www.unibw.de/inf/studium/studiengang-cyber-sicherheit

US Cyber Command: Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command. (2018. április). Online: www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010www.cyber.mil.pl/artic-les/o-nas-f/2018-10-23c-centrum-operacji-cybernetycznych/Cyber.Mil.Pl: O Nas. (2021). Online: www.cyber.mil.pl/o-nas

Bundeswehr rüstet gegen Attacken aus dem Internet. (2016. április 26.). Online: www.zeit.de/politik/deutschland/2016-04/ursula-von-der-leyen-bun-deswehr-aufruestung-cyberkrieg-angriffe-internet

Jogi források:

2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Kibertéri kognitív befolyásolás az információs műveletekben

Prof. Dr. Haig Zsolt, mk. ezredes, egyetemi tanár
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar,
Elektronikai Hadviselés Tanszék, Budapest
haig.zsolt@uni-nke.hu

Bevezetés

Napjainkban a regionális feszültségek előfordulási gyakorisága növekszik. E konfliktusok műveleti környezete jelentősen különbözik a tradicionális állam-állam elleni fegyveres konfliktusoktól. Ezeknek az új típusú katonai műveleteknek a negyedik generációs hadviselési modellen belül számos elnevezése van, mint például aszimmetrikus, irreguláris, felkelés elleni vagy hibrid hadviselés, de a kibertéri műveletek is ide tartoznak. A negyedik generációs hadviselésnek egyik fő jellemzője, hogy a katonák mellett civilek is megtalálhatók a műveleti területen, és szemben álló félként pedig nem állami szereplők is megjelennek. A műveleti területen tehát a lakosság és a semleges érintettek is a katonai műveletek részesévé válnak. Ennélfogva pedig a konfliktus a társadalom egészét érinti. Ezért e műveletekben a szemben álló fél mellett a nem állami szereplők és a lakosság befolyásolása kiemelt szerepet kap. Egy korábbi tanulmány szerint a negyedik generációs katonai műveletekben az információs műveletek során a kognitív befolyásoláson alapuló úgynevezett adaptív információs fölény kialakítására törekszenek. Ez esetben ugyanis nem a saját erők előnyösebb információkezelési és döntési képességén van a hangsúly, hanem a célközönség gondolatainak, véleményének átalakításán, valamint meggyőzésén, esetleg manipulálásán. A korszerű hálózatos infokommunikációs technológia napjainkban jelentősen növeli a kognitív befolyásolás lehetőségeit. Megfelelően kiépített infokommunikációs infrastruktúra megléte esetén a kibertérben a különféle befolyásoló és manipulációs tevékenységek nagyobb hatékonysággal alkalmazhatók, mint a hagyományos technikák. A kiberteret felhasználva ugyanis a befolyásoló vagy megtévesztő információkat rövid idő alatt nagy tömegekhez lehet eljuttatni. A hatásokat pedig tovább fokozzák az internetes hírportálokon, illetve a közösségi médiában egyre terjedő álhírek, amelyek jelentősen átformálhatják az egyének véleményét. Az álhírek alkalmazása társadalmi, politikai, katonai és marketingszempontból is igen kifizetődő a terjesztőjének, hatékonyságához pedig manapság nemigen fér kétség. Ebből fakadóan az álhírek terjedése a világhálón és benne a közösségi médiában egyelőre megállíthatatlan. Mindezek alapján a tanulmány célja, hogy a befolyásolás elméletére alapozva kiemelje a kibertéri kognitív tevékenységek fontosságát, ismertesse a befolyásolás és manipuláció kibertéri technikáit, és bemutassa azok információs műveleteken belüli egymásra hatását.

A befolyásolás szociálpszichológiai háttere

A társadalmi befolyásolás a szociálpszichológiához kapcsolódó tevékenység, amely a célközönség gondolkodására, viselkedésére, vélekedésére és érzelmeire hat annak érdekében, hogy azok a befolyásoló érdekeinek megfelelően alakuljanak. E tudomány egyik jeles alakja volt Herbert Kelman, aki szerint a társadalmi befolyásolásnak az alábbi formái léteznek: megfelelés, azonosulás és internalizáció. A megfelelés azt jelenti, hogy a befolyásolt célközönség a saját véleményét megtartva fogadja el a befolyásoló érveit, és a célcsoport az addig megszokott viselkedés és attitűd helyett az elvárt hozzáállást és gondolkodást mutatja. A megfelelés a befolyásolás legalsó szintje, így ha a befolyásoló információk és üzenetek megszűnnek, akkor a célközönség a saját korábbi véleményéhez tér vissza. Ennek következtében tartós hatás nem, csak rövid távú viselkedési megfelelés érhető el, ami azt is jelenti, hogy az információs műveletekben alkalmazott kognitív befolyásolás során ezen állapot elérése a legkevésbé kívánatos. Az azonosulás során a célközönség azért azonosul a befolyásoló véleményével, mert olyan szeretne lenni, mint ő. Az azonosuló befolyásolás függ a célcsoport befogadó képességétől, valamint a közte és a befolyásolást végző közötti kapcsolat formájától és minőségétől. Optimális esetben az azonosulással elért gondolkodás- és viselkedésváltozás hosszabb ideig is fennmaradhat, így negatív hatásokkal kevésbé kell számolni. Emiatt az információs műveletek keretében végzett kognitív befolyásolással elért ilyen állapot segítheti a befolyásolási célok teljesítését. Az internalizáció esetében a befolyásolt célközönség teljes mértékben elfogadja a befolyásoló nézeteit, és magára nézve fenntarás nélkül érvényesíti azokat. Az információs műveleti kognitív befolyásolás esetén ez tartós tudati és viselkedésbéli változást eredményez, ugyanakkor ennek az állapotnak az elérése is a legnehezebb.

Az információs műveletek és a kibertéri műveletek értelmezése

Az információs műveletek újszerű értelmezését egy korábbi tanulmányban már elemeztük. Ennek lényege, hogy az információs műveletek az információs környezet fizikai, információs és kognitív dimenziójában érvényesülő, integrált, egymással összehangolt és koordinált információs tevékenységek összessége, ami a műveletek célkitűzéseinek elérése érdekében közvetlenül kognitív befolyásolással, illetve közvetetten technikai ellentevékenységgel és védelmi tevékenységekkel hatásokat gyakorol a műveletekben érintett célközönség szándékára, helyzetértelmezésére és képességeire. Általános megközelítésben az információs műveletek technikai és kognitív képességei közé az alábbiakat sorolhatjuk:

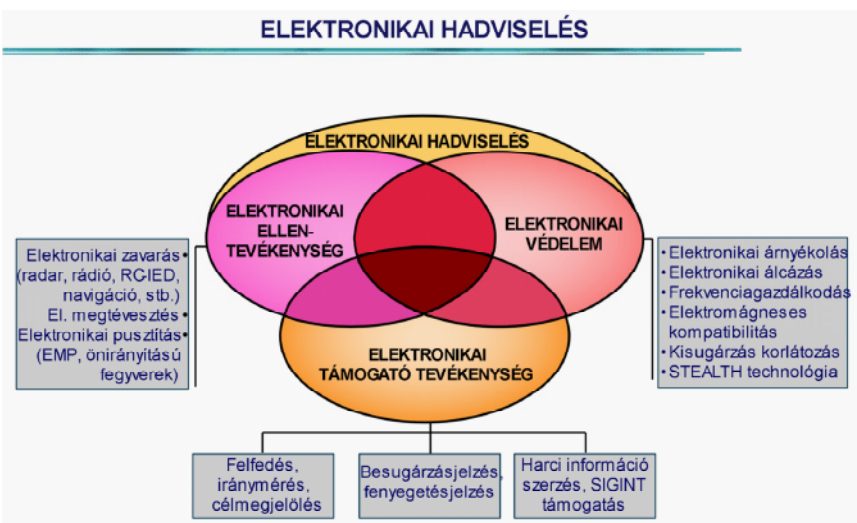
technikai képességek:

- elektronikai hadviselés
- számítógép-hálózati műveletek
- információs célpontok fizikai megsemmisítése
- műveleti biztonság technikai képességei
- megtévesztés technikai képességei

kognitív képességek:

- pszichológiai műveletek (psychological operations, PSYOPS)
- közügyek és tömegtájékoztatás
- civil-katonai együttműködés (civil-military cooperation, CIMIC)
- műveleti biztonság kognitív képességei
- megtévesztés kognitív képességei.

Napjainkra az információs műveletekben a technikai információs képességek mellett a kognitív térben a célközönséggel szembeni közvetlen információs hatások jelentősége felértékelődött. Az információs műveletek kognitív képességei az információ tartalmára fókuszálnak, és pozitív, negatív vagy semleges befolyásolási technikákat, tájékoztatási eszközöket és módszereket alkalmazva közvetlenül érik el a célközönséget.



E képességek alkalmazása során különféle eszközöket és módszereket használnak, és jól megszerkesztett üzenetekkel, közvetlenül az emberek tudati tevékenységére hatnak. Az információs műveletek kognitív képességeinek célja minden esetben a humánum befolyásolása, manipulálása, a hatásuk tehát az információs környezet kognitív dimenziójában jelentkezik. Emellett a hálózatos technológia rohamos terjedése következtében a kibertér az információs környezet fontos tartományának tekinthető, így az e tartományban zajló kibertéri műveletek egyre jelentősebbé válnak. A NATO kibertéri műveletek doktrínája általánosságban adja meg a kibertér definícióját, amely szerint az egy „globális tartomány, amely magában foglal minden egymással összekapcsolt kommunikációs, információtechnológiai és egyéb elektronikus rendszert, hálózatot és azok adatait, beleértve az elkülönült vagy független rendszereket is, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak". A kibertér az információs környezet része, így annak mindhárom dimenziójában, vagyis a fizikai, az információs és a kognitív tartományban egyaránt megjelenik. Az előzőkben hivatkozott doktrína és más irodalmak is a kibertér három rétegét értelmezik, úgymint: fizikai réteg, logikai réteg és kiberszemélyiség-réteg.

A fizikai réteg hardverekből, infrastruktúrákból és kapcsolódó eszközökből áll, amelyek a kibertérben az információ tárolását, szállítását és feldolgozását végzik. Ide tartoznak a hálózati infrastruktúrák, számítógépek, szerverek, routerek, vezetékes és vezeték nélküli kapcsolatok stb. A hálózatos vezeték nélküli kapcsolatok növekedése miatt a fizikailag definiálható elektromágneses spektrum, azon belül is különösen a rádió-frekvenciás tartomány is a fizikai réteghez sorolandó. A logikai réteg a digitális információs és parancsréteg, amely adatokból és kódokból áll, mint például firmware-ek, operációs rendszerek, átviteli és címzési protokollok, szoftveralkalmazások, valamint adatkomponensek, adatbázisok. A kiberszemélyiség-réteg a szervezetek és egyének virtuális reprezentációiból áll. Ezek közé tartoznak az e-mail-címek, felhasználói azonosítók, közösségimédia-fiókok, IP- és MAC-címek stb. A fentieken kívül e réteg teszi lehetővé a személyek kapcsolati hálóinak kialakítását, valamint a közösségi háló tagjainak interakcióit. A kibertérben az egymással szemben álló felek különféle műveleteket folytatnak, amelyek érintik a kibertér mindhárom rétegét. A kibertéri műveleteknek ma már számos értelmezése ismert. A NATO szakterületi doktrínája megadja a kibertéri műveletek általános definícióját, miszerint „a kibertérben vagy azon keresztül végzett tevékenységek, amelyeknek célja a saját erők cselekvési szabadságának megőrzése a kibertérben és/vagy a parancsnokok

céljainak elérését szolgáló hatások előidézése". A kibertéri műveletek szoros összefüggést mutatnak az információs műveletekkel. A célok és az alkalmazható eszközök és módszerek sok esetben ugyanazok, illetve át is fedhetik egymást. A különbség abban áll, hogy míg az információs műveletek a teljes információs környezetben zajlanak, addig a kibertéri műveletek az információs környezet egy speciális színterén, a hálózatos infokommunikációs technológia által kreált kibertérben folynak. Az információs környezet és a kibertér szoros összefüggése lehetővé teszi, hogy az információs műveletek definíciójának analógiája mentén a NATO meghatározásánál konkrétabban definiáljuk és értelmezzük a kibertéri műveleteket. Ez alapján a kibertéri műveletek a kibertérben alkalmazott információs tevékenységek koordinált alkalmazásának összessége, amelyek, az infokommunikációs hálózatokat felhasználva, a közvetlen kognitív, illetve közvetett technikai eszközökkel és módszerekkel hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire. Általánosan bevett gyakorlat szerint a kibertéri műveletek értelmezésekor általában klasszikus számítógép-hálózati támadás és védelem technikai módszerek alkalmazását hangsúlyozzák, mint például a hálózathoz, adatokhoz, adatbázisokhoz való hozzáférés; kártékony programokkal adatbázisok módosítása, törlése; túlterheléses támadások stb., illetve az ezek elleni védekezés lehetőségei. Ugyanakkor a kibertér háromrétegű értelmezése és az azokban megvalósuló kibertéri műveletek kapcsán a kognitív képességek egyre fontosabbakká válnak. Ezek a képességek a kibertérben való befolyásolásra és manipulálásra fókuszálnak. A tanulmány témája szempontjából a kognitív befolyásolás és manipuláció a kibertér mindhárom rétegében megvalósulhat a hálózatos infokommunikációs rendszereken keresztül továbbított valós vagy hamis információkkal, hatásuk azonban minden esetben a kiberszemélyiség-rétegen keresztül a felhasználókban közvetlenül jelentkezik.

Kognitív információs műveletek a kibertérben

A hálózatos infokommunikációs technológia igen jó lehetőségeket teremt a kognitív hatásokat előidéző különféle eszközök és módszerek alkalmazására. Az internet és benne a közösségi média pedig jelentősen kiszélesítik a kognitív befolyásolás és manipuláció lehetőségeit. Ezeknek az új kibertéri technológiáknak számos olyan tulajdonsága van, amelyek meghatározzák a különféle kognitív információs tevékenységek alkalmazásának hatékonyságát.

Kibertéri kognitív információs tevékenységek jellemzői

Svetoka elemzése rámutat, hogy a kibertéri technológiák a hagyományos befolyásolási módszerekhez képest az alábbi hatékonyságnövelő tulajdonságokkal rendelkeznek:

- hozzáférhetőség: a vezeték nélküli mobil technológiáknak, okostelefonoknak köszönhetően az információkhoz való hozzáférés és azok megosztása jelentősen leegyszerűsödik bárki számára
- sebesség: a röplapokhoz, újságokhoz és más hagyományos információterjesztő formákhoz képest a közösségi médiában a befolyásoló vagy manipulációs célú üzenetek igen gyorsan terjeszthetők, ami lehetővé teszi, hogy azok hatása is sokkal gyorsabban jelentkezzen
- anonimitás: a névtelenség és gyakran a beazonosíthatatlanság nagyobb szabadságot ad a vélemények kifejtésének
- információdömping: a közösségi médiában rendkívül sok a lényegtelen, nem releváns, esetleg hamis információ, amelyeket igen nehéz beazonosítani és elkülöníteni a valós tényeket tartalmazó információktól
- földrajzi és információtartalmi határok nélküliség: az előző sajátosságokból adódóan is a hagyományos médiához képest sokszor tartalmi megkötések és földrajzi határok nélkül lehet információt megosztani és terjeszteni.

E sajátosságok alapján a kibertér befolyásolási célból való felhasználásának egyik legnagyobb előnye, hogy a célok elérése érdekében gondosan megválogatott információk rövid idő alatt széles tömegeket érhetnek el, és a megcélzott közönség is megsokszorozódhat. Emellett a vezetők vagy véleményvezérek közösségi oldalakon való célzott befolyásolásával az irányításuk alatt álló csoport tagjainak véleménye, gondolkodása is könnyebben alakítható, esetleg manipulálható. A felsorolt hatékonyságnövelő tulajdonságokra alapozva a befolyásolás mindhárom formája, vagyis a megfelelés, az azonosulás és az internalizáció is hatékonyabban elérhető a kibertérben. A leginkább kívánatos internalizáció kialakítása a kibertéri technológia felhasználásával jóval eredményesebben valósítható meg. A kibertéri kognitív módszerekkel nagyobb hatékonysággal lehet elérni, hogy a befolyásolt célközönség teljes mértékben elfogadja a befolyásoló nézeteit, és magára nézve fenntartás nélkül érvényesítse azokat. E módszer további nagy előnye, hogy az anonimitást kihasználva a kibertérben a befolyásoló könnyebben rejtve maradhat, így a célközönség csak az információ tartalmára fókuszálhat, és azt nem tudja összekapcsolni a befolyásoló személyével. Ez pedig jó lehetőségeket kínál a befolyásoló számára akár szélsőséges narratívák, álhírek vagy manipuláló információk terjesztésére is.

Kibertéri kognitív információs tevékenységek

Az előzőkben bemutatott információs műveletek képességei és a kibertéri műveletek jellege alapján a kibertérben is alkalmazható és különféle kognitív hatásokat előidéző információs képességek közé sorolhatjuk:

- a pszichológiai műveleteket (PSYOPS)
- a kognitív megtévesztést
- a civil-katonai együttműködést (CIMIC) és
- a kognitív műveleti biztonságot.

A PSYOPS-ot és a kognitív megtévesztést a befolyásolás, illetve a manipuláció kategóriájába sorolhatjuk, a CIMIC és a kognitív műveleti biztonság pedig alapvetően a tájékoztatás és kapcsolatépítés, valamint a biztonságtudatosság területéhez tartozik. A PSYOPS a NATO meghatározása szerint a „jóváhagyott célközönség felé irányuló kommunikációs módszerek és egyéb eszközök felhasználásával tervezett tevékenységek, amelyek célja, hogy befolyásolják a politikai és katonai célok elérésére hatással lévő felfogást, attitűdöt és viselkedést". A célközönség helyes kiválasztása és meghatározása az egyik kritikus pontja a PSYOPS végrehajtásának, ugyanis az üzenetek tartalmának és a célba juttatás módszereinek alkalmazkodni kell a befolyásoltak etnikai, kulturális, vallási és egyéb értékeihez, valamint a célterületen lévő infrastrukturális lehetőségekhez. Mivel a NATO-doktrína szerint a PSYOPS valós és hiteles információkon alapul, az üzenetek tartalmának összeállításakor – a célközönség sebezhetőségének figyelembevételével – hitelt érdemlő, de befolyásoló hatású témákat kell kiválasztani. Kedvező infrastrukturális feltételek megléte esetén a PSYOPS-üzenetek célba juttatására a hagyományos módszerek mellett, mint például röplapok, szóbeli kommunikáció, nyomtatott sajtó stb. a legkorszerűbb hálózatos technológiák is felhasználhatók. Ennek megfelelően a kibertéri PSYOPS során a hálózatos rendszereket felhasználva, valós információkon alapuló üzeneteket közvetítenek a kiválasztott célközönség felé. Az internet, a közösségi média és a mobil kommunikáció széles lehetőségeket nyújtanak a hatékony PSYOPS megvalósításában, amelyet a befolyásolók egyre eredményesebben használnak ki. Emiatt a kibertéri PSYOPS-ot a fizikai és logikai rétegben alkalmazzák, hatása azonban minden esetben a kiberszemélyiség-rétegben, vagyis a felhasználók kognitív tudatában jelentkezik (lásd az 1. táblázatot).A legismertebb kibertéri PSYOPS-műveletek közé sorolhatjuk többek között a 2016-os amerikai elnökválasztási kampány befolyásolását, amelyben többek között szerepet játszott a Cambridge Analytica és a Facebook felhasználói adatbotránya és a szentpétervári székhelyű Internetkutató Ügynökség (Agentstvo Internet Issledovaniya) nevű „trollgyár" is. Az orosz–ukrán konfliktus 2022. február 24-ig terjedő szakaszában – a hibrid hadviselés elveinek megfelelően – a technika kiberképességek mellett a kognitív módszerek is jelentős szerepet kaptak az orosz érdekek érvényesítésében. A hagyományos média (Sputnik, Russia Today) mellett az online médiát és a közösségi hálót is nagy hatékonysággal használták a célzott üzenetek továbbítására. A 2022. február 24-én kitört orosz–ukrán forró háborúban

pedig azt láthatjuk, hogy a pszichológiai műveleteket mindkét fél egyaránt nagy intenzitással alkalmazza mind a saját lakosság meggyőzésére, támogatásának elnyerésére és fenntartására, mind pedig a nemzetközi közvélemény befolyásolására. Az ukrán elnök szinte naponta szólítja meg a nemzetközi közvéleményt, illetve az egyes országokat, hogy támogassák Ukrajnát a háborúban, és hozzanak még szigorúbb intézkedéseket Oroszországgal szemben. Az ukrán lélektani műveletek részét képezik és az Oroszország elleni fellépés fokozását célozzák azok az internetes portálokon és a közösségi médiában terjesztett képek, videók is, amelyek például a bucsai civilek megölését mutatják be, és amit Oroszország tagad és provokációnak tart. Az orosz vezetés pedig az információs kontrollt alkalmazza, amikor korlátozza a Facebook vagy a Twitter elérését az orosz lakosság számára, illetve a hírcsatornákon a „különleges katonai művelet" jogosságát hirdeti, amivel a lakosság és az egész társadalom támogatását akarja elérni. 2022. március 31-én egy közösségimédia-csúcstalálkozón a szakértők megállapították, hogy Oroszország, aki eddig élen járt a kibertéri befolyásolásban, a háborúban hátrányos helyzetbe került Ukrajnával szemben e téren. Az ukrán tisztviselők és civilek aktívan használják a közösségi hálózatot a közvélemény megnyerésére és a támogatások megszerzésére. Volodimir Zelenszkij elnök pedig hatékonyan alkalmazza a hagyományos, a közösségi és a titkosított médiát egyaránt az információk terjesztésére. A Telegram erre különösen jó platform, amelyet az ukránok sikeresen használnak a tartalom terjesztésére és a hasonló gondolkodású közönséggel való kapcsolatteremtésre szerte a világon. A videó különösen fontossá vált a háború eseményeinek bemutatásában. Szinte minden platformon elérhetővé váltak a videókkal támogatott közösségimédia-tartalmak, amelyeknek igen erős a befolyásoló hatásuk. Ukrajna például számos videót mutat be Zelenszkij elnökről, amint a lebombázott és feldúlt városokban tájékozódik, ezzel is hangsúlyozva vezetői képességét és hajlandóságát a harc folytatására. Ezzel szemben Oroszország például Vlagyimir Putyin elnök beszédeit sugározza, vagy olyan felvételeket mutat be, amelyeken Putyin az íróasztalánál ül. Ezek azonban ma már nem elég hatékonyak szemben a rövid idejű, gyorsan közzé tehető videótartalmakkal. Megjegyzendő ugyanakkor, hogy a kibertéri PSYOPS-célú kognitív befolyásolás igen gyakran nem a valós tényeken alapul, ezért e tevékenység átcsúszik a kognitív megtévesztés területére, így pedig a klasszikus NATO-értelmezés szerinti lélektani műveletek és a megtévesztés közötti határ egyre inkább elmosódik. A tapasztalatok azt mutatják, hogy a kibertéri PSYOPS gyakran nagyobb erőbefektetést igényel, azonban ugyanakkora vagy még nagyobb hatást hamis információk terjesztésével, álhírekkel is el lehet érni. Ez esetben az eredmény ugyanaz, csak a megvalósítás módja különbözik.

A kognitív megtévesztés napjaink egyik gyakran alkalmazott kibertéri manipulációs technikája. A NATO értelmezésében a megtévesztés „olyan szándékos tevékenységeket jelent, amelyek a megcélzott döntéshozók félrevezetésére irányulnak annak érdekében, hogy azok a parancsnok céljai szempontjából előnyös módon cselekedjenek". A kibertérben a megtévesztés megvalósítható technikai módszerekkel (mint például a spoofing vagy közbeékelődéses támadás), illetve kognitív információs tevékenységekkel, és alkalmazható hálózatok támadására, védelmére vagy a felhasználók kognitív befolyásolására egyaránt. A kibertérben folytatott kognitív megtévesztés egyik hatásos technikája a social engineering, amely az emberi hiszékenységet aknázza ki. A social engineering tulajdonképpen olyan lélektani manipuláció, amely az emberek bizalomra való hajlamát használja ki a számítógép-hálózatokba való bejutáshoz. E tevékenység keretében a felhasználóktól a hálózat gyenge pontjaira vonatkozó érzékeny adatokat, jelszavakat szereznek meg manipulációval, megtévesztéssel, esetleg zsarolás útján. Ezzel a módszerrel könnyedén megkerülhetők a különféle biztonsági megoldások, mint például tűzfalak vagy behatolásdetektáló rendszerek, így csak kisebb erőbefektetés szükséges a hálózat technikai jellegű támadásához. A másik elterjedt kognitív befolyásolási technika az álhírek terjesztése. Az álhírek olyan szándékosan közzétett és valós hírként interpretált valótlan információk, amelyek célja, hogy félrevezessék a célközönséget. Létrehozásukat és terjesztésüket elsősorban gazdasági haszonszerzés és politikai befolyásolás generálja, de jelentős a katonai célokra való felhasználásuk is. Az álhírek terjesztése nem új keletű, azonban az internet és a közösségi média különösen jó táptalajt biztosít a hamis információk nagy tömegekhez való gyors eljuttatásához. A kibertéri hálózatos technológiák e tekintetben kiemelten fontos szerepet játszanak, mivel azok sajátosságai jelentősen növelik az emberek félreinformálásának hatékonyságát. A szenzációhajhász, „nagy érdeklődést kiváltó" információk mielőbbi megosztásának lehetősége hozzájárul az álhírek rohamos terjedéséhez, aminek köszönhetően az emberek manipulációs lehetőségei mára új színteret kaptak. A közösségi médiában megvalósított álhírterjesztéshez három fontos összetevő szükséges. Ezek az az alábbiak:

- az online eszközök, szolgáltatások és a humán erőforrás, akik, és amelyek lehetnek trollok, követők, lájkolók, automaták, esetleg álhírterjesztő botnethálózatok
- a közösségi hálózatok mint a terjesztés médiumai, valamint
- a motiváció, amely alapvetően gazdasági, politikai és katonai jellegű lehet.

A legjelentősebb hatásokat a szakszerűen összeállított, nagy számban generált, és terjesztett politikai és katonai célú álhírek okozzák, amelyeket szervezetten, különféle csoportok vagy úgynevezett „álhírgyárak" hoznak létre. Oroszország számos alkalommal használt álhírgyárak által előállított és terjesztett hamis

információkat. A legismertebb álhírgyár a korábban említett Internetkutató Ügynökség, amely fizetett rollokat alkalmaz arra, hogy a közösségi médiában az orosz kormány számára kedvező álhírkampányt folytasson. Az ügynökség a 2016-os amerikai elnökválasztásba való beavatkozás mellett részt vett többek között a szíriai konfliktus során alkalmazott befolyásolási és manipulációs kampányban is. A kibertéri megtévesztés a 2014-óta tartó ukrajnai konfliktusban is jelentős szerepet játszik mindkét fél oldalán. Egy kutatás például igazolta, hogy 2014-től a Twitteren jelentősen megnőtt az Ukrajnával foglalkozó bejegyzések száma. Ezeket a befolyásoló, manipuláló üzeneteket és nagyon gyakran álhíreket döntően szintén a szentpétervári trollgyár állította elő. 2014. július 18-án, a malajziai repülőgép lezuhanásának napján például több mint 44 ezer, a következő napon pedig több mint 25 ezer üzenetet tettek közzé. Ezekben 297 fiók terjesztett olyan információkat, amelyek szerint Ukrajna volt a felelős a maláj gép lelövéséért. A 2022. február 24-e óta tartó orosz–ukrán háborúban a kibertéri megtévesztés mindkét fél részéről rendkívüli méreteket ölt. Mindezeket pedig kiegészítik a háborúban közvetlenül nem részt vevő, de valamelyik oldal felé elkötelezettek által kreált különféle álhírek, hamisított videók, amelyek a háborús felek és a semleges közvélemény megtévesztését célozzák. A közösségi médiában, internetes portálokon rendre nagy számban jelennek meg olyan hírek, információk, amelyek valódiságtartalma erősen megkérdőjelezhető. Az egyik ilyen, elsősorban videótartalmak közzétételére szolgáló platform a fiatalok körében rendkívül népszerű TikTok kínai videómegosztó közösségi hálózati szolgáltatás. A Meta – a Facebook és az Instagram anyavállalatának – jelentése a közösségi média dezinformációinak megugrását jelezte, beleértve az Oroszország ukrajnai inváziójához kapcsolódó tartalmak növekedését is. A jelentés szerint a Kremlhez köthető csoportok dezinformációkat terjesztenek az ukrajnai inváziról, miközben odahaza felerősítik az oroszbarát összeesküvés-elméleteket. A Meta például több tucat ukrán parancsnok közösségimédia-fiókjának feltörését detektálta és akadályozta meg, amelyeken megpróbáltak videókat feltölteni legyőzött és magukat megadó ukrán katonákról. A támadást egy Ghostwriter néven ismert hacker-szervezetre vezették vissza, amelyet korábban Oroszország szövetségesével, Fehéroroszországgal hoztak kapcsolatba. A videótartalmak mind ez idáig bizonyító erejűnek számítottak, azonban a deepfake megjelenésével már e felvételek sem mindig a valóságot mutatják, A deepfake egy mélytanuláson és hamisításon alapuló szintetikus médiatechnika, amely esetében egy képen vagy videón lévő személyt meggyőzően manipulálnak annak érdekében, hogy elhitessék, olyasmit csinál vagy mond, amit valójában nem tett vagy mondott. A deepfake-technikát mindkét fél alkalmazza. Putyinról például manipulált videót osztottak meg a Twitteren, amelyen az látszik, hogy arra buzdítja az orosz katonákat, hogy tegyék le a fegyvert, és térjenek haza. A Deutsche Welle oroszországi szolgáltatása azon-

ban leleplezte a manipulációt. Egy Zelenszkijt ábrázoló manipulált videó pedig márciusban terjedt el a közösségi médiában, amelyen láthatóan az ukrán vezető azt mondja katonáinak, hogy tegyék le a fegyvert, és adják meg magukat Oroszországnak. Üzenetét az Ukraine 24 műsorszolgáltató honlapján is közzétették, de a hírügynökség nem sokkal ezután közleményt tett közzé, miszerint az oldalt feltörték, a hamisított videót pedig eltávolították. A civil-katonai együttműködés (CIMIC) napjainkban a megváltozott műveleti környezetben kiemelt fontosságúvá vált, ugyanis a katonai feladatok végrehajtása gyakran a lakossággal és a közigazgatási szervekkel való együttműködésben valósul meg. A műveletekben részt vevő katonai erők és a civil szervek közti kapcsolatok kialakítása a CIMIC feladata, amely esetben a kibertér szintén jelentős hatékonyságnövelő színtér lehet. A NATO vonatkozó doktrína szerint a CIMIC „a NATO parancsnokok és a civil szereplők, köztük a nemzeti lakosság és a helyi hatóságok, valamint a nemzetközi, nemzeti és nem kormányzati szervezetek és ügynökségek közötti koordináció és együttműködés a műveletek támogatása érdekében". A CIMIC során a kapcsolatteremtés, -építés és együttműködés elsősorban a személyes kapcsolatok kialakításával valósulhat meg. Megfelelő hálózatos infrastruktúrával rendelkező műveleti területen azonban a kibertéri hálózatos technológiák, mint a mobil kommunikáció, az e-mail és az elektronikus online médiaszolgáltatások (weboldalak, közösségi média) jelentősen lerövidíthetik és hatékonyabbá tehetik a kapcsolat kialakítását. A kibertéri CIMIC során tehát a fizikai és a logikai rétegben alkalmazhatunk különféle eszközöket és módszereket, a hatásuk pedig a kiberszemélyiség-rétegben érvényesül.

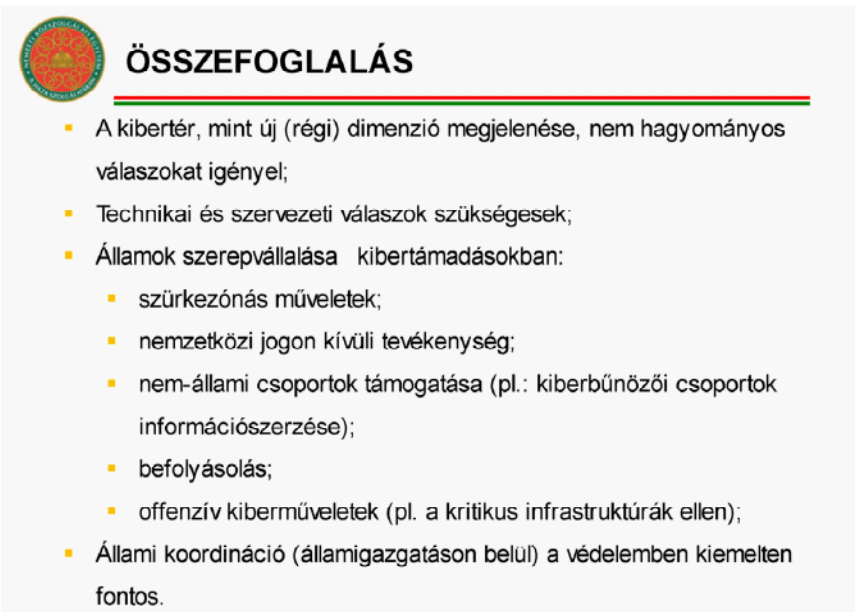
A kognitív műveleti biztonság szintén fontos szerepet játszik a kibertéri kognitív információs műveletekben. A NATO információs műveletek doktrína szerint: „A műveleti biztonság (OPSEC) egy folyamat, amely passzív vagy aktív eszközökkel és módszerekkel megfelelő szintű biztonságot nyújt a katonai művelet vagy gyakorlat számára azáltal, hogy megakadályozza, hogy az ellenség tudomást szerezzen a saját erők elhelyezkedéséről, képességeiről vagy szándékairól." Az információs műveleti képességek közül a műveleti biztonságnak a kibertérben – a megtévesztéshez hasonlóan – van technikai és kognitív értelmezése is. A műveleti biztonság technikai módszerei a fizikai és a logikai rétegben alkalmazott fizikai biztonság és elektronikus információbiztonság rendszabályaiban értelmezhetők. A kibertéri kognitív műveleti biztonság képességei elsősorban a felhasználók képzésére, felkészítésére és biztonságtudatosságának fejlesztésére fókuszálnak. A felhasználók biztonságtudatossági felkészítése elsősorban a hálózat különféle szolgáltatásaihoz való hozzáférési szabályok betartására, a jelszókezelésre, illetve az alapvető vírusvédelmi megoldásokra irányul. A kognitív műveleti biztonság alkalmazását és hatását tekintve is a kiberszemélyiség-rétegben jelenik meg.

A kibertéri műveletek lényege az információs műveletekhez hasonlóan a különböző információs tevékenységek összehangolásában és integrálásában rejlik. Ennek köszönhetően a kibertéri kognitív információs tevékenységek szoros kapcsolatban állnak egymással, gyakran pedig a határok is elmosódnak köztük, lásd a kibertéri kognitív megtévesztés és PSYOPS viszonyát. Ennek során mindegyik kognitív tevékenység a kiberteret, vagyis az internetet és benne a közösségi médiát használja fel. Az egyes tevékenységek egymástól elkülönülten értelmezhetők, és a végrehajtás során a kibertérnek akár mindhárom rétegét felhasználhatják. Ugyanakkor a hatások mindegyik esetben a kibertér kiberszemélyiség-rétegében érvényesülnek, és ezen keresztül a célközönség kognitív képességeit, tudatát, gondolkodását, viselkedését befolyásolják. Az információs műveletek analógiájának mentén tehát a kibertéri kognitív képességek egymással és a kibertéri technikai képességekkel való összehangolt tervezése és végrehajtása jelentősen növeli az egyes tevékenységek egymásra gyakorolt hatását és azok eredményességét.

Összegzés, következtetések

Napjainkra a hálózatos technológiáknak és a közösségi hálózatoknak köszönhetően a kibertér újszerű értelmezést nyert. E tér ma már nem csupán virtuális, logikai tartományként értelmezhető, hanem amellett a fizikai és a kognitív tartomány is fontos részét képezi. Ebben a tartományban az információs műveletekkel szoros kapcsolódást mutató, annak részét képező kibertéri műveletek zajlanak. Az információs műveletekkel analóg módon, a kibertéri műveletekben is az integrált, egymás hatásait kihasználó technikai és kognitív információs tevékenységeket alkalmazzuk, de nem a teljes információs környezetben, hanem annak csak a hálózatokkal jellemezhető tartományában, vagyis a kibertérben. Az információs műveletekben kiemelt fontosságú a célközönség kognitív befolyásolása, a kibertéri műveletekben pedig ma ez a tevékenység szintén jelentősen felértékelődik. Ahol megvan az infrastrukturális feltétele, és a célközönség aktívan használja a hálózatos infokommunikációs technológiát, vagyis a kiberteret, ott a kibertéri kognitív befolyásolás és manipuláció jelentős erősokszorzó képességet jelenthet. A kibertéri kognitív tevékenységek szorosan kötődnek az információs műveletek kognitív képességeihez, céljukat tekintve megegyeznek azokkal, ugyanakkor a hatások eléréséhez a kibertéri műveletekben az internetet és benne a közösségi médiát használják. Alapvető céljuk a befolyásolás és a manipuláció, amely megvalósulhat hiteles és valós információkkal, valamint manipulált üzenetekkel, álhírekkel. A kibertéri befolyásolásra ennek megfelelően elsősorban az információs műveletek kognitív tevékenységeit, vagyis a PSYOPS-ot és a kognitív megtévesztést használják, emellett pedig alkalmazható még a CIMIC és a kognitív műveleti biztonság is. Az internet és a közösségi

hálózat nagy előnye, hogy e médiumokat felhasználva sokkal eredményesebben lehet megvalósítani a kognitív befolyásolást és manipulációt. Minderre jó példa az álhírek terjedése, az elmúlt évek néhány nagy nyilvánosságot kapó eseményei, mint például az amerikai elnökválasztási kampányba való beavatkozás, valamint az ukrajnai háborúban mindkét fél részéről megfigyelhető kibertéri befolyásolás és manipuláció.



Összességében megállapíthatjuk, hogy a hálózatos technológiák evolúciójából, az információs műveletek fejlődéséből, illetve a kibertér és a kibertéri tevékenységek elemzéséből levonható következtetések, valamint az elmúlt évek megtörtént és a jelenleg is zajló háború kibertéri eseményei alapján igazolható, hogy:

- a kibertér meghatározása és struktúrája új értelmezést nyert, a virtuális logikai réteg mellett a fizikai és kiberszemélyiség-réteg is fontos tartományaiként jelennek meg;
- a kibertéri kognitív információs tevékenységek a kibertér mindhárom rétegében megvalósulhatnak, hatásaik azonban minden esetben a kiberszemélyiség-rétegben érvényesülnek;

- a kibertérben a megszokott technikai információs tevékenységek, mint például a számítógép-hálózatok támadása és védelme mellett a kognitív képességeknek is egyre növekvő jelentőségük van;
- a kibertéri kognitív tevékenységek egymással, illetve kibertéri technikai képességekkel való összehangolásának jelentős hatása van.

Mindez azt jelenti, hogy a NATO és a nemzeti haderő fejlesztése során előtérbe kerülő kibertéri képességek kialakításakor nemcsak a kiberelrettentés és a kibervédelem területe kell hogy fókuszba kerüljön, hanem törekedni kell a kognitív kiberképességek megteremtésére is. Ehhez pedig megfelelő szervezeti struktúrára és a társadalmi befolyásolásban jártas és a hálózatos infokommunikációs technológiát jól alkalmazó, képzett szakemberekre van szükség.

Felhasznált irodalom

Baig, Rachel: Fact Check: The Deepfakes in the Disinformation War between Russia and Ukraine. DW, 2022. március 18. Online: www.dw.com/en/fact-check-the-deepfakes-in-the-disinformation-war-between-russia-and-ukraine/a-61166433

Brown, Sara: In Russia–Ukraine War, Social Media Stokes Ingenuity, Disinformation. MIT Sloan, 2022. április 6. Online: https://mitsloan.mit.edu/ideas-made-to-matter/russia-ukraine-war-social-media-stokes-ingenuity-disinformation

Charap, Samuel – Elina Treyger – Edward Geist: Understanding Russia's Intervention in Syria. Research Report. RAND Corporation, 2019. Online: www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3180/RAND_RR3180.pdf

Gu, Lion – Vladimir Kropotov – Fyodor Yarochkin: The Fake News Machine. How Propagandists Abuse the Internet and Manipulate the Public. A TrendLabs Research Paper, 2017. Online: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf

Haig Zsolt: Információs műveletek a kibertérben. Budapest, Dialóg Campus, 2018.

Haig Zsolt: Novel Interpretation of Information Operations in Today's Changed Operational Environment. Scientific Bulletin, 25. (2020), 2. 93–102. Online: https://doi.org/10.2478/bsaft-2020-0013

Inglis, C: Cyberspace – Making Some Sense of It All. Journal of Information Warfare,15. (2016), 2. 17–26. Online: www.jstor.org/stable/26487528?seq=1Joint Chiefs of Staff: JP 3-12Cyberspace Operations (2018. június 8.). Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Kelman, Herbert C.: Compliance, Identification, and Internalization: Three Processes of Attitude Change. Journal of Conflict Resolution, 2. (1958), 1. 51–60. Online: https://doi.org/10.1177/002200275800200106

Kovács László – Krasznay Csaba: Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. Nemzet és Biztonság,10. (2017), 3. 3–15. Online: https://doi.org/10.32576/nb.2017.3.1

Ministry of Defence: AJ P-3 .10.1Allied Joint Doctrine for Psychological Operations. Edition B Version 1, NATO Standardization Office, 2014. Online: https://bit.ly/3Bva39r

Nadelnyuk, Oleksandr: How Russian "Troll Factory" Tried to Effect on Ukraine's Agenda. Analysis of 755 000 Tweets. VoxUkraine, (é. n.). Online: https://voxukraine.org//longreads/twitter-database/index-en.html

NATO: AJ P-3 .10Allied Joint Doctrine for Information Operations. Edition A Version 1, NATO Standardization Office, (2015).

NATO: AJP-3.20 Allied Joint Doctrine for Cyberspace Operations. Edition A Version 1, NATO Standardization Office, (2020. január). Online: https://bit.ly/3B5YCDu

NATO: AJ P-3 .10. 2Allied Joint Doctrine for Operations Security and Deception. Edition A Version 2,

NATO Standardization Office, (2020. március). Online: https://bit.ly/3QEdVt6

Paul, Kari: Russian Disinformation Surged on Social Media After Invasion of Ukraine, Meta Reports. The Guardian, 2022. április 7. Online: www.theguardian.com/world/2022/apr/07/propaganda-social-media-surge-invasion-ukraine-meta-reports

Rózsa Tibor: Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a Magyar Honvédség feladatrendszerében. Doktori (PhD) értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2016. Online: https://doi.org/10.17625/NKE.2017.04

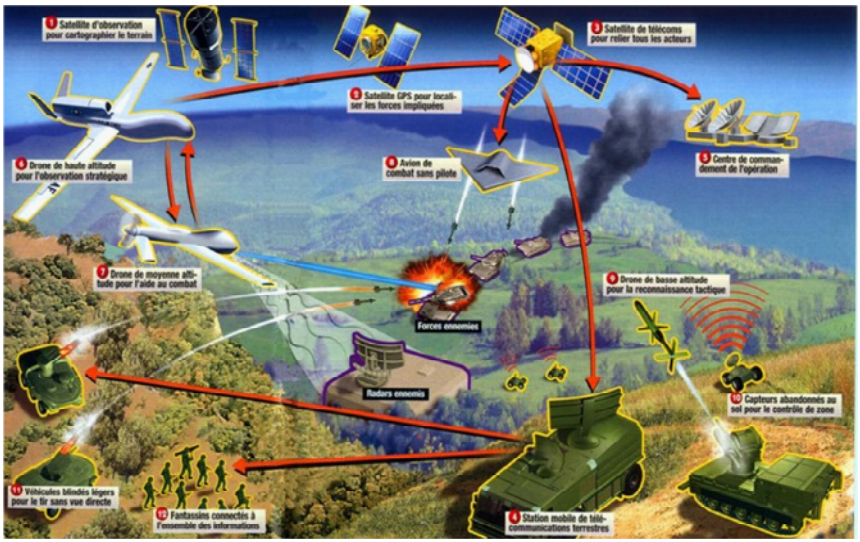
Svetoka, Sanda: Social Media as a Tool of Hybrid Warfare. Riga, NATO Strategic Communications Centre of Excellence, 2016. Online: www.stratcomcoe.org/social-media-tool-hybrid-warfare

A digitális hadszíntér

Prof. Dr. Rajnai Zoltán, egyetemi tanár, dékán
Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
rajnai.zoltan@bgk.uni-obuda.hu

A tábori alaphírhálózat a csapatvezetés érdekében telepített, stratégiai fontosságú híradó infrastruktúrát biztosít a szárazföldi csapatok vezetés érdekében a Szárazföldi Vezérkar (gépesített hadtest) és alárendeltjei részére. Ez a hálózat biztosítja a vezetés igényeinek megfelelően – *képességei szerint* – az összeköttetést a gépesített hadosztályokkal, a közvetlenekkel és az összfegyvernemi tartalékkal. A hálózat minősített esetekben legfeljebb nyolc alaphírközponttal mintegy 18-30.000 km2 lefedésére, híradó infrastruktúra biztosítására képes. Ez az alaphírközpont-sűrűség a korszerű hálózatok mértéket – *amely a NATO tagországok hadseregeiben ennek közel háromszorosa* - meg sem közelíti, manőverező képessége, a helyzetek gyors és éles változásához történő alkalmazkodása alacsony szintű. Telepítéséhez szükséges idő hosszú, melyet a kábeles viszonylatok építési, bontási és újratelepítési ideje még tovább növel, tartalékai nincsenek, csak abban az esetben, ha az alaphírközpontok közül nem települ mindegyik. Ez esetben a manőverező képesség ugyan javul, könnyebben telepíthetők újabb alaphírközpontok, de ez az amúgy is gyenge hálózatsűrűséget tovább rontja. Kifejezetten hátránya a hálózatnak, hogy csak a gépesített had-test részére biztosít összeköttetést a hadosztályok, valamint a hadtest közvetlen egységekkel, ám azok szervezettszerű erőikkel saját hírrendszerüket is telepítik és biztosítják a híradó infrastruktúrát a vezetés részére. A tábori alaphírhálózat tehát csak a gépesített hadtest szintjén létezik, a hadosztályoknál csak a vezetési pont hírközpontokhoz csatlakozhatnak az alárendeltek. Így az alaphírközpontok, vagy vezetési pontok valamelyikének kiesése esetén az összeköttetések helyreállítása, szükség szerinti átterhelése más vezetési pontra, vagy kerülőirány létesítése a hálózaton jelentős időt vesz igénybe. Ez alatt az idő alatt a csatlakozó vezetési pontok csak egycsatornás rádióeszközökkel tarthatnak összeköttetést az elöljáróval, ami a hadműveleti vezetés szintjén nem elegendő. Az alaphírközpontokat alkotó híradó technikai eszközök hagyományos, analóg rendszerűek, távbeszélő központjaik kézi kapcsolásúak, melyek szolgáltatásokkal nem rendelkeznek.

Az alaphírközpontokban nagyon magas a kapcsolások száma, a távbeszélő központok terheltsége igen magas. A tervezett géptávíró összeköttetések létesítése bonyolult, adatátviteli sebességük alacsony. A hálózat csatornakapacitása kicsi, manőverezési lehetőségei gyengék, ennek megtervezése a hadműveletek során hosszas és precíz tervezőmunkát, magas szakmai ismeretet igényel.



A csatlakozó vezetési pontok száma a hálózat képességeihez viszonyítva magas, a viszonylatok kiszolgálása jelentős humán erőforrást igényel; a technikai eszközök kezelése bonyolult, a kiképzéshez szükséges idő aránytalanul magas. Figyelembe véve, hogy a sorkatonai szolgálat ideje fokozatosan csökken, az állomány felkészítése még a kiképző központokban is nagy nehézséget okoz, és a felkészítés eredményessége jelentős mértékben függ a sorállomány szakképzettségétől, iskolai végzettségétől.

A tábori alaphírhálózat elemei technikailag és erkölcsileg elavultak, jelentős részük az 1960-70-es – vagy azt megelőző – évek színvonalán álló, nagy részük elektroncsöves technológiájú, melyek már nem képesek a kor színvonalán álló távközlési eszközök szolgáltatásaival felvenni a versenyt. Fenntartási költségük nagyon magas, zömük a volt Szovjetunióból származik, vagy licenc alapján, hazai bázison gyártott eszközök, ipari felújításuk évek óta elmarad a gyártó vállalatok megszűnése miatt. A szükséges javító anyagok beszerzése nehézkes, egyes berendezésekhez már lehetetlen. Az alaphírhálózat által biztosított híradó infrastruktúra nem ad lehetőséget az informatikai eszközök végződtetésére, tehát multimédiás funkciók betöltésére informatikai eszközökkel nem képes, csak a hagyományos értelemben vett hírközlésre (beszéd, fax, géptávíró) alkalmazható.

Humán erőforrás tekintetében szintén rossz az arány a NATO hírrendszereket üzemeltető egységekkel szemben, mert amíg az alaphírhálózat központjaiban 15-18 híradó állomás és – a logisztikai kiszolgáló állománnyal együtt – átlagosan 200 fő biztosít egy-egy alaphírközpontot, addig a NATO harcászati rendszerek

hírközpontjaiban 3-5 híradó állomást és 10-30 főt találhatunk. Nagy problémát okoz, hogy a tábori alaphírhálózat rádiós csatlakozási felülettel nem rendelkezik, rádióállomások illesztését nem teszi lehetővé, így mobil harccsoportok, harcászati kötelékek, hadrendi elemek alkalmazása esetén azok közvetlen vezetésére csak hálózaton kívüli rádióállomások vehetők igénybe. Ez azt is jelenti, hogy a tábori alaphírhálózat létrehozása mellett egy másik rendszer létesítésére is szükség van, mely közvetlen összeköttetések formájában biztosít információcsere lehetőséget az alárendelt katonai szervezetekkel, vagy alegységekkel a hálózatot létesítő híradó eszközökön kívül, így a hadműveleti vezetéshez szükséges híradó típusgépjárművek száma tovább nő, ami a híradás létesítését végrehajtó állomány létszámát is tovább növeli. A stacioner távközlő hálózatokhoz történő csatlakozás technikai lehetőségei az 1992-ben megalkotott távközlési törvényt követő távközlés-politikai intézkedések hatására fokozatosan tovább romlottak.

Az új hálózat kialakításának célja egy digitális alapú, integrált szolgáltatásokat biztosító egységes kommunikációs rendszer létrehozása, mely tábori körülmények között is képes azonos vezetési feltételeket biztosítani a csapatvezetésben résztvevők számára, hasonlóan a béke elhelyezési körletekhez. E rendszernek már illeszkednie kell az országos távközlő hálózatokhoz, az egyes zártcélú és különcélú rendszerekhez éppúgy, mint a NATO állandó jellegű integrált híradó rendszeréhez (NATO ICS), a Magyar Honvédség állandó jellegű hálózataihoz, és más tagországok harcászati kommunikációs hálózataihoz egyaránt. E célokból kiindulva tehát egy olyan rendszer kialakítása szükséges, mely széleskörűen megfelel a nemzetközi polgári szabványoknak és a NATO STANAG-ekben foglaltaknak egyaránt. Az új hálózat elemzését a rendszerstruktúrából kiindulva célszerű megkezdeni. Ez a rendszer mindenképpen a NATO tagországok haderejében már alkalmazott rácsrendszerű, területlefedő hálózatot kell, hogy jelentsen, mely a hadműveleti területen a szükséges rácspont sűrűséggel biztosítja a hadműveleti vezetés és a harcászati alegységek részére egyaránt a kommunikációs feltételeket.

Manapság egyre több szó esik azokról a mobil rádiórendszerekről, melyek különböző készenléti szervezetek, például rendőrség, tűzoltóság vagy akár a kormányzati szervek munkáját segítik. Ezek a rendszerek önálló infrastruktúrát igényelnek, melyek kiépítése felülmúlhatja a GSM rendszer kiépítési költségeit is. Felmerült a gondolat, hogy a különböző felhasználók ne több, párhuzamos hálózat kiépítésével alkossanak önálló hálózatokat, hanem az ún. virtuális há-

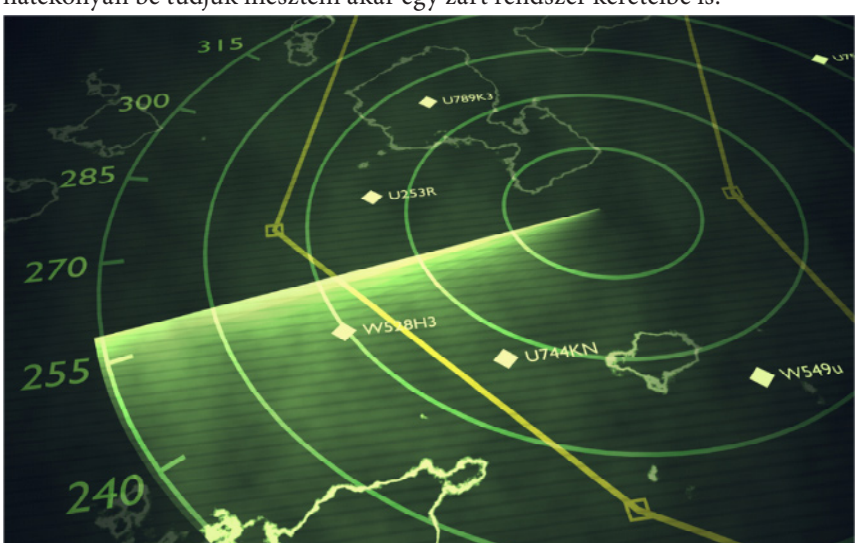
lózat koncepciót figyelembe véve egyazon hálózaton belül, de egymástól mégis elválasztva dolgozzanak. Több szervezet használhat együttesen egy közös hálózatot, annak ellenére, hogy funkcióhalmazuk és rendszerfelépítésük egészen eltérő. Követelmény viszont, hogy külön-külön minden egyes szervezetnek teljes mértékben, kézben kell tartania rendszere hozzá tartozó részét. Ezen elv alapján állították fel a virtuális hálózat koncepcióját.

Felismerve a zárt célú hálózatok piacán lévő lehetőségeket, a GSM rendszer szolgáltatói, készülék gyártói igen figyelemre méltó fejlesztésekkel rukkoltak elő a közelmúltban. A jelenlevők számára talán nem ismeretlen az a fogalom, hogy GSM PRO. Ez a GSM rendszer kiterjesztése, oly módon, hogy egy külön szerver elérésével biztosítható a PMR (különcélú hálózat) néhány kulcsfontosságú szolgáltatása. A különböző speciális hívásfajták mellett meg-jelenik a vészhívás funkciója, amelyet ugyanúgy a diszpécser tud lekezelni.

A csoporthívás vonatkozásában a GSM PRO szerveren keresztül biztosítható a csoport tagjainak összekötése egymással. Megfontolandó azonban az alkalmazás a hívás-felépítési idő vonatkozásában, hiszen a GSM PRO rendszerű készülékek messze nem képesek a 0,3 sec-os szint biztosítására. Ugyancsak a PMR rendszer javára billenti a mérleget a közvetlen kapcsolat lehetősége a végkészülékek között. Ez akkor hasznos, ha a felhasználók az infrastruktúra lefedettségén túl kénytelenek használni a rendszert, illetve, ha direkt ez a célja kommunikációban. Az adatátvitel vonatkozásában viszont előrehaladás várható, ha a GSM rendszer fejlődését tekintjük. A modulációs mód változtatásával és több időrés összevonásával túlszárnyalható a jelenlegi 28,8 kbps jelsebességű adatátvitel, amely például a TETRA rendszer sajátja. A zárt célú hálózatok fejlődési lehetőségei nehezebben körvonalazhatóak, mint a cellás mobil rendszereké, (amikhez általában viszonyítani szokták). A mobil telefónia sikere és jövőbeli kilátásai, fejlesztése magával hozzák azokat az előrelépési lehetőségeket, amelyek alapján megpróbálom prognosztizálni a PMR jövőjét, legalábbis egy ígéretes újdonsághoz kapcsolva. Kezdetnek itt van mindjárt a W@P. A Wireless Application Protokoll megalkotása a WAP Fórum nevezetű formáció produktuma, és fő célként egy globális protokoll specifikáció kidolgozását irányozták elő, amely az összes vezeték nélküli rendszeren használható. Maga a protokoll az Internet és egyéb adatállományok letöltését biztosítja. Eddigi fogalmaink szerint az Internetes állományok meg-tekintéséhez és letöltéséhez PC-re van szükségünk, különösen a grafikus állományok (forgó GIF emblémák stb.) esetében.

Nyilvánvaló, hogy egy mobil egységgel egy komplett HTML oldal nehézkesen értelmezhető, ezért a WAP Fórum egy új programnyelvet alkotott meg, a WML-t (Wireless Markup Language), amely hasonló a HTML nyelvhez, de attól egyszerűbb. A mobil készülék egy mikroböngészőt tartalmaz, amely alkalmazkodik a készülék fizikai valójához: kijelző mérete, kis memóriaméret, energiafelhasználás. A WAP hozzáférés segítségével ugyanúgy lehet böngészni az Interneten, csupán a tartalom az, ami egyszerűbb. Elképzelhető azonban, hogy a fejlődés ezt a kis apróságot is leküzdi és feltűnnek az utcán bóklászó Internet szörfö-zők. Jelenleg viszont meg kell elégedni a WML 1.3-as verziójú „szövegszerkesztőjével". Ha belegondolunk a zárt célú hálózatok rendeltetésébe, ellentmondást érezhetünk a nyílt Internet hozzáférés előretörése és maga a hálózat funkciója között.

Zárt célú hálózatot azért hozunk létre, hogy kizárjuk az illetékteleneket a háló forgalmazásából, akkor hogy jön ide az Internet, kérdezhetjük. Az ellentmondás feloldható annak ismeretében, hogy a mindent behálózó Internet jóval túllépett a kiváltságosok hobbijának lenni, naponta több ezer új WEB site jelenik meg (igaz tiszavirágszerűen meg is szűnik). Az információtartalom hozzáférhetősége nem szükségszerűen kell, hogy kétirányú legyen, gondoljunk csak a különböző titkosítási algoritmusok elterjedtségére. Mód és lehetőség van saját hálózatunk információit megvédeni illetéktelenek elől, de ugyanakkor szabadon „böngészhetünk" a WAP szerver nyújtotta lehetőségeken belül. Véleményem szerint nem szabad rögtön elvetni egy új ötletet, csak azért, mert nem illeszkedik körülhatárolt világunkba, sokkal inkább fel kell ismerni a lehetőséget, hogy hatékonyan be tudjuk illeszteni akár egy zárt rendszer kereteibe is.



Napjainkban a csapatok törzseiben, egységeiben, alegységeiben tevékenykedők, a feladatok kidolgozásában és végrehajtásában közreműködők munkájuk során különböző irodai alkalmazású kommunikációs eszközöket (számítógépek, híradó berendezések), rendszereket (LAN, strukturált hálózatok, stb.) használnak. Ezen törzsek, parancsnokok jogos elvárása, hogy hadműveleti feladatok előkészítése, kidolgozása és végrehajtása során a hadműveleti területen is képesek legyenek hasonló, esetenként még több szolgáltatás és adatbázis igénybevételére, mint béke elhelyezési körleteikben, helyőrségeikben. Mint ahogy egy vállalatnál a számítógépes és kommunikációs hálózat, az Internethez történő hozzáférés és alkalmazás, vagy az IP alapú telefónia biztosítja a feltételeket az információk megszerzésére, tárolására és továbbítására a felhasználók felé, úgy azonosítható ezzel egy laktanya, vagy helyőrség információs rendszere is. Kimondhatjuk tehát, hogy egy (polgári) vállalati rendszer és egy katonai rendszer között jelentős eltérés csak a rendszerek speciális, hierarhizált tulajdonságaiban van. Maga a rendszer, annak felépítése, üzemeltetése, eszközrendszere megegyezik. Ebből következően megállapítható, hogy a honvédség által alkalmazott hálózatok struktúrája, szolgáltatásai hasonlóak egy vállalati rendszerhez, amit hadműveleti területen éppúgy alkalmazni kívánnak a felhasználók, mint standard körülmények között. De vajon képesek vagyunk-e biztosítani mindezeket hadműveleti területen és alkalmazás közben? Erre kell keresni a megoldásokat és a lehetőségeket.

Az ATM alapú hálózat alkalmazásának szükségessége Az elektronikai technológia, a távközlési- és informatikai eszközök és rendszerek robbanásszerű fejlődése következtében a NATO tagállamokban megkezdődött a PCM alapú rendszerek leváltása egy korszerűbb, nagyobb adatátviteli sebességet biztosító tábori digitális hálózatokra A hadműveleti és harcászati vezetés szintjén a multimédiás szolgáltatások kiemelt szerepet kapnak, ahol a hang- és adatátvitel mellett a videokonferencia szolgáltatások nagyfokú igénybevétele történik. Ehhez azonban már csak elégséges feltétel lesz a PCM alapú tábori hálózat, ahol elsősorban a

polgári kivitelű CB telefonok, militarizált LB telefonok és a G3 szabványtípus követelményeit kielégítő FAX berendezések találhatók a végberendezések szintjén, míg ISDN szolgáltatásokra alkalmas adapter csatlakoztatása esetén a kapcsolóközpontokhoz illesztett multimédiás számítógépek és videokonferencia terminálok biztosíthatnak szolgáltatásokat. A hadműveleti-harcászati vezetés azonban az információkat reál- (valós) időben kívánja feldolgozni és felhasználni, ezért azt nagy átvitelt nagysebességű hálózaton kell továbbítani magas szintű szolgáltatási minőséggel (QoS). A nagy felbontású képek, videokonferenciák és egyéb jellegű információk egyidejű továbbítása esetén a szükséges csatornakapacitás esetenként már a néhány tíz Mb/s-os jelfolyam sebességet is megköveteli. Erre a feladatra az ATM technológia nagyon megfelelő. Ez a technológia nem más, mint a széles sávú ISDN (B-ISDN) megvalósításának lehetősége, amely biztosíthatja a hálózati videózás, a mozgóképes multimédiás elektronikus küldemények továbbítását, LAN hálózatok összekapcsolását és a nagysebességű átvitelt csomagkapcsolt formában. Az ATM hálózat adatátviteli sebessége 155 MB/s, ami a keskenysávú ISDN sávszélességének 2500 szorosa.

Nyugat-Európában több ország is felismerte ezt a problémát, melynek kiküszöbölésére az ATM alapú kommunikációs rendszereket kezdték rendszerbe állítani. Ilyen rendszert alakított ki haderejében Franciaország, a vezetési pontok kommunikációs hálózatában Németország, az USA, majd Belgium, Nagy-Britannia, és Olaszország is. Ezekben a NATO tagországokban felismerték a reális idejű adattovábbítás, a több résztvevős videokonferenciák és konferenciabeszélgetések jelentőségét. Az ilyen jellegű összeköttetéseket tömegesen alkalmazták

például az Öböl-háború idején is. A kommunikációs feltételek biztosításához tehát rendelkezésre állnak a polgári életben az említett jellegű összeköttetések biztosításához szükséges távközlő és informatikai eszközök, így ezek alkalmazása, katonai körülményekhez történő igazítása lesz a kommunikációs rendszerek kialakításának előfeltétele, melynek során például a szélsőséges hőmérsékleti viszonyoknak, a rázkódásnak kell megfeleltetni az eszközöket.

A hadműveleti helyzetek gyors változása nem teszi tehát lehetővé a vezetési pontok hálózatainak hosszú idejű kiépítését és telepítését, konfigurálását, vagy áttelepítését, ezért ki kell alakítani a minimális telepítési idejű rendszert, a kezelők rövid idő alatti telepítési és beállítási feladatait, vagyis a lehető legnagyobb automatizáltságra kell törekedni. Ennek lehetőségét is nagymértékben képesek biztosítani a polgári kereskedelemben vásárolható eszközök, melyek megfelelnek a Plug and Play (PnP) automatikus ki- és belépési rendszer létrehozásának. Ezt, ha egy konkrét helyzetre, a válságkezelésre vizsgáljuk megállapítható:

- a zászlóalj harccsoportok és a dandár operatív csoport vezetési pont hírközpontja települ a válságkezelés kezdeti időszakában;
- a helyzet további eszkalálódása után már a dandár szervezetének más cellái, az összfegyvernemi-, fegyvernemi- és szakalegységek is alkalmazásra kerülhetnek;
- a hadtest és a dandár tábori vezetési pontjai fokozatosan települnek ki a hadműveleti területre, és a teljes hadrend folyamatosan alakul ki. Az újonnan belépő cellák saját információs rendszereikkel kívánnak csatlakozni, vagy éppen leválni a hálózatról. Ezek a változások rendszer szinten nem jelenthetnek semmilyen befolyásoló hatást a hálózat működésére éppúgy, mint ha egy-egy kapcsolóközpont, vagy router meghibásodna.

A hálózat kialakításakor tehát egy olyan protokollt kell kiválasztani, amely a speciális katonai tényezőket figyelembe veszi, mint például a nagy adatátviteli sebesség, a könnyű kezelhetőség, a nagyfokú automatizáltság, a speciális dimenziók a rendszer felépítésében és működésében pedig kiszolgálják a felhasználókat igényeiknek megfelelően.

Az ATM alapú rácsrendszer felépítése

A NATO Katonai Bizottsága a „Tactical Communications Post-2000" (TACOM post-2000) megnevezéssel egy új architektúra típust javasolt a szárazföldi erők harcászati (mobil) kommunikációs rendszereihez. Ezt a nyugati haderők többségében már elfogadták, és rendszereiket ez alapján alakítják át, modernizálják. Ez az architektúra típus a hadműveleti erők számára lehetővé teszi:

- a vezetési (parancsnoki) lánc folytonosságát a hadtesttől a zászlóalj-, század szintekig;
- az információs rendszerek összekapcsolhatóságát minden szinten;
- az összekapcsolt hálózatok interoperabilitását a nemzeti törzsek szintjétől a hadműveleti feladatokat végrehajtó csapatokig, és a szövetséges erők nemzetei között is a kommunikációs eszközök széles skáláján.

Az ATM alapú hálózathoz csatlakozó hadtest-, dandár-, ezred- és zászlóalj vezetési pontok azonos képességekkel (jelfolyamokkal) csatlakoznak hírközpontjaikkal ehhez a rendszerhez az alacsonyabb vezetési szintek (pl.: század, harcrendi elemek) mobil felhasználóként rádióállomások alkalmazásával rádiótelefon jellegű kapcsolattal tartanak folyamatos összeköttetést a hálózaton keresztül az elöljáró szervezetekkel és más felhasználókkal.

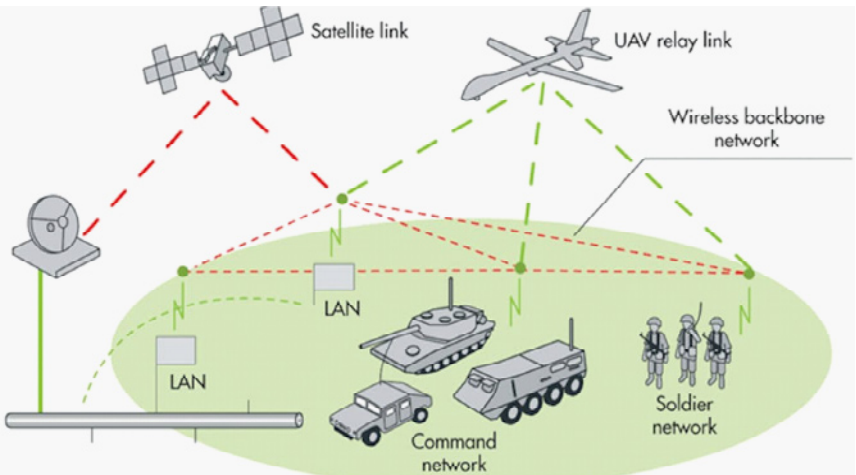
A csomópontokból tehát a hálózat kialakítása érdekében biztosítani kell a szomszédos csomópontok irányába mikrohullámú összeköttetéseket, és képesnek kell lenniük a különböző szintű csatlakozó hírközpontok mikrohullámú berendezéseinek fogadására is. A hálózat csomópontjai egymástól 15-30 km-re települhetnek a hadműveleti területen, és ezeket több helyen illeszteni kell a stacioner területi hálózat csomópontjaihoz, valamint más NATO tagország kommunikációs rendszerével, és a polgári távközlési objektumokkal történő együttműködési képességre is alkalmassá kell tenni azokat.

A vezetési pontok belső kommunikációs hálózata

Az ATM alapú hálózat kialakításánál nagyon fontos a vezetési pontok belső kommunikációs rendszerének meghatározása, majd az erre épülő hadműveleti-harcászati csatlakozási sík felépítése. A vezetési pontok belső hálózatánál biztosítani kell, hogy a katonai szervezet törzscellái (G1-G6, S1-S6, stb.) egyidőben és széles körben alkalmazhassanak informatikai eszközökkel támogatott multimédiás kapcsolatokat a döntéselőkészítés, az elhatározás, és az adattovábbítás során, valamint ezzel párhuzamosan a digitális távbeszélő szolgáltatásokat ugyanazon kommunikációs hálózaton keresztül vehessék igénybe, hiszen a korszerű kommunikációs rendszereknek ezeket a szolgáltatásokat egy hálózaton belül kell biztosítania az informatikai és a távközlő hálózatok integrálásával. Ehhez olyan kapcsolókat kell kialakítani, melyek képesek analóg- és digitális

trönköket, számítógép hálózatokat fogadni NATO STANAG-eknek és polgári szabványoknak megfelelően, valamint biztosítani szabvány Ethernet típusú kapcsolatot számítógépek, munkaállomások, hub-ok, szerverek és routerek részére. Ezeket a berendezéseket egy készülékbe építve olyan kapcsolókat kaphatunk, melyek egyidőben képesek:

- ATM kapcsolóként,
- Fast Ethernet és IP kapcsolóként, valamint
- Hagyományos PABX kapcsolóként üzemelni.



Az így kialakított berendezések a szolgáltatások jellegéből adódóan multimédiás kapcsolóknak (továbbiakban MUK) nevezhetők.

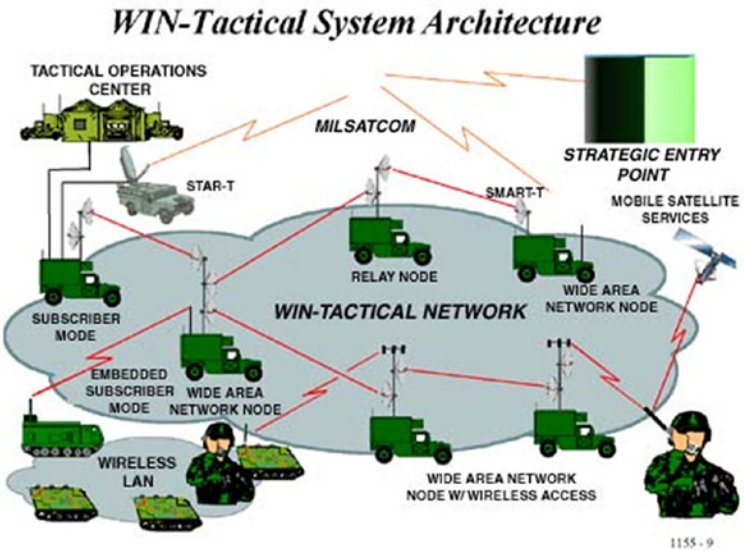
A vezetési pontokon a harcvezetésben és a hadműveletek különböző biztosítási feladatainak tervezésében, szervezésében és végrehajtásában részt vevő felhasználók igénye azonban nem csak az, hogy az informatikai hálózaton keresztül saját szervezetük törzsének más felhasználóival tarthassanak kapcsolatot, hanem igényük van arra is, hogy ezzel egyidőben, fizikailag egy másik LAN hálózathoz csatlakoztatott felhasználóval cserélhessenek információt munkaállomásaikról, vagy adhassanak utasításokat. Egy konkrét példán keresztül bemutatva: a hadtest G3 (hadművelet) cella hálózatában dolgozó tüzér főnökség nem csak a hadtest törzs más felhasználóival kíván adatcserét és információs csatornákat, hanem a hadműveleti feladat végrehajtásában részt vevő tüzér egység vezetéséhez is adatokat szeretne részükre továbbítani, vagy tőlük kapni. Ezek a csapatok azonban termináljaikat saját törzsük informatikai hálózatához kapcsolva alkalmazzák, melyek egy-egy másik önálló LAN hálózatot jelentenek. Az ATM technológia

alkalmazása esetén ezeket a hálózatokat nem szükséges közvetlen fizikai kapcsolattal összekötni, hanem elegendő egy közös csomóponti hálózathoz kapcsolni. Ezért a kapcsolatok realizálásához a vezetési pontokon egy-egy híradó állomásra van szükség, mint átviteli utat biztosító elemre, a csomóponti hálózathoz történő csatlakozás érdekében. Ezzel azonban még csak az adattovábbítás lehetősége biztosított. A további probléma feloldására az ATM rendszer megoldási lehetőséget a korábban említett virtuális áramkörök, és kapcsolatok létesítésével nyújt. Így megvalósítható a különböző vezetési szintek fizikailag közvetlenül össze nem kötött (nem azonos LAN hálózatban üzemelő) számítógépeinek és felhasználóinak kapcsolata logikai összeköttetések felhasználásával a közös csomóponti hálózat használatával. A különböző LAN hálózatok termináljai közötti kommunikációhoz tehát nincs szükség fizikai kapcsolat kiépítésére, mert a csomóponti hálózat tölti be ezt a szerepet. E szolgáltatás katonai alkalmazásának vizsgálatát segíti az ábra, ahol a gépesített hadtest vezetési pontjának virtuális hálózatkialakításának részlete látható egy lehetséges változatban.

A hadtest LAN hálózata optikai kábellel kiépített gyűrű struktúrában kerül telepítésre. A vezetési ponton a törzs felhasználói (G1-G6) saját termináljaikat e hálózatba integrálva használják, ugyanakkor az alárendelt fegyvernemi- és szakalegységekkel, a csapatok vezetési pontjaival az egyes cellák képesek virtuálisan (a valóságban fizikailag közvetlenül össze nem kötötten) hálózatot kialakítani. (Az egyes VLAN rövidítések az ábrán a virtuális hálózat kialakítási lehetőségére utalnak, ahol az ábrázolt sejtek önálló LAN hálózatai mellett jelenik meg a virtuális kapcsolat.) E módszer alkalmazásával a hálózati szolgáltatásokon és a virtuális kapcsolatokon kívül továbbra is biztosított a saját törzseken belül üzemeltetett katonai üzenetkezelő rendszer (MMHS) funkcionális működtetése is.

A virtuális hálózat tehát a LAN hálózat mellett képes biztosítani az elöljáró fegyvernemi- és szolgálati ág főnökök virtuális csatornáit, melyek a beszéd kapcsolat mellett a multimédiás szolgáltatásokra is vonatkoznak. A vezetési pontokon e rendszerszolgáltatás biztosítására tehát a cellák felhasználói részére tehát olyan berendezés szükséges, amelyik lehetővé teszi az ATM technológia szolgáltatásainak igénybevételét a beszéd-, kép- és adatátvitel területén egyaránt. Ezt a szerepet a multimédiás kapcsoló egységek (MUK) tölthetik be az ATM alapú tábori kommunikációs hálózatokban. Ezek a berendezések biztosítják a csatlakozási felületet a hálózati elemek (munkaállomások) részére, valamint lehetőséget adnak az átviteli utat biztosító híradó állomás szükség szerinti csatlakoztatására is. A multimédiás kapcsolók között, és a csomóponti hálózathoz csatlakozó híradó állomás között a nagysebességű adatátvitel érdekében tábori kivitelű optikai kábelek szükségesek, melyek lehetőséget adnak a hálózaton belüli 155 Mb/s jelátvitelre, így a hagyományos szolgáltatások mellett a multimé-

diás szolgáltatások is biztosítottak lesznek a felhasználók részére. Egy így kialakított hadtest vezetési pont kommunikációs igényei kiszolgálására létrehozott LAN hálózat elvi felépítését mutatja az ábra, ahol a cellák egymáshoz kapcsolt rendszere mellett az átviteli utat biztosító híradó állomás is megtalálható. Ez a változat akár egy védett vezetési ponton, béke elhelyezési körletben (laktanyában), vagy tábori körülmények között is megvalósítható.

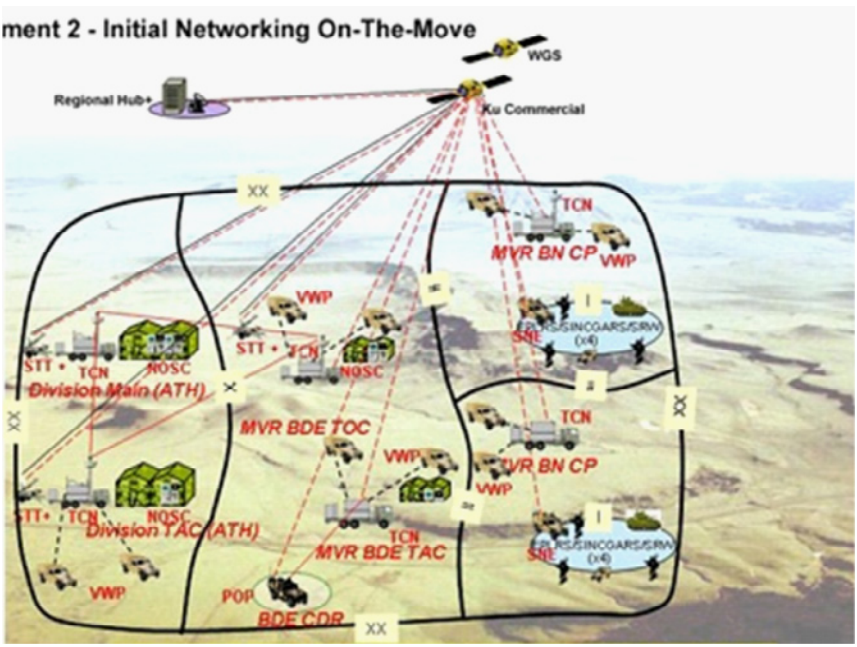


A cellákban található, egymáshoz kapcsolt multimédiás kapcsolók biztosítják tehát a felhasználói terminálok és más kommunikációs eszközök csatlakoztatását, így összességében egy vegyes topológiájú információs hálózatot alakítanak ki, ahol a vezetési cellák munkaállomásai csillagtopológiát alkotnak, addig a multimédiás kapcsolók a LAN hálózaton belül gyűrű- és csillag topológiában helyezkednek el.

A csillag topológiában minden egyes elem egy-egy közös kapcsolóhoz csatlakozik, így ennek előnye az egyszerű és gyors telepíthetőség, valamint az, hogy az egyes terminálok meghibásodása nincs hatással a topológiában található más munkaállomás működésére, így a hálózat megbízhatóan használható.

A multimédiás kapcsolók önállóan is működőképesek, a kapcsolók telepítésével rugalmasan bővíthető hálózat alakul ki PnP rendszerben vagyis a hálózathoz történő csatlakoztatásuk és az onnan történő kilépésük automatikus; a hálózat érzékeli az újabb becsatlakozó kapcsolók megjelenését, vagy távozását és a felhasználói hálózatot a rendszer automatikus konfigurálással alakítja ki.

Egyes kapcsolók esetenkénti meghibásodása ez esetben nem okoz problémát a hálózat szintjén, mert a rendszer ettől függetlenül tovább üzemel, kiesés csak az adott kapcsolóhoz tartozó végberendezéseknél lehet. Egy-egy vezetési ponton a multimédiás kapcsolók száma elsősorban nem annak nagyságától, hanem a vezetési pontokon lévő felhasználók számától és az alkalmazott végberendezések számától függ. Így például dandár vezetési ponton már egy-kettő, hadtest vezetési ponton három-négy multimédiás kapcsoló is elégséges a vezetési ponton települt cellák összeköttetései minden fajtájának biztosítására.



Ezeknek a multimédiás kapcsolóknak biztosítaniuk kell egyidőben 10-12 munkaállomás (PC) fogadását, 10-12 (szükség esetén információvédelemmel ellátott) analóg távbeszélő- és/vagy G3 típusú FAX berendezés csatlakoztatását, 3-4 S0 összeköttetés létesítését (ISDN digitális telefon, G4 típusú FAX, videokonferencia terminál, stb.), valamint 3-4 ATM (155Mb/s) irány fogadását optikai kábelen. Ezeknek a csatlakozási felületeknek meg kell felelniük mind a polgári, mind a NATO csatlakozások normáinak (STANAG 5040, 4206, 4249). A vezetési pontokon található kapcsolók egymással optikai kábellel kerülnek összekötésre, így azok képesek biztosítani a nagysebességű adatátvitelt a munkaállomások és felhasználók között, és egyúttal biztosítják az Internet protokoll alapú (IP) és a virtuális hálózati szolgáltatásokat egyaránt. A hadtest vezetési

pontokon a törzs celláinak munkaállomásai mellett a multimédiás kapcsolókhoz kell csatlakoztatni a különböző szervereket (pl.: E-mail), valamint a C3I rendszer teljes körű működését biztosító adatbázis szervert is. E rendszerben a törzs cellák azon munkaállomásai láthatók, amelyek a virtuális LAN hálózatokban üzemelhetnek, vagyis az alárendeltek felhasználóival tarthatnak információs kapcsolatot. A virtuális hálózati munkaállomások mellett azonban üzemeltetni kell az INTERNET/INTRANET szervereket. Ennek oka az, hogy a helyi LAN hálózatokról kilépést kell biztosítani más hálózatokba is, illetve tudni kell fogadnia más felhasználók csatlakozását, ezért tűzfalakkal ellátott szerverek szükségesek, melyek az illetéktelen belépőket kizárják a hálózati felhasználásból. A vezetési pontok informatikai hálózatának eszközparkján kívül ugyanez a kapcsoló látja el az irodai alkalmazású munkaállomások LAN hálózatban történő üzemeltetését, a videokonferencia szerverek, az analóg és digitális mellékek működőképességének biztosítását.

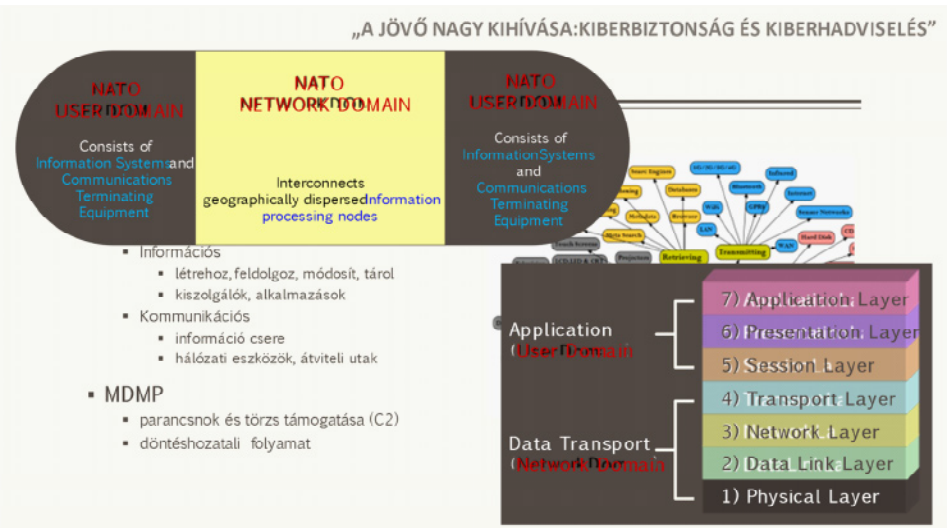
A tábori alaphírhálózat korszerűsítése során további cél lehet a híradó állomások típusszámának csökkentése, ami azt eredményezi, hogy megszűnik a vezetési pont hírközpontok nagy mérete, az ott található híradó állomások nagy száma, és helyüket korszerű, digitális eszközöket tartalmazó típusgépjárművek váltják fel. Ezeket a híradó állomásokat – jó kialakítás esetén- fel lehet használni csomóponti hírközpontok, vezetési pont hírközpontok és esetenként stacioner telepítésű területi hálózat elemeiként a kommunikációs rendszer kialakítására, így homogén, néhány híradó típusállomásból álló rendszer jön létre, ahol csak a hordozó járművek jellege és a digitális kapcsoló központok konfigurációja kell, hogy változzon a csapatok alkalmazásának, a résztvevő felhasználók számának megfelelően. Így a csomóponti- és a vezetési pont hírközpontok típusállomásaiból egyenszilárd kommunikációs rendszer építhető fel.

NATO-elvű infokommunikációs hálózatok katonai műveletekben

Dr. habil. Farkas Tibor százados, egyetemi docens, tanszékvezető-helyettes
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék
farkas.tibor@uni-nke.h

Védelmi kommunikációs rendszerek

A főbb védelmi kutatási irányok meghatározására minden esetben hatást gyakorolnak az aktuális nemzeti- és nemzetközi események. A napjainkban végbemenő történések megkövetelik a védelmi szektor minden területének folyamatos megújulását, amelyre nagy hangsúlyt kell fektetni a kutatások során.



A hadművészeknek már nem csak a fegyveres küzdelem objektív törvényszerűségeit kell ismerni, nem elég már a hadügy jövőjének tudományos előrelátása, a kutatásoknak ki kell terjedni a „joint" (katona-rendőr-civil) tervezésre és tevékenységre is. (Boda[et.al] 2016. 6. o.) Az infokommunikációs hálózatokhoz tartozó kutatási részegység másik nagy eleme a műszaki terület, amely új irányvonalainak meghatározása, behatárolása szintén nagy jelentőséggel bír. A műszaki tudományterületen folytatott nemzetközi kutatások fő irányait, fókuszálva az államtudományokkal való összefüggésekre, a *„Műszaki kutatások és hatékony kormányzás"* című publikáció foglalja össze, nagy hangsúlyt fektetve az infokommunikációs technológiák szerepére. (BLESZITY J. [et.al] 2016.) Mindezeket figyelembe véve a védelmi szervezetek vezetését és irányítását kiszolgáló, támogató infokommunikációs rendszerek elemzése és vizsgálata szükséges a fejlesztési

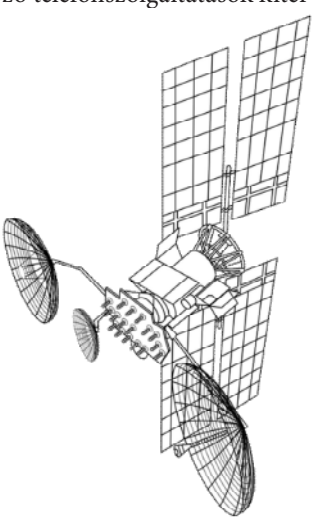
irányok meghatározása érdekében. Ennek megfelelően az infokommunikációs technológiák hálózati megjelenése jelentősen befolyásolja a hálózat támogató képességét, a szolgáltatásokat és az üzemeltetés területeit.

A Belügyminisztérium önálló jogi személyiséggel rendelkező központi költségvetési szerv, amelynek alapító okirata tartalmazza a közfeladatot, amelyet a minisztérium ellát, amelyért a tárca felel.

Ez a közfeladat magába foglalja mindazon területeket, amelyek jelentősen befolyásolják az ország, valamint az állampolgárok életét.

Az országot érő különböző katasztrófahelyzetek, válsághelyzetek felszámolásában jelentős szerepet töltenek be az Országos Katasztrófavédelmi Főigazgatóság szervezetein túl az egyéb, a belügyminisztérium alá tartozó szervezetek. Az alaprendeltetésük, tevékenységük és feladatuk nagymértékben eltér egymástól, mégis az esetlegesen bekövetkező válsághelyzetekben a különböző szervezetek jól kiegészítik egymást.

A kormányzati tevékenységet támogató kommunikációs rendszerek mindenkor kiemelt jelentőséggel bírtak, és ezek a hálózatok, rendszerek és technikai eszközök minden esetben az elsők között kerültek fejlesztésre a sikeres kormányzás támogatása érdekében. A ’90-es évek elején a digitális távközlésre történő áttérést kellett megerősíteni, amely nagymértékben befolyásolta az információk mennyiségi és minőségi továbbítását. Ennek egyik első lépése az országos, nagykapacitású gerinchálózat kialakítása volt, amely optikai és mikrohullámú összeköttetésekkel került kiépítésre. A ’90-es évek második felében elsősorban a telefon szolgáltatás mennyiségi fejlesztése, majd a különböző telefonszolgáltatások kiterjesztése jelentette a fejlesztés főbb irányvonalát. A 2000-es évek elején az ISDN technológia kiterjesztése, valamint a megjelenő korszerű szolgáltatások biztosítása vált hangsúlyossá. A technológia fejlődését a jogszabályi és szervezeti változások egymással párhuzamosan követték, amely biztosította a korszerűsítés végrehajtását.



A különböző hálózati elemek meghatározása, szabályozása szükségessé vált, hiszen érezhető volt az elkülönülés a különböző felhasználói platformok, rendszerek között.

A távközlési gerinchálózat és a „mellékágak” folyamatos fejlesztése továbbra is kiemelt feladat volt, amely során mind a polgári, mind a kormányzati hálózat fejlesztése végrehajtásra került.

A védelmi szektor szempontjából fontos terület a honvédelmi ágazat is, amely nem csatlakozik „direkt" hálózatként a kormányzati rendszerhez, hanem elkülönülve működik. Jelenleg a Honvédelmi Minisztérium hálózata a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata (HM KCEHH), amely béke- és minősített időszakban támogatja az MH vezetési és irányítási rendszerét. A hálózat további speciális tulajdonsága, vele szemben támasztott képessége, hogy csatlakozzon a szövetséges infokommunikációs hálózathoz, a NATO Általános Célú Kommunikációs Rendszeréhez (NGCS2) ezáltal biztosítva az együttműködést.

A Belügyminisztérium kommunikációs támogatását biztosító szakmai irányító szervezet 2002-ben alakult meg, mint BM Távközlési Szolgálat, amely szakirányítói és központi üzemviteli feladatokat látott el. A szervezet 2007. január 1-ig működött.

A tárca különleges helyzetben volt, hiszen az alárendelt szervezetek (pl. rendőrség) nem rendelkeztek önálló, saját kommunikációs hálózattal, hanem bérelt vonalon került kialakításra az összeköttetés a szolgáltatók hálózatainak felhasználásával. A hálózatok egyre nagyobb méretű kiterjesztése, valamint a megjelenő új technológiák és szolgáltatások a 2000-es évektől nagy hatással voltak a rendszer továbbfejlesztésére és bővítésére. 2010-ben még több olyan cég is jelen volt a piacon (Antenna Hungária Zrt., Invitel Távközlési Zrt., GTS Datanet Távközlési Kft., Magyar Telekom Távközlési Nyrt., Magyar Villamos Művek Zrt.), amelyek közel országos kiterjedésű hálózattal rendelkeztek és biztosították a szolgáltatásokat mind a kormányzati, mind a polgári szervezetek, személyek részére.

A korábban Egységes Belügyi Digitális Hálózatot (2006. június 30-ig), majd az Elektronikus Kormányzati Gerinchálózatot, amelynek része volt a Rendészeti Hálózat, felváltotta a Nemzeti Távközlési Gerinchálózat (NTG) valamint a Zártcélú Rendészeti Hálózat. Mindezeket figyelembe véve tehát látható, hogy a folyamatos változások ellenére, a kormányzati szintű szolgáltatásokat biztosító rendszer minden esetben rendelkezésre állt. A változást a fejlesztések eredményének köszönhető bővítés és a felhasználók köre jelentette

Míg az NTG szolgáltatásait a NISZ, addig a hálózatot az MVM Zrt. tulajdonában lévő MVM Net biztosítja a kormányrendeletben behatárolt felhasználók számára. Az előzőekben leírtaknak megfelelően tehát az NTG által biztosított elektronikus hírközlési szolgáltatásokat ma már állami tulajdonú szervezetek, társaságok biztosítják, amely lehetővé tette a „piaci szolgáltatóktól" megrendelt szolgáltatások kiváltását. Ez természetesen számos előnnyel jár, mint a költséghatékonyság, vagy a megbízható állami szervezetek alkalmazása. Természetesen a hálózati szolgáltatások is jelentős mértékben növekedtek, akár a végpontok és a sávszélesség is.

„104 állami intézmény szolgáltatásainak korszerűsítésével több, mint 3600 végpontra épült ki új hálózati csatlakozás, a rendszer alapkapacitása tízszerese a korábbinak, míg az adatforgalom közel háromszorosára emelkedett." (Nemzeti Távközlési Gerinchálózat)

Az NTG MVM Net Zrt. által üzemeltetett hossza meghaladja a 6000 km-t, amelyen folyamatos, 24 órás üzemeltetői és monitorozó szolgálatot biztosít a zavarmentes kommunikáció biztosítása érdekében. A NTG jelentős mértékben meghaladta elődje, az EKG szolgáltatásait, kapacitásait és végpontjainak számát.

A hálózat nyújtotta képességek, szolgáltatások biztosítják a felhasználók számára a megbízhatóságot, a magas szintű rendelkezésre állást a menedzselt szolgáltatásokat és a kiemelt fontosságú skálázhatóságot! 2015-ben befejeződött egy nagy hangsúlyú fejlesztési periódus, amely a hangszolgáltatások minőségi hatékonyságát javította, illetve a biztonsági feltételek megteremtésének előmozdítását valósította meg. Mindezek elősegítik a NISZ által biztosított hírközlési szolgáltatások kihasználtságát. Összegezve tehát a NTG egy nagy kapacitású, magas megbízhatósággal rendelkező távközlési szolgáltatásokat nyújtó hálózat, amely alkalmas a kormányzati szegmens kiszolgálására.

A NTG biztosítja a rendvédelmi szervek országos hálózatba integrálását, amelyet az MVM Net Zrt. hálózata, valamint a NISZ Zrt. szolgáltatásai tesznek lehetővé a Belügyminisztérium irányítása mellett. A belügyi szervezetek részére minden esetben fontos, hogy a magas fokú rendelkezésre állás biztosított legyen, hiszen a szervezetek eltérő telephelyei között gerinchálózat biztosítja az információcsere lehetőségének platformját. Ennek megfelelően fontos, hogy a hálózathoz történő csatlakozás egyszerűen megvalósítható és stabil kapcsolat legyen; támogassa minden típusú információ (hang-, adat-, videó-szolgáltatás) cseréjének fizikai platformját; valamint az egymással együttműködő szervezetek közötti szolgáltatások megosztását. Az együttműködés minden esetben a belügyi szervek mellett a más kormányzati szervezetek irányában is megvalósítható kell, hogy legyen. Az NTG-hez történő kormányzati, közigazgatási végponti csatlakozás biztosítja az előbbiekben felsorolt szolgáltatások és kapcsolatok elérését. A belügyi tárca ennek megfelelően egy saját, egységes hálózatot üzemeltet, amely MPLS technológia alkalmazásával, valamint VPN csatornák kialakításával teszi lehetővé az elkülönített hálózati hozzáférést.

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

A jövő nagy kihívása: kiberbiztonság és kiberhadviselés

Az Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
és a
Magyar Természettudományi Társulat
konferencia-sorozata – 2.

A DRÓNOK HARCA – VESZÉLYEK ÉS LEHETŐSÉGEK

A konferencia-sorozat szervezői:
Prof. Dr. Rajnai Zoltán, PhD, dékán (Óbudai Egyetem)
és Dr. Tardy János, PhD, üv. elnök (MTT)

HELYSZÍN
Internet (Zoom)
IDŐPONT
2020. március 31., 14:00 óra

PROGRAM
14:00-14:10 Köszöntések
14:10-14:30 **Prof. Dr. Rajnai Zoltán,** PhD, egyetemi tanár, dékán
(Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Biztonságtechnikai Intézeti Tanszék)

Drónok alkalmazhatósága a védelmi szférában

14:30-14:50 **Dr. habil. Czajlik Zoltán,** CSc, tszv. egyetemi docens
Dr. Rupnik László, PhD, egyetemi tanársegéd
(ELTE BTK Archeometria, Régészeti Örökség és Módszertan Tanszék)

A repülőgépes felderítéstől a drónos felmérésig.
Régészeti célú légi fényképezés különböző platformokon

14:50-15:10 **Dr. Őszi Arnold** egyetemi adjunktus
(Óbudai Egyetem Gépészeti és Biztonságtudományi Intézet, Biztonságtechnikai Intézeti Tanszék)

A drónok veszélyei

15:10-15:30 **Dr. habil. Nagy Balázs,** PhD, egyetemi docens (ELTE TTK, Természetföldrajzi Tanszék)
Dr. Mészáros János, PhD (ATK TAKI Talajtérképezési és Környezetinformatikai Osztály)

Drónok a klímaváltozás vizsgálatában – térképezés magashegységi környezetben, Ojos del Salado, Chile

15:30-15:45 Kérdések, hozzászólások

15:45-16:05 **Dr. Gulyás Zoltán,** PhD (Nemzeti Élelmiszerlánc-biztonsági Hivatal, Növény-, Talaj- és Agrárkörnyezet-védelmi Igazgatóság)
Sillinger Fanni, doktorandusz
(Magyar Agrár- és Élettudományi Egyetem)

A drónok jelenlegi és jövőbeni alkalmazási lehetőségei a mezőgazdaságban

16:05-16:25 **Dr. Kovács Béla,** PhD, egyetemi adjunktus
Hajdinákné Vörös Fanni doktorandusz
Pál Márton doktorandusz
(ELTE Informatikai Kar, Térképtudományi és Geoinformatikai Intézet)

Légből kapott képek elemzése. A drónok használata a térképészetben

16:25-16:45 **Bíró György,** környezetvédelmi főtanácsos (MAVIR Zrt.)
Haramia Ákos drónfejlesztő (FiiHaa Engineering):

Drónok a természetvédelem szolgálatában

16:45-17:05 **Dr. Bertalan László,** PhD, egyetemi tanársegéd
Szopos Noémi, doktorandusz
Nagy Bálint, doktorandusz
Dr. Szabó Gergely, PhD, egyetemi adjunktus
(Debreceni Egyetem Természetföldrajzi és Geoinformatikai Tanszék)

Kanyarulatfejlődés a drónok szemszögéből - Új módszerek a folyóvízi parterózió és a felszíni vízsebesség tanulmányozásában

17:05-17:20 Kérdések, hozzászólások

Drónok alkalmazhatósága a védelmi szférában

Prof. Dr. Rajnai Zoltán, PhD, egyetemi tanár, dékán
Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar,
Biztonságtechnikai Intézeti Tanszék
rajnai.zoltan@bgk.uni-obuda.hu

A harci drónok átalakítják a katonai erő használatával kapcsolatos attitűdöket. A katonai áldozatok és a konfliktusok költségei megcsapolják a háború, valamint a politikai és katonai vezetők állami támogatását. A harci drónok példátlan képességet kínálnak arra, hogy egyszerre csökkentsék ezeket a költségeket a pontosság növelésével, a polgári lakosságot érintő kockázatok csökkentésével és a katonai személyzet védelmével a károktól. Ezeknek az előnyöknek népszerűbbé kell tenniük a dróncsapásokat, mint a szárazföldi csapatokat érintő műveleteket. Sok kritikus azt állítja, hogy a drónháború túlságosan hajlandóvá teszi a politikai vezetőket a háborúk engedélyezésére, ami gyengítheti az erő alkalmazásának etikai és jogi korlátait Mivel a támadó drónok megjelenése viszonylag új jelenség, ezek az érvek nagyrészt anekdotákon, néhány közvélemény-kutatáson alapulnak, vagy elméleti spekulációk.

Napjainkban kísérleti kutatásokat használnak fel a harci drónok hatásának elemzésére, így például az amerikaiak erő alkalmazásának támogatására. Sokan társadalomtudományi elméletekből merítenek véleményalkotáskor, elvárásokat fogalmaznak meg, majd felmérési kísérletek sorozatával értékelik ezeket a feltételezéseket. Megállapításaik – miszerint a drónok fontos, de árnyalt hatást gyakoroltak az erő alkalmazásának támogatására – hatással vannak a katonai fellé-

pés és a polgári-katonai tevékenység demokratikus ellenőrzésére, kapcsolatokat, és betekintést nyújtanak abba, hogy a jelenlegi és jövőbeli katonai technológiák fejlődése és elterjedése hogyan befolyásolja a külpolitikát és a belpolitikát.

A növekvő pénzügyi és emberi költségek, különösen a katonai áldozatok, közvetlenül csökkentik a felkelések elleni küzdelem támogatását. Vietnám, Irak és Afganisztán jól illusztrálja ezt a dinamikát; az áldozatok számának növekedésével minden esetben csökkent az erőszak alkalmazásának társadalmi támogatottsága.

MQ-9 Reaper pilóta nélküli repülőgép

A technológiai fejlődés ma már lehetővé teszi olyan fegyverek létrehozását, amelyek közül a legkiemelkedőbbek a felfegyverzett, pilóta nélküli légi járművek vagy "drónok", amelyek azt ígérik, hogy megkönnyítik a mindkét kihívás kezelése. Ezeknek a harci drónoknak két releváns jellemzője van a felkelés elleni küzdelem költségeinek kezelésében és a siker esélyeinek javításában. Az első a szelektivitás, amely egy jól meghatározott célpont – például egy adott épület, jármű vagy egyén – azonosításának és eltalálásának képességét jelenti, miközben a közeli nem harcolók és a polgári infrastruktúra károsodásának minimalizálása. A fegyverek szelektívebbek, ha aktívan irányíthatók a célpontjaikhoz, például a rakétákhoz, amelyeket meghatározott földrajzi koordinátákra irányítanak. A szelektivitást az is növeli, ha a fegyver több hírszerzési adatfolyammal van integrálva – amelyeket maga a fegyverplatform vagy más rendszerek, például műholdak vagy kommunikációs lehallgatások gyűjtenek össze –, amelyek információt szolgáltatnak a célpont személyazonosságáról és helyéről. A nagyobb szelektivitás azt jelenti, hogy a fegyver jobban képes megoldani az azonosítási problémát, lehetővé téve az ellenséges militánsok hatékonyabb felderítését és célzását, miközben a csapásokat úgy időzíti, hogy csökkentse a polgári áldozatok lehetőségét. A drónok a szelektivitás mindkét aspektusa szempontjából előnyökkel rendelkeznek, mivel ezen eszközök az elhúzódó felderítő küldetések

végrehajtására a feltételezett ellenséges harcosok nyomon követésére és a támadások elindítására viszonylag csekély mennyiségű lőszerrel, így csökkentik a polgári áldozatok kockázatát.

A második jellemző a pilóta sebezhetetlensége: a harctéri győzelmek elérésének képessége, miközben minimalizálja azt a kockázatot, amellyel a katonai személyzet szembesül az ellenséges erők bevonásakor. A pilóta sebezhetetlensége jelentős hasznot hoz a fegyveres erők részére.

Légi felderítésben alkalmazott Predator

Általánosságban elmondható, hogy minél nagyobb a hatótávolság, annál kevésbé sebezhető a fegyver kezelője az ellenséges tűzzel szemben. A tábori tüzérség például jellemzően sokkal nagyobb hatótávolsággal rendelkezik, mint az aknavetők, ami azt jelenti, hogy az előbbieket legénységet ellátó katonák, ha minden más feltétel azonos, kisebb kockázatnak vannak kitéve, mint az utóbbiakat üzemeltetők. Hasonlóképpen, az irányított rakétákkal felfegyverzett repülőgépek személyzete kevésbé sebezhető, mint az egyszerű "gravitációs" bombákat ledobó repülőgépekkel rendelkező társaik, amelyeknek közelebb kell repülniük a célpontjaikhoz, hogy növeljék pontosságukat.

Ez a sebezhetetlenség a pilóta, nem pedig a gép jellemzője. A drónok eltávolítják emberi kezelőiket a veszélytől, de magukat a gépeket megtámadhatják és megsemmisíthetik. A jelenlegi generációs drónok általában érzékenyebbek a támadásokra, mint a fedélzeti személyzettel rendelkező repülőgépek, mert hajlamosak

lassabban repülni, korlátozott védelmi képességekkel rendelkeznek, és rosszul teljesítenek az ellenséges repülőgépek elleni levegő-levegő harcban. A drónokat feltörhetik, meghamisíthatják, vagy zavarhatják vezérlőrendszereiket. Ezek a korlátozások a gépeket támadás vagy meghibásodás kockázatának teszik ki, a pilóták mégis sebezhetetlenek maradnak, mert olyan szélsőséges távolságban vannak a csatatértől, hogy sorsuk teljesen elválik a repülőgépétől. Az egész amerikai drónerőt le lehetne lőni anélkül, hogy emberéleteket követelnének; ugyanez már nem mondható el a fedélzeti személyzettel ellátott repülőgépekről.

Német katonai drón

Mindkét jellemzőnek erőteljes politikai következményei vannak, különösen akkor, ha ugyanabban a fegyverrendszerben egyesülnek. Ez nem kapott kellő figyelmet részben azért, mert egészen a közelmúltig a fegyverek tervezői a szelektivitás és a pilóta sebezhetetlensége közötti kompromisszummal szembesültek. A fent bemutatott példák folytatásaként az aknavetők jellemzően szelektívebbek, mint a tüzérség, de a csapatokat nagyobb ellentámadási veszélynek teszik ki. A lézervezérelt bombákkal felfegyverzett csapásmérő repülőgépek rendszeresen eltalálhatnak bizonyos célpontokat, de ez a szelektivitás csökken, ha nagyobb magasságban repülnek, hogy elkerüljék a légvédelmi tüzet. Emiatt sok elemzés a szelektivitásra vagy a kísérleti sebezhetetlenségre összpontosított, miközben feltételezte, hogy ezeket a célokat nem lehet egyszerre megvalósítani. Az 1920-as évekre visszanyúlóan erőteljes vita folyik például arról, hogy a szelektivitás hogyan befolyásolja a politikai és katonai eredményeket.

Más munkák azt vizsgálták, hogy a pilóták sebezhetetlensége hogyan csökkenti az erő alkalmazásának költségeit és kockázatait, például azáltal, hogy lehetővé teszi a nagy hatótávolságú repülőgépekkel történő támadásokat a földi csapatok használatához képest.

A közelmúlt technológiai fejlődése élesen leszűkítette a szelektivitás és a pilóták sebezhetetlensége közötti kompromisszumot. A harci drónok – a levegő-föld rakétákkal felfegyverzett távirányítású repülőgépek – a legjobb példa egy olyan fegyverrendszerre, amely mindkét jellemzőt magában foglalja. A drónok szelektívebbek, és nagyobb biztonságot nyújtanak kezelőiknek, mint a leginkább hasonló fegyverrendszerük, a fedélzeti személyzettel rendelkező csapásmérő repülőgépek. Mindkettő pontos, irányított lőszerekkel van felfegyverkezve, és a fedélzeti érzékelőktől hírszerzési információkat gyűjthetnek a potenciális célpontokról. A drónok előnye, hogy sokkal hosszabb ideig képesek loiterálni, több időt hagyva az intelligencia integrálására, a célpontok pozitív azonosítására és a csapás időpontjának kiválasztására, amely maximalizálja a célpont károsodását, miközben minimalizálja a nem harcolók veszteség-kockázatát. A modern csapásmérő repülőgépek jelentős mértékben képesek elkerülni az ellenséges tüzet, beleértve a nagy sebességű, védekező fegyvereket és bizonyos esetekben a "lopakodó" jelleg kialakítást. De legénységük mindig ki van téve annak a veszélynek is, hogy lelőjék vagy meghibásodást tapasztalnak, míg a drón pilótái több ezer mérföldre lehetnek a csatatértől, és mentesek a fizikai sérülésektől. Fontos, hogy a drónok javulást jelentenek mind a szelektivitásban, mind a pilóta sebezhetetlenségében más fegyverrendszerekkel szemben.

A kísérleti repülőgépek például növelhetik támadásaik szelektivitását azáltal, hogy közelebb repülnek a célpontjaikhoz, de ez növeli személyzetük sebezhetőségét a földi tűzzel vagy balesetekkel szemben. A drónok nem igényelnek ilyen kompromisszumot; lehetővé teszik a szelektívebb támadásokat, miközben kiküszöbölik a katonai személyzet fizikai sérülésének kockázatát. A szelektívebb fegyverek, például a drónok azon képessége, hogy enyhítsék a háború politikai nehézségeit – a csatatéren való győzelem és a hazai támogatás megszerzése – a légierő huszadik század eleji megjelenése óta vitatott.

A vitát alakító kampányok közé tartozik a brit légierő bevetése a lázadók ellen Észak-Irakban és Wazirisztánban az 1920-as években, valamint az Egyesült Államok kiterjedt bombázása a felkelő Viet Cong egységek ellen a vietnami háború alatt. E támadások többségét ember által vezetett repülőgépekről ledobott gravitációs bombákkal hajtották végre, amelyeket nem lehetett nagy pontossággal a célpontjaikra irányítani, és amelyek veszélybe sodorták legénységüket. A későbbi értékelések arra a következtetésre jutottak, hogy ezek kevés hatást gyakoroltak az általuk megcélzott felkelőkre, vagy valójában erősítették azokat. A valóban szelektív fegyverek használata sokkal ritkábban fordult elő vagy volt tartós. Az Egyesült Államok cirkálórakétákat indított az al-Kaida szudáni és afganisztáni bázisai ellen az amerikai nagykövetségek elleni 1998-as támadások után, de ezeket a támadásokat nem tartották fenn elég sokáig ahhoz, hogy aláássák a csoportot. Izrael helikopterekről, merevszárnyú repülőgépekről és drónokról kilőtt rakétákat, valamint mesterlövészeket és szárazföldi csapatokat alkalmazott a Ciszjordániában és a Gázai övezetben fegyveres palesztin csoportok ellen irányuló "célzott gyilkosságok" kampányában, az Egyesült Államok pedig hasonló erőszaktechnológiákat használt Irakban és Afganisztánban. Ezek a hadjáratok minden bizonnyal szelektívebbek voltak, mint elődeik, bár katonai hatékonyságukról vita folyt, és továbbra is a katonai személyzetet tették ki kockázatának.

A drónok alapvetően megváltoztathatják ezeket a kompromisszumokat és általánosabban a fegyveres erő alkalmazásának költségeit és előnyeit. A nemzetközi politika tudósai régóta úgy gondolják, hogy a konfliktus költségei befolyásolják a potenciális harcosok hajlandóságát a fegyverkezésre. A közelmúltban végzett munka azt a feltételezést használja, hogy a különböző érdekekkel és preferenciákkal rendelkező államok és más szereplők alkudoznak egymással e különbségek megoldása érdekében.

Az erőszak alkalmazása vagy az ezzel való fenyegetés az egyik olyan stratégia, amelyet egy szereplő alkalmazhat, hogy engedményekre kényszerítse ellenfelét. De még a sikeres katonai akció is költséges; veszélyezteti a katonai személyzet és a civilek életét, pénzügyi szempontból drága, és csökkenti az erő alkalmazásának képességét más hadszíntereken vagy más ellenfelek ellen. Mielőtt katonai erőhöz folyamodnának, az államok és más szereplők levonják az e költségekre vonatkozó becsléseiket azokból az előnyökből, amelyeket az ellenség sikeres kényszerítéséből várnak. Ez létrehoz egy "alkutartományt", amelyet olyan tárgyalásos megállapodásokként értünk, amelyek okán mindkét fél szívesebben viselik a háború költségeit és kockázatait. Ha az alku hatóköre nagyobb, több potenciális alku van, amelyek kapcsán a felek inkább háborúzhatnak.

A háború költségei jelentősen befolyásolják az alku nagyságát. Ahogy ezek a költségek változnak, úgy változik a békés rendezések skálája is, amelyeket mindkét fél előnyben részesítene a fegyveres konfliktusokkal szemben. A haditechnika és a

doktrína innovációja az egyik módja annak, hogy a háború költségei megváltozzanak. A háborút költségesebbé tevő innovációknak nagyobb alkutartományt kell létrehozniuk, és így csökkenteniük kell a háború valószínűségét. Jó példa erre a nukleáris fegyverek hatása az államközi konfliktusokra. Sokan arra a következtetésre jutnak, hogy megfelelő körülmények között a nukleáris fegyverek megakadályozhatják a konfliktusokat azáltal, hogy jelentősen megemelik azok költségeit.

A nukleáris fegyverek növelik a háború költségeit, míg a drónok csökkentik azokat. Ez azt jelenti, hogy a fegyveres drónok birtoklása erősítheti a szereplők arra irányuló ösztönzését, hogy konfliktusokat kezdjenek vagy tartsanak fenn. A pilóták sebezhetetlensége, amelyet a drónok tesznek lehetővé, kiküszöböli a katonai akció egyik legfontosabb költségét: a katonai áldozatokat, amelyek aláássák a konfliktus belpolitikai támogatását. Szelektivitásuk azt jelenti, hogy a drónokról indított fegyverek nagyobb valószínűséggel érik el harctéri céljaikat, növelve az ellentétes oldalra kivetett költségeket. A szelektivitás csökkenti annak esélyét is, hogy az ilyen fegyverek szabadon bocsátása kárt okozzon a civileknek, ami a katonai áldozatokhoz hasonlóan a hazai és külföldi politikai szereplőket kevésbé hajlandóvá teheti a konfliktus támogatására. A drónműveletek tovább csökkentik a nagy előretolt katonai bázisok iránti igényt, csökkentve (de nem szüntetve meg) a katonai műveletek pénzügyi költségeit és a szövetségesekre való támaszkodás szükségességét, akik engedményeket követelhetnek együttműködésükért cserébe. A háború költségeinek csökkenése különösen erős a drónokkal rendelkező harcosok számára, akik olyan ellenségekkel néznek szembe, akik nem tudják megsemmisíteni ezeket a fegyvereket a harcban, vagy könnyen más költségeket róhatnak az ellenségre. Ez volt a helyzet számos olyan konfliktusban, amelyben terrorista és militáns szervezetek vettek részt, amelyek ellen az Egyesült Államok 2002 óta fegyveres drónokat vetett be.

A drónok jelentősen csökkentették a konfliktusok költségeit az Egyesült Államok számára. Az aggodalom az, hogy ez vonzóbbá tette a fegyveres konfliktusokat az Egyesült Államok számára. A nukleáris fegyverekkel ellentétben, amelyek csökkenthették az államközi háború valószínűségét, a dróntechnológia fejlesztése egyre hosszabb konfliktusokat ösztönözhet. A harci drónok használata az Egyesült Államok által a huszonegyedik században tehát fontos változást jelent ezekhez a korábbi konfliktusokhoz képest. Az Egyesült Államok és más országok az 1970-es évek óta komolyan fejlesztenek precíziós irányítású lőszereket. De egészen a közelmúltig ezeket a fegyvereket nem használták elég rendszeresen ahhoz, hogy lehetővé tegyék hatásuk folyamatos elemzését. Emiatt a szelektív fegyverek legtöbb értékelése anekdotikus volt. Az elmúlt másfél évtized drónkampányai során több száz csapást mértek militáns szervezetekre, a legtöbbet Pakisztán szövetségi igazgatású törzsi területein, további csapásokat Jemenben, Szomáliában, Irakban és Szíriában. Ez a hosszú időn át tartó támadások nagy száma biztosítja az első lehetőséget annak szisztematikus értékelésére, hogy az ilyen fegyverek tartós használata hogyan befolyásolja az erő alkalmazásának nyilvános támogatását.

Az erő alkalmazásának támogatása

Ez a cikk arra törekszik, hogy megértse, hogy ismertesse, a harci drónok fejlődése hogyan befolyásolja az Egyesült Államok által alkalmazott erő társadalmi támogatását. A közvélemény és a külpolitika kapcsolatának vizsgálata hosszú múltra tekint vissza a politikatudományban. Az e területen a közelmúltban végzett munka nagy része három nagy gondolkodási iskolába sorolható. Az első iskola, és az, amellyel a cikk a legközvetlenebbül foglalkozik, arra összpontosít, hogy az egyének hogyan értékelik a katonai erő alkalmazásának vagy más külpolitikai akciókban való részvételnek a költségeit és előnyeit. Az állami támogatás az előnyök növekedésével, a költségek csökkenésével vagy mindkettővel növekszik. Az erőszak alkalmazásának előnyei közé tartozhat az Egyesült Államok biztonságát fenyegető államok (vagy nem állami szereplők, például terrorista vagy militáns csoportok) elrettentése, az államok és nem állami szereplők arra kényszerítése, hogy olyan intézkedéseket hozzanak, amelyek az Egyesült Államok javát szolgálják, de amelyeket ezek a szereplők egyébként inkább elkerülnének, megakadályozva, hogy ezek a szereplők tömeggyilkosságokat vagy más atrocitásokat kövessenek el, vagy a szövetséges államok támogatása az őket fenyegető veszélyekkel szemben. Jelentős kutatások azt mutatják, hogy a közvélemény különböző súlyokat tulajdonít ezeknek a "fő politikai célkitűzéseknek" az értékéhez, és hogy ezek a súlyok változhatnak, mivel az amerikai érdekeket és értékeket fenyegető veszélyek idővel változnak. Például a hatalmas államok agressziójának elrettentése különösen fontos volt a hidegháború idején, amikor

ez volt az amerikai külpolitika fő célja, míg a terrorizmus elleni küzdelem fontossága a 2001. szeptember 11-i terrortámadások óta nőtt.

Ezen érvelés szerint a közvélemény ezeket a potenciális előnyöket egyensúlyba hozza az erő alkalmazásának költségeivel. A legnagyobb figyelmet a katonai áldozatok kapták, amelyekről bebizonyosodott, hogy következetesen és jelentősen befolyásolják az ilyen hozzáállást. Számos kutatás arra a következtetésre jutott, hogy a katonai áldozatok előfordulása, aránya, otthoni állapota, faji és etnikai hovatartozása, társadalmi-gazdasági státusza, időzítése és keretezése befolyásolja az amerikaiak hozzáállását.

Egy másik fontos költség annak lehetősége, hogy a katonai fellépés nem fogja biztosítani az amerikai érdekeket. A közelmúltban végzett befolyásos munka arra a következtetésre jutott, hogy az amerikai közvélemény hajlandó elviselni a katonai áldozatok kockázatát, ha ez biztosítja a fontos amerikai érdekek biztosítását. Más kutatás vizsgálta, hogy a közvélemény hogyan értékeli az amerikai katonai fellépésből eredő polgári áldozatok költségeit. Egyesek arra a következtetésre jutnak, hogy az ilyen áldozatok kevés szerepet játszanak a polgárok költség-haszon számításaiban, bár az újabb munkák azt sugallják, hogy sokan jelentős súlyt tulajdonítanak annak, hogy elkerüljék a „nem harcosok" károsodását.

Ez a cikk azt kívánja megérteni, hogy a harci drónok használata hogyan befolyásolja ezeket a költség-haszon számításokat. Ez fontos hozzájárulás a közvélemény attitűdjeinek tanulmányozásához. A közvéleményről és az erőszak alkalmazásáról szóló eddigi kutatások többsége gyakran implicit módon feltételezi, hogy a katonai akció az amerikai katonákat a csatatéren éri.

A harci drónok talán legszélesebb körben tárgyalt következménye, hogy a pilóta sebezhetetlensége kiküszöböli a katonai áldozatokat. A drónok szelektivitása a harc számos költségének csökkentésére is képes. Ha a drónok képesek a felkelők és a terrorista szervezetek vezetői ellen irányulni, használatuk alááshatja-e harcosok politikai és katonai hatékonyságát, ami rövidebb vagy kevésbé véres konfliktusokhoz vezethet. A drónok azon képessége, hogy csökkentsék a polgári áldozatok számát a katonai erő más, kevésbé szelektív formáihoz képest, kevésbé veszélyeztetheti a nem harcolók halálát az amerikai közvélemény számára. Ha a drónok csökkentik ezeket a harci költségeket, akkor ez fontos következményekkel járna a konfliktusok kezdeményezésére és folytatására vonatkozó döntésekre nézve. Ha az Egyesült Államok sokkal alacsonyabb költségeket tud fizetni a harcban való részvételért, ez növelheti a fegyverekhez való folyamodásra való ösztönzést, és csökkentheti a békés megoldások megtalálására való hajlandóságot. Ez pedig arra késztetheti az országot, hogy céljai elérése érdekében több, esetleg meggondolatlanabb háborúba kezdjen.

Drónok és a katonai akciók támogatása

Két oka van azt gondolni, hogy a drónok támadásai több támogatást kaphatnak, mint a személyzettel rendelkező repülőgépekkel vagy a földi harci személyzettel történő támadások. Az első az a sebezhetetlenség, amelyet a drónok nyújtanak üzemeltetőiknek. Az Egyesült Államok katonai erejének gyakorlását korlátozó egyik legszélesebb körben elismert korlátozás a politikai vezetők aggodalmai a lakosság áldozatokkal szembeni ellenszenvével kapcsolatban. Egyes beszámolók szerint az amerikaiak nagyon érzékenyek a katonai áldozatokra, és az áldozatok növekedésével gyorsan kiábrándulnak a háborúból. Hasonlóképpen, sok kommentátor annak a félelemnek tulajdonítja az amerikai vonakodást, hogy teljes erejét bevesse a kis háborúkban, attól tartva, hogy az amerikai közvélemény nem hajlandó viselni e konfliktusok költségeit. A baleseti ellenszenv mértéke vitatható, egyes tanulmányok szerint csekély hatása van, hogy jobban befolyásolja az elitet, mint a nagyközönséget, vagy hogy csak más tényezőkkel együtt működik. Mindazonáltal még azok is, akik kételkednek abban, hogy az áldozatoktól való idegenkedés döntő tényező, általában annak tulajdonítják, hogy valamilyen szerepe van a háború támogatásának visszafogásában. Üzemeltetők nélkül a drónok döntően megváltoztathatnák a számításokat arról, hogy mikor kell harcolni, megkönnyítve az Egyesült Államok számára, hogy támogassa szövetségeseit, elrettentse riválisait és részt vegyen a humanitárius beavatkozásokban.

Az izraeli „Searcher"

Másrészt a drónok előnyben részesíthetők más típusú katonai erőkkel szemben, ha úgy ítélik meg, hogy nagyobb valószínűséggel érik el a katonai célokat. A fegyveres drónok csak a közelmúltban kerültek be az amerikai hadsereg arzenáljába, és elsősorban a terrorista és felkelő csoportok elleni küzdelemre vetették be őket. Amint azt az fentebb is láttuk, az ilyen típusú támadások egyik fő problémája a harcosok megkülönböztetése a nem harcolóktól. A drónok szelektivitásának csökkentenie kell annak esélyét, hogy a katonai erő eltévessze célpontját vagy kárt okozzon a nem harcolóknak, amelyek mindegyike visszafogja a katonai akciókban való részvétel támogatását. A drónok még azt is lehetővé tehetik, hogy elkerüljék az alacsony rangú ellenséges személyzet károsodását, akik vezetőik megölése után hatástalanok vagy nem hajlandók harcolni. A drónok technikai képességei különösen hatékonnyá tehetik őket a célpontválasztás problémájának megoldásában, ami arra készteti őket, hogy felvegyék a versenyt a csúcstechnológiájú szuperfegyverekkel szemben, hasonló nagy precizitású és irányítású fegyverekkel.

Politikusok, a hadsereg tagjai és a média kommentátorai bátorították ezt a felfogást azzal, hogy magasztos ígéreteket tettek a drónok képességeire. Az Obama-kormányzat rendszeresen nyilvánosságra hozta a legfontosabb terrorista vezetőket megölő csapások eredményeit, és ezeket bénító akcióknak tulajdonította, amelyek terve az volt, hogy megtámadják az Egyesült Államokat.

Ha a nyilvánosság tagjai úgy látják, hogy a drónok szelektívebbek, mint a személyzettel ellátott repülőgépek és a földi erők, akkor hajlandóbbak lehetnek támogatni a dróncsapásokat. A drónok ezért minden eddiginél hatékonyabban kínálhatják a háború vonzó ígéretét, amely hatékonyabban elégíti ki a diszkrimináció és arányosság elveit. Ez különösen igaz, ha a drónokat a személyzettel ellátott repülőgépekhez hasonlítják, amelyeket a huszadik századi háborúk során e normák legegyértelműbb megsértésének véltek.

A drónhadviselés azáltal, hogy csökkenti a közvélemény konfliktus költségeivel kapcsolatos aggodalmát vagy a rájuk fordított figyelmet, veszélyes következményekkel járhat. Az amerikai katonák védelme az ellenséges tűztől azáltal, hogy fizikailag eltávolítják őket a csatatérről, és drónokkal helyettesítik őket, megkönnyítheti az Egyesült Államok számára a katonai erő alkalmazását, amikor az indokolt. De elősegítheti az agresszív vagy indokolatlan háborúkat is. A háborús költségek csökkentése megszüntetheti a meggondolatlan és szükségtelen konfliktusok felbecsülhetetlen politikai korlátját, lehetővé téve a vezetők számára, hogy könnyebben kezdeményezzenek háborúkat, és elkerüljék a hivatalukból való eltávolítást, ha a háborúk rosszul mennek. A pilóta nélküli fegyverplatformok egyes ellenzői még odáig is elmennek, hogy azzal érvelnek, az a képesség, hogy áldozatok nélkül harcoljanak, drámaian csökkenti a hábo-

rúk kezdeményezésének küszöbét, és elősegíti a nyilvánosság elszakadását az erőszakkal kapcsolatos döntésektől.

Még akkor is, ha a drónok bizonyos küldetések esetében hatékonyabbak, mint más fegyverrendszerek, a szelektivitásukba vetett bizalom veszélyes túlzott támogatáshoz vezethet ezekre a fegyverrendszerekre. Különös aggodalomra ad okot az a lehetőség, hogy "erkölcsi kockázatot" okozhatnak azáltal, hogy olyan mértékben csökkentik a harcok költségeit, hogy az amerikai közvélemény akkor is lelkesedjen az erő alkalmazásáért, ha a győzelem nem valószínű. A végső kockázat itt az, hogy a drónok megugorhatják a szükségtelenül választott háborúk előfordulását, amelyek embereket ölnének meg és tönkretennék az infrastruktúrát, miközben kevés stratégiai előnnyel járnak az Egyesült Államok számára.

A kritikusok azt állítják, hogy a szelektivitásnak a drónok támogatói által kiemelt javulása nagyrészt illuzórikus. A szelektivitást hibahatáron belül mérik, amely mindig esendő, különös tekintettel a drónok hibás működésének esélyére, a tévesen azonosított célpontok elleni támadások indítására vagy az ártatlan járókelők megütésére a terrorista vezetők megölésének folyamatában. Ami még ennél is rosszabb, hogy a drónok szelektívebbnek és pontosabbnak való ábrázolása paradox módon kikövezheti az utat a civilek elleni fokozott erőszak előtt azáltal, hogy megkönnyíti a lakott területeken végrehajtott támadások támogatásának megszerzését.

Míg az amerikai közvélemény azt hiheti, hogy a városok elleni tömeges légi bombázások lelkiismeretlen hatással lennének a civilekre, az embereket vitathatatlanul hamis biztonságérzetbe ringathatják, hogy egy városra irányuló pontos támadások sorozatának alig vagy egyáltalán nincs káros hatása. Ráadásul bizonytalan, hogy az amerikaiak egyáltalán mennyire törődnek a külföldi civil áldozatokkal, különösen, ha az amerikai veszteségek hiánya gyakorlatilag észrevehetetlenné teszi a háború költségeit.

A repülőgépes felderítéstől a drónos felmérésig. Régészeti célú légi fényképezés különböző platformokon

*Dr. Rádai Ödön (1927 - 2004) emlékének**

Dr. habil. Czajlik Zoltán, CSc, tszv. egyetemi docens
ELTE BTK Régészettudományi Intézet, Archeometria, Régészeti Örökség és Módszertan Tanszék
czajlik.zoltan@btk.elte.hu
Dr. Rupnik László, PhD, tudományos főmunkatárs
ELTE BTK Régészettudományi Intézet, Archeometria, Régészeti Örökség és Módszertan Tanszék
rupnik.laszlo@btk.elte.hu

A régészet és a légi fényképezés kapcsolata nem újkeletű, több mint 120 évre nyúlik vissza. A 19. század végén a római *Forum Romanum*ról, később *Ostiá*-ról is készültek légi felvételek, de a leghíresebbé a *Stonehenge*-i kőkör 1906-os fotója vált (1. ábra). Philip Henry Sharpe hadnagy egyik felvétele ugyanis már 1907-ben megjelent az Archaeologia c. folyóiratban és nemcsak a kőkör elemei, hanem más régészeti jelenségek is látszanak rajta. Ezek a korai légi fényképek rögzített ballonokból készültek, közel függőleges, vagy enyhén ferde kameratengellyel, átrajzolásra viszonylag könnyen alkalmazhatók voltak. Problémát

1. Stonehenge (Egyesült Királyság). Katonai ballonrepülés során készített légi fénykép (Philip Henry Sharpe hadnagy felvétele, 1906, BARBER 2011, 20) a kőkörről és a külső földművekről

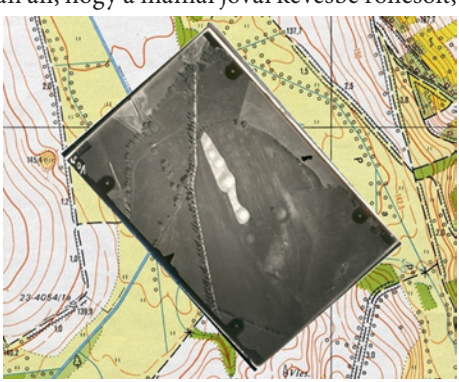
* Dr. Rádai Ödön, aki az idén lenne 95 éves, Tardy János támogatásával rendkívül sokat tett az 1990-es években Magyarországon elterjedő légi régészeti kutatásokért. Akkori segítségükért máig hálával tartozunk.

okozott azonban a ballonok irányítása, a kamerák viszonylag hosszú záridejе (1/100 másodperc), a kis magasság pedig nem engedte meg a komolyabb elmozdulásokat (SZABÓ 2018, 35).

A technikai problémákra – ha nem is azonnal – de reális választ adott az új platform használata. Az első világháborúban a légi felderítésre már repülőgépeket alkalmaztak. Az új eszközt elsősorban manőverező képessége tette hatékonnyá, de a repülési magasság növelése is hasznos volt. Fejlődtek a kamerák, az új Zeiss-berendezések legrövidebb záridejе már 1/600 másodperc volt (SZABÓ 2018, 47), ami – a gépek akkori sebességét is figyelembe véve – már viszonylag kis magasságból is lehetővé tette az éles, jó minőségű felvételek elkészítését. Ezek nyersanyaga üvegnegatív volt, amit az 1930-as évektől váltottak fel a kevésbé kényes celluloid-filmek.

A felderítő légi régészeti kutatások az első világháborúban kezdődtek el. Theodor Wiegand, az isztanbuli Német Régészeti Intézet igazgatójának szervezésében már 1916-tól szisztematikusan fényképezték a régészeti lelőhelyeket a Negev-sivatagban (Sínai-félsziget). A leghíresebbé George Adam Beazeleynek a Royal Air Force segítségével, az első világháború végén, a Tigris és Eufrátész mentén végzett repülései váltak, amelyek során – részben az ellenséges vonalak mögé is berepülve – óriási romvárosokat, csatorna-rendszereket térképezett fel.

Magyarországon – Európai összehasonlításban is nagyon korán – már az 1920-as években megkezdték a régészeti lelőhelyek légi fotózását. Ebben úttörő szerepe volt Neogrády Sándornak, aki az első világháborúban az észak-olasz fronton felderítő légi fényképezéseket folytatott, majd az egyik megszervezője lett az önálló magyar állami légi felvételezéseknek. Feladata elsősorban a topográfiai térképezéshez szükséges légi fényképes alapok biztosítása volt, de már 1924-től régészeti lelőhelyekről is készített felvételeket (NEOGRÁDY 1948-1950, 289). Neogrády felvételei többnyire akkor már ismert régészeti lelőhelyekről készültek (2. ábra), ezek fontossága elsősorban abban áll, hogy a mainál jóval kevésbé roncsolt, a nagyüzemi mezőgazdaság megjelenése előtti állapotokat rögzítettek.



2. Nagyberki – Szalacska (Somogy vármegye) A kora vaskori halomsírmező északi halomcsoportja. Neogrády Sándor archiv felvetele, 1929. július. A törött üvegnegatívot Suba János azonosította az MN Hadtörténeti Intézet gyűjteményében, digitális restaurálását es EOTR-térképbe való beillesztését Holl Balázs készítette el 2005-ben

A dunapentelei (ma Dunaújváros) Koszider-asztalról készített fotója pedig egy azóta teljes mértékben beépített területről biztosít számunkra régészeti információkat.

Az 1920-as évek legfontosabb változása a légi régészetben az a felismerés, hogy a kutatások nemcsak, sőt nem elsősorban a már ismert lelőhelyek esetében fontosak, ennél jóval nagyobb jelentőségűvé vált az új lelőhelyek felfedezése, dokumentálása. Ennek nemzetközi szinten a legfontosabb kutatója Osborne Guy Stanhope Crawford volt, aki már 1923-ban meg volt győződve arról, hogy a módszer új korszakot nyit a brit (azaz a világ) régészetében (CRAWFORD 1923). Felismerte, hogy a talaj és a növényzet elszíneződései, valamint az elsősorban a ferde megvilágítás révén megmutatkozó domborzati anomáliák régészeti jelenségekről biztosítanak számunkra információkat. Erre jött rá ugyanebben az időszakban Neogrády Sándor is, aki egy 1950-ben megjelent munkájában először rendszerezte magyarul azokat a tényezőket, amelyek alapos ismerete mindmáig feltétele az eredményes légi régészeti kutatásoknak (NEOGRÁDY 1948-1950).

A második világháború az éppen kialakuló légi régészeti kutatásokat teljesen ellehetetlenítette, ugyanakkor – elsősorban Nyugat-Európában – rengeteg katonai felderítő légi fényképezés folyt. A főként az angolszászok által készített anyagok nagy része elérhető a National Collection of Aerial Photography, NCAP, Edinborough, https://ncap.org.uk/collections) rendszerén keresztül COWLEY et al. 2013). A II. világháború előtti hazai légi felvételek a Hadtörténeti Intézet és Múzeum Hadtörténeti Térképtárában, az 1953-tól készült térképészeti célú anyagok a HM Zrínyi Nonprofit Kft. gyűjteményében, az 1959-től a polgári célú térképzések számára rögzített légi fényképek pedig a Lechner Tudásközpontban vannak (részletesebben lásd: MIKLÓS et al. 2011, BÖDŐCS et al. 2019). Közös jellemzőjük, hogy régészeti szempontból nem optimális időszakban (általában tavasszal) és az ideális 300 m helyett jóval magasabbról készültek. Ennek ellenére sikeresen használják őket nagyobb régészeti jelenségek, így a római kori határvédelmi rendszer, a *ripa Pannonica* kutatásában (VISY 2000).

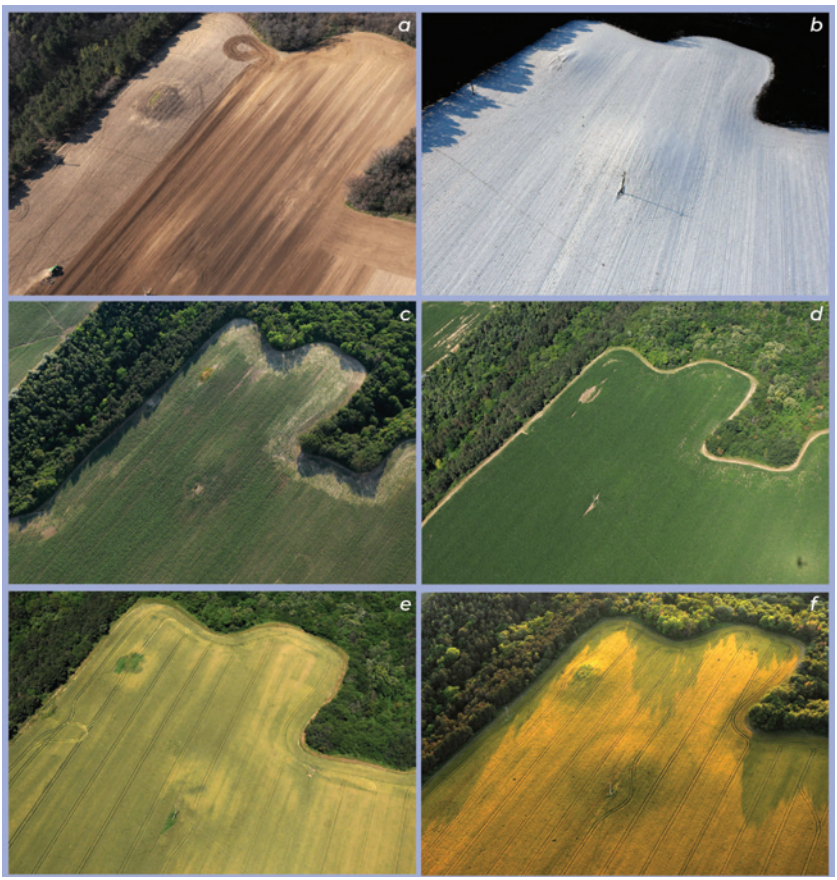
Az 1960-as évek végétől a régészetben is új platformot jelentett a műholdak alkalmazása. Az értékelhető minőségű és térbeli felbontású anyagok 1995-től, az Egyesüld Államok kém-műholdjai által készített felvételek felszabadításával (Declassified Intelligence Satellite Photography, azaz DISP) váltak elérhetővé. Legsikeresebb alkalmazási területük a más módon nehezen kutatható kis-ázsiai és közel-keleti régió. A műholdas platform igazi népszerűségét a régészeti kutatásokban a 2009 óta ingyenesen hozzáférhető Google Earth-rendszer hozta meg. Ritka kivételektől eltekintve a műholdas anyagok sem a közép-európai szempontból legfontosabb kora nyári időszakban készültek és a térbeli felbontásuk is csak a legutóbbi időkben kezd alkalmassá válni a régészeti jelenségek

megfigyelésére. Ugyanakkor számos, nagyobb kiterjedésű, vagy markánsabb megjelenésű régészeti lelőhely, így a várak, erődítések nyoma azonosítható segítségével (összefoglalóan lásd: KUZMA 2013).

A felsorolt platformok mellett a II. világháború után először Nagy-Britanniában, majd fokozatosan egész Európában egy új platform, a kisgépes, ferdetengelyű légi fényképzés kezdett elterjedni. Részben a jól manőverezhető sportrepülőknek (főként a Cessna-típusoknak), részben a professzionális kisfilmes kameráknak és a fordítós filmeknek köszönhetően az 1970-es évek végére a módszer a régészeti légi fényképezés legfontosabb eljárásává vált. Félmillió fotót meghaladó régészeti gyűjtemények (pl. Cambridge, München) jöttek létre, a hidegháború végén, az 1990-es évektől pedig megkezdődött a ferde tengelyű, kézi kamerás technika közép-európai adaptációja. Az újonnan létrejövő gyűjtemények (pl. Poznan, Ljubljana, Budapest, Pécs) viszonylag hamar, a 2000-es évektől átálltak a digitális kamerák használatára.

Az elsősorban a szántóföldi gabona-növények kora nyári éréséhez kötődő gabona-jeleknek köszönhetően Magyarország jelentős része (a Dunántúl északi és keleti része, valamint a Duna – Tisza-köze) nagyon hatékonyan kutatható a kisgépes módszerrel (3. ábra). A két nagyobb hazai gyűjteményben (ELTE BTK Régészettudományi Intézet Légifotó Archívuma, Budapest); illetve PTE BTK Légirégészeti Téka, Pécs) sok ezer, korábban ismeretlen régészeti lelőhelyről őriznek felvételeket. A digitális technológiának köszönhetően a módszer korábbi Achilles-sarka, a felvételek térképi illesztése és aprólékos, térinformatikai rétegekre bontott interpretációja is megoldhatóvá vált, nagy, összefüggő területekről készíthetők légi fotó térképek (CZAJLIK et al. 2011).

A hagyományos repülőgépekkel végzett felderítésnek is megvannak azonban a korlátai. A nagyobb repülési magasság, a körözésen alapuló röppálya és a magasabb fajlagos költség miatt egy-egy lelőhely részletes, térképészeti igényű felmérésére a módszer nem ideális. Mindeközben a régészet fejlődése töretlenül és gyorsan halad a rendelkezésre álló adatok térinformatikai környezetben történő integrációjának és elemzésének irányába. Az eredetileg katonai célokra fejlesztett drónok polgári felhasználásban történő fokozatos elterjedésének köszönhetően megjelent az ehhez szükséges új platform a régészeti kutatásban. A drón mellett leggyakrabban használt – részben katonai környezetből átvett – UAV (Uncrewed/*Unmanned Aerial Vehicle*) vagy UAS (*Unmanned Aerial System*) kifejezések mellett számos további mozaikszó is elterjedt (REMONDINO 2014) A magunk részéről egyetértünk azzal a felvetéssel, hogy a távolról vezérelt légi jármű (RPAS – *Remotely Piloted Aircraft System*) szavatosabban írja le ezt a kategóriát (SZABÓ 2016, 60-65; SZABÓ 2018, 149). Az ide tartozó légi járművek műszaki szempontból rendkívül sokfélék. A meghajtás nélküli, levegőnél könnyebb eszközök,



3. Süttő – Sáncföldek (Komárom – Esztergom megye). A kora vaskori halomsírmező ÉK-i része 2013-2018 között Cessna kisgépből, illetve Robinson helikopterből fényképezve (Czajlik Zoltán felvételei)

mint a ballonok és sárkányrepülők a légi régészet hőskoráig nyúlnak vissza, de szerepük egyre kisebb. Eközben a motorral rendelkező merev- és forgószárnyas járművek mennyisége és jelentősége egyre nő a nemzetközi és hazai régészeti kutatásban egyaránt. A fejlődés iránya világos, egyre hosszabb ideig, egyre nagyobb tömeget magasba emelő, egyre távolabbra küldhető eszközök válnak elérhetővé. A rendelkezésre álló technikai lehetőségeknek a pilóta képességei mellett, elsősorban a légi közlekedés biztonságát szem előtt tartó jogi szabályozás szabhat határt.

Jelen kiadvány kereteit meghaladná a távolról vezérelt légi járművekkel végzett szerteágazó régészeti kutatások történetének részletes ismertetése. A módszer régészeten belüli terjedése nem is irható le lineáris folyamatként, számos műhelyben, egymástól függetlenül zajlik a fejlesztés. A 2000-es években általában egyedi tervezésű és építésű, komoly mérnöki tudást igénylő légi járművek születtek (PRENTISS 2016). A technológia gyors fejlődése és a fokozódó kereslet hatására a piacon elérhető drónok egyre fejlettebbé váltak, ami a házi fejlesztéseket részben okafogyottá tette, ugyanakkor kedvezett a távolról vezérelt légi járművek szélesebb körben történő elterjedésének.

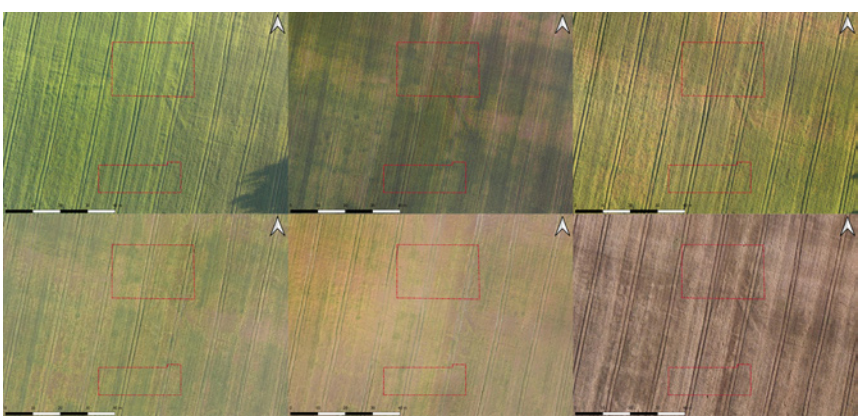
A magyarországi régészeti kutatás szintén felismerte az új platformban rejlő lehetőségeket. Szabó Máté és Balogh András a Cserdi mellett található, nagy kiterjedésű római villagazdaság kutatása során tesztelte és fejlesztette az egyes eszközöket és adatgyűjtési módszereket. Repüléseik során FPV (First Person View) technológiát, merev- és forgószárnyas eszközöket egyaránt alkalmaztak a lelőhely részletes vizsgálatára. Az eltemetett falak feltérképezéséhez előre programozott nyomvonalon haladó légi jármű által készített felvételek sokaságán alapuló, geodéziai GPS-szel bemért földi illesztő pontokkal georeferált (GCP) fotó 3D feldolgozást hívtak segítségül BALOGH–SZABÓ 2013; SZABÓ 2016, 60-75). A távolról vezérelt légijárművel készített fényképeken alapuló ortofotók és digitális felületmodellek egyik első alkalmazása volt a bodajki honfoglaláskori temetők feltárásának és környezetének dokumentálása, amelyet Mészáros János készített el. Harkakötöny határában pedig szarmata temető halomsírjainak dokumentálásában, illetve addig nem ismert temetkezések felfedezésében mutatkoztak meg az új módszer előnyei (MÉSZÁROS et al. 2017). A ferde tengelyű, konvencionális felvételek mellett a drónnal készített légi felvételeken alapuló ortofotók és 3D modellek a csókakői vár feltárásainak és még álló falainak dokumentálásában is szerepet kaptak (POKROVENSZKI et al. 2016). A pozitív példák sorolását hosszan lehetne folytatni, az új platform régészeti célú használata örvendetes módon terjed. Ugyanakkor a folyamat nem egységes és nem egyenletes, a szükséges szakemberek és az anyagi források megléte vagy hiánya nagymértékben befolyásolja.

Az ELTE BTK Régészettudományi Intézetének kutatásaiban 2016-ban kezdtük el a távolról vezérelt légi járműveket alkalmazni. Előbb a DJI Phantom 4 típus két változata (Advanced, Pro), később ugyanezen gyártó Mavic 2 Pro kvadrokoptere került beszerzésre. A korábbi nemzetközi és hazai tapasztalatok alapján törekedtünk az eszközökben rejlő lehető legnagyobb potenciál régészeti célú kihasználására.

A legegyszerűbb alkalmazási terület, amikor egy ismert régészeti helyszínről, álló emlékről vagy ásatásról készülnek új perspektívából felvételek, amelyek

főként illusztrációs, illetve a helyszín jobb megértését elősegítő célból készülnek. Ezekben az esetekben nem feltétlenül új adatok, növényi- vagy talajjelek felfedezése az elsődleges cél, bár ideális körülmények között ez sem zárható ki, hanem a más nézőpont adta lehetőségekből táplálkozó tudományos gondolkodás elindítása. Sok helyszín kifejezetten nagy kiterjedésű, a földfelszínről nem átlátható, teljes bejárása csak sok idő ráfordításával, vagy a növényzeti fedettség, rossz megközelíthetőség miatt egyáltalán nem oldható meg. A lelőhely állapotának felmérésében, az esetleges rongálások dokumentálásában is szerepet játszhatnak ezek az eszközök.

A lelőhelyek hagyományos légi régészeti módszerekkel történő felderítésére ezek a távolról vezérelt légi járművek kevésbé alkalmasak. Ugyanakkor egy-egy kisebb, a korábbi kutatások vagy egyéb adatok miatt fontosnak ítélt terület ellenőrzésére, vagy alaposabb átvizsgálására költséghatékonyabb megoldást kínálnak. Brigetió római kori legiotáborának helye régóta jól ismert, a korábbi hagyományos légi felderítések során több esetben sikerült a romokra utaló növényzeti jeleket dokumentálni. A terület jobb megismerésének reményében 2016 nyarán eltérő fényviszonyok és a gabona fejlődésének különböző fázisai mellett folyamatosan vizsgáltuk a lelőhelyet (4. ábra). Ennek során más és más részletek, régészeti jelenségek növényi jelei voltak élesebben megfigyelhetők. Földi illesztőpontok alkalmazásával vagy RTK képességű drón használata esetén ezek az eltérések pontosan térképre vihetők.



4. Szőny/Brigetió (Komárom – Esztergom megye). A brigetiói római katonai tábor északi bejárata. Rupnik László 2016. májusa és júliusa között készült drónfelvételei

Napjainkban a távolról vezért légi járművek régészeti célú alkalmazásának messze legfontosabb területévé a fotogrammetriai feldolgozást célzó felmérések váltak (DE REU et al. 2013; BALOGH–KISS 2014; SZABÓ 2016, 66-73). Ezek a repülések főbb technikai alapjaikat tekintve kevéssé térnek el a földtudományok, vagy akár az építőipar, bányaipar gyakorlatában alkalmazott módszerektől. Bizonyos részletekben a pontos régészeti cél függvényében viszont különbözők lehetnek.

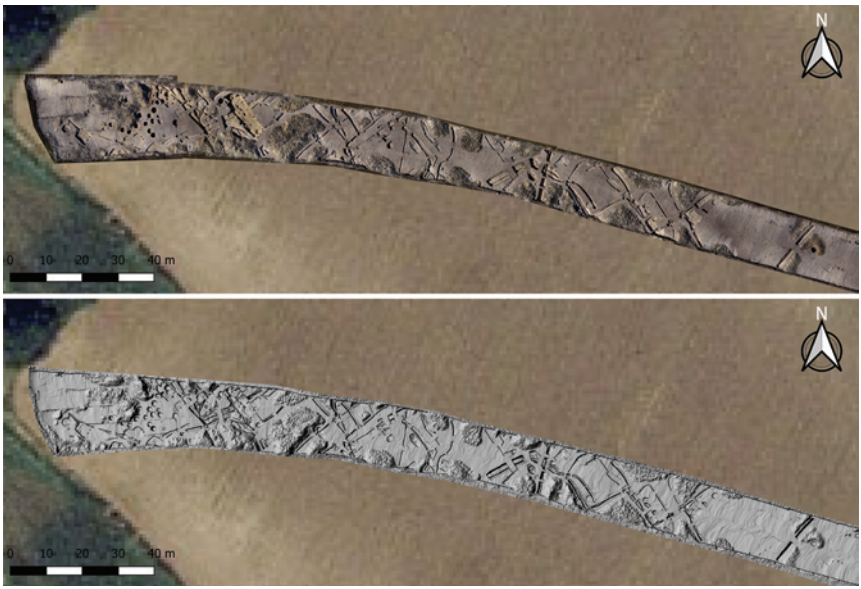
Ilyen cél lehet a régészeti feltárás területének és közvetlen környezetének dokumentálása, a kibontott jelenségeket mutató ortofotó és felületmodell készítése. A kis felületű, néhány tíz négyzetméteres területű tervásatásoktól, a több hektáros, építkezéseket megelőző régészeti feltárásokig egyaránt alkalmaztuk a módszert. Célunk elsősorban a hagyományos leíró és rajzos régészeti dokumentáció kiegészítése volt, de tapasztalataink alapján a rajzi dokumentációs folyamatok jelentős részét a fotó 3D technológia kiválthatja. Ennek integrálása a régészeti protokollba még hiányzik, a módszer még keresi pontos helyét a szakmai gyakorlatban. Ennek legfőbb oka, hogy a régészeti rajzi dokumentálás hagyományosan egy megfigyelő és értelmező folyamattal jár együtt, amelynek során a fontosabb dolgok kiemelésre a kevésbé jelentős részletek pedig akár elhagyásra kerülhetnek. Ez a fázis a légi felvételezés során kimarad, illetve egy későbbi időpontra, a laboratóriumi utómunkára helyeződik át. Ez magában hordozza annak lehetőségét, hogy lényeges információk elvesznek. A rajzolás sok esetben rendkívül időigényes folyamat, amiből az építkezésekhez kapcsolódó régészeti szakfeladatok ellátása során az esetek túlnyomó többségében kevés áll rendelkezésre. Amennyiben az építkezés nem rombolja a régészetileg érintett rétegeket, a feltárás helyett foltdokumentációra és a jelenségek elfedésére kerül sor. A gyakorlatban ez sokszor azt jelenti, hogy órákban mérhető az az idő, ami alatt a dokumentálást el kell végezni. Ez egy több hektáros terület esetében más módszerrel, mint a légi fényképezés és fotogrammetria alkalmazása, nem képzelhető el. Hasonló a helyzet a mezőgazdasági művelés alatt álló területeken, ahol a mélyszántás által felszínre forgatott régészeti objektumok nyomainak dokumentálására csak egy nagyon rövid időablak áll régész rendelkezésére. Ezekben az esetekben a távolról vezérelt légi jármű olcsó, rugalmas használhatósága, illetve az egységnyi idő alatt lefedhető terület nagysága jelenti a döntő előnyt. A kisebb felületű és tervszerű ásatások esetében ezek a szempontok kisebb súllyal esnek a latba. Ugyanakkor a fotó 3D által nyújtott modellek és ortofotók a munka folyamatos, bontási fázisonként elvégzett fényképezésével az ásatás háromdimenziós nyomon követését teszik lehetővé. Olyan összetett felületek, mint például a tető- vagy freskóomladékok a földi és/vagy légi alapú fényképezés (hibrid) alkalmazásával a rajzi dokumentálás pontosságát és részletgazdagságát meghaladva örökíthetők meg.

A magunk részéről úgy gondoljuk, hogy a tapasztalatok növekedésével kidolgozható az a gyakorlat, amelyben az régészeti munkák légi távérzékelésen alapuló dokumentálása megtalálja a maga helyét.

Az említett esetek a távolról vezérelt légi jármű használata a repülési profil és fényképezési módszer szempontjából sokféle lehet. A kisebb szelvények dokumentálásánál, mint például a brigetiói *porta praetoria* feltárása (5. ábra) a repülési magasság alacsony: a néhány méteres relatív magasságtól legfeljebb 10-15 méterig terjed. A repülést és fényképezést ilyenkor teljesen a pilóta végzi, az

5. Szőny/Brigetió (Komárom – Esztergom megye). A brigetiói római katonai tábor északi bejáratának feltárása (2020, ásatásvezető Bartus Dávid). A drónfelvételek alapján készített ortofotó mozaik Rupnik lászló munkája.

automatikus repülési profilok szerepe kisebb. Ez egyúttal azt is jelenti, hogy az optimális képmennyiség és képek közötti átfedés biztosításához megfelelő gyakorlatra van szükség. A függőleges tengelyű felvételek mellett elegendő számú ferde tengelyű képre is szükség van, annak érdekében, hogy a felület tagoltságából, illetve holt zónákból fakadó hibákat a későbbi 3D modellből kiküszöböljük. Példaként a Pusztaszabolcs melletti vasútépítkezést megelőző feltárás közeli légi távérzékelésen alapuló felmérését és fotogrammetriai utófeldolgozását említjük (6. ábra). Ezen a helyszínen a repülés relatív magassága 15-25 méter között volt, automatikus repülési útvonalat nem alkalmaztunk. A felvételek illesztéséhez földi kontrollpontokat használtunk (GCP). A repülési magasság megválasztá-



6. Pusztaszabolcs – Dohányos-völgy, északi part (Fejér megye). A feltárások drónfelvételek alapján készített ortofotó mozaikja (felül) és árnyékolt domborzat-ábrázolása (VÁCZI et al. 2020, fig. 4; készítette Rupnik László).

sában a részletgazdagság és a rendelkezésre álló akkumulátorok száma közötti kompromisszum megtalálására törekedtünk. Szem előtt tartottuk azt is, hogy ne gyűjtsünk be indokolatlanul sok adatot, mivel mind a tárolás, mind az utófeldolgozás esetében a hardveres lehetőségek korlátozottak. A felmérés eredményei itt nem váltották ki a rajzolást, de azok digitalizálása és a térképek elkészítése során nagy segítséget nyújtottak az esetleges hibák pontosításában és az utódokumentáció elkészítésében. Emellett a lelőhelyhez tartozó további régészeti jelenségek pozitív növekedési jeleit is dokumentáltuk a nyomvonal melletti területen.

A régészeti feltárások felmérése mellett ez a módszer lelőhelyek területéről készített felület, illetve az abból levezetett domborzatmodellek készítésére ugyancsak alkalmas. Ez különösen a földépítmények (sáncok, utak, árkok, halmok) esetében igazán fontos eszköz, mint például a Süttő-Sáncföldek lelőhelyen található, kora vaskori halomsírmező (7. ábra). A kutatási terület északi részéről rendelkezésre állt légi lézerszkennelésen (korábban lásd: CZAJLIK et al. 2019, fig. 14) alapuló domborzatmodell, amelyet az erdő által nem borított déli zónában fénykép alapú 3D felméréssel egészítettünk ki. A közel 75 hektáros területet hat repüléssel, több különböző időpontban, részben hóval, részben néhány centire kikelt vetéssel borított felszín mellett végeztük el. Ekkora területnél a felmérést előre programozott

7. Süttő – Sáncföldek (Komárom – Esztergom megye). Repülőgépes lézeres szkenneléssel (északi rész, feldolgozás: Király Géza) és drónos fotogrammetriai módszerrel (délnyugati rész, repülés és feldolgozás: Rupnik László) készített felületmodell.

módon, DJI Ground Station és Drone Deploy alkalmazásokban terveztük meg és hajtottuk végre. A frontális átlapolás 75%, míg az oldalsó 65 % volt. A repülési magasság 50-70 méter volt, ami 1,5-2 cm körüli kiinduló felbontást tettek lehetővé. A kihelyezett földi illesztőpontok valós idejű korrekcióval ellátott GPS-szel történő bemérésének köszönhetően az ortofotó és a felületmodell néhány centiméteres pontossággal illeszthető volt. Az utófeldolgozást Agisoft Metashape szoftverben végeztük el. Az elkészült domborzatmodell kiegészítette az ALS felmérés területét és alapul szolgált az egyéb módszerekkel történő régészeti adatgyűjtés térinformatikai feldolgozása számára (8. ábra). A módszer számos további helyszín esetében alkalmazható, a külföldi és hazai példák egyértelműen mutatják, hogy az épített örökség emlékeinek felmérésében ugyancsak nő a szerepe.

Az ismertetett példák a viszonylag könnyen elérhető, alacsonyabb áru, RGB kamerával ellátott távolról vezérelt légi járművekkel végezhető feladatokba engednek betekintést. Ezek a légi járművek, méretüktől függően ugyanakkor platformként szolgálhatnak hő-, multispektrális- vagy hiperspektrális kamerák, vagy lézerszkenner számára. A cikk írásával párhuzamosan került beszerzésre egy multispektrális kamerával felszert DJI Phantom 4 kvadkopter az ELTE BTK

8. Süttő – Sáncföldek (Komárom – Esztergom megye). Magnetométeres felmérés eredményeinek (feldolgozás: Puszta Sándor) megjelenítése a drónos fotogrammetriai módszerrel készített felületmodellen (repülés és feldolgozás: Rupnik László).

Régészettudományi Intézetében. A Magyar Nemzeti Múzeum Nemzeti Régészeti Intézete pedig egy DJI Matrice által hordozott lézerszkennerrel végzett felméréseket többek között Oroszlány-Gyertyános római kori villájának és Felsőpetény középkori templomának helyén, illetve annak környezetében*. Hasonló drónos lézerszkennelések az ELTE BTK Régészettudományi Intézete számára is készültek Ács, illetve Süttő környékén.

A fejlődés remélhetőleg folytatódik és egyre több intézménynek lesz megfelelő háttere a különböző érzékelőkkel ellátott, távolról vezérelt légi járművek használatához. Jelenleg még kisebb kihívást jelent, de idővel a nagy mennyiségű adat kezelésének kérdése kerülhet előtérbe. Emellett a légterek zsúfoltsága és az ezzel járó kockázatok jogi és gyakorlati környezetének alakulása jelentősen befolyásolhatja a távolról vezérelt légi járművek elterjedését, a régészeti kutatásban betöltött valódi szerepét.

** Látos Tamás és Vida István szóbeli közlése alapján.*

Záró gondolatok

A távérzékeléses régészeti kutatások története és aktuális technikai lehetőségei is azt mutatják, hogy a módszer sikeressége erőteljesen függ az elérhető platformok alkalmazásától. Vannak eljárások, amelyeket bár kipróbáltak (ballonos repülések) hamar kikerültek a gyakorlatból, nehézkességük, magas költségeik miatt. Ugyanakkor az ásatási területek precíz, térképészeti minőségű dokumentálásának igénye fennmaradt, amit az elérhető áru, fejlett technológiájú, távolról vezérelt légi járművek mai gyors terjedése jelez.

A kisgépes légi régészeti kutatás fejlődése sem volt töretlen, sajátos, költséghatékony módszerei csak az 1960-as évektől kezdtek igazán elterjedni. A módszer egy-egy lelőhely megfigyelésére, dokumentálására soha nem számított hatékonynak. Ugyanakkor az a tény, hogy e technológia korszerűsített változatával kedvező időjárási körülmények esetén néhány nap alatt fél Magyarország átkutatható légi régészeti szempontból, egyelőre a felderítések során ezt a módszert a drónnal szemben is versenyképessé teszi.

Példáinkkal (Brigetió, Süttő) arra igyekeztünk rávilágítani, hogy a különböző platformok használata nem váltja ki egymást, feladattól függő kombinálásuk hozza a legjobb eredményeket, amint arra a százhalombattai halomsírmező 2015-2016-os kutatása (részletesen lásd: T. NÉMETH et al. 2016) is rávilágított (9. ábra)

9.a. Százhalombatta – Százhalom (Pest megye), kora vaskori halomsírmező részlete. A 49-es halom és környezete repülőgépes légi felvételen (Czajlik Zoltán, 2015. február 7.)

9.b. Százhalombatta – Százhalom (Pest megye), kora vaskori halomsírmező részlete, a 49-es halom a feltárást követően (ásatásvezető: T. Németh Gabriella). Czajlik Zoltán repülőgépes légi fotójába illesztett drónfelvétel (Rupnik László, 2016. október).

Köszönetnyilvánítás

Kutatásainkat az Iron-Age-Danube Interreg Európai Uniós program, az NKFIH 119520-as, 134522-es és 134635-ös pályázatai, a Felsőoktatási Kiválósági Program és a Tématerületi Kiválósági Program támogatták.

Irodalomjegyzék

Balogh A. – Kiss K.: Robotrepülőkkel készített légifelvételek feldolgozása/ Photogrammetric processing of aerial hotographs acquired by UAVs. Magyar Régészet/ Hungarian Archaeology 2014 tavasz (Spring 2014), 1-8.

Balogh A. – Szabó M.: RPAS – robotrepülők a régészet szolgálatában/Robot planes in the service of archaeology. Magyar Régészet/Hungarian Archaeology 2013 tél (Winter 2013), 1-7.

Barber, M.: A History of Aerial Photography and Archaeology. Mata Hari's glass eye and other stories. Swindon 2011.

Bödőcs, A. – Rupnik, L. – Doneus, M.: Archival and cartographic aerial photographs,

satellite images. In: Czajlik,Z. – Črešnar, M. – Doneus, M. – Fera, M. – Hellmuth *Kramberger, A. – Mele, M. (eds.):* Researching Archaeological Landscapes Across Borders. Strategies, Methods and Decisions for the 21th Century. Graz – Budapest 2019, 86-90.

Cowley, D. C. – Ferguson, L. M. – Williams, A.: The Aerial Reconnaissance Archives: A Global Photographic Collection.In: Hanson, W. – Oltean, I. (eds): Archaeology from Historical Aerial and Satellite Archives. New York 2013, 13-30. DOI 10.1007/978-1-4614-4505-0_2

Crawford, O. G. S.: Air Survey and Archaeology. The Geographical Journal 61,5 (1923) 342-360.

Czajlik, Z. – Rupnik, L. – Losonczi, M. – Timár, L.: Aerial archaeological survey of a buried landscape: The Tóköz project.In: Cowley, D. C. (ed.): Remote Sensing for Archaeological Heritage Management. Proceedings of the 11th EAC Heritage Management Symposium, Reykjavik, Iceland, 25-27 March 2010. Bruxelles 2011, 235-241.

Czajlik, Z. – Fejér, E. – Novinszki-Groma, K. – Jáky, A. – Rupnik, L. – Sörös, F. Zs. – Bödőcs, A. – Csippán, P. – Darabos, G. – Gergácz, R. – Györkös, D. – Holl, B. – Király, G. – Kürthy, D. – Maróti, B. – Merczi, M. – Mervel, M. - Nagy, B. – Puszta, S. – B. Szöllősi, Sz. – Vass, B. – Czifra, Sz.: Traces of prehistoric land use on the Süttő plateau. In: Črešnar, M. – Mele, M. (eds.): Early Iron Age Landscapes of the Danube Region. Graz – Budapest 2019, 185-219.

De Reu, J. – Plets, G. – Gheyle, W. – Bourgeois, J. – Verhegge, J.: Towards a three-dimensional cost-effective registration of the archaeological heritage. Journal of Archaeological Science 40 (2013), 1108–1121.

Kuzma, I.: Archeologicke naleziska na Google Earth. Študijne zvesti 53 (2013) 183-230.

Mészáros J. – Pánya I. – Petkes Zs. – Szücsi F.: Térinformatika és fotogrammetria alkalmazási lehetőségei a régészetben.In: Dr. Balázs Boglárka (szerk.) Az elmélet és a gyakorlat találkozása a térinformatikában VIII. (Theory meets practice in GIS) Debrecen 2017, 223-231.

Miklós Zs. – Bödőcs A. – Czajlik Z. – Szabó M. – Visy Zs.: Légi fényképezés. In: Müller R. (főszerk.): Régészeti kézikönyv. Budapest 2011, 40-70.

Neogrády S.: A légifénykép és az archeológiai kutatások. Térképészeti Közlöny 7 (1948-1950) 283-332.

Gabriella T. Németh – Zoltán Czajlik –Katalin Novinszki-Groma – András Jáky: Short report on the archaeological research of the burial mounds no. 64. and no. 49. at Érd-Százhalombatta. DissArch Ser. 3. No. 4 (2016) 291-306.

Pokrovenszki, K. – Vágvölgyi, B.- Tóth, Z.: A csókakői vár feltárása során alkalmazott 3D fotogrammetriai módszerek gyakorlati tapasztalatai / Practical experience with the 3D photogrammetric methods used at the excavation of Csókakő Castle. Magyar Régészet / Hungarian Archaeology 2016 ősz (Autumn 2016), 31-38.

Prentiss, A. M. (ed.): Drones in archaeology. Special issue. The SAA archaeological record 16/2 (2016)

Remondino, F.: UAV: Platforms, regulations, data acquisition and processing. In: Remondino, F. – Campana, S. (ed.): 3D Recording and Modelling in Archaeology and Cultural Heritage. Theory and best parctices. BAR International Series 2598, 2014, 74-90.

Szabó M.: Régészet madártávlatból. Fejezetek a Pécsi Légirégészeti Téka 20 éves történetéből. Budapest 2016.

Szabó M.: Repülés a múltba. A légi régészet története. Pécs 2018.

Váczi, G. – Rupnik, L. – Czajlik, Z. – Mesterházy, G. – Bittner, B. – Fülöp, K. – M. Löhnhardt, D. – Szabó, N.: The results of a non-destructive site exploration and a rescue excavation at the site of Pusztaszabolcs – Dohányos völgy északi part. Dissertationes Archaeologicae Ser. 3. 8 (2020) 165-179.

Visy Zs.: A ripa Pannonica Magyarországon. Budapest 2000.

A drónok veszélyei

Dr. Őszi Arnold, egyetemi adjunktus
Óbudai Egyetem Gépészeti és Biztonságtudományi Intézet, Biztonságtechnikai Intézeti Tanszék
oszi.arnold@bgk.uni-obuda.hu

Tartalmi összefoglaló

A drónok iparága nagyon látványosan, robbanásszerűen fejlődik. Ami ma itt a csúcstechnológia, az néhány hónap múlva már lehet, hogy elavultnak számít. Egyre szélesebb a paletta mind a tudásban, mind pedig az árban. A komolyabb darabok igen nagy felszállótömeggel, hosszú repülési idővel és lélegzetelállító technikai tudással is rendelkezhetnek.

Ennek a ténynek a következménye, hogy egyre kevesebb összegből lehet megvásárolni ezeket az egyre több képességgel rendelkező, akár gyerekek számára is irányítható eszközöket.

Kire jelentenek ezek az eszközök veszélyt? Tudni kell, hogy hazánkban minden egyes évben 10%-kal növekszik a nagy és kisgépes légiforgalom. Ez azt jelenti, hogy a kereskedelmi és egyéb repülés egyre jobban kihasználja a rendelkezésre álló légtereket. Ugyanakkor a drónok száma ennél az említett értéknél sokkal drasztikusabb mértékben emelkedik. Így könnyen belátható, hogy egyre növekszik az összeütközés veszélye is. Már 2020-ban is igen jelentős, 10.000-es nagyságrendű volt a drónok száma Magyarországon.

Egy esetleges drón-repülőgép ütközés a vizsgált esetekben végzetes kimenetelű a kisebbik félre nézve, ugyanakkor jelentős károsodást tud szenvedni a repülőgép szárnya, hajtóműve, vagy egyéb elemei is. Tisztán látható, hogy egy ilyen baleset nagyon könnyen végződhet súlyos katasztrófával. Ezért kell kiemelt figyelemmel kezelni ezt a kérdést.

Jelenleg a különböző nemzetközi szabályzások biztosítják azt, hogy a légijárművek egymástól elkülönítve közlekedjenek. Esetünkben saját, egyéni légteret kap minden drón, amelyet csak ő használhat egyedül, így szintén kizárt az ütközés veszélye.

Azonban mindig vannak olyan esetek, amikor a pilóta nem tartja be a szabályokat. Erre számos példát láttunk már a világban, de országunkban is. Ezeket a légi járműveket első körben detektálni kell. Amennyiben ez sikeres, akkor következik az azonosítás fázisa, ahol ki kell deríteni, hogy jogszerű-e a levegőben tartózkodás. Amennyiben nem, akkor következik a beavatkozás, végül pedig a szankcionálás.

Elő szokott fordulni, hogy ezek a szerkezetek valamilyen oknál fogva egyszerűen leesnek az égről. Egy zuhanó nagyobb tömegű drón jelentős sérüléseket

tud okozni, ezért számolni kell ezzel a veszéllyel is. Napjainkban döntő többségben lítium-polimer (Li-Po) cellákban tárolják a repüléshez szükséges energiát. Ez a típusú akkumulátor igen sok veszélyt rejt magában, például érzékeny a környezetére, a töltésre és a mechanikai behatásokra is. Igen sok esetről tudunk, ahol kisebb vagy nagyobb tüzet okozott az ilyen típusú cella.

Könnyen megsérthetők az emberek privát szférái, akár az oda berepüléssel, akár felvételek készítésével. Ez is jelentős kockázat, amivel fontos foglalkozni.

Végül pedig szót kell ejteni arról is, hogy napjainkban, a mindenhol teret hódító mesterséges intelligencia a pilóta nélküli repülő eszközöket is elérte. Már találkozhatunk olyan repülő szerkezettel, amelyik önmagát irányítja és nem csak előre programozott útvonalon halad, hanem saját maga felismer objektumokat, útvonalat választ és döntést hoz az elvégzendő műveletekről. Ezek jelentős veszélyt hordoznak, amelyekre nehéz felkészülni és igazi kihívás védekezni ellenük.

A drónokról

A drón definíció szerint egy pilóta nélküli légi jármű. Az EU rendelet is meghatározza a drón definícióját, eszerint ez egy olyan légi jármű, amely fedélzetén nem tartózkodik pilóta, irányítása vagy a távolból történik, vagy képes saját magát vezetni. Rövid fogalommeghatározás: drón az, aminek irányítását nem a fedélzeten ülő pilóta végzi. Eszerint lehet távolról végezni az irányítást, de a drón is irányíthatja önmagát. Tehát drónnak minősülnek a több légcsavarral rendelkező távirányítós repülő szerkezetek, de ide tartoznak a merevszárnyú távirányított repülőgépek és modell helikopterek is. Amennyiben a távirányítós repülő eszköz nem rendelkezik kamerával, akkor is drónnak minősül. Nem számít drónnak például a pöttyöslabda, teniszlabda, de a tűzijáték sem, mert ezek nem tartoznak a járművek kategóriájába. A drónok közé nem soroljuk be a távirányítós autókat és a hajókat sem, mert azok nem a levegőben közlekednek. 2020. július 1. előtt drónt használni csak eseti légtérben lehetett legálisan. Ma lakott területen kívül telefonos applikációt használva lehetővé vált a kisebb drónok legális reptetése. A drónokkal kapcsolatban számos veszélyt lehet felsorolni. Ezeket érdemes csoportokba, vagy kategóriákba rendezni.

Más légi járművek veszélyeztetése

Amennyiben két légi jármű repül egy légtérben, akkor fennállhat ezek ütközésének veszélye. Ezt úgy tudjuk kikerülni, ha minden drón egy olyan saját légtérben repül, amelybe más légi jármű nem repülhet be. Előfordulhat, hogy több drónnak kell egyszerre egy területen repülnie, ebben az esetben ki kell jelölni egy felelős személyt, aki a koordinálásukat megoldja. A szabályokat nem mindenki tartja be és előfordulhatnak ütközések nem csak drónnal, hanem más légijárművekkel is. Az ütközés lehet vétlen vagy szándékos. A veszély egyre növekedik, mert például évente körülbelül 10%-al növekszik a nagygépes légiforgalom.

Egy kísérletben Szatymazon ütköztettek repülőgépekkel drónokat, hogy teszteljék az ütközések hatásait. Először azt vizsgálták, hogy a pilóta mennyire képes észrevenni a drónokat. Megdöbbenve tapasztalták, hogy egyáltalán nem veszi észre a pilóta a drónt. Amennyiben egy utasszállító gép hajtóművébe drón kerül, akkor az nagy eséllyel súlyos kimenetelű, például azt a hajtóművet a keletkező vibráció miatt valószínűleg le kell állítani. [1]

A drónok iparága robbanásszerűen fejlődik. Ezzel a sebességgel sokáig nem tudott kellő sebességgel lépést tartani a szabályzás. Magyarországon jelenleg kizárólag eseti légtérben lehet lakott terület felett repülni. A katonai légügyi hatóságnál lehet ilyet igényelni jelenleg.

Magyarországon a Hungarocontrol végzi a légterek kijelölését és a repülések engedélyezését, koordinálását, irányítását. Jelenleg a különböző típusú légterek biztosítják azt, hogy a legálisan közlekedő gépek ne ütközhessenek össze. Például a műszerek által emberi beavatkozás nélkül irányított gépek (IFR, Instrument Flight Rules) nem találkozhatnak a kézzel irányított puszta szemes látásra hagyatkozó gépekkel (VFR, Visual Flight Rules), így nem is ütközhetnek össze egymással.

Minden drónos repüléshez eseti légteret kellett korábban igényelni. Sajnos ezt a szabályt nagyon kevesen tartották be és talán még ennél is több azoknak a száma, akik nem is tudtak a szabály létezéséről. Amennyiben eseti légtérben repülünk, akkor jelenteni kell a felszállást és a leszállást is telefonon a légiforgalmi irányítóknak.

Magyarországon a légtérszerkezet folyamatosan változik. Például az F légtér kivezetésre került, de például a fővárosi repülőtér TMA szerkezete is néhány évente átrajzolódik. Új légterek is keletkeznek. A délről érkező illegális bevándorlók miatt létrehoztak a déli határ mentén olyan légtereket, amelyekben csak határvédelmi céllal lehet repülni. Jelenleg az Ukrajnai háborús konflis miatt hoztak létre a keleti országrészben a honvédelelem számára fenntartott légtereket, amiben más légi jármű nem repülhet, így drón sem. [2]

A térképen szereplő légterek azonban nem mindig aktívak. A passzív légteret tekinthetjük úgy, mintha ott sem lenne. Például a netbriefing.hu oldalon tájékozódhatunk, hogy mely légterek mikor fognak várhatóan működni.

A DronHive.com honlapon korábban adatbázisba gyűjtötték a drónos repüléseket. A pilóták, regisztrálták saját magukat, a légi járműveiket és a repüléseiket. Nagyon jó kimutatásokat lehetett készíteni, hogy az ország mely részein repülnek többet, milyen gyakorisággal, kik a legtapasztaltabb pilóták. A rendszer további előnye volt, hogy a repüléseket előre is be lehetett jelenteni, így elvileg lehetővé vált, hogy mások is felkészüljenek arra, hogy hol várható drónos tevékenység.

Jelenleg az oldal már nem üzemel, a mydronespace átvette a szerepét. Történelmi jelentősége azonban van, hiszen egy olyan működő rendszer volt, amely azt a rendszert előzte meg, amely használata jelenleg kötelező.

Napjainkban a drónos repülések feltétele, hogy legyen bejelentve a repülés. Erre jelenleg a telefonos mydronspace alkalmazás használata kötelező, amennyiben nem eseti légtérben repülünk. Az alkalmazás használatával lehetőség nyílik rá, hogy a kisebb drónokkal legyen lehetőségünk úgy repülni, hogy nem igénylünk eseti légteret a repüléshez.

Amennyiben nem saját földterület felett repülünk, akkor érdemes engedélyt kérni a terület tulajdonosától. A legjobb, ha írásban történik, de ha szóban meg lett beszélve, akkor tudjuk, hogy nem fog minket elzavarni, vagy feljelenteni.

A légtérsértés számos veszélyt tartalmazhat. Talán a leghíresebb eset az, amikor Washingtonban a Fehér Ház területére repült egy drón és ott lezuhant. Nem okozott semmi kárt, de a szakértők figyelmét felhívta rá, hogy az ilyen eseteket meg kell előzni. A drón szállíthatott volna akár robbanóanyagot is. Magyarországon a felcsúti eset híresült el, ahol újságírók légtérigénylés nélkül repültek kamerás drónnal. A pilótát a rendőrség eljárás alá vonta, mert nem a szabályzásnak megfelelően használta a drónját, nem volt sem légtere, és nem volt engedélye a terület tulajdonosától sem.

Igen sok olyan esetről tudunk, amikor repülőtereket kellett lezárni azért, mert drónok repültek a repülőtér környékén. Egy esetleges drón-repülőgép ütközés általában megsemmisíti a drónt de a repülőgépben is súlyos károkat okoz. Ebben az esetben a drón pilóta követi el a légtérsértést. A repülőtér lezárása súlyos károkat okoz a légitársaságoknak is, mivel az utas és teherszállító gépek nem tudnak leszállni és felszállni. Több esetben jelentős késéssel tudnak megérkezni a repülőgéppel utazó utasok.

Emberek veszélyeztetése

A drón mozgási energiája is jelentős tud lenni, azonban ennél is nagyobb veszélyt jelent a légcsavarja. Nem csak fizikailag veszélyezteti az embereket a drón. Veszélyt jelenthet a magánéletére, a vagyontárgyai biztonságára is.

Alapvető szabály, hogy emberek felett nem repülhetünk, mert egy esetleges meghibásodás esetén az emberekre való rázuhanást el kell kerülni. Egy nagy méretű kamerás drón zuhant le egy sípályán verseny közben úgy, hogy az majdnem a síelőre esett. Nem sokon múlott, hogy eltalálja a versenyzőt. Az ilyen esetek megelőzése érdekében hozták ezt a szabályt. A lezuhanó gép súlya is megsebesíthet embereket, de a nagy sebességgel forgó légcsavar is jelentős veszélyforrás. A drónpilótának ismernie kell az ide vonatkozó szabályokat és be kell tartania. A szabályok célja, hogy biztonságos legyen a drónok használata. Az etikai szabályokat is be kell tartania a pilótának.

1. ábra: Egy több, mint 7kg felszállósúlyú drón

Többször fordult már elő, hogy engedély nélkül készítettek felvételt távirányítású légi járművel, ezért a törvény külön kitér az ilyen eszközökre. A fénykép és videó felvételek készítése már korábban is szabályozva volt, amelyeket a profi fotósok ismertek is. Arra külön fel kellett hívnia drónpilóták figyelmét, hogy kamerás drónokra is ugyanezek a szabályok érvényesek. Ezekkel a légi eszközökkel készíthetőek akár kompromittáló felvételek is, amely egy közismert veszélyforrás.

2. ábra: Drónnal készített felvétel

Amennyiben a drón hajtóműve meghibásodik, általában irányíthatatlanná válik és lezuhan. Az érzékeny alkatrészek az akkumulátor, a motorvezérlő ESC, a motor, a légcsavar, a drón irányító és érzékelő berendezései. Tehát igen sok alkatrésze van egy forgószárnyas drónnak, amely hiba esetén az egész légi jármű zuhanását okozza. A hibáknak igen sok oka ismert.

A pilóta is egy komoly veszélyforrás tud lenni. A pilótának gyakran repülés közben kell felelősségteljes döntéseket meghoznia. Amennyiben rosszul dönt, a drón könnyen veszélyessé válhat. A pilóta szándékosan is képes kért okozni. Ennek elkerülése érdekében a drónokat különböző biztonsági rendszerekkel láthatják el.

Egyéb dolgok veszélyeztetése

A drón nem csak az emberre jelent veszélyt, hanem más légijárművekre, gépjárművekre, épületekre és minden egyéb vagyontárgyra. Ezt felismerve a drónokra a felelősségbiztosítás kötése kötelező lett hazánkban.

A drónokban szinte kizárólag Lítium-polimer (Li-Po) akkumulátorokat használnak. Ezek előnye, hogy kis súly mellett nagy energiát képesek eltárolni. A repülésben minden gramm számít, amit fel kell emelni, így gyakorlatilag csak ez az egy féle energiaforrás terjedt el bármilyen kategóriájú drónról is beszéljünk. További előnye, hogy nincs memória effektusa, így a cellákat bármilyen töltöttségi szint esetén lehet tölteni. A cellák maximális feszültségszintje 4,2V. Ekkor a cella teljesen feltöltött állapotban van. Léteznek úgynevezett HV Li-Po cellák is, amelyek elviselik, hogy üzemszerűen még magasabb feszültségi szintre töltsük fel őket. Ezek 4,35V feszültségig tölthetőek.

A Li-Po akkuk azonban sok negatív tulajdonsággal is rendelkeznek. Amennyiben ez a típusú akku túlzott mértékben lemerül, akkor általában visszafordíthatatlanul károsodik. Az akku ki tud gyulladni és fel tud robbanni. Ekkor nagyon könnyen meggyújtja a környezetében lévő éghető anyagokat. Az ilyen tüzet szinte lehetetlen eloltani. Az egyetlen módszer, amivel próbálkozhatunk az az, ha betemetjük homokkal a lángoló akkut. Az akku több ok miatt is meggyulladhat. Ilyen például a túltöltés. Ebben az esetben a töltés helyén gondoskodni kell róla, hogy esetlegesen meggyulladó akku ne okozzon nagyobb tüzet, ne tudja meggyújtani a környezetében lévő tárgyakat. Sajnos a normál módon lezajló töltések alatt is fordultak elő tűzesetek, ezért a töltést csak felügyelet mellett szabad végezni, illetve érdemes az akkut Li-Po bag-be tenni. Ez egy olyan tasak, amely tűzálló, az esetlegesen meggyulladó akku, amely benne van, nem gyújtja meg a környezetében lévő tárgyakat. Az akku jelentősebb mechanikai behatásra is meggyulladhat, ilyen például a nagyobb ütődés. Fontos védeni a fizikai behatásoktól az akkut. A gyártók legtöbbször erős burkolattal látják el az egységet, így ütődéskor, vagy ütődéskor védik az érzékeny részt.

3. ábra: A drónokban használt Li-Po akkumulátor (szürke színnel, piros hevederrel átkötve)

A drónok lehetnek gyorsak, vagy nehezek, esetleg mindkettő együtt. Ezek a paraméterek adják a mozgási energiát. Sok esetben a drón mozgási energiája összemérhető a lőfegyverek lövedékének mozgási energiájával. Ezzel a mozgási energiával már jelentős károkat lehet okozni mind tárgyakban, mind pedig élőlényekben vagy emberekben.

A légcsavar tömege kisebb a drón tömegéhez képest, azonban a sebessége jóval nagyobb. Az emberre jelent ez igen nagy veszélyt, a bőrt könnyen átvágja a közepes méretű drón, a nagyobb drónok légcsavarjai pedig ennél nagyobb sérüléseket is tudnak okozni.

Még nem jellemző, hogy robbanószert, más veszélyes anyagot vagy lőfegyvert szállít egy civil drón, de a jövőben ezzel is számolni kell majd.

Védekezés drónok ellen

A fejezet leírja a detektálás, azonosítás, beavatkozás lehetőségeit. A drónok detektálása nem mindig könnyű feladat és a legtöbb esetben igen költséges. Szerencsére több módszer közül is lehet választani, esetleg ezeket együtt is lehet használni.

A legismertebb módszer a klasszikus radar. A jelenlegi radarok a nagygépes forgalom monitorozására lettek optimalizálva. Napjainkban szükség volt rá, hogy ezt megváltoztassák, hiszen a radarok képesek az igen kis méretű repülő tárgyakat is észrevenni az égbolton ha a beállításai megfelelőek. A radar meg tudja határozni a drón pontos repülési irányát, magasságát és távolságát is. Emellett meg lehet beszülni a méreteit is. [3]

Használhatunk a detektálásra mikrofont is. A drónoknak jellegzetes hangjuk van, ezt a hangot mikofonnal lehet detektálni, erősíteni, beazonosítani. A hang-

ból a drón méretére, vagy akár a típusára is lehet következtetni. A mikrofonos detektálási módszert befolyásolja a szél és a héttérzaj mértéke is.

Jó módszer lehet még a rádiójelek monitorozása a térben. Az ilyen légijárműveket rádiós kapcsolattal irányítják. A legtöbb esetben a drón is bocsájt ki magából rádiójeleket, például telemetria adatokat vagy élőképet sugároz a kezelő felé. Ez a rádiójel más számára is látható, így a drón detektálható.

Végül a kamerás rendszerek is alkalmasak a drónok jelenlétének beazonosítására. Léteznek 360 fokos kamerák, forgatható és zoomolható PTZ kamerák amelyek akár egymással kombinálva egyesíteni tudják a két rendszer előnyét. Például a 360 fokos kamera lát néhány pixeles repülő tárgyat, ezután ráfordul a PTZ kamera és egy részletgazdag, nagyfelbontású képet ad a drónról. Használhatunk hőkamerát is, amely igen jól detektálja a levegőben közeledő légi eszközöket. [4]

4. ábra: Hőkamerák alkalmazása drónok detektálása

Az elhárításnak számos módja lehetséges. A távirányított légi járművek irányító jeleit lehet zavarni, ekkor a drón nem tudja értelmezni a jelet, amely őt irányítaná. Olcsóbb drónoknál előfordulhat, hogy elrepül, felemelkedik, a drágább modellekben bekapcsol ilyenkor egy Fail Safe rendszer, amely egy előre megadott vészhelyzeti repülési programot futtat le a légijárművön. Ez lehet több féle, például szálljon le, repüljön a felszállás helyére és ott szálljon le, folytassa a korábbi repülési feladatot. Olyan Fail Safe program is létezik, amely azonnal leállítja a légcsavarokat, a drón leesik és nem tesz kárt a forgó légcsavarjaival a környezetében, illetve nem repül el túl messzire. Az irányítás átvételére is láttunk példákat, de ezek a gyakorlatban nem mindig működnek. Elképzelhető, hogy a jövőben ez a terület is jelentős fejlődésen fog átesni.

Gyakori megoldás, hogy egy másik drónnal elkapják az idegen drónt. Ekkor általában hálót használnak, amelybe belegabalyodik a légcsavar. Az így röpkép-

telenné vált drón le lehet hozni a levegőből. Az elkapásra használhatunk még ragadozó madarakat is. Ezeket tréningezik, a madarak elkapják és lehozzák a levegőből az idegen drónokat. [5]

A földről is meg lehet semmisíteni az idegen repülő eszközöket. Erre lehet használni klasszikus fegyvereket, de létezik drón elhárító lézeres fegyver is.

Bármelyik módszerre is esik a választás, fontos, hogy a jelenlegi jogszabályi környezetben csak a hatóság jogosult a földre kényszeríteni a repülő eszközöket.

Mesterséges intelligencia is képes egy drónt irányítani. 2019-ben írt ki egy nemzetközi versenyt a lockheedmartin.com. A megmérettetés érdekessége, hogy nem ember, hanem mesterséges intelligencia irányította a légi járműveket. Ezt a versenyt egy holland csapat nyerte, az ő drónjuk teljesítette a leggyorsabban a pályát. Ez a drón versenyzett egy másik ugyanilyennel, amelyiket az egyik legjobb drónpilóta, Gabriel Kocher irányított. A versenyt Gabriel nyerte, aki hat másodperc alatt ért célba. Öt másodperccel volt gyorsabb annál a gépnél, amit a győztes mesterséges intelligencia vezetett. Ez mutatja, hogy nincs nagyságrendi különbség az időeredmények között, az AI fejlődésével hamarosan megfordulhat ez a rangsor. [6]

Az önvezető drónok új fejezetet nyithatnak a repülésben, számos új veszélyt jelenthetnek. Előfordulhat, hogy nem lehet őket irányítani, illetve lehetséges, hogy teljes rádiócsendben repülnek, hiszen az irányítóegységük a fedélzeten található.

A drónra ható veszélyek

Drónokkal veszélyt jelenthetünk a környezetünknek, de a drónt is fenyegetik veszélyek. Ezeket mutatja be a cikk a következő részben.

Az időjárás meghatározza, hogy mikor repülhetünk biztonságosan a drónunkkal. Szép időben természetesen semmilyen időjárási tényező nincs, ami veszélyt jelenthetne.

A szél egy gyakori veszélyforrás. Amennyiben az erőssége nagyobb, mint a drón maximális sebessége, akkor elsodorhatja azt. Kisebb szélsebesség esetén is elsodorja, ekkor a pilótának kell korrigálnia a szél hatását. A drágább modellekben GPS alapú stabilizáló egység dolgozik, ez érzékeli, ha a drónt elsodorja a szél és kompenzálja azt. Ekkor rá dől a szélre és ellen tart annak, egy helyben marad a talajhoz képest. A levegőben előfordulnak nem csak vízszintes, de függőleges légáramlatok is. Ezek a kompenzálására is figyelnie kell a pilótának.

A zivatarra jellemző az erős szél, amelynek mind a vízszintes, mind a függőleges komponense igen jelentős. Mivel ezek általában nagyobb sebességek, mint a drón sebessége, ezért el fogja sodorni azt és még maximális teljesítményen működtetve sem lehet megakadályozni a sodródást.

A levegő hőmérséklete is befolyásolja a légi üzemet. A levegő sűrűsége a hőmérséklettől is függ, ez hatással van a sebességre, a hatótávra, a felemelhető teher maximális tömegére és a maximális üzemidőre is.

Az eső általában meghiúsítja a repüléseket. Szinte az összes drón érzékeny a vízre, így esőben nem repülhetnek ezek az eszközök. Csupán néhány darab van, amelyet vízálló módon alakítottak ki, ezek nem terjedtek el.

Amennyiben a pára le tud csapódni a drónon, az is okozhat problémát. Általában a drón akkuja melegszik, az elektromos motorok is jelentős hőt termelnek működés közben. Tudjuk, hogy a felmelegedett tárgyakon kevésbé csapódik le a pára, azonban lehetnek olyan alkatrészek, amelyek kihűlnek, vagy a menetszél lehűt. Itt a páralecsapódás ronthatja a repülési tulajdonságokat, súlyosabb esetben akár elektromos rövidzárlatot is képes okozni, ami a repülő eszköz lezuhanásához vezet.

A drónokra veszélyt jelentenek azok a személyek, akik nem látják azt szívesen. Van, akit a hangja zavar, van, aki attól fél, hogy valamilyen felvételt készít, amibe ők nem egyeztek bele, és sértheti őket. Az ilyen emberek meg szoktak próbálkozni azzal, hogy lehozzák a drónt a levegőből, vagy összetörjék azt. Hivatalosan egy magánszemélynek nem lenne joga ahhoz, hogy kért okozzon más drónjában, azonban a tapasztalatok sajnos mást mutatnak. Ezért fontos az, hogy betartsuk a szabályokat, például csak a terület tulajdonosának a beleegyezésével repüljünk.

A drónokra más légijárművek is veszélyt jelentenek. Léteznek gyorsasági drónversenyek, itt gyakori, hogy a drónok egymásnak ütköznek. Ezt persze megpróbálják elkerülni a pilóták, de ez ellen úgy védekeznek, hogy igen erős szénszálas kompozit anyagból készítik a gépeket. Az esetleges zuhanás esetén sem szokott összetörni az ilyen gép. A jog gondoskodik róla, hogy a drón ne ütközhessen más légijárművel. Egy eseti légtérben csak egy légi jármű szokott tartózkodni, az aki ezt megigényelte és megkapta. Más légijárművek ezeket az eseti légtereket kikerülik, nem repülnek bele. Van arra is lehetőség, hogy a légtér tulajdonosa több légi járművet is enged a légterében repülni, ekkor ő tartozik azért felelősséggel, hogy ezek ne ütközzenek össze.

Drónt készen vásárolhatunk, de arra is van lehetőségünk, hogy saját magunk építsük meg alkatrészeiből. A fő kérdés, hogy milyen biztonsági elemeket építünk be és mennyire megbízható alkatrészekből építjük össze a légi járművet.

Előfordulhat, hogy egy drón felett valaki harmadik fél átveszi az irányítást. Ekkor az eredeti pilótának már nincs hatása a drón felett. Az ilyen támadások csak elvi szinten léteznek, azonban a jövőben erre is fel kell készülni.

Milyen a biztonságos drón

Egy biztonságos drón nem okoz balesetet. Ezt két módon érhetjük el. Az egyik, ha a pilótát részesítjük képzéseken, és a tudását ő vizsgákon bizonyítja. A másik út, ha a drón rendelkezik olyan biztonsági elemekkel, amelyek megakadályozzák azt, hogy baleset jöjjön létre. Ilyen lehet például a FailSafe rendszer, vagy egy távolságérzékelő, amely nem engedi, hogy a drón például egy ház falának nekivezessük. Egyes drónok ellenőrzik a saját helyzetüket, és amennyiben túl közel tartózkodnak egy repülőtérhez, akkor nem lehet velük elemelkedni a talajról.

A nagyobb drón gyártók tárolják és elemzik a repüléseket. Ezekből ajánlásokat fogalmaznak meg, hogy hogyan lehet biztonságosan használni az eszközeiket. Ezeket érdemes figyelemmel kísérni és követni.

Hivatkozások

[1] Drón – repülő itthoni ütközési teszt videón link: https://www.securinfo.hu/hirek/10739-dron-repulo-itthoni-utkozesi-teszt-videon.html.

[2] légtér.hu: A Magyar légtér szerkezete, link: https://legter.hu/tudastar/legterek/.

[3] Drón detektálás, link: https://mydronespace.hu/aktualitasok/dron_detektalas.

[4] dr. Rottler Violetta: A drónok rendészeti alkalmazása, link: https://www.detektorplusz.hu/index.php?m=23684.

[5] Thuy Ong: Dutch police will stop using drone-hunting eagles since they weren't doing what they're told, link: https://www.theverge.com/2017/12/12/16767000/police-netherlands-eagles-rogue-drones.

[6] AlphaPilot — Lockheed Martin AI Drone Racing Innovation Challenge, link: https://www.lockheedmartin.com/en-us/news/events/ai-innovation-challenge.html.

Drónok a klímaváltozás vizsgálatában: térképezés extrém magashegységi környezetben *(Ojos del Salado, Száraz-Andok, Chile)*

Nagy Balázs[1,2] – Mészáros János[3]
[1] *Eötvös Loránd Tudományegyetem, FFI, Természetföldrajzi Tanszék, Budapest*
[2] *PermaChile Network, Földgömb Alapítvány, permachile.com*
[3] *Agrártudományi Kutatóközpont, Talajtani Intézet, Budapest*
balazs@afoldgomb.hu – meszaros.janos@rissac.hu

Összefoglalás

A Föld legmagasabb vulkánján, az inaktív, 6893 m magas Ojos del Saladón és tágabb környezetében, a száraz Puna de Atacama fennsíkon zajló magyar klíma- és környezetváltozás elemző program – a terület beműszerezésével, 2012-től – a Föld legmagasabb környezeti monitoringhelyszínén működik. A kutatás elsősorban a jelen klímaváltozás folyamatait vizsgálja – főként a jégjelenlét változásaira koncentrálva. Feltárja a mai permafroszt-elterjedést, az örökfagy degradációját, elemzi és modellezi az aktív réteg viselkedését.

A program a környezetváltozás egyes folyamatait nagyfelbontású helyszíni térképezéssel is vizsgálja. Az UAV eszközzel végzett légi térképezés, a megfelelő felbontású ortofotómozaik és domborzatmodell előállítása alapvető a morénák kormeghatározása céljából végzett mintavételek és az egykori jégkiterjedés megállapítása során, de a poligonhálózatok, és a felszíni vízjelenlét vizsgálatához, valamint a folyamatosan működő, telepített hőmérsékletmérő-hálózat adatainak értékeléséhez is kiváló alapadatokat ad.

A légi felmérés legalacsonyabb helyszíne 4200 m-en húzódik, ahol a Puna de Atacama fennsík – mérőhelyszínnek is helyet adó – poligonrendszerét vizsgáltuk. A korábbi gleccserek morénasáncait, a felszín alatti hó és firn mai olvadásához kötődő alakzatokat, a szaggatott permaroszt területen jelen lévő folyóvízi erózió és akkumulációt 5200-5300 m-en térképeztük, de a repülések egészen 6000 m-es magasságig zajlottak.

A feladatok elvégzéséhez egy magashegységi környezetre optimalizált UAV eszközt alkalmaztunk, melynek tervezése során figyelembe vettük a rendkívül nagy tengerszint feletti magasságot, a területre jellemző erős szelet és alacsony hőmérsékletet, illetve – a gyalogos terepi mozgás miatt – a könnyű szállíthatóságot is.

A geoinformatikai alkalmazások és a felmérések terepi elemezhetősége kapcsán is fontos kritérium a koordinátarendszerbe illesztés. Ehhez szükség volt a légifelvételek pontos pozíciójának meghatározására, melyet az alkalmazott fényképezőgép és a hozzákapcsolt utófeldolgozásra képes GPS vevőegységgel oldottunk meg.

Bevezetés

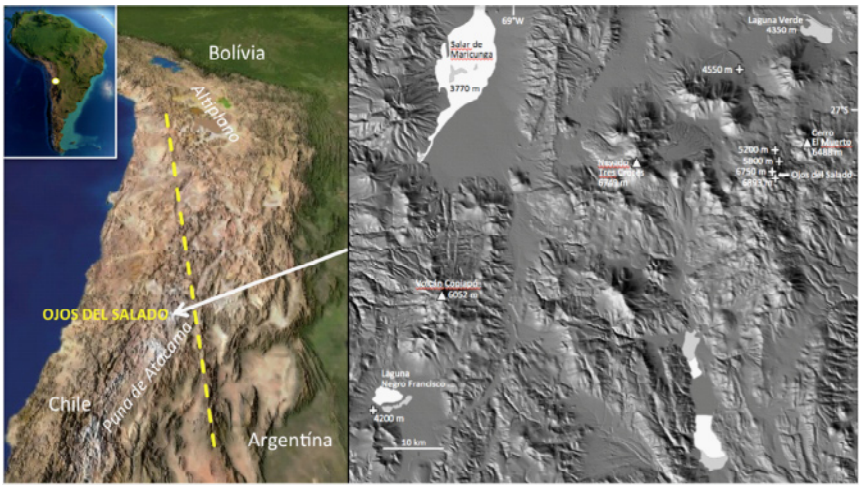
A Föld legnagyobb magasságban működő, 2012-ben kezdődött műszeres klíma- és környezeti monitoringja magyar vezetéssel zajlik a Száraz-Andok legmagasabb részén. A 4200 és 6893 m közötti folyamatos mérések a permafroszt, az aktív réteg és ezeken keresztül a vízbázis változását elemzik. Olyan dinamikus folyamatokat vizsgál a rendszer, amelyek a klímaváltozás pontos indikátorai, és számszerű információkat adnak a magashegyi melegedésről, valamint ennek környezeti következményeiről.

A megszakítás nélküli, dataloggerekre épülő adatgyűjtéshez terepi mintavételek (üledékek, vízminták, mikroorganizmusok), műholdas elemzések (hóborítás, vízjelenlét) és nagy pontosságú, drón alapú domborzatfelmérések kapcsolódnak. Ez utóbbiak a szélsőséges terepi és időjárási körülmények között különösen nagy kihívást jelentenek, de az innen származó adatok mind a kormeghatározásokhoz, mind a gyors környezeti átalakulások elemzéséhez is nélkülözhetetlenek.

Helyszín

A D.sz. 28-22° között Chile és Argentína területén húzódó Puna de Atacama magasföld – a Száraz-Andok részeként – a Föld egyik legextrémebb környezete. Az „andoki száraz átló" mentén elhelyezkedő rendkívül száraz régió sivatagi területekre jellemző csapadékkal (évi 100 mm körüli, kizárólag hó formájában érkezve) és a csapadékhoz képest tízszeres párolgási értékekkel rendelkezik (Messerli et al. 1997, Vuille és Amann 1997, Ahumada 2002, Kull et al. 2002; Houston és Hartley 2003). A felföld átlagos tengerszint feletti magassága 4000 m, területén számos óriásvulkán emelkedik (1. ábra). Ezek legnagyobbika a 6893 m magas alvó vulkáni komplexum, az Ojos del Salado (27°06'34.6" D, 68° 32'32.1" Ny).

E régióban van a Földön – az extrém hideg és száraz klíma miatt – a legmagasabban a hóhatár (7000 m környékén, Clapperton 1994, Kull et al. 2002). Az aktív jégborítás nem jellemző, a felszín alatt mégis jelen van a jég, erre a periglaciális felszínformák és a permafroszt-modellezések eredményei is rámutatnak (Corte 1982, Trombotto 2000, Ahumada 2002, Gruber 2012; Azócar et al. 2017, Nagy et al. 2019, 2020). Az alacsony csapadékmennyiség, a magas evaporáció és a gleccserek korlátozott jelenléte miatt a permafrosztban levő jég – mint a krioszféra legjelentősebb itteni formája – igen jelentős szerepet játszhat a térség hidrológiájában és ökológiájában (Grosjean és Veit 2005, Azócar és Brenning 2010, Aszalós et al. 2016, 2020).



1.ábra. A vizsgálati helyszín elhelyezkedése a Száraz-Andokban, az "andoki száraz átló" (szaggatott vonal) mentén. Az Ojos del Salado a Puna de Atacama fennsíkon emelkedik – számos 6000 m-nél magasabb csúcs szomszédságában. Közöttük sósivatagok (salarok), sós tavak, és kősivatagok húzódnak.

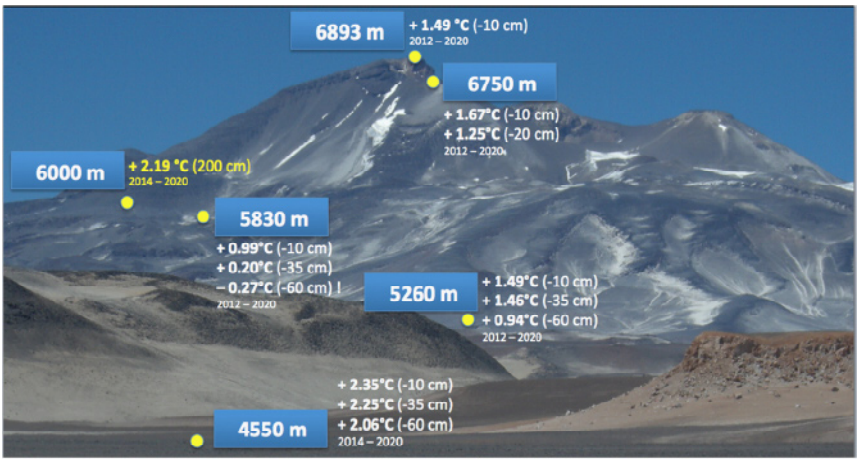
Módszerek

A hosszú távú vizsgálatsorozat alapvető céljának megfelelően a 2012-ben telepített, főként a felszín alatt működő műszerhálózat segítségével (2. ábra) a mai permafroszt-elterjedést tárjuk föl, mérjük az örökfagy degradációját, elemezzük és modellezzük az aktív réteg viselkedését, a Föld egyik legszárazabb magashegyi sivatagában vizsgáljuk az eolikus folyamatokat és a múlt jégkiterjedéseit is rekonstruáljuk.

A környezetváltozás legdinamikusabb folyamatait azonban 2019-ben nagyfelbontású helyszíni dróntérképezéssel is vizsgáltuk: a folyamatosan működő, telepített hőmérsékletmérő-hálózat adatainak értékelését a periglaciális és eolikus felszínformákról, a morénarendszerekről, valamint a folyóvízi eróziós és akkumulációs folyamatokról készült felmérésekkel is segítjük.

Az UAV eszközzel végzett légi térképezés, a megfelelő felbontású ortofotómozaik és domborzatmodell előállítása alapvető a morénák kormeghatározása céljából végzett mintavételek és az egykori jégkiterjedés megállapítása során is, de a poligonhálózatok, valamint a magashegyi tómedencék felméréséhez és a szélépítette hordalékfodrok ("megaripples") vizsgálatához is kiváló alapadatokat ad.

A feladatok elvégzéséhez egy egyedi építésű, Ardupilot-alapú magashegységi környezetre optimalizált UAV eszközt alkalmaztunk (3. ábra). A négymotoros helikopter (quadkopter) tervezése során figyelembe vettük a rendkívül nagy



2.ábra. Monitoringhelyszínek az Ojos del Salado masszívumán és a hőmérsékletváltozás értékei 2020. nyarának végéig a havi középhőmérsékletek alapján számolva.

tengerszint feletti magasságot, a területre jellemző erős szelet és alacsony hőmérsékletet, illetve – a gyalogos terepi mozgás miatt – a könnyű szállíthatóságot és javíthatóságot is.

3.ábra. A magashegyi körülményekre optimalizált UAV a Laguna Negro Francisco medencéjében, 4200 m-en.

A geoinformatikai alkalmazások és a felmérések terepi elemezhetősége kapcsán is fontos kritérium volt a koordinátarendszerbe illesztés. Ehhez szükség volt a légifelvételek pontos pozíciójának meghatározására, melyet az alkalmazott fényképezőgép, egy Ricoh GR II (4. ábra) és a hozzákapcsolt L1 frekvenciás, utófeldolgozásra képes GPS vevőegységgel oldottunk meg. Két Emlid Reach GPS-egységet használtunk, az egyiket egy könnyű, háromlábú állványra épített bázisállomásként, a másik egységet pedig a quadkopterre integráltuk, ami egy

Ricoh GR II digitális kamerával együtt lehetővé tette a képi pozíciók rögzítését a felmérési repülések során (5. ábra). Később az RTKLib függvénykönyvtár programjait (Takasu és Yasuda 2009) használtuk a rögzített GPS-adatok utólagos feldolgozására, hogy pontos képkoordinátákat számítsunk a légi felvételek későbbi fotogrammetriai feldolgozásához. Ezzel a módszerrel a szélsőséges terepviszonyok között ki tudtuk küszöbölni a földi kontrollpontok használatát, 5-6 cm átlagos belső hibával ortorektifikált képblokkokat képeztünk. A terepviszonyok és a nagy magasság miatt a terepmunka során nem helyeztünk ki és nem mértünk ellenőrző pontokat, azonban pár, jól azonosítható tereptárgy segítségével más adatrendszerekhez (pl. szabadon hozzáférhető nagy felbontású műholdképekhez) hasonlítva az UAV-felmérésből származókat, nem tapasztaltunk 1 méternél nagyobb hibákat.

4.ábra. Ricoh GR, az ortofotokészítéshez használt, UAV-re szerelt kamera

5.ábra. Az Emlid Reach rover-bázis páros egységei 5200 m-en (Fotó: Nemerkényi Zsombor).

Eredmények, következtetések

4200 m, poligonmező

A Puna de Atacama magasföldjén zajló környezeti átalakulások értelmezésénél rendkívül fontos, hogy megtaláljuk e száraz, hideg magashegységi terepen a periglaciális környezet alsó határást, egyben azt a határzónát ahol a víz, ill. a nedvesség környezetformáló hatását elsősorban fagyott állapotban fejti ki. Ehhez olyan terepeket kell találni, ahol fellelhetők a periglaciális környezet indikátorjelenségei. Ilyenek lehetnek a jéghez kötődő lejtős tömegmozgások, maga a jégtartalmú permafroszt, vagy a fagymintás, poligonális felszínek. Ám mivel

mindegyik nedvességhez kötődik, egy rendkívül száraz, óriási kiterjedésű, sivatagos területen korlátozott a jelenlétük, megtalálásuk, mintaterületként és monitoringhelyszínként való használatuk komoly kihívást jelent.

A Laguna Negro Francisco 4150 m-en húzódó medencefenekének közelében, 50 m-rel a tó vízszintje fölött, hordalékkúpok, törmeléklejtők és inaktív eróziós patakmedrek között, terepbejárások során találtunk olyan kőtörmelékes sík terepet, amely alkalmasnak tűnt a hosszútávú mérőhelyszín szerepre. E kősivatagok felszíni áttekintése azonban – magaslatok, helyszíni rálátás nélkül – alig lehetséges, a hozzáférhető űrfelvételek felbontása pedig nem elég a néhány deciméteres, vagy max. 1-2 méteres felszínformák mintázatának elemzéséhez.

A nyári UAV-repülések során sikerült 2-3 cm-es térbeli felbontású ortomozaikot készíteni a területről (itt a tökéletesen vízszintes felszínen – ellentétben a magasabban elhelyezkedő helyszínekkel – nem volt kiemelt cél a digitális domborzatmodell készítése).

A néhány tíz méteres magasságból készült nagyfelbontású mozaikon már kirajzolódott a térség kőpoligon-hálózata, amelynek területén 2012-ben a felszín alatti hőmérsékletet több mélységben is monitorozó mérőhelyszínt építettünk ki (6. ábra).

Az UAV felmérésből (a lényegesen kisebb felbontású űrfelvételekkel együtt alkalmazva) világossá vált, hogy a poligonhálózatok (mint az egykori vagy mai periglaciális környezet kiváló indikátorjelenségei) csak olyan helyszíne-

6. ábra. A poligonmező részletének UAV-alapú ortofotója és elhelyezkedése (űrfelvétel: GoogleEarth 2020. október) a Laguna Negro Francisco medencéjének szélén, 4200 m-en.

ken jelenhetnek, ill. maradhatnak meg, ahol a nagyon ritka csapadék okozta lejtőleöblítés, a hegylábfelszínképződés nem-periglaciális folyamatai, a hordalékkúp-épülés és az időszakos aktív vízvezetés érintetlenül hagyja a terepet. A folyamatosan képződő törmelékbe temetkező hegyek, a rendkívül kiterjedt pedimentek között, a platókon a vízszinteshez közeli, friss felszínbolygatástól mentes, foltszerűen megjelenő terepek esélyesek a kialakulásukra és megőrződésükre. De csak ott, ahol időnként nedvességet kap a regolit (pl. felszín alatti szivárgással), így jégtartalmú permafroszt keletkezhet.

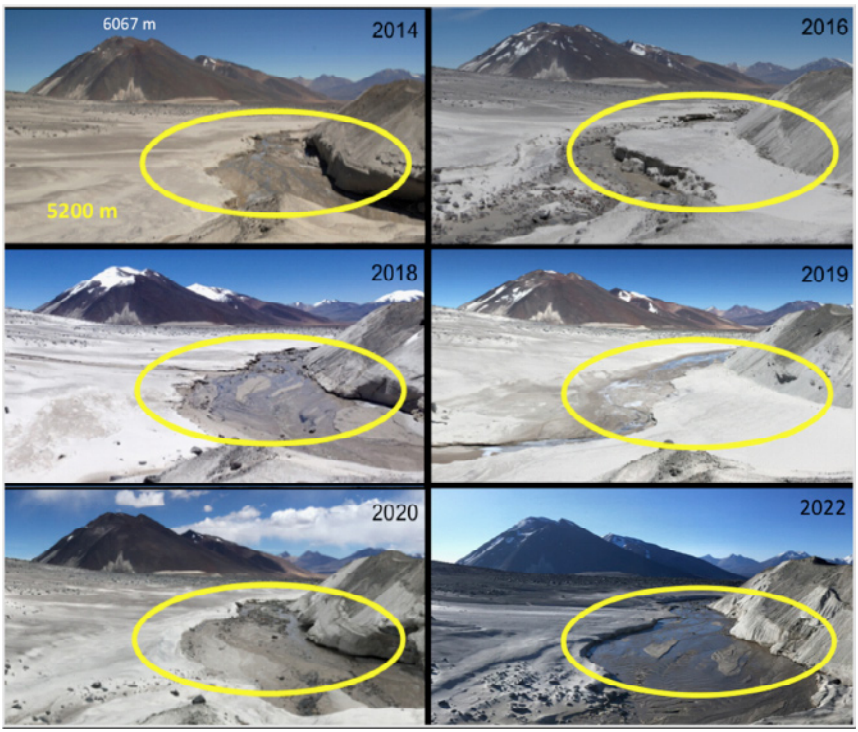
A hosszú távú, folyamatos hőmérsékletméréseink alapján azonban kimutattuk, hogy e terepeken sincs már jégtartalmú permafroszt (Nagy et al. 2019), vagyis e jelenségek fosszilis formának tekinthetők, az aktív, üledékáramlással, krioturbációval rendelkező periglaciális környezet magasabban kezdődik. Egy következő tereplépcsőn, 4550 m-en működő mérőhelyszín adatai arra mutattak rá, hogy még ott sincs egész éves jégcement, ráadásul ott a teljesen száraz regolit miatt poligonális formák sem keletkeztek.

5200-5300 m, folyóvízi erózió, akkumuláció + eolikus akkumuláció

Az Ojos del Salado térségében a ritkán előforduló felszíni víz a hóolvadásból, valamint a felszíni és felszín alatti jégtestek olvadásából származik. Mivel a rendszertelenül érkező hócsapadék olvadásából hirtelen sok víz származhat, ugyanakkor az erősödő felmelegedés hatására a jégolvadás fokozódik, a vízfolyások eróziós tevékenységének ereje nagy szórást mutat, ám dinamizmusa feltűnően nagy. A völgytalpak, medrek kifejezetten instabilak, átalakulásuk éves léptékben is számottevő (7. ábra). Az olvadékvíz völgytalpi eróziója és üledékakkumulációját ráadásul a völgyi hófelhalmozódások és a havat konzerváló évszakos homokleplek is befolyásolják. Az így létrejött összetett alakzatok gyakran rövid életűek, gyorsan változók – az űrfelvételeken a felbontási problémák miatt nagyrészt követhetetlenek.

Az Atacama Camp (5260 m) közelében végzett UAV-repülések során a glecscservölgymaradvány alján kialakuló formakincs aktuális 2019-es állapotát sikerült felmérni (8. ábra). Ennek során kirajzolódtak a pszeudokarsztos folyamatok alakzatai (pszeudodolinák, a homoktakaróval borított felszín alatti hó és firn olvadása által okozott nedves üledékfoltok, épp keletkező hótölcsérek felszín alatti helyei, stb.).

Az ilyen jellegű térképezéssel – amennyiben lehetőség van az ismétlődő, idősoros felmérésekre – pontosan nyomon követhetők az eolikus folyamatokkal kísért folyóvízi eróziós és akkumulációs jelenségek. Mindezek pedig megadják, hogy mi történik a stagnáló vagy növekvő vízmennyiség esetén a völgyek magashegységi, felső zónájában. Ezek pedig alapvetően fontos információk, mivel

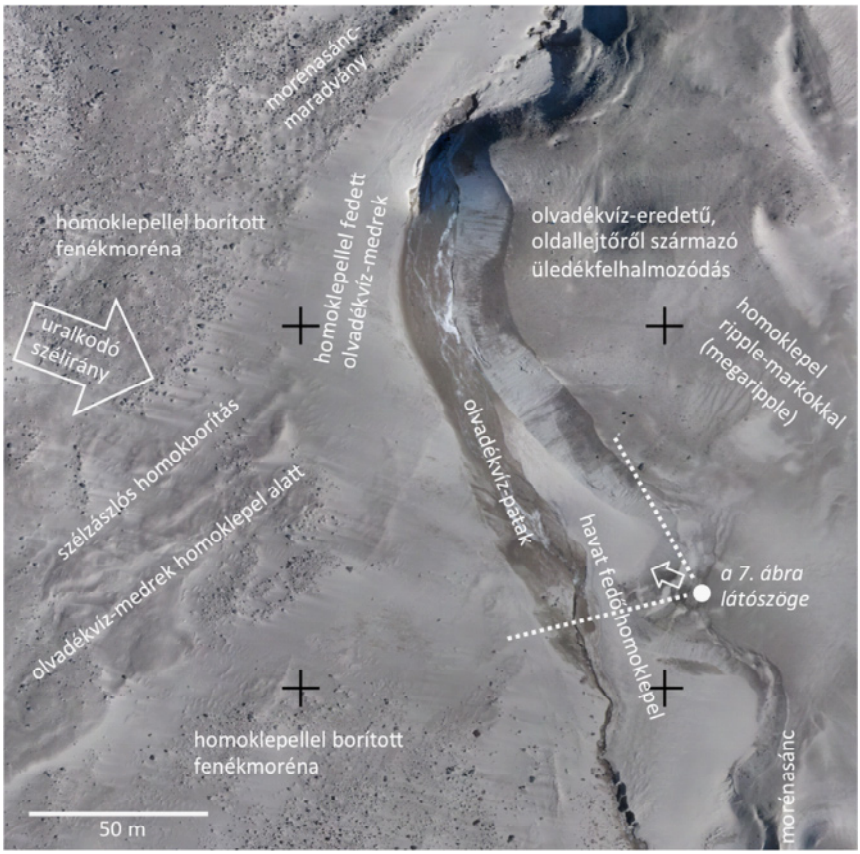


7. ábra. Az Ojos del Salado holtjégfoltjaiból érkező olvadékvízpatak eróziója, völgyaljformálása és a hófelhalmozódásokra rátelepült homokleplek jelenléte, változása.

a hőmérsékletemelkedés okozta olvadás fokozódásával az erózió és az akkumuláció is dinamikusan változik, így a víz üledékben/hordalékban történő elnyelődése vagy épp a víz folyamatos felszíni jelenléte is átalakul.

A fentiek azért is nagy jelentőségűek, mert ez a zóna a szaggatott permafroszt térsége. 10 évre visszamenő felszín alatti hőmérsékletméréseink szerint itt ugyan még nincs összefüggő örökfagy, de ez a terület a felszakadozó permafroszt területe, ahol a víztartó jeges aljzat folytonosságának hiánya széleskörű mélybe szivárgást okoz, így az olvadékvizek felszíni jelenléte nem állandó.

A melegedéssel a permafroszt fölötti aktív réteg víztartó képessége csorbul, hiszen mélyülésével, ill. aztán az örökfagy eltűnésével könnyen elérhetővé válnak az olvadékvíz számára a felszín alatti mélyebb rétegek. Épp ezért a felszíni jelenségek monitoringja alapvető annak meghatározásában, hogy milyen a felszíni vízvezetés kiterjedése, iránya, állapota.



8. ábra. A 7. ábra helyszíne, a 2019-es állapot az UAV-felméréssel készített nagyfelbontású ortofotón (tágabb környezete a 9. ábrán látható).

5200-5300 m, morénasáncok

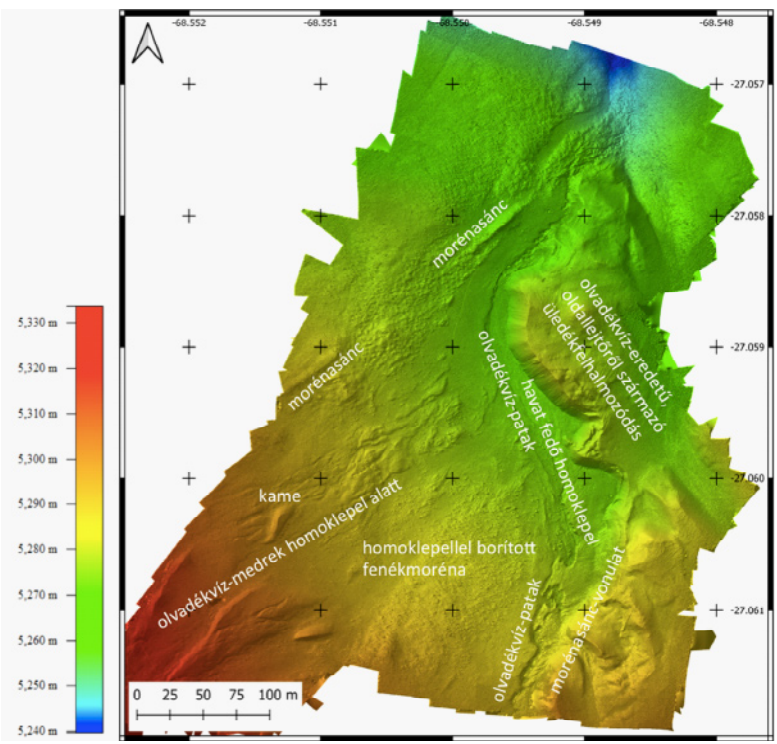
Bár az Ojos del Salado masszívumán ma már nincs aktív gleccser, a múltban voltak olyan éghajlati periódusok, amikor az Andok ezen száraz része is eljegesedett, mivel a hóhatár alacsonyabban húzódott (Kull et al. 2002). Az eljegesedések, a gleccserelőrenyomulások kormeghatározása azonban rendkívül nehéz, mivel az elmúlt évezredekben az arid körülmények között hatalmas mennyiségű aprózódástermék és eolikus hordalék került az idősebb felszínformákra, ráadásul a posztglaciális tömegmozgások, valamint a folyóvízi erózió és akkumuláció is átalakították a glaciális felszínformákat.

Ennek következtében már az utolsó eljegesedések korát tisztázó mintavételek is problémásak. Rendkívül nehéz azonosítani a morénának tekinthető alakzato-

kat, kérdéses, hogy ezek mennyire alakultak át a holocénben, és pontosan honnan érdemes mintákat gyűjteni, hogy a jégelőrenyomulást jelző morénák korát meghatározhassuk.

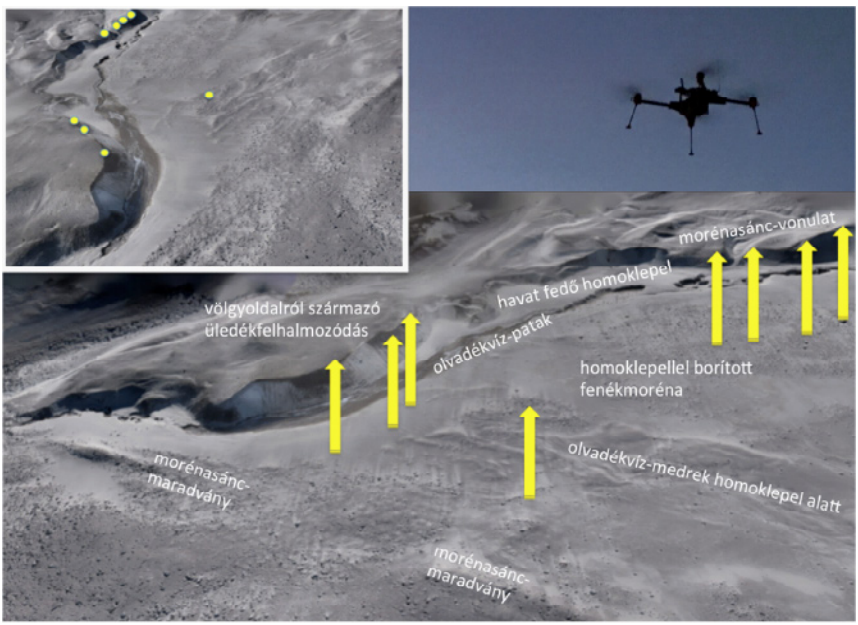
A kormeghatározások post-IR IRSL-225 lumineszcens módszerrel történtek (ELTE FFI, Természetföldrajzi Tanszék, Novothny Ágnes). Az ehhez szükséges mintákat olyan helyről kell venni, ahol az alkotórészek a helyszínre kerülés óta fénytől elzárt helyen voltak. A mintamagok megbízhatóságát növeli, ha éjszaka gyűjtjük be, így kisebb a fényszennyeződés veszélye.

Ugyan a morénaalakzatok elég nagyok ahhoz, hogy az ingyenesen is hozzáférhető űrfelvételeken láthassuk a futásukat, meghatározhassuk, hogy melyek a legalacsonyabban fekvők, amik a gleccserelvégződéshez kapcsolódtak, de azonosításuk csak a terepen lehetséges, a mintavételi helyszínek pontos térbe helyezéséhez, az alakzatokhoz kötéséhez azonban részletes domborzati felmérésre van szükség (9. ábra). Ez nélkülözhetetlen a kapott koradatok értelmezéséhez is,



9. ábra. Az egykori gleccservölgy 5200-5300 m közötti szakaszáról, a gleccserelvégződéshez közeli zónában készült domborzatmodell, amely a felszínfejlődési rekonstrukcióhoz és a mintavételi helyszínek meghatározásához is alapvető segítséget ad.

hiszen a morénák és környezetük formakincse a dinamikusan átalakuló terepen korántsem biztos, hogy az utolsó eljegesedések idejének domborzati viszonyait tükrözik. Ezzel együtt a pontos domborzati felmérés segít a mintavételi hibák kiküszöbölésében is: így meghatározható, hol helyezkednek el az utólagos ráhordódások, vagy a ma is mozgó, folyamatosan átalakuló rétegek ill. alakzatok és elkerülhető, hogy a nem reprezentatív helyekről vegyünk mintákat (10. ábra).



10. ábra. A moréna-maradványokról és a völgytalpról készült UAV-felmérés domborzatmodellje (két látószögből) a kormeghatározásokra vett minták helyszíneivel (nyilak és pöttyök).

A 20-30 ha közötti, nehezen belátható és járható vizsgálati terület több napos felmérési időt tett szükségessé, minden repülés előre programozott útvonalon és magasságban zajlott, meghatározott fényképezési gyakorisággal és átfedési értékekkel. Mindez szinte végig erős szélben, valamint a fel- és leszállást jelentősen nehezítő horzsaköves-homokos aljzaton. A megfelelő méretű, stabil indító/érkezőfelület biztosítása alapvetően fontos – úgy, hogy e platform (összehajtva) még könnyen, háton is szállítható legyen.

A könnyű málházhatóság és a helyszíni javíthatóság ebből a szempontból rendkívül fontos – túl a nagyteljesítményű motorok alacsony hőmérsékleten és "ritka levegőben" történő megbízható működésén. Keserű terepi tapasztalat, hogy a fényképezőgépek még a drónoknál is érzékenyebbek az anomáliákra (homokszennyeződés, ütődés).

A felmérés eredményeként született 2-3 centiméteres térbeli felbontású domborzatmodell minden olyan finom felszínformát tartalmaz, amely a domborzatelemzéshez szükséges. Az apró szélzászlóktól a fenékmoréna kövein-szikláin át, a vízrendszer elemein túl a morénamaradványok minden részlete kiválóan látszik, és megfelelő perspektívákat alkalmazva tisztázhatók a felszínfejlődés vitás kérdései.

Így – bár a morénák anyaga (kőzettani/ásványtani összetétele miatt) itt is csak gyengén alkalmas a kormeghatározásokra – az utolsó morénaképződési időszakra 18.8+/-1.0 ka időszakot adott a datálás, ami az utolsó glaciális maximum (LGM) végének megfelelő periódus. Az UAV-felmérés tette lehetővé azt is, hogy a sokkal fiatalabb koradatokat (1-5.2+/-0.3 ka) adó minták helyszíneinek domborzatát is értelmezni tudjuk. A morénarendszerhez kapcsolódó, formakincsében hasonló alakzatok az elhagyott gleccservölgy oldallejtőiről érkező olvadékvizek hordalékfelhalmozódásaiból keletkeztek, az eljegesedésekhez már nincs közük.

Összegzés

A Száraz-Andok nagy magasságú helyszínein, szélsőséges időjárási és terepkörülményei között végzett munka igen körültekintő UAV-felmérési előkészületeket igényel. Ez leginkább a helyszíni tapasztalatok birtokában teljesíthető, a váratlan események még így sem kivédhetők. A szélsőséges körülmények közötti munkára azonban mindenképpen szükség van. A terepen nehezen átlátható felszínek felmérése, térbeli, morfológiai rendszerbe helyezése, illetve a dinamikusan átalakuló helyszínek monitoringja is ezt erősíti. Ez utóbbi szempontból a felmérések ismétlése is követelmény, mivel a nagy pontosságú felmérések lehetővé teszik a változások részletes dokumentálását és magyarázatát. A magasság növekedésével erősödő logisztikai és üzemeltetési kihívások a kutatási célú drónokat erősebben érintik, mint a kereskedelmi, kisméretű szerkezeteket (az Ojos del Saladón 7200 m-en is repült már viszonylag egyszerű drón), mivel a terepfelmérés lényegesen hosszabb tartózkodással, sokszoros repülési idővel, a repülést nehezítő terepkörülményekkel, jelentős szállítókapacitás- és nagy energiaforrás-igénnyel jár együtt.

Az eredmények azonban azt mutatják, hogy egy nehezen járható és áttekinthető, az emberi tevékenységet is jócskán korlátozó magashegyi helyszínen a terepértelmezésben, a változáselemzésben kifejezetten sikeres és nélkülözhetetlen lehet a használatuk.

Irodalom

Ahumada, A.L., 2002.: Periglacial phenomena in the high mountains of northwestern Argentina. South African Journal of Science. 98, 166-170.

Aszalós, J.M., Krett, G., Anda, D., Márialigeti, K., Nagy, B., Borsodi, A.K., 2016.: Diversity of extremophilic bacteria in the sediment of high-altitude lakes located in the mountain desert of Ojos del Salado volcano, Dry-Andes. Extremophiles. 20(5), 603-620.

Aszalós, J.M, Szabó, A., Megyes, M., Anda, D., Nagy, B., Borsodi, A.K. 2020.: Bacterial diversity in a high-altitude permafrost thaw pond on Ojos del Salado volcano, Dry-Andes. Astrobiology 20 (6), 754-765.

Azócar, G.F., Brenning, A., 2010.: Hydrological and Geomorphological Significance of Rock Glaciers in the Dry Andes, Chile (27°-33°S). Permafrost and Periglacial Processes. 21, 42-53.

Azócar, G.F., Brenning, A., Bodin, X. 2017.: Permafrost distribution modelling in the semiarid Chilean Andes, The Cryosphere, 11, 877–890

Clapperton, C.M., 1994.: The quaternary glaciation of Chile: a review. Revista Chilena de Historia Natural. 67, 369-383.

Corte, A.E., 1982.: Geocriología Argentina general y aplicada. Revista del Instituto de Ciencias Geológicas. 5, 87-120.

Grosjean, M., Veit, H., 2005.: Water Resources in the Arid Mountains of the Atacama Desert (Northern Chile): Past Climate Changes and Modern Conflicts. In: Huber, U.M., Bugmann, H.K.M. and Reasoner, M.A. eds. Global Change and Mountain Regions: An Overview of Current Knowledge. The Netherlands: Springer Netherlands. pp. 93-104.

Gruber, S. 2012.: Derivation and analysis of a high-resolution estimate of global permafrost zonation. The Cryosphere, 6, 221–233.

Houston, J., Hartley, A.J., 2003.: The central Andean west-slope rainshadow and its potential contribution to the origin of hyper-aridity in the Atacama Desert. International Journal of Climatology. 23, 1453-1464.

Kull, C., Grosjean, M., Veit, H., 2002.: Modelling modern and Late Pleistocene glacio-climatological conditions in the North Chilean Andes (29-30° S). Climatic Change. 52, 359-381.

Mari, L., Nagy, B., heiling, Zs., Nemerkényi, Zs. 2014.: Pszeudokarszt a Száraz-Andokban? Az Ojos del Salado olvadáshoz köthető felszínformái . Karsztfejlődés XIX. pp. 231-241.

Messerli, B., Grosjean, M., Vuille, M., 1997.: Water availability, protected areas, and natural resources in the Andean desert Altiplano. Mountain Research and Development. 17(3), 229-238.

Nagy, B., Ignéczi, Á., Kovács, J., Szalai, Z, Mari, L. 2019.: Shallow ground temperature measurements on the highest volcano on Earth, Mt. Ojos del Salado, Arid Andes, Chile. Permafrost Periglac 30(1):3-18.

Nagy, B., Kovács, J., Ignéczi, Á., Beleznai, Sz., Mari, L., Kereszturi, Á., Szalai, Z. 2020.: The Thermal Behavior of Ice-Bearing Ground: The Highest Cold, Dry Desert on Earth as an Analog for Conditions on Mars, at Ojos del Salado, Puna de Atacama-Altiplano Region. Astrobiology 20 (6), 701–722.

Vuille, M., Ammann, C., 1997.: Regional snowfall patterns in the high, arid Andes. Climatic Change. 36, 413-423.

Takasu, T., Yasuda, A. 2009.: Development of the low-cost RTK-GPS receiver with an open source program package RTKLIB, International Symposium on GPS/GNSS, International Convention Center Jeju, Korea, November 4-6, 2009

Trombotto, D., 2000.: Survey of cryogenic processes, periglacial forms and permafrost conditions in South America. Revista do Instituto Geológico, São Paolo. 21(1/2), 33-55.

Légből kapott képek elemzése. A drónok használata a térképészetben

Dr. Kovács Béla, egyetemi adjunktus
Hajdinákné Vörös Fanni, doktorandusz
Pál Márton, doktorandusz
ELTE Eötvös Loránd Tudományegyetem, Informatikai Kar, Térképtudományi és Geoinformatikai Intézet
climbela@map.elte.hu

A drónos repülések jogi hátteréről

A magyarországi légtérben a drónok (a magyarul is elterjedt általános elnevezés az angol *drone* = ”méh/here” illetve „zümmögés” elnevezésből került át a mindennapi használatba), pontosabban az UAV/UAS rendszerek (Unmanned Aerical Vehicle – vagyis személyzet nélküli légi jármű/Unmanned Aerical System – rendszerek) használatát a Lt. (Légiközlekedésről szóló 1995. évi XCVII. törvény) szabályozta részlegesen. Egészen 2020. decemberéig ez a szabályzás nem követte le, nem szabályozta megfelelően a drónok fejlődésének rohamos változását, sem a drónok használatának elterjedését a mindennapi életben. Sajnos az új törvénymódosítást rohammunkában előkészítők megalkották Európában (és talán tágabb környezetében) az egyik legszigorúbb szabályzást, aminek a technológia elterjedésének korlátozó hatását talán a törvényalkotók sem látták/láthatták át teljesen. A szinte csak korlátozásokat tartalmazó szabályozás a dróntechnológia hazai elterjedésének sebességét, a technológia fejlődését gyakorlatilag nullára csökkentette – hosszabb időre. Az addig használt sokezer kereskedelmi, mezőgazdasági, távérzékelési és hobbi célú drón gyakorlatilag hónapokra, ha nem évekre földre kényszerült. A legális felszállási lehetőségek, repülések, mérések, kutatások, permetezések, öntözések és egyéb célú professzionális, továbbá a hobbi/szórakozás célú drónozások egyik napról a másikra ellehetetlenültek.

Napjainkra a „dróntörvény” többszörös módosításainak hatására ez némileg megváltozott. Lássuk mi volt a legális drónozás jogi háttere 2020. december közepéig, lépésről lépésre:

- Rendelkeznünk kellett egy drónnal (gyakorlatilag bármely nagyáruház polcain kapható eszközök megfelelőek a hobbi célú repülések végrehajtására), a professzionális célú drónok elterjedése még épp csak felfutó ágra szállt – talán párszázas nagyságrendet képviselt a sokezres játékgépek mellett.
- A kiszemelt területről kiterjedt helyismerettel kell rendelkeznünk, vagy az első repülés előtt pilótaszemmel is fel kell mérnünk a veszélyeket/lehetőségeket (felszállás helye, repülést korlátozó tényezők, fák, távvezetékek, esetleges egyéb veszélyforrások stb.)

- A légtér használatához ún. „Eseti légtér” engedélyt kellett kérni az illetékes hatóságtól. Mindezt legkevesebb 30 nappal a tervezett felszállás előtt kellett igényelni, 3000 forintos illeték megfizetése mellett). Az engedélyt elektronikusan, ügyfélkapun keresztül lehetett intézni. Amennyiben nem tiltott, vagy védett objektumok (katonai, vagy polgári célú repterek) közelében, védett épületek, üzemek felett (pl. paksi atomerőmű, KFKI (Központi Fizikai Kutatóintézet), a magyarországi nemzetközi repülőterek stb.), vagy mások által már lefoglalt terület felett szerettük volna reptetni eszközünket, az illetékes légügyi hatóság általában megadta az engedélyt pár héten belül. Az engedélyt általában max. 30 napra lehetett igényelni, de ettől eltérő időtartamra is kiadta a Honvédelmi Minisztérium Állami Légügyi Főosztálya – vagyis az illetékes hatóság – megfelelő kérelmezői indoklás esetén.
- Felelősségbiztosítással javasolt (később kötelező) volt rendelkezni, hisz esetlegesen a drónnal másoknak okozott kár megtérítése igencsak megterhelte volna a pénztárcáját a távpilótának. (Gyakorlatilag a gépkocsik „kötelező GFB” biztosításának mintájára, néhány biztosítónál lehetett – a gépkocsikkal kb. egyező összegű – drón-biztosítást kötni).
- Egyes dróngyártó cégeknél a gépkocsis „CASCO”-s biztosítások analógiájára lehetett önrészes vagy teljeskörű eszközbiztosítást is kötni a saját/töréskárra (ez természetesen nem volt kötelező, és a kisebb, hobbi célú drónokra nem is volt költséghatékony megoldás, de egy sokmilliós, távérzékelési szenzorokkal felszerelt drónnál ez természetesen megtérülhetett: pl. egy madárrajjal történő ütközés, vagy egy műszaki hiba miatti baleset esetén)
- Javasolt volt valamilyen egyesületnek (pl. DOE (Drónpilóták Országos Egyesülete), MNME (Magyar Nemzeti Mentődrónpilóták Egyesülete), MDISZ (Magyar Drón Ipari Szövetség), stb.) tagja lenni, hisz ezek a drónos érdekképviseletek a vitás kérdésekben segíthették a pilótákat jogi, biztosítási és technikai tanácsokkal is.
- Nemhivatalosan és hivatalosan is sok szervezet, egyesület, cég „drón/pilótavizsgákat” szervezett, amelyek egyedi, (jobb esetben) saját tananyag által összerakott tanfolyamokat, pilótavizsgákat indítottak. Az ilyen helyeken megszerezhető drónpilóta/kompetencia vizsga nem volt kötelező (nem volt olyan egységes kritérium, mint pl. a gépkocsivezetői jogosítványok esetében), de megléte a hatósági ellenőrzések során szintén segíthette a hatósággal történő eredményes kommunikációt.
- Speciális esetekben a szabályos/jogkövető repülésekhez egyéb hatóság engedélyét/jóváhagyását/hozzájárulását is be kellett szerezni (pl. természet-

védelmi területek feletti repülésnél az illetékes hatóságok engedélye, vagy repterek/leszállók, gyakorlópályák környezetében az illetékes szervek hozzájárulása a repülésünkhöz). Ez érthető volt, hiszen pl. egy kórházi helioport esetében szükséges és jó, ha a repülésirányítók tudtak az esetleges légtérben repülő eszközeinkről. Ezen engedélyek zöme a repülésbiztonság növelése miatt volt javasolt, és csak a legritkább esetben kellett érte sokat fizetni.

- A repülés napján az illetékes hatóságot a tervezett repülés előtt ~60 perccel telefonon értesíteni kellett, így lezárták mások előtt – illetve biztosították – a számunkra kijelölt ideiglenes légteret. A repülés napján a terepre érkezve, az UAV eszközünk ún. ellenőrzési listáján végig menve – ha minden rendben volt – már fel is szállhattunk. Természetesen az ellenőrzési lista némileg rövidebb mint az utasszállító gépek checklist-jei, de a repülésbiztonság miatt létfontosságú minden pontja.
- A repülés végén szintén fel kellett hívni a hatóságot, hogy „visszaadjuk" a légteret, és a repülési korlátozásokat szüntessék meg a területünk felett. Amennyiben az engedélyezett 30 napon belül ugyanazon a területen belül szerettünk volna repülni, akkor már nem kellett a teljes engedélyeztetési procedúrán átesni, csak a repülés megkezdését bejelenteni majd a végén a kijelentkezést kellett megejteni.
- A hatóság bármikor azonnali leszállásra kötelezhette a drónpilótát.

Az általános adatvédelmi rendelet (EU 2016/679 GDPR) a magánszemélyek, közszereplők, tulajdonok „sérthetetlenségét" csak részben szabályozza. Nem szabályozhatta megfelelően korábban, hisz a technológia hihetetlen sebességgel fejlődött, a jogi szabályozás pedig csak leköveti azt. A képalkotás minősége, a szenzorok felbontása már a hobbi célú drónoknál is a technológiai fejlődés „Moore-törvényét" is túlszárnyalva, rohamosan nőtt. Az első kereskedelmi drónok kameráinak minősége/felbontása alig volt jobb a kilencvenes évek „buta" mobiltelefonjainak fényképező paramétereitől. Mára a tenyérnyi repülőeszközök FullHD-s kamerával rendelkeznek, de nem ritka a 8K-s felbontású, akár 60 képkocka/másodperc sebességű videókat is készíteni képes képfelvevő, ami a drónba helyezett memóriakártyán tárolhatja felvételeinket, vagy akár streamelve is képesek valós idejű élőképet közvetíteni (akár a világhálóra is), a repülőeszköz látókörébe eső területről. Az optikai felbontás ezeknél az eszközöknél akár 100 méter feletti repülési magasságból is jól felismerhetővé teszi a képen látható személyeket. A professzionális UAS eszközök kamerái, szenzorai a felmérési repülési magasságból akár pár mm/pixel felbontású képeket is képesek készíteni. Természetesen a fenti felbontás egy geodéziai légi térképezésnél, felmérésnél, vagy egy híd, objektum, távvezeték vizsgálatánál, egy épület régésze-

ti/restaurálási felvételezésekor szükséges lehet, de egy esetleges, illegális célú megfigyelés, más tulajdona, ingatlana feletti betekintés esetén rengeteg törvényi passzust sérthet.

A magyar kormány 2020 decemberében az EU-s jogharmonizációs kötelezettség miatt (amit az Európai Unió 2019/947. rendelete egyes kérdéseket tagállami hatáskörbe utalt) beterjesztett, előtte sokáig halasztgatott, majd villámgyorsan elfogadott, azóta többször módosított – a köznyelv által csak „dróntörvénynek" nevezett – szabályozást az Országgyűlés 2020. december 16-án elfogadta. A 2020. évi CLXXIX. törvény, amely három már eddig is létező passzust módosít: a légi közlekedésről szóló 1995. XCVII. törvény (Lt.), a szabálysértésekről, eljárásokról és nyilvántartási rendszerről szóló 2012. II. törvény (Szabs. tv.) valamint a BTK 2012. évi C. törvényt (Btk.)).

A 2020. december 22-én a Magyar Közlöny 285. számában kihirdetett új szabályozás olyan passzusokat tartalmaz, amelyek szinte teljesen ellehetetlenítették a drónos repüléseket idehaza, hisz 2021. január elsején lépett életbe, de több pontjához nem jelentek meg addig a végrehajtási szabályok/leírások. Néhány pontja ugyan 2021. február 10-ig némi haladékot adott a felhasználóknak, de az EU-s rendelettől sok esetben eltért, sokkal szigorúbb feltételeket szabott (ezt a szigorítást az EU-s rendelet lehetővé teszi) a drónokat kezelő pilótáknak és a légijárműveket is másképp kategorizálja.

Hazai specialitások

A hazai szabályok a 120 g teljes felszállótömeg alatti, kamera/képrögzítő nélküli légi járműveket sorolják a „játék" kategóriába. Ezekkel teljesen szabadon, szinte bárhol, bármikor repülhetünk azzal a feltétellel, hogy az eszköz ne tudjon 100 m-nél nagyobb távolságra eltávolodni a pilótától.

Az EU-s rendelet a 250 g-ot tekinti a 120 g helyetti határtömegnek. A piaci termékeket vizsgálva láthatjuk, hogy míg Európa nagyobb részében egy „normál, hobbicélú", de akár 2/4k-s felbontású kamerával szerelt eszköz is viszonylag egyszerűen röptethető, addig idehaza csak a nagyáruházak polcairól maximum pár 10 ezer forintért megvásárolt játékok esnek ebbe a kategóriába.

A műveleti kategóriák beosztása zömmel két tényezőtől, a be nem vont személyektől való távolságtól és a drón paramétereitől függ. Ez utóbbival kapcsolatos részletes követelmények a 2019/945 Felhatalmazáson alapuló rendeletben (EU 20192) olvashatók.

A gyártóknak C0/C1/C2/C3/C4 osztályokba kell sorolniuk az UAV/UAS eszközöket:

- A C0 osztályba tartozó UAV-ok 250 g-nál könnyebbek, nem képesek 10 m-nél magasabbra repülni, vízszintesen max. 19 m/s-al képesek haladni,

követési mód esetén max. 50 m-re tudnak eltávolodni a pilótától, valamint elektromos árammal kell működniük (24 V egyenáram vagy ezzel egyenértékű váltakozó áram).

- A C1 osztályú gépek az előző kategóriától annyiban különböznek, hogy maximális tömegük 900 g, rendelkezniük kell sorozatszámmal, GPS-szel, távoli azonosításra alkalmas rendszerrel, valamint az éjszakai láthatóságot biztosító lámpákkal, amelyek révén egyértelműen megkülönböztethetők a pilótával rendelkező repülőgépektől.
- A C2-es drónok hajthatnak végre műveleteket az A2-es kategóriában. Ennél fogva bizonyos esetekben akár 5 m-re is megközelíthetnek embereket. Felszállótömegük max. 4 kg lehet, 120 m-nél nem repülhetnek magasabbra (ha képesek rá, a funkció legyen korlátozható), rendelkezzenek alacsony sebességű móddal, ahol a max. vízszintes sebesség 3 m/s, elektromos árammal működjenek (48 V egyenáram vagy ezzel egyenértékű váltakozó áram), legyenek ellátva sorozatszámmal, GPS-szel, távoli azonosításra alkalmas rendszerrel, valamint éjszakai láthatóságot biztosító lámpákkal, amelyek révén egyértelműen megkülönböztethetők a pilótával rendelkező repülőgépektől.
- A C3 osztályba azok a nagyobb drónok kerülnek, amelyekre a következő feltételek igazak: szerkezetük könnyebb, mint 25 kg, méretük 3 m-nél kisebb, 120 m-nél nem repülnek magasabbra (ha képesek rá, a funkció legyen korlátozható), elektromos árammal működnek (48 V), van sorozatszámuk, GPS-ük, távoli azonosításra alkalmas rendszerük, valamint rendelkeznek éjszakai láthatóságot biztosító lámpákkal, amelyek révén egyértelműen megkülönböztethetők a pilótával rendelkező repülőgépektől.
- A C4-es osztályú gépekre kevés kritériumot határoz meg a jogszabály: 25 kg-nál könnyebbnek kell lenniük, valamint ne lehessen őket automatikusan irányítani.

A fenti kategóriákat a gyártóknak 2023. január elsejétől kötelező lesz alkalmazniuk az új forgalomba kerülő drónok jelölésére, illetve a már meglévő drónokat is be kell kategorizálniuk a C0-C4 csoportokba.

A nyílt műveleti kategóriában (A1/A2/A3) a szabályozás az alábbiakat tartalmazza:

A 120 g felszállótömeg fölötti (akár képrögzítővel felszerelt) gépekkel ún. nyílt kategóriájú (A1/A2/A3) műveleteket végezhetünk. Szükségünk van ilyen jármű röptetése esetén hatósági díjazású drónregisztrációra (az eszköz és az üzembentartó nyilvántartásba vétele is kötelező) is. Erre a műveleti kategóriára az alábbi általános szabályok vonatkoznak:

- a drón maximális felszállótömege 25 kg,
- emberektől biztonságos távolságra kell repülnünk,
- ebből következően nem repülhetünk embertömeg fölött,
- maximum 120 méter magasra távolodhatunk el a földfelszínnek a drónhoz legközelebbi pontjától (kivéve akadály esetén, jogszabályi indokkal),
- a távpilótának a repülés alatt végig látnia kell a drónt (kivéve követési mód vagy megfigyelő személy alkalmazása esetén),
- nem szállíthat veszélyes árut, valamint nem szórhat le semmilyen anyagot.

A nyílt kategóriára vonatkozó egyéb részletek a 2019/947 sz. végrehajtási rendelet mellékletének „A" részében olvashatók (EU 20191). A szabályozásban 2023. január 1-ig átmeneti időszak van érvényben. Ennek oka az, hogy a gyártók kötelesek lesznek ekkorra 5 kategóriába (C0/C1/C2/C3/C4) sorolni az UAV-okat. Eddig van idejük felkészülni a törvényben rögzített gyártási feltételekre, valamint osztályba sorolni az eddig forgalmazott eszközöket. Az ehhez kapcsolódó részletszabályok a 2019/945 sz felhatalmazáson alapuló rendeletben (EU 20192) olvashatók.

A most forgalomban lévő, de 2023-ig osztálybesorolással nem rendelkező 250 g feletti felszállótömegű drónok csak A1 és A3 műveleti alkategóriákban repülhetnek majd – ez általánosan vonatkozik az otthon épített, a 25 kg feletti nem osztálybesorolt és modellgépekre is.

- Az A1 műveleti alkategóriába tartoznak a legkönnyebb drónok. Otthon épített eszköz 250 g alatt, C0 osztályú eszköz 250 g alatt, C1 osztályú eszköz 900 g alatt, valamint az átmeneti időben osztálybesorolás nélküli eszköz 500 g alatt végezhet tevékenységet ebben a kategóriában. 250 g MTOM (Maximum Takeoff Mass – teljes felszállótömeg) alatt átrepülhetünk egyének fölött, de ennél nehezebb drón esetében nem szabad olyan területre repülnünk, ahol emberek tartózkodhatnak, embertömeg fölé pedig egyáltalán nem mehetünk. Ha véletlenül mégis emberek közelébe érünk, haladéktalanul, biztonságos módon el kell mozgatnunk a légi járművet.
- Az A2 műveleti alkategóriában a C2 osztályba tartozó 4 kg-nál kisebb, valamint az átmeneti időszakban osztálybesorolás nélküli 2 kg-nál könnyebb gépek végezhetnek műveletet. Embertömeg fölé ebben a kategóriában sem repülhetünk, viszont C2 osztályú drónnal 30 m-re megközelíthetünk a műveletbe be nem vont személyeket, amely távolság bekapcsolt alacsony sebességű repülési üzemmód esetén vízszintesen mért 5 m-re csökkenthető az 1:1 szabály (a nem bevont személyektől olyan vízszintes

távolságot kell tartanunk, amilyen magasan repülünk) betartása mellett. Osztálybesorolás nélkül maximum 50 m-re közelíthetünk meg be nem vont személyt.

- Az A3 műveleti alkategóriába azok a műveletek tartoznak, amelyek során:
  - a légi jármű maximális felszálló tömege 25 kg alatti,
  - C2, C3, C4 vagy ezeknek megfelelő osztályba tartozó, otthon épített eszközzel repülünk,
  - be nem vont személyekhez közel és föléjük nem repülünk, minimum 30 m távolságot tartunk tőlük az 1:1 szabály értelmében,
  - 150 m-es vízszintes távolságot tartunk lakott, kereskedelmi, ipari vagy szabadidős területtől,
  - a C2 és C3 kategóriájú drónok rendelkeznek aktív közvetlen távoli azonosítási rendszerrel és GPS-szel,
  - nem lehet közelebb bevont személy, mint a drón maximális sebességen 2 másodperc alatt megtett útja.

A speciális és engedélyköteles műveleti kategóriák zömében a személyszállítás, áruszállítás, illetve az anyagkijuttatás (permetezés) tevékenységét írják le. A kategóriák részletei és szabályozása a mai napig nem készültek el.

Felszállás?

Lássuk, hogyan lehet 2021. január elsejétől kezdve legálisan Magyarországon drónnal felemelkedni a talajról (akárcsak 1 cm-t is, hisz az is már légtérnek minősül, akár a saját udvarunkon is):

Az eseti légtérigénylés szabályainak legfontosabb változásai:

- csak lakott terület feletti repülés esetén kötelező.
- 9000 HUF-ra emelkedett az igazgatási szolgáltatási díj (ITM részére).
- Legalább 30 nappal a tervezett repülés előtt kell benyújtani, kizárólag elektronikus formában a Honvédelmi Minisztérium Állami Légügyi Főosztályához.
- Esetenként max. 7 egymást követő repülési napra igényelhető.
- Kötelező a „mydronspace" alkalmazás használata a mobilunkon (ha nincs térerő, mobilnet lefedettség: tilos a repülés bármilyen kategóriában).
- „No Drone Zone" légtereken tilos drónozni (kivéve: eseti légtér engedéllyel).

A pilótáknak a műveleti kategóriának megfelelő hatósági (KTI) távpilóta kompetencia vizsgát kell tennie (az A1/A3, illetve az A2-es vizsgák érhetők el napjainkban, amelyek komoly elméleti meteorológiai, műszaki, technológiai, repüléstechnikai, fizikai ismereteket és gyakorlati repülési tudást igényelnek).

Amennyiben fénykép készítésre nem alkalmas (vagyis játék) drónnal rendelkezünk, vagy lakott területen kívül szeretnénk reptetni a drónt, akkor viszont sokat egyszerűsödik a repülés. Gyakorlatilag csak a „mydronespace" alkalmazás használatával vagyunk kötelesek bejelenteni a felszállás előtt a drónozásunkat, és amennyiben „szabad" a légtér, már fel is szállhatunk. Itt is érvényes, hogy már elmúltunk 16 évesek, vagy van felelős nagykorú személy/ „drónpilóta" a közelünkben (természetesen a tiltott/veszélyes/ipari/lakott területek meghatározott távolságában/felett továbbra sem repülhetünk).

A drónt és az üzembentartót is regisztrálni kell a vásárlást követően és az első repülést megelőzően (ez gyakorlatilag a „gépkocsi rendszám" analógiájára történik: minden repülőeszköz kap egyedi azonosítót, amit kötelesek vagyunk látható módon elhelyezni a drónunkon).

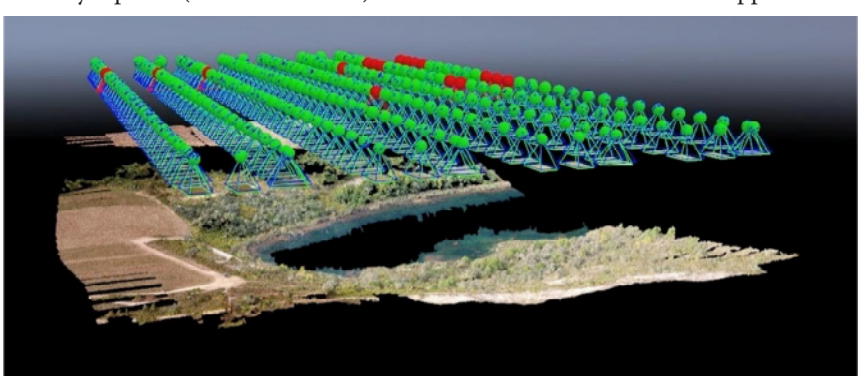
Hurrá, repülünk!

A rengeteg előzetes jogszabály és törvény betartását követően, ha minden repülési feltétel is adott (nem esik az eső, tiszta az ég, nincs erős szél, sem madarak, egyéb korlátozó tényezők), megvannak az esetlegesen szükséges engedélyek, hozzájárulások, a biztosításunk érvényes, a drón műszakilag rendben van: felszállhatunk. A következőkben néhány oktatási/kutatási feladatunkat mutatjuk be.

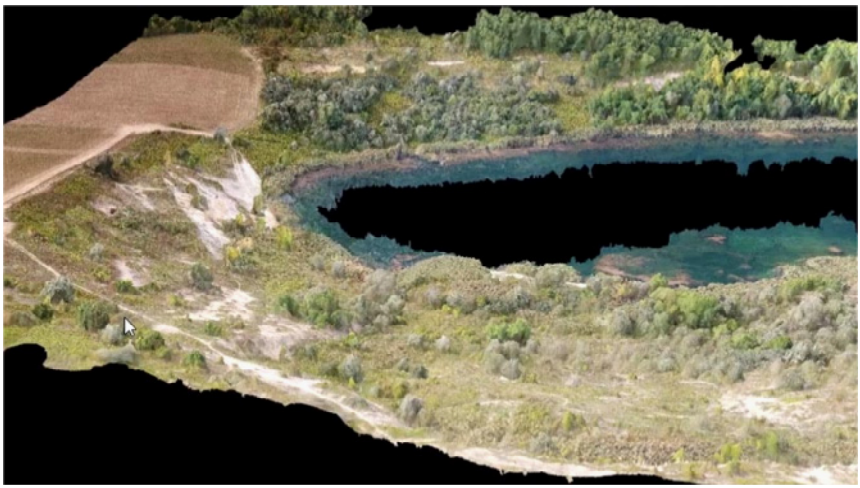
Bajna–Hantospuszta, a rekultivált bányaterület felmérése és a talaj mikroerózió vizsgálata. A mintaterületünk Budapesttől bő 50 km távolságra a Gerecse lábánál található. Az érdekessége, hogy semmilyen állandó repülési korlátozás nincs a területen, nem TvT (Természetvédelmi Terület), nem lakott terület stb., így a terület felett nagyon egyszerű megszervezni az oktatási és kutatási célú repüléseket és a hallgatóinkat is itt taníthatjuk meg a drón használatra – a lehető legkevesebb adminisztratív kötelezettséggel.

A fenti képen a mára feltöltött, és teljesen rekultivált egykori bányagödör, napjainkban: mesterséges tó látható. A kép alján lévő terület erózióvizsgálatára használjuk a drónra szerelt nagyfelbontású RGB és multispektrális szenzorainkat. Ez a kép 100m magasságból készült, 45° állású RGB kamerával, DJI Matrice 210 RTK V2-es drónról (2021-es felvétel).

A hantospusztai mintaterület függőleges kameraállásban, 500 m magasságból fényképezve (2020-as felvétel!). Az eredeti felbontás kb. 20cm/képpont.

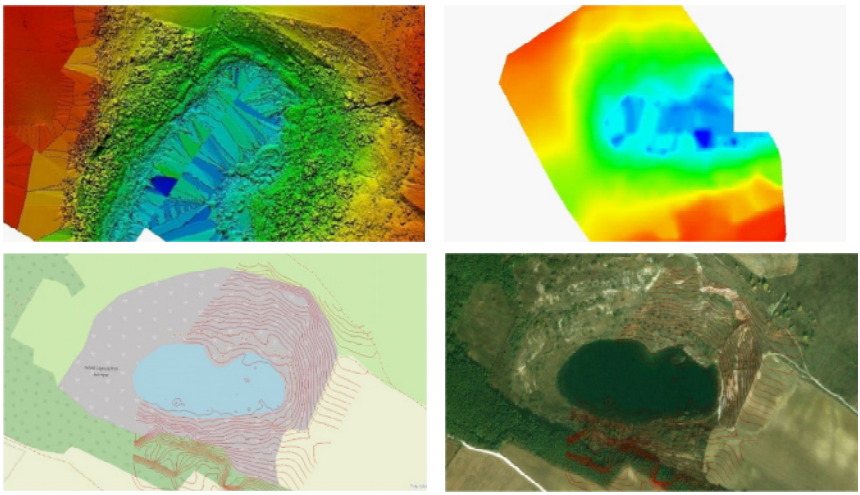


A terület nagyfelbontású felmérése: a képen az egyes képkockák exponálásának és a lefedett terület egyedi képkockáinak pozíciója látható. Az ortofotóhoz/pontfelhőhöz több, mint 400 felvételt készítettünk az illesztésekhez szükséges 70%-os átfedéssel. A repülési magasság 80 m volt a tó felszínétől mérve a multispektrális szenzor használata miatt (ettől magasabban repülve az elvárt ~2 cm/pixel felbontás csökkent volna).



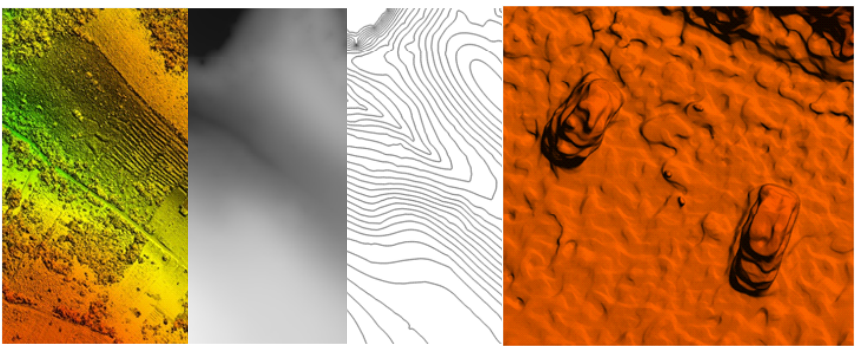
A mesh (háromszögháló) alapján felépített 3D-s modell a mintaterületről. A víz felülete a szenzorok számára „kemény dió" hisz pl. az enyhe szél miatti fodrozódás teljesen ellehetetleníti a pontos illesztést és képalkotást. A nyers felvételen jól látható a térbeli elrendezés és a vízfelület döntő részének „feketesége" – vagyis kiértékelhetetlensége.

A fenti kivágaton egy 6x4 m terület látható, amelyen az idősoros elemzés alapján jól követhető lesz a partfalak eróziója a tervezett folyamatos havi ismétlésű felvételsorozatokon. A programozott repülések előnye, hogy a drónt akármikor, akárhányszor tudjuk pontosan ugyanazon a rögzített/tervezett nyomvonalon reptetni. A felvételek így mindig ugyanabból a szögből készülnek, pontosan ugyanabból a pontból.

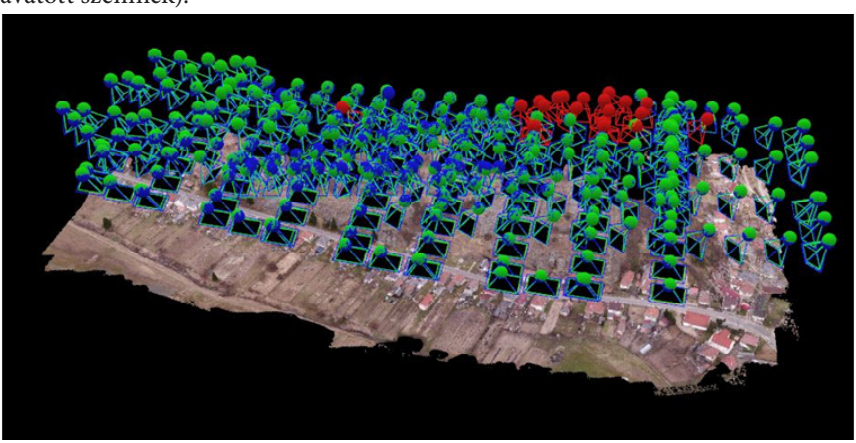


A hantospusztai területről készített DSM (digitális felszínmodell). Jól elkülöníthető a növényzetborítottság, a szántó és a mikrodomborzat. A hamis színezés segíti az elemzők munkáját. A vízfelület az előbbiek során említettek miatt nem definiálható jobban automatikus feldolgozás esetén. A DTM (digitális terepmodell) már a növényzetborítás nélküli modell, amelyből szintvonalas térkép készíthető pár kattintással a célszoftverekben. Az automatikusan generált térképünk összevethető előző légifelvételekkel vagy űrfelvételekkel is. A pontosságunk (~2 cm/képpont) nagyságrendekkel jobb, mint a területről korábban készített felvételeké/légi felméréseké.

A fenti kép Mogyorósbánya külterületén készült ősszel, ahol a háttérben látható nagyfelbontású raszteres orthomozaikból automatikusan készített vektoros digitális térképfedvény látható. Az ilyen programozott automatizált térképkészítés nagyságrendekkel gyorsíthatja egyes terepi felmérési feladatok elvégzését. Természetesen nem helyettesíthető teljesen az emberi erőforrás, de a lassú monoton munkafázis részben/teljesen kiváltható.

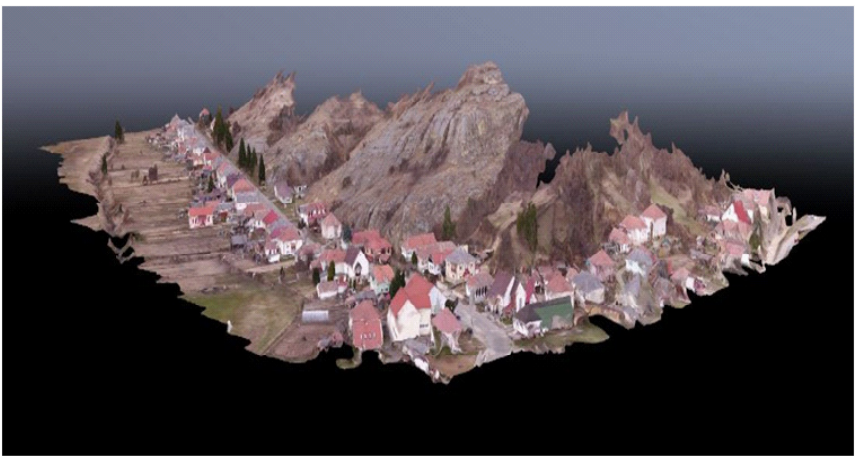


A fenti képsorozaton a mogyorósbányai (felhagyott és újratelepített) szőlőültetvények láthatók, DSM/DTM és automatikusan generált szintvonalas térképpel (a jobboldali 50x nagyítású képen a 3D-s modellünk felbontását mutatjuk be. Ezen a két terepi autónk, illetve közte a három pilóta is jól felismerhető az avatott szemnek).

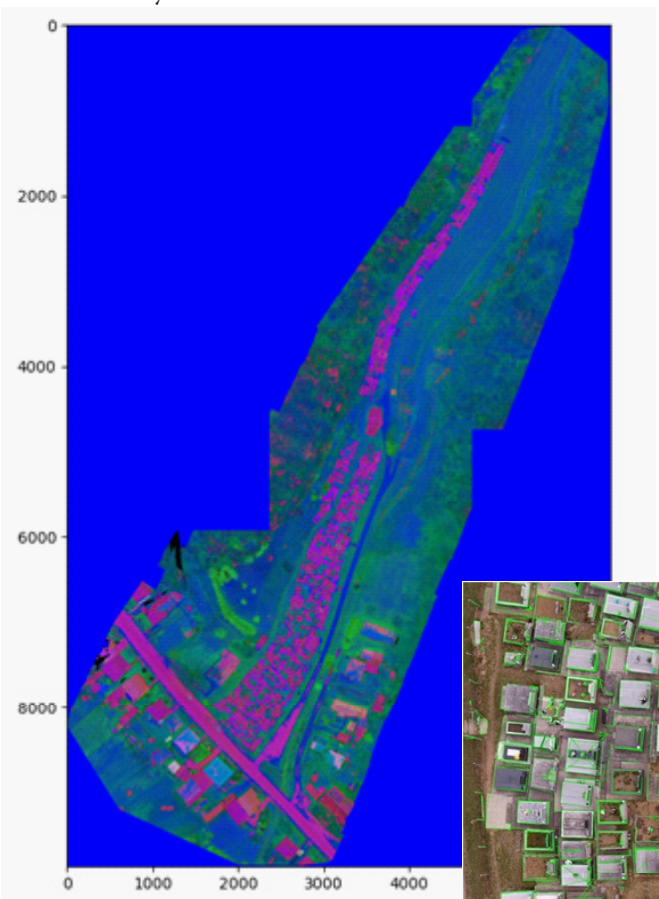


Egy újabb mintaterületünk: Istenmezeje (Noé szőlőbirtoka, vagyis a Pétervásárai homokkő). A 3D-s modellkészítéshez a tervezett repülés és az elkészített felvételek pozíciója, és a következő képeken az elkészült 3D-s modell különböző nagyításban látható (az ilyen modellek elkészítése napjaink korszerű számítógé-

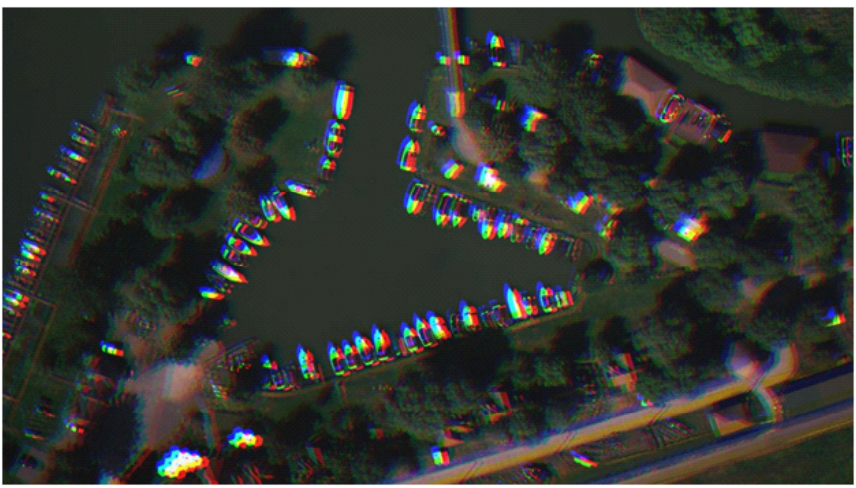
peinek is „egy teljes éjszakai műszakot” igényelnek gépidőben). Sajnos a papírnyomaton nem lehet bemutatni a 3D modell minden részletét, a lenti grafikai megjelenítés nem fénykép, hanem térben mérhető, elforgatható, elemezhető ponthalmazból épül fel.



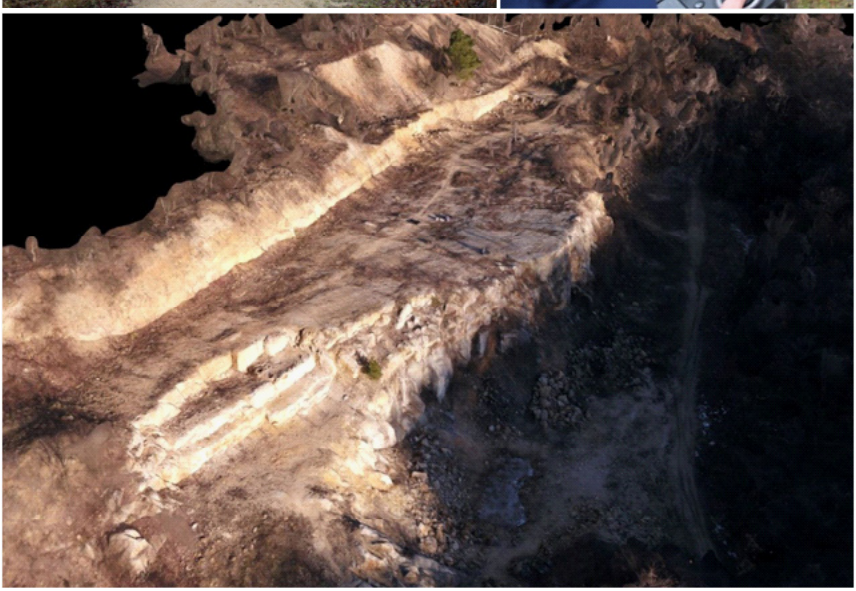
Az automatikusan végrehajtott tervezett repüléssel, majd komolyabb programozással a raszteres felvételeken objektum detektálás is történhet. A baloldali képen az istenmezejei temető látható multispektrális felvételen. Jobbra a terület egy kis része és az automatikus objektum felismerés eredménye (világoszöld keretek a felismert sírok, síremlékek körül). Még dolgozunk rajta, de már kecsegtető eredményeket láthatunk a felvételeinken:



Példa a multispektrális RAW szenzorkalibrálásra a következő képpár. Az első képen nem nyomdahiba látható, hanem a sokcsatornás MicaSense szenzorunk eredeti nyers csatornáinak képe a tiszafüredi Kormorán kikötőről. A következő kép a kollégáink szenzorkalibrációinak eredménye. Az eltolódott csatornák a helyükre kerültek, kialakult az éles szenzorfelvétel (talán sima fényképnek is nevezhetnénk, de ez nem pontosan az, ez egy mérhető adatbázis vizualizációja!)

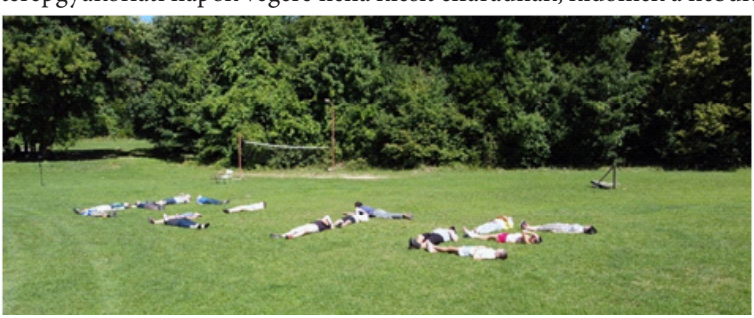


Természetesen, aki dolgozik az hibázhat is: Budapest mellett, Ezüsthegyen a felhagyott bánya területén geológiai célból szerettünk volna részletes drónos felmérést készíteni. Sajnos mire összeállt a rendszerünk és az időjárás is kegyessé vált, elállt a nagy szél, sok idő eltelt és a napállás változásával nem számoltunk. A felvételeinkből összerakott orthomozaik nagy része árnyékos, használhatatlan adathalmaz lett. A kép részleteiben elemezhető, de egészében a kontrasztarányok kuszasága miatt nem. Az alsó felvételen kb. 800 felvételből összerakott többhektárnyi terület látható. Rajta kissé elrejtve: a felmérést végző kollegák is jól felismerhetők.



A másik drónról elkövetett felvételen az ELTE IK „drónos” csapata, vagyis a cikk szerzői és a felméréseinkhez használt DJI gyártmányú Matrice 210 V2 RTK típusú UAS látható felszállás közben:

Az eszközeinket természetesen egyetemi oktatására is felhasználjuk. A nyári terepgyakorlati napok végére néha kicsit elfáradnak, kidőlnek a nebulóink…



Vagy mi is látható, ha repülőgépünkről más perspektívából tekintünk ugyanarra a csapatra?

Leltár: A felvételek elkészítéséhez használt eszközök, és az előadó…

A cikk az EFOP-3.6.3-VEKOP-16-2017-00001 és a TKP2020-NKA-06 pályázatok támogatásával készült.

Ajánlott irodalom:

1995. évi XCVII. törvény a légiközlekedésről (Lt.):https://njt.hu/jogszabaly/1995-97-00-00 (utolsó elérés dátuma: 2021.12.14)

2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről (Szabs. tv.):https://njt.hu/jogszabaly/2012-2-00-00 (utolsó elérés dátuma: 2021.12.14)

2012. évi C. törvény a Büntető Törvénykönyvről (Btk.):https://njt.hu/jogszabaly/2012-100-00-00 (utolsó elérés dátuma: 2021.12.14)

Alex Elliott (2017): Drónok kézikönyve. CSER Kiadó, Budapest

DJI (2020): MATRICE 200 SERIES V2: M200 V2 / M210 V2 / M210 RTK V2. Online elérhető felhasználói kézikönyv: https://dl.djicdn.com/downloads/m200_v2/20200630/M200_Series_V2_User_Manual_en3.pdf (utolsó elérés dátuma: 2021.12.14)

Drónpilóták Országos Egyesülete (2021): Szabályos Drónhasználat folyamatábra A1/A3 Open – tájékoztató jellegű segéd-let. Online: https://doe.hu/szabalyos-dronhasznalat-folyamatabra (utolsó elérés dátuma: 2021.12.14)

Európai Bizottság (2019)1: 2019/947 Végrehajtási rendelet: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0947&from=HU#d1e2148-45-1 (utolsó elérés dátuma: 2021.12.14)

Európai Bizottság (2019)2: 2019/945 Felhatalmazáson alapuló rendelet: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0945&from=HU (utolsó elérés dátuma: 2021.12.14)

Légtér (2021): Drónozás nyílt kategóriában. Online: https://legter.hu/blog/dronozas-nyilt-kategoriaban/ (utolsó elérés dátuma: 2021.12.14)

Légtér (2021): Drón törvény 2021 – érthetően szakértőktől. Online:https://legter.hu/blog/dron-torveny-2021-erthetoen-szakertoktol/ (utolsó elérés dátuma: 2021.12.14)

Major Krisztina, Kozma-Bognár Veronika, Enyedi Attila, Váradi Ádám & Berke József (2016): Távirányítású drónok kutatási célú vizuális adatainak alkalmazása az oktatásban. XXII. „Multimédia az Oktatásban" nemzetközi konferencia, Keszthely.

MicaSense (2020): MicaSense Altum™ and DLS 2 Integration Guide. Online felhasználói kézikönyv: https://support.micasense.com/hc/en-us/articles/360010025413-Altum-Integration-Guide-PDF- (utolsó elérés dátuma: 2021.12.14)

Dr. Palik Mátyás [szerk.] (2013): Pilóta nélküli repülés profiknak és amatőröknek. Nemzeti Közszolgálati Egyetem

Pál Márton, H. Vörös Fanni, Dr. Kovács Béla (2021): Szabálykövető drónhasználat az ELTE-n: milyen feltételeknek kell megfelelnünk, hogy repülhessünk? Geodézia és kartográfia, 2021/5 (73.évf.) pp. 23-29., DOI: 10.30921/GK.73.2021.5.3

Restás Ágoston (2017): A drónok közszolgálati alkalmazásának lehetőségei. Új magyar közigazgatás. KÖZSZÖV, Gödöllő, 10:3, pp. 49-63.

A drónok jelenlegi és jövőbeni alkalmazási lehetőségei a mezőgazdaságban

Dr. Gulyás Zoltán[1], Sillinger Fanni[2]

[1] *növényvédelmi mérnökszakértő, Nemzeti Élelmiszerlánc-biztonsági Hivatal Növény-, Talaj- és Agrárkörnyezet-védelmi Igazgatóság, Fenntartható Gazdálkodás Osztály (NÉBIH NTAI FGO)*

[2] *PhD-hallgató, Magyar Agrár- és Élettudományi Egyetem (MATE)*

gulyas.zoltan770314@gmail.com

Aktualitások, rövid nemzetközi kitekintés

Az elmúlt időszakban, elsősorban a megelőző három-öt esztendőben, jól megfigyelhető az a tendencia, hogy a drónok világszerte egyre markánsabb szerepet játszanak az emberiség mindennapi életében, legyen szó akár állami feladatellátásról, üzleti- vagy éppen szabadidős célú felhasználásról. Nem szükséges nagy bátorság annak a kijelentéséhez, hogy drónok alkalmazásának jelentősége számos területen tovább fog erősödni az elkövetkező időszakban.

Svédországban például már sikerrel alkalmaznak drónokat arra a célra, hogy életmentő eszközt – automata defibrillátort – juttassanak el a lehető leggyorsabban a célszemélyhez (1. kép).

1. kép: Defibrillátor szállítása drónnal Svédországban
(Forrás: https://droninfo.blog.hu/2018/06/14/eletmento_dronok_a_magyar_mentoszolgalatnal)

Olaszországban úgynevezett vízi mentő drón felügyel egyes strandokat és szükség esetén késedelem nélkül mentőövet szállít a bajba jutott személynek (2. kép).

2. kép: Vízi mentő drón az olasz tengerparton
(Forrás: https://dronvilag.blog.hu/2015/01/18/vizimento_dron_felugyeli_az_olasz_strandokat)

Az USA-ban hegymászó életét sikerült drón segítségével megmenteni. Ebben az esetben a drónt fényforrásként használták, így a segítők pontosan azonosíthatták a helyet, ahová a hegymászó került, majd, amikor a hegyi mentők megtalálták őt és elkezdték a biztonságos elszállítását, a drón a levegőből világított tovább a művelethez.

Angliában a rendőrség mellett működő kereső-mentő egység hőkamerás drónt vetett be egy autóbaleset miatt autójából kieső férfi megtalálására.

Észak-Amerika ritkán lakott területein levélküldemények és kisméretű, könnyű csomagok szállítására, Új-Zélandon pedig pizza-kiszállításra használnak drónokat.

A különböző katonai alkalmazások fejlesztése is kifejezetten előrehaladott állapotban van, elég az amerikai vagy éppen a török hadsereg ilyen típusú, a közelmúltban végrehajtott bevetéseire gondolni.

A filmipari alkalmazásoktól (3. kép) kezdve egészen az ún. szelfi drónokig (4. kép) nagyon sok példát lehetne még felsorakoztatni ebben a vonatkozásban.

3. kép: Példa filmipari drónalkalmazásra
(Forrás: http://dronerz.hu/cikk/dronok-hasznalata-a-filmes-vilagban)

4. kép: Olcsó szelfi drón kezdő felhasználók részére
(Forrás: https://namerre.hu/wp-content/uploads/dji-ryze-tello-szelfi-dron-kezdoknek-olcson.jpg)

Hazai helyzetkép, Magyarországi Drón Koalíció, Drón Stratégia

Hazánkban is számos területen teljesítenek jó szolgálatot a drónok, illetve fognak teljesíteni a közeljövőben, hiszen Magyarország élenjáró szerepre tör a drón-technológia lehető legszélesebb körben történő alkalmazása tekintetében.

Ennek a kijelentésnek az alátámasztására ehelyütt is mindenképpen bemutatásra, illetve ismertetésre érdemes a Magyarországi Drón Koalíció (a továbbiakban: MDK), illetve a koalíció által megalkotásra kerülő Drón Stratégia.

Az MDK hivatalos honlapján (HTTP1) olvasható információ szerint az MDK az Innovációs és Technológiai Minisztérium, a Széchenyi István Egyetem, a Budapesti Műszaki és Gazdaságtudományi Egyetem, valamint a HungaroControl Zrt. kezdeményezésére alakult meg 2021. május 4-én.

Alapító tagjai között – amelyek száma meghaladta a hatvanat – minisztériumok, háttérintézmények és érdekképviseleti szervek, valamint akadémiai és iparági szereplők egyaránt megtalálhatók (a koalíció taglétszáma megalakulásának napja óta folyamatosan növekszik). A szervezet koordinációs feladatait a Közlekedéstudományi Intézet és a Digitális Jólét Program látja el.

Az MDK legfontosabb céljai:

- hazánk a pilóta nélküli járművek használata terén mihamarabb a világ élvonalba kerüljön, ezáltal Magyarország a nemzetközi közösség fontos referenciapontjává váljon;
- az egységes európai uniós szabályozás alkalmazásában Magyarország mintaként szolgáljon Európának, támogató jogszabályi környezet kialakításával;
- a személyiségi jogok tiszteletben tartása mellett a pilóta nélküli légi járművek, illetve az azokon alapuló fejlesztések széleskörű elterjedésének és alkalmazásának köszönhetően jelentősen erősödjön a hazai vállalkozások versenyképessége;
- a magyar startupok és kkv-k nagy arányban vegyenek részt pilóta nélküli légi járművek fejlesztésében és gyártásában, illetve az azokon alapuló megoldások használatában – akár nagyvállalati, egyetemi vagy nemzetközi partnerségben;
- nemzetgazdasági szinten mérhető versenyképesség-növekedés elérése váljon lehetségessé a pilóta nélküli légi járművek és az azokon alapuló technológia széleskörű alkalmazásával.

Az MDK alapvetései:

- a pilóta nélküli légi járművek elterjedésének nélkülözhetetlen előfeltétele a kiszámítható és támogató szabályozói, technológiai és működési, alkalmazási környezet;
- a mintaüzemek és tesztelési infrastruktúrák és eljárások létrehozatala fontos a kutatásfejlesztési eredmények előzetes validálása érdekében;
- a pilóta nélküli légi járművek a szabályozási, működési, alkalmazási és támogatói környezetének kialakításakor a biztonságos – különösen közlekedésbiztonsági szempontoknak megfelelő – használat kiemelt szempont kell, hogy legyen;
- az alapítók szándéka, hogy egy stratégiai és szakmai platformot teremtsenek a kormányzat, a kutatói és akadémiai szféra, a piaci szereplők, az érdekképviseleti szervezetek és a felhasználók számára a magyarországi pilóta nélküli járművek használatával és fejlesztéseikkel kapcsolatban;
- az MDK hozzá kíván járulni egy világszínvonalú ökoszisztéma és tesztkörnyezet kialakításához a pilóta nélküli légi járművek területén, továbbá a magyarországi Drón Stratégia kidolgozásához és megvalósításához.

A Drón Stratégia várhatóan a 2022. év elején-közepén hivatalosan kihirdetésre kerül, jelenleg közel végleges munkaanyagként érhető el az arra illetékesek szá-

mára. A stratégia a 2022. év, valamint az elkövetkező évek legfontosabb céljait, a célok mihamarabbi eléréséhez szükséges eszközöket, a követendő irányvonalakat, a megoldandó problémák, továbbá az elvégzendő feladatok leírását tartalmazza, minden szükséges részletre kiterjedően.

A Drón Stratégia stratégiai térképe (tervezet):

- Kiemelt programok
- Felhasználási és hasznosítási területek:
  - állami feladatellátás,
  - üzleti célú felhasználás,
  - szabadidős célú felhasználás
- Széleskörű alapozó pillérek:
  - oktatás, tudatosítás, társadalmi digitalizáció és kompetenciafejlesztés elősegítése;
  - kutatás, fejlesztés, innováció, tesztelési és tanúsítási környezetek;
  - alaptechnológia – légi járművek és támogató rendszerek;
  - UTM szolgáltatások: Unmanned Traffic Management: UAS (Unmanned Aerial/Aircraft Systems, azaz Pilótanélküli Légi Rendszerek) biztonságos és hatékony mozgásának biztosításához szükséges légi és földi funkciók alkalmazott összessége az üzemeltetés minden fázisában;
  - szabályozás.
- Társadalmi alapértékek biztosítékai:
  - társadalmi jólét és komfort
  - nemzetbiztonság és védelem
  - repülésbiztonság
  - magánszféra védelme
  - környezet védelem, fenntarthatóság

A Drón Stratégia kiemelt programjai:

- Kritikus egészségügyi eszközök szállítása (életmentő orvosi- és segédeszközök, pl.: vér kórházak között, baleseti helyszínre);
- Határvédelmi hatékonyság növelése (megfigyelés, ellenőrzés, elhárítás);
- Precíziós mezőgazdaság (drónos permetezés, monitorozás: NDVI, tápanyag- és vízellátottság, fertőzések, kártevők, érési folyamatok, termésbecslés, fagykár, vadkár, …) elindítása;

- Állami infrastruktúra monitorozási szolgáltatás kialakítása (hidak, szélerőművek, közmű- és közúthálózat, telekommunikációs torony- és antennahálózat, távvezeték-hálózat stb.);
- Csomagkézbesítés;
- „Okos város" megoldások alkalmazása az állami feladatellátásban (illegális hulladéklerakás azonosítása, illegális építkezés-kivitelezés detektálása, stadion- és irodaház-fertőtlenítés);
- Társadalmi digitalizáció elősegítése drónok használatával (a drónok technológiájának, használatának, alkalmazási lehetőségeinek bemutatására, ismeretterjesztésre tematika, tananyag kidolgozása köznevelési intézmények számára).

A drónok szerepe a mezőgazdaságban

A drónok a mezőgazdaságban, azon belül a precíziós gazdálkodás területén is, évről évre egyre több célra és egyre gyakrabban kerülnek alkalmazásra, sőt a szakemberek a jelenlegi és jövőbeni precíziós gazdálkodás kiemelt fontosságú technológiai elemeként tekintenek a drónokra (HTTP2).

A következőkben – a teljesség igénye és szüksége nélkül – néhány felhasználási gyakorlat kerül bemutatásra röviden, a későbbiekben pedig a drónos légi permetezésről, illetve szabályozási környezetéről lesz szó részletesen, mert az a lehetséges mezőgazdasági alkalmazások közül az egyik legperspektivikusabb.

HTTP3 szerint egyre komolyabb gondokat okoznak a szőlő- és gyümölcsültetvényekben a seregélyek okozta károk. Erre a problémára kínálhatnak megoldást a különböző kialakítású és működési elvű riasztó drónok. A ragadozó madár alakú drónok például úgy viselkednek, mint a halrajok között a cápa. Míg a hangjelzést adó ágyúkat és a fix helyre kihelyezett eszközöket viszonylag gyorsan megszokják a károsító madarak, addig a riasztó drónok jó hatásfokkal dolgozhatnak, mert a seregélyek nem tudják őket megkülönböztetni a ragadozó madaraktól.

Radar is felszerelhető a drónokra, amelynek segítségével három dimenzióban láthatóak a mezőgazdasági területek, így megállapítható többek között a tőke- vagy fahiány, meghatározhatóak a fagyzugos területek, a vízösszefolyások helye és a mikro domborzat, a vegetációs tömeg, továbbá az árnyék- és szélhatás is. Az 5. kép mezőgazdasági terület drónos felvételezését szemlélteti.

Nagy problémát okoz a világban, hogy a beporzást végző méhek populációja drasztikusan csökken. Erre jelenthetnek megoldást a jövőben a robotméhek vagy méh-drónok (6. kép).

5. kép: Mezőgazdasági terület felvételezése drónnal
(Forrás: https://www.agronaplo.hu/szakfolyoirat/2018/04/gepesites/dronok-es-robotok-szerepe-a-digitalis-mezogazdasagban)

6. kép: Méh-drón akcióban
(Forrás: https://www.technokrata.hu/tudomany/2017/02/14/a-black-mirror-ismet-megjosolta-a-jovot)

Világszerte egyre kevesebb a szakképzett munkaerő a mezőgazdálkodás területén. Nincs ez másképpen a juhászok körében is. Nagy segítséget nyújthat számukra a terelőként alkalmazható drón. Nem csak az elkóborló egyedeket lehet könnyen észlelni a segítségükkel, hanem hangszóró alkalmazásával terelni is lehet a nyájat.

A klímaváltozás és az emberi figyelmetlenség következtében az elmúlt időszakban gyakoribbá váltak az erdőtüzek. Megelőző tevékenységként elképzelhető egy tűzfészek monitoring rendszer, amely azonnali jelzést küld az illetékes szerveknek. A már leégett területen, illetve nehezen megközelíthető terepen nagyon munkaigényes az újratelepítés. Erre lehet megoldás a telepítő drón, amely tápanyaggal ellátott kapszulákat lő a földbe.

A speciális mezőgazdasági alkalmazások kapcsán természetesen szükség van az egyértelmű szabályozási környezet teljes körű megalkotására. Kiváltképp igaz ez a megállapítás a permetező drónokra (7. kép).

7. kép: Permetező drón munka közben kukorica fölött
(Forrás: https://agroforum.hu/agrarhirek/gepinfo/a-kinai-xag-agri-tech-orias-20-millio-hektar-teruleten-alkalmazza-novenyvedo-dronjait)

A drónos permetezés szabályozási környezete

A permetező drónnal történő növényvédő szer kijuttatás területén több érdemi és konkrét előrelépés is történt az elmúlt hetekben. Ezek a lépések a következőkben időrendi sorrendben kerültek összefoglalásra. A bemutatásra kerülő kulcsfontosságú és sikeres lépések természetesen nem terelhetik el az illetékesek fokozott figyelmét a további megoldandó problémákról, illetve elvégzendő feladatokról, hiszen akad még bőven teendő ezen a területen.

Permetező drónok legális forgalomba hozatala

A 2021 decemberét megelőző időszakban problémát jelentett az a helyzet, hogy hiába voltak széles választékban elérhetőek a permetező drónok a piacon, nem állt rendelkezésre a hazai kereskedelmi forgalomba hozatalra vonatkozó jogi szabályozási háttér, azaz a permetező drónok Magyarországon történő értékesítése nem számított legális tevékenységnek.

A növényvédelmi tevékenységről szóló 43/2010. (IV. 23.) FVM rendelet 2021. decemberi módosításának köszönhetően rendeződtek a permetező drónok hazai kereskedelmi forgalomba hozatalával kapcsolatos problémák. A forgalomba hozatali engedélyek kiadását eredményező kötelező **típusminősítési eljárások**at a Magyar Agrár- és Élettudományi Egyetem (MATE) folytatja le. Az eljárások a 2022. év elejétől folyamatban vannak.

A korábban forgalomba hozott permetező drónok esetében a drónokat gyártó, illetve forgalmazó vállalatok 2022. április 30-ig kaptak haladékot a hiányzó engedélyek pótlására. 2022. május 1. után permetező drón kizárólag érvényes engedéllyel kerülhet forgalomba Magyarországon. Ez nem visszamenőleges rendelkezés, hanem a jogellenesen forgalmazott drónok legalizálására ad lehetőséget.

A MATE által, pozitív eredménnyel típusminősített, azaz forgalomba hozatali engedéllyel rendelkező permetező drónt szabad csak tehát kereskedelmi forgalomba hozni hazánkban. Az érvényes engedély meglétét matrica felragasztásával is igazolni kell (8. kép).

A típusminősítés lefolytattatása a permetező drónt gyártó/forgalmazó vállalat kötelessége a 45/2021. (XII. 1.) AM rendelettel módosított 43/2010. (IV. 23.) FVM rendeletben foglaltak szerint, vagyis a típusminősítési eljárás megkezdését a gyártónak/forgalmazónak kell kezdeményeznie a MATE-nál.

A permetező drónokra vonatkozó agrotechnikai követelmények az alábbiakban kerültek felsorolásra. A típusminősítéssel kapcsolatos, minden szükséges részletre kiterjedő tájékoztatás elérhető a MATE honlapján (HTTP4).

8. kép: Forgalomba hozatali engedély meglétét igazoló matrica (Forrás: https://mgi.naik.hu/hirek/forgalomba-hozatalra-engedelyezett-novenyvedelmi-gepek-jegyzeke)

Általános előírások:

- Permetlétartály (felület, feltöltés, ürítés, szintjelző);
- Szivattyú (szállítási teljesítmény);
- Tömlők és vezetékek (meghajlítási sugár, megvezetés);
- Szűrők (lyukbőség, hozzáférhetőség, tisztíthatóság);
- Fúvókák (rögzítés, utáncsepegés, szórásteljesítmény);
- Nyomásmérő (leolvashatóság, pontosság, osztás/felbontás);
- A kijuttatandó folyadékmennyiség beállítása (pontosság, reprodukálhatóság, leállíthatóság, nyomásesés);
- Eloszlás (variációs együttható).

Speciális előírások:

- Pozíció meghatározó rendszer;
- Kijuttatás;
- Biztonság;
- Megjelölések (fúvókák, szűrők);
- Használati útmutató (kiemelések).

Permetező drónokkal történő jogszerű munkavégzés

Az idei évet megelőzően szintén gondot okozott, hogy a mező- és erdőgazdálkodási tevékenység keretében végezhető légi munkavégzésről szóló jogszabály nem szabályozta a pilóta nélküli légi járművekkel, mint a légi munkavégzés lehetséges eszközeivel végzett munkát.

2022 februárjában a **mező- és erdőgazdasági légi munkavégzés**ről szóló 44/2005. (V. 6.) FVM-GKM-KvVM együttes rendelet módosításra, illetve pontosabban fogalmazva kiegészítésre került annak érdekében, hogy drónokkal is lehessen növényvédő szert kijuttatni. A módosítás tulajdonképpen nem tartalmaz sok új előírást (kivételt jelent például a növényvédelmi drónpilóta képzés, amelyről a későbbiekben lesz még szó), a vonatkozó EU irányelvnek megfelelően a korábbi, repülőgépekre és helikopterekre érvényes szabályozás került kiterjesztésre a permetező drónok vonatkozásában (HTTP5a; HTTP5b).

A mező- és erdőgazdasági légi munkavégzésről szóló együttes rendelet módosításának hatályba lépése teszi lehetővé azt is, hogy a növényvédelmi drónpilóta képzettség felvételre kerüljön a szabályozott szakmák közé. Amint ez a folyamat eredményesen lezárult, a Nemzeti Élelmiszerlánc-biztonsági Hivatal (Nébih) a növényvédelmi drónpilóta alapképzést szervezni kívánó intézményeknek szóló felhívását megjelenteti a honlapján. Minden olyan intézmény be fog kerülni a kapcsolódó nyilvántartásba, amely teljesíti a vonatkozó feltételeket.

A drónos növényvédelem jogszerű végzéséhez szükséges lépések

Amennyiben egy jelenleg „laikus" személy drónnal, esetleg drónflottával (drónrajnak is nevezik) szeretne növényvédő szert kijuttatni saját árutermelési, illetve szolgáltatási céllal, akkor – jelen állás szerint – a következő lépéseken kell végig mennie ahhoz, hogy az általa végzett növényvédelmi tevékenység jogszerű legyen. A 9. képen permetező drónokból álló flotta látható munka közben.

Az előzőekben leírtakhoz hasonlóan hiánypótló tevékenységnek ítélhető, hogy a megelőző hetekben kidolgozásra került az illetékesek által a következő forgatókönyv, annak ellenére, hogy az alábbiakban leírtak kisebb-nagyobb részben még módosulhatnak az elkövetkező időszakban.

9. kép: Permetező drónokból álló flotta munka közben
(Forrás: https://www.hellovidek.hu/gazdasag/2019/03/14/veszelyes-is-lehet-tilos-a-permetezo-dron-hasznalata-magyarorszagon)

1. A MATE által típusminősített permetező drón beszerzése

2022. május 1. után permetező drón kizárólag érvényes forgalomba hozatali engedéllyel kerülhet forgalomba Magyarországon. Az engedély meglétét matrica felragasztásával is igazolni kell.

2. A megvásárolt drón regisztrációja

Minden drónt kötelező regisztrálni, amely nem a „játék" kategóriába tartozik.

3. Növényvédelmi drónpilóta képzettség megszerzése

- a képzettség megszerzésének feltételei:
  - A2 kategóriájú drónpilóta képzés abszolválása;

- érvényes zöld könyv rendelkezésre állása (legalább II. kategóriájú növényvédő szer vásárlási engedély);
- érettségi bizonyítvány megléte;
- pilóta nélküli légi járműves növényvédelmi alapképzés elvégzése és 2 évenként növényvédelmi szakmai továbbképzésen történő részvétel.

Az A2 drónpilóta képzések folyamatosan elérhetőek az érdeklődők számára a Közlekedéstudományi Intézet (KTI) szervezésében.

4. Műveleti engedély vagy LUC megszerzése

- felhasználói szempontból a legfontosabb különbségek:
  - időbeli hatály: műveleti engedély: 2 év ↔LUC: visszavonásig;
  - országhatár átlépése: műveleti engedély: nem lehetséges ↔LUC: lehetséges;
  - megszerzés: LUC: nehezebb, időigényesebb (akár 6-9 hónap).

Az illetékes hatóság álláspontja, hogy a drónos permetezés a „A Bizottság (EU) 2019/947 végrehajtási rendelete (2019. május 24.) a pilóta nélküli légi járművekkel végzett műveletekre vonatkozó szabályokról és eljárásokról" 6. cikk (1) bekezdés b) iii. pontja szerint az „engedélyköteles" UAS-művelet kategóriába tartozik, mert a művelet veszélyes áruk (veszélyes anyagok) szállítását is magában foglalja, ami baleset esetén nagy fokú kockázatot jelenthet harmadik felek számára.

Az Innovációs és Technológiai Minisztérium részéről – további releváns szervezetekkel együttműködésben – folyamatban van egy felhasználóbarát segédlet kidolgozása, amely célja, hogy a jövőbeni potenciális felhasználók a lehető legegyszerűbben és leggyorsabban megszerezhessék az általuk elérni kívánt jogosultságot.

5. Drónos kijuttatásra jóváhagyott növényvédő szer rendelkezésre állása

Hazánkban egyelőre nincs pilóta nélküli légi járművel való kijuttatásra (drónos permetezésre) engedélyezett növényvédő szer. A benyújtott kérelmek támogató és gyors elbírálása folyamatos az engedélyező hatóság (Nébih) részéről. A közeljövőben várhatóan ebben a tekintetben is megnyugtató megoldásra lehet számítani.

A mai napig 4 db kérelem érkezett az engedélyező hatósághoz, amelyekben a kérelmezők összesen 1-1 db gyomirtó, gombaölő, rovarölő szer és adjuváns forgalomba hozatali és felhasználási engedélyének módosítását kérelmezték a hatóságtól permetező drónnal történő kijuttatásra.

2 db kérelem elutasításra, 1 db eljárás pedig felfüggesztésre került, hiánypótlásra történő felhívás kíséretében, 1 db eljárás pedig jelenleg is folyamatban van.

6. Megyei Kormányhivatal felé történő bejelentés

- kijuttatási terv az adott naptári évre tervezett kezelésekről az első kezelés előtt minimum 30 nappal – engedélyezési eljárás, vagy
- ad-hoc bejelentés (igazolhatóan indokolt esetben) a kezelést megelőző munkanap – formanyomtatvány kitöltése.

Ezeket a növényvédelmi szakirányító feladata elkészíteni, nem a gazdálkodót terheli és nem is a drónos szolgáltató feladata.

Röviden összegezve a leírtakat kijelenthető, hogy a drónok alkalmazása a mezőgazdaságban és az élet bármely más területén számos előnyt rejthet magában. Nem lehet és nem is szabad egyetlen társadalmi szereplőnek sem a fejlődés útjába állni, hanem mindenkinek a maga eszközeivel támogatnia kell az ilyen típusú fejlesztéseket. A felhasználás kockázatait természetesen fel kell ismerni és kezelni kell azokat. Amennyiben sikerül az előnyökkel felelősen élni, a drónokat biztonságosan használni, hosszú távon is nagy segítséget jelentenek majd az emberiség számára.

Hivatkozott források:

1. HTTP1: https://dronkoalicio.kti.hu/rolunk - letöltés dátuma: 2022. 02. 14.

2. HTTP2: https://www.agronaplo.hu/szakfolyoirat/2018/04/gepesites/dronok-es-robotok-szerepe-a-digitalis-mezogazdasagban - 2022. 02. 17.

3. HTTP3: https://magyarmezogazdasag.hu/2020/10/06/dron-mint-madarijeszto-washingtoni-egyetemen-kiprobaltak?page=1# - letöltés dátuma: 2022. 02. 20.

4. HTTP4: https://uni-mate.hu/egyetemi-laborkozpont - letöltés dátuma: 2022. 02. 21.

5. HTTP5a: https://net.jogtar.hu - letöltés dátuma: 2022. 02. 21.

6. HTTP5b:https://magyarkozlony.hu/dokumentumok/a8d6818a8514dd1b9898e8f359d4a15737e689e2/megtekintes - letöltés dátuma: 2022. 02. 21.

Drónok szerepe a madárvédelemben. A MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító ZRt. küldetése.

Bíró György, LIFE projektkoordinátor
birogyorgy@yahoo.com

A MAVIR elsődleges feladata a folyamatos villamosenergia-átvitel biztosítása, mely a nagyfeszültségű átviteli hálózaton történik. Amikor az átviteli hálózatot létrehozták, még nem voltak nemzeti parkok, természetvédelmi területek, nem foglalkoztak madárvédelemmel. Így a védett területeket átszelő vezetékek esetében jelentkező madárvédelmi problémák megoldása csak az elmúlt évtizedekre került napirendre. Ezért, ha madárütközések veszélye merül fel az átviteli hálózat mentén, azokat a már meglévő és üzemelő távvezetékeken kell megoldani, sok esetben azok lekapcsolása nélkül, mivel a hálózat terheltsége miatt a feszültségmentesítésre csak ritkán van lehetőség.

A megoldásokban a technika legújabb vívmányait is segítségül kell hívnunk a veszélyeztetett madarak védelme és az energiaellátás biztosítása érdekében. Így kerülnek képbe a drónok, amelyeknek békés célú felhasználásáról ritkán hallhatunk napjainkban.

Előkötél-behúzás drón segítségével távvezeték létesítésénél

A távvezetékek létesítésekor a forgalmas csomópontok feletti keresztezés során nem állíthatják le a forgalmat az autópályán még akkor sem, ha a keresztező

távvezetékeket át kell húzni az út felett. Ilyen esetekben az út két oldalán már készen álló oszlopok között drón segítségével húzzák át azt a könnyített kötelet, amire majd a vastagabb, és végül a végleges kábelt csatlakoztatják, így juttatva át azt biztonsággal az úton közlekedő forgalom felett. Ezt nevezik előkötél-telepítésének, ahol már rutinná vált a kötél drónnal történő behúzása. A munkát végző drónnak stabil repülési tulajdonságokkal és a kötél húzásához szükséges teherbírással kell rendelkeznie.

Fokozottan védett madarak költésének megfigyelése drón segítségével

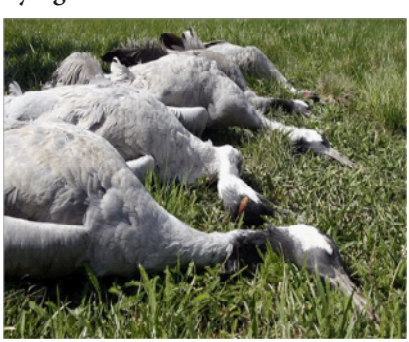
Szinte minden megfigyelő drón képes arra, hogy eljusson oda, ahová az ember csak nehezen képes, és onnan továbbítsa a valóságot a digitális technika segítségével. Ugyanerre a 400 kV-os távvezeték elektromágneses erőterében csak kevés drón képes, mert a térerő hatására irányíthatatlanná válik. Pedig erre a szolgáltatásra szükség van, mivel a fokozottan védett ragadozómadarak (pl. kerecsensólyom) az urbanizációtól menekülve a távvezeték-oszlopokra kihelyezett műfészkekben költenek. A költési folyamatot, a költés sikerét csak akkor tudják ellenőrizni a nemzeti parkok ornitológusai, ha lehetőség nyílik a rálátásra. Ha nem járna veszélyekkel a működő távvezetékre való felmenetel, a madarak zavarása miatt akkor sem tehetnék meg ezt. Ezért ma már szinte minden nemzeti park használ olyan speciális drónokat, amelyek repülését nem zavarja meg a térerő, és rendelkezik a megfigyeléshez szükséges optikai tulajdonságokkal. Minél jobb a képfelvevő képesség és minél immunisabb a navigáció a vezeték körüli térerő miatt, annál jobb felvételeket tud továbbítani a kutatók számára.

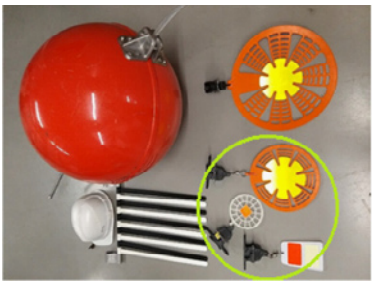
A MAVIR madárütközés védelmi tevékenységéről

A MAVIR-nál a dróntechnológia alkalmazása a legjelentősebb az ütközésvédelem terén. Ennek ismertetése előtt nézzük a megoldandó problémát.

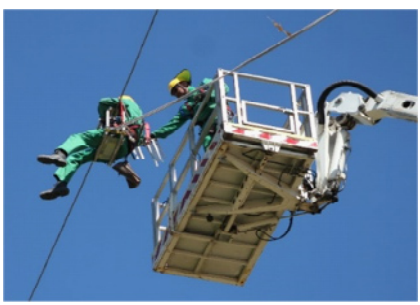
Vannak olyan madárfajok, amelyek az elmúlt évszázad során nem tudtak alkalmazkodni az urbanizációhoz.

Nekirepülhetnek a távvezetékeknek és elpusztulhatnak a vándorlásuk során.





Nekünk kell a vezetékeket láthatóbbá tenni úgy, hogy azt ők időben észleljék. A láthatóság növelése madáreltérítő szerelvények telepítésével érhető el. Ezek a szerelvények méretük, fényvisszaverő képességük és alkonyatban való fluoreszkáló hatásuk miatt észrevehetőbbé teszik a veszélyes vezetékszakaszokat. Mivel általában a meglévő vezetékekre kell utólag telepíteni az eszközöket, ez meglehetősen problémás feladat. Egyrészt, mert a terhelt vezetékeket ahhoz, hogy azon dolgozni tudjanak, feszültségmentessé kell tenni. Onnan már csak egy olyan kosaras darura van szükség, ami fel tud állni a mezőkön, és esetenként akár 100 m magasságba fel tudja vinni a szerelőket.



A probléma megoldását olyan eszköz jelentette, amit egy mozdulattal installálni lehetett. Erre alkalmasak a Svéd HAMMARPRODUKTER által gyártott Birdmark, Fire-Fly és egyéb madáreltérítő szerelvények, melyeket egy a helikopterből kiálló szakember egy speciális rúd segítségével könnyen tud telepíteni. Az, hogy nem terjedt el ez a fajta tevékenység széles körben, annak egyrészt az volt az oka, hogy a helikopter drága üzemideje miatt csak abban az esetben éri meg az alkalmazás, ha egyszerre többszáz eszköz felrakása a feladat. Természetesen az elektromágneses térerő miatt ezt a tevékenységet is csak lekapcsolt vezetékek mentén lehetett végezni, ráadásul a szél és a vezetékek közelsége miatt is veszélyesnek bizonyult.

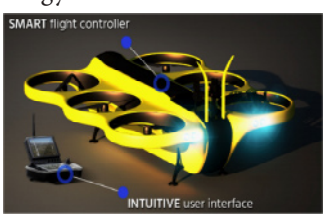
A drónok megjelenése új lehetőséget adott a feladatok megoldására, mivel a távirányított helikopter esetében az emberi élet veszélyeztetettségével nem kell számolni. Ez adta az ötletet a drónok használatához.

Madáreltérítő szerelvények telepítése, speciális eszközzel, speciális drónnal

A madárvédelemben használt drónok fejlesztése Ákos Haramia drón konstruktőrhöz és fejlesztő csapatához fűződik Európában. Jelenleg is ők látják el speciális drónjaikkal az átviteli hálózat madárvédelmi drónos tevékenységeit.

Az első ilyen eszközt azzal a céllal fejlesztették, hogy képes legyen a madáreltérítő szerelvények installálására. 29 kg súlyú volt, és 6 elektromos motor hajtotta. Az eszközön elhelyezett fordítható tár segítségével öt Birdsmark típusú eltérítőt tudott installálni úgy, hogy egy rásegítő villa segítségével fogta be a vezetéket, és a felfelé irányuló erő segítségével rögzítette azokat. Az öt eltérítő installálására 20 perc állt rendelkezésre, egy pilóta és egy navigátor dolgozott együtt.

A konstruktőrök kidolgozták a drón továbbfejlesztését is, ami egyszeri repüléssel még több eltérítőt tudott volna installálni, és a fenntartózkodási ideje is nőtt volna. A gyakorlat azonban más irányba térítette el a konstruktőröket.



A drónok továbbfejlesztése

A nehéz és bonyolult drónt egy egyszerűbb megoldás váltotta fel. Az új típus mindössze 1,5 kg súlyú, de egyszerre csak egy eszköz installálására alkalmas.

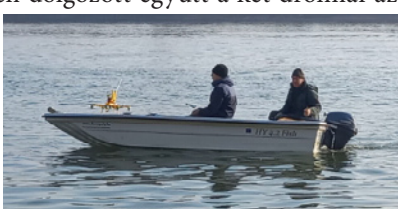
Ennek a működtetéséhez is kell egy pilóta és egy navigátor, akik a vezetékek alatt sétálva az installálási hely alatt öt percen belül el tudják végezni egy madáreltérítő felrakását. Mivel az új és olcsóbb drón motorjait modulárisan pótolni lehet, és a műanyagból készült elemeket leesés esetén 3D nyomtatóval újra el lehet készíteni, a leesésből eredő meghibásodás kockázata jóval kisebb, mint nehéz és bonyolult elődei esetében. Az új drón esésbiztos része a vezérlő egység, amely a leesés túlélése mellett a 400 kV okozta elektromágneses térő jelenlétében is működtetni tudja a drónt.

Időközben a madáreltérítő eszközök méretbeli megjelenítésével kapcsolatban is megváltoztak az elvárások, amelynek hatására nagyobb lamellával rendelkező eszközöket kezdtek el gyártani. Ehhez természetesen nagyobb teherbírású drónokra volt szükség,

így egy újabb fejlesztés eredményeként a konstruktőrök egy még speciálisabb eszközt készítettek. Ez is el tudja végezni a feladatát a távvezetékek kikapcsolása nélkül, és a súlya sem növekedett számottevően. Napi 200-300 madáreltérítő installálására képes kedvező időjárás esetén. Fontos ugyanis, hogy drónok munkáját korlátozza az 5 km/órás szél és az eső. Ettől rosszabb meteorológiai körülmények között nem repülnek, mert nő a rotorok vezetékekkel való ütközésének kockázata.

Drón a víz felett

Mivel a vonuló madarak túlnyomó része a folyómedreket követve vándorol, a folyókat keresztező nagyfeszültségű távvezetékek is kockázatot jelentenek. Szükségessé vált ezeknek a kritikus távvezeték-szakaszoknak a jelölése. A DANUBE FREE SKY LIFE Európai Uniós projekt keretében a Duna folyó felett eddig négy helyen jelölték drónok segítségével a vezetékeket. Ennek a munkának az elvégzéséhez már nem volt elég egy drón. Az ún. munkadrón mellett egy navigációs drónra is szükség volt, mivel ebben az estben a navigátor nem tud a víz miatt a vezeték alatt segítséget nyújtani a pilótának. A két pilóta sikeresen dolgozott együtt a két drónnal az installálás érdekében.



A szélesebb folyószakaszok esetében a pilótáknak is csónakra kellett szállniuk a drónokkal együtt, amelyek a csónakból startoltak és ott landoltak az installálást követően.

Ily módon többezer eltérítő szerelvényt helyeztek fel azok elvesztése nélkül.

A sérült madáreltérítő szerelvények eltávolítása drónnal

A már bemutatott madáreltérítő szerelvények lamellái a nagy szél és a kopás hatására 5-10 év után leeshetnek, a tartó pofák viszont fennmaradnak, és a koronajelenségnek köszönhetően növelik az átvitel energiaveszteségét. Ezért célszerű ezeknek a csonkoknak az eltávolítása a vezetékekről. Ezt a munkát is csak nagy nehézségek árán lehetne elvégezni kosaras daruk segítségével, ha nem állnának rendelkezésre a drónok. 2022-ben sikerült olyan drónt szerkeszteni, ami képes az elhasználódott egységek visszaszedésére. Jelenleg az eszköz tesztelése zajlik a MAVIR tesztpályáján. Remélhetőleg a következő évben megkezdhető a használhatatlanná vált eszközök eltávolítása.

Drónos kihívások a madárvédelemben a következő évtizedekre

Az Európa-szerte megnövekedett energiaigény az energiaátviteli teljesítmény növekedését várja el az átviteli hálózattól. Ennek érdekében nagyobb teljesítményű vezetékekre van szükség, amik meg tudnak felelni az elvárásoknak. Az új ACCC-sodronyok, amelyek képesek a nagyobb átviteli teljesítményre, esetenként nagyobb hőmérsékleten való üzemelést vonnak maguk után. Ezeken a vezetékeken nagyobb hőmérsékletet is kibíró madáreltérítő eszközökre és olyan drónokra van szükség, amelyek a magasabb hőmérsékleten is el tudják látni feladataikat.

Madáreltéritö telepítése drónnal

Haramia Ákos, drónfejlesztő, ügyvezető
FiiHaa Engineering, Pozsony
akosharamia@gmail.com

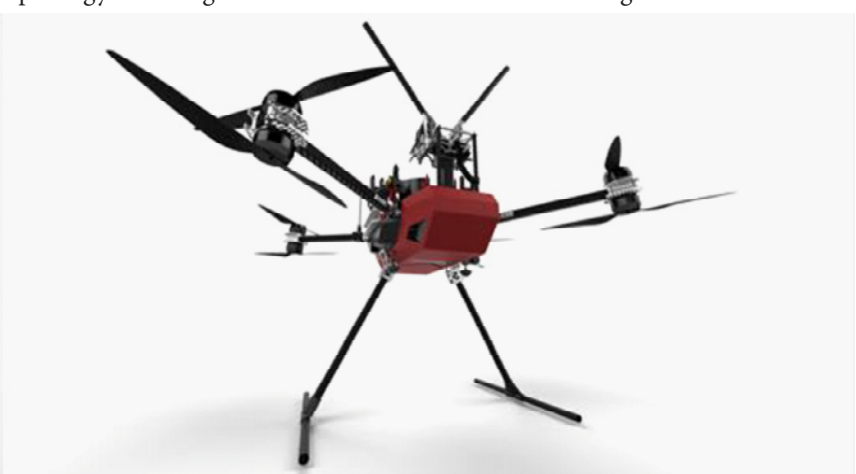
2016 tavaszán egy egyetemi diákcsoport úgy döntött, hogy drónokkal fognak foglalkozni. Nem tudták még, hogy mitől lesz ez a drón más, de kitartásukkal eljutottak oda, hogy néhány év alatt kifejlesztették a BDC-MINI-t.

Hittek abban, hogy a fiatalokból álló cég figyelemre méltó termékeket képes gyorsan és hatékonyan szállítani. Madáreltéritő telepítést szolgáló fejlesztésükkel gyorsan kijutottak a világpiacra. A BDC-MINI egy egyedülálló UAV megoldás, amelynek alkalmazásával képesek megoldani az UAS területén felmerülő összetett, multidiszciplináris problémákat.

BDC – X8

Az első drón, amely képes madárjelöléseket elhelyezni a nagyfeszültségű vezetékeken. A drónplatform és a mechatronikai rendszer kombinációjával nagyfeszültségnek ellenálló megoldást alkottunk.

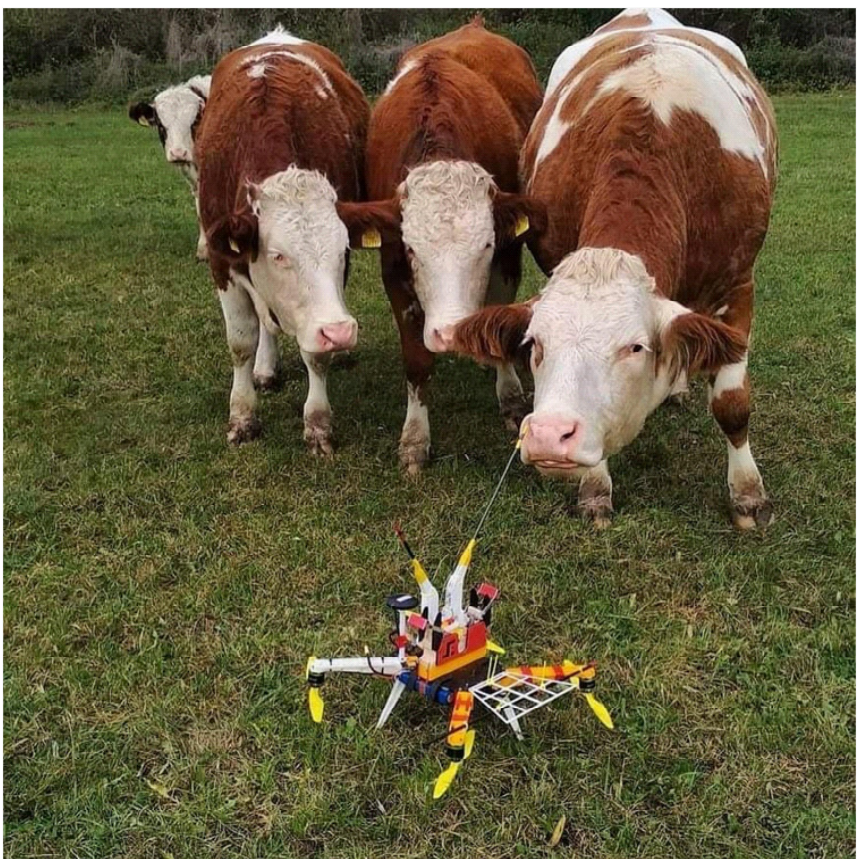
Hardveres és szoftveres K+F-ben szerzett tapasztalatainkat felhasználva olyan drónt tudtunk létrehozni, amely stabil és biztonságosan kölcsönhatásba lép a nagyfeszültségű vezetékek közelében lévő elektromágneses mezővel.



Második generációs drón, amely képes madárterelőket felszerelni a nagyfeszültségű vezetékekre. A BDC-MINI készülék telepítési tapasztalatainak ismeretében úgy döntöttünk, hogy más módon közelítjük meg a következő generációkat. A drónt kisebbre, könnyebbre építettük, és leegyszerűsítettük a deflektor

beszerelési mechanizmusát. Ennek köszönhetően növeltük a készülék munkájának hatékonyságát, valamint a felhasználási lehetőségeket. Ez egy kisebb drón, amely még barátságtalanabb terepi körülmények között is képes működni.

Az eszközt több EU-országban és az USA-ban is kereskedelmi forgalomba helyezték.

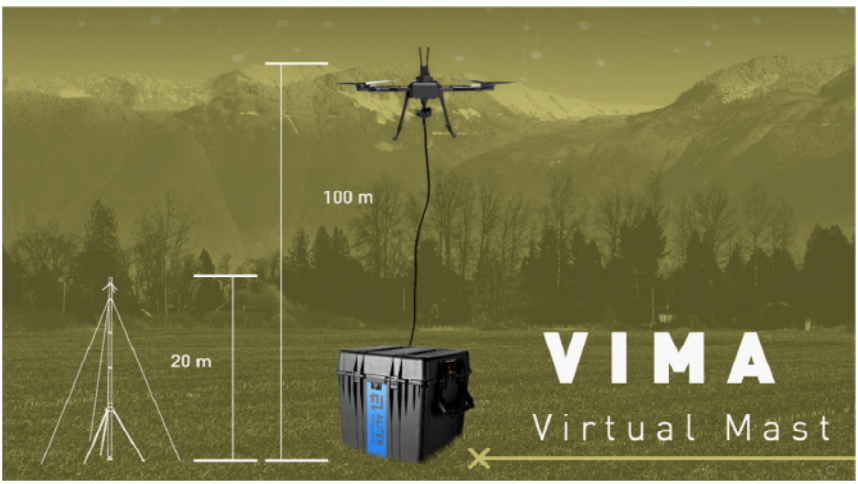


ViMa – Virtual Mast

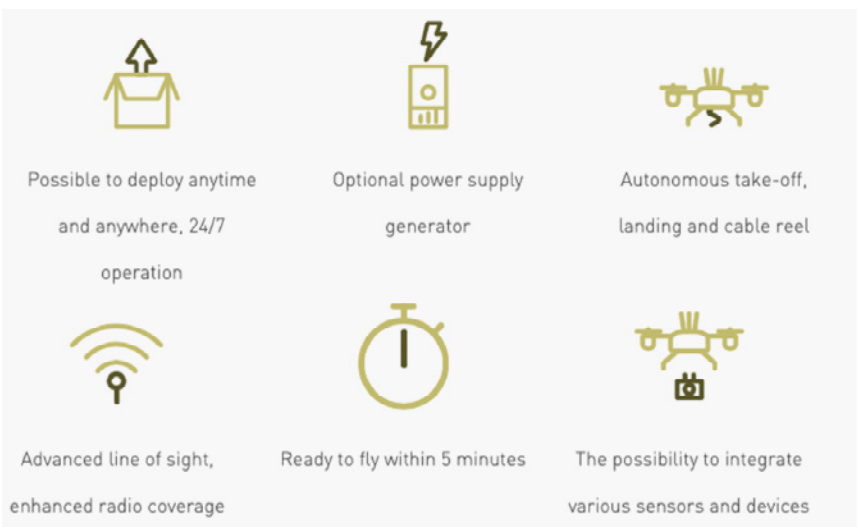
A VIMA egy olyan megoldás, amely teljesen felváltja a klasszikus mechanikus árbócot, amelyet kamerák, antennák, rádiók és egyéb eszközök és érzékelők hordozójaként használnak taktikai bevetésre.

A VIMA ötvözi a modern technológiát a vevő magas követelményeivel: gyors beállítás különböző környezetekben, ahol nagyobb magasságból kell monitorozni, mint amit a statikus árbóc képes biztosítani. Felszállása, repülése és

leszállása teljesen automatizált, a földi állomásról érkező áramnak köszönhetően folyamatos működése biztosítható.



ViMa jellemzők



Biztonság

Az autonóm működést speciális rendszer garantálja, amely képes észlelni a potenciálisan veszélyes helyzeteket. Képes érzékelni az erős szeleket, és szükség esetén csökkenteni tudja magasságát, vagy önállóan leszáll.

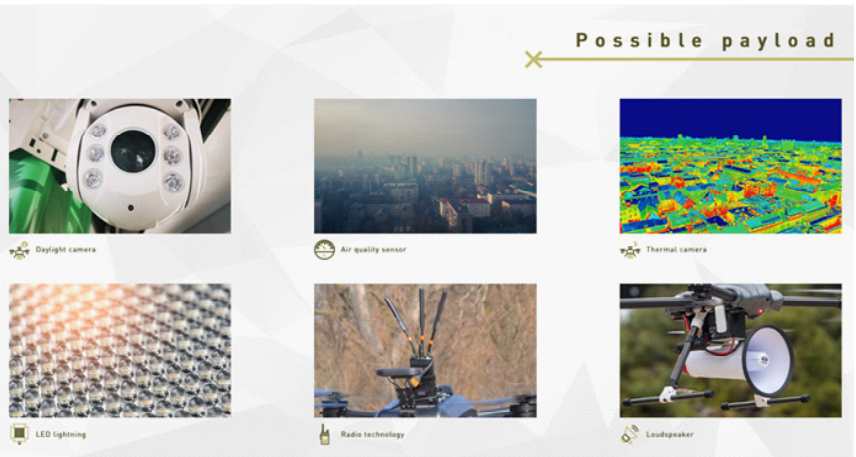
Könnyen telepíthető

A rendszer nagyon intuitív és könnyen használható. Nincs szükség hosszú vagy speciális képzésre, és 30 perc elteltével az alapismeretek elsajátítását követően a kezelő készen áll a rendszer maximális kihasználására.

Automatikus kábel

A kábel kezelése a drón magasságának vagy helyzetének megfelelően történik. Amikor a drón magassága csökken, annak kábelét visszatekeri a csörlő.

Lehetséges hasznos teher



Alkalmazások

Forgalomirányítás

Ad hoc forgalmi dugók, balesetek vagy forgalomfigyelés esetén a VIMA autópályák, kereszteződések közelében telepíthető, és élő forgalomfigyelés végezhető a fedélzeti rádión keresztül történő képek továbbításával.

Természeti katasztrófák

Természeti katasztrófák esetén a bevetett VIMA a helyzet megfigyelésére használható, ha a területről gyorsan ki kell költözni, könnyen visszahúzható és elmozdítható a kritikus helyszínről.

Sportesemények

A VIMA sportesemények közvetítésére is használható. Kameraállványok építése helyett a VIMA használható lefedettségre nagy távolságú jelátvitelhez és helyzetfelismerésre is.

Tűzoltás

Nagy kiterjedésű tüzek esetén a tűzoltási tevékenységek irányítását segítendő, a VIMA segítségével nyomon követhető a tűz kialakulása, terjedése. Az oltás után a tűz helyének hosszú távú megfigyelésére és hőfelügyeletére is használható.

Biztonság

Ipari területek megfigyelése, behatolók, biztonsági veszélyek vagy általános felügyeleti tevékenységek. Levegőminőség-érzékelővel szerelhető fel a levegő összetételének figyelésére.

Tömegrendezvények

A VIMA segítségével megfigyelhetők a nagy létszámú tömegrendezvények. Használható tömegkezelésre tüntetések, politikai gyűlések, de koncertek, zenei fesztiválok idején is. Hangszóróval is felszerelhető, hogy szükség esetén kommunikáljon a tömeggel.

Drónok a víz felett: Folyóvízi medertérképezés új módszerei a Sajó példáján

Dr. Bertalan László, PhD, egyetemi adjunktus
Szopos Noémi doktorandusz
Nagy Bálint, doktorandusz, tudományos segédmunkatárs
Dr. Szabó Gergely, PhD, egyetemi docens,
Debreceni Egyetem, Természetföldrajzi és Geoinformatikai Tanszék
bertalan@science.unideb.hu

Bevezetés

A folyómedrek, valamint az árterek geomorfológiai változásai nagyon összetett hidrológiai és környezeti paraméterek alapján működnek (Bertalan et al. 2019). Az alaktani szempontú elemzések segíthetnek az ártéri folyamatok komplexebb értelmezésében és az esetleges problémák kezelésében, ehhez pedig elengedhetetlen nagyfelbontású topográfiai adatok rögzítése (Fonstad et al., 2013). A laterális (oldalazó) erózió a meanderező folyók elmozdulását irányító alapvető folyamat, mely kiterjedésétől és intenzitásától függően súlyos károkat tud okozni a mezőgazdasági művelés alatt álló területeken vagy a lakott területek mentén (Das et al. 2012; Konsoer et al. 2016). A részben szabályozott vagy akár teljes mértékben szabályozatlan meanderező folyók horizontális medermintázata jelentős ütemben (akár több méter/év) képes tovább fejlődni; ezért kulcsfontosságú, hogy a morfológiai változások vizsgálata és kimutatása rendszeresen történjen, az értelmezéshez pedig előzetesen a korábbi mederfejlődési dinamika rekonstrukciója is nagyban hozzájárulhat (Mířijovský et al. 2015; Bertalan et al. 2016).

A topográfiai adatokat korábban hagyományos földi felmérési módszerekkel gyűjtötték. Ezek közé tartoznak az optikai szintezők, és újabban a geodéziai mérőállomások, valamint a globális helymeghatározó rendszerek (GPS). Ezek a műszerek egyedi, szabályos vagy szabálytalan távolságban lévő földfelszíni adatokat (XYZ) gyűjtenek. A felmérési eredményeket ezután számos keresztmetszet és hosszprofil segítségével jellemzik (Bangen et al., 2014). Ez azonban nem nyújt információt a mért területek közötti adathiányos területekről. A nem mért pontok interpolációját és koordinátáinak becslését lineáris interpolációs módszerekkel állítják elő. Az ilyen jellegű geodéziai felmérések általában a sekély és alacsony sodrású folyómedrek esetében szolgáltatják a legmegbízhatóbb eredményeket. Ezek a módszerek azonban nem praktikusak ott, ahol nehéz vagy lehetetlen megközelíteni a távoli partokat, a meredek partfalakat és a mélyebb, gyorsabban folyó szakaszokat. Az említett korlátok miatt a mérések gyakran túlságosan nagy térközzel kerülnek megvalósításra az adott szakaszon, emiatt az interpolációs módszerek nagy távolságokon kevésbé megbízhatóak (Bangen et al., 2014).

A nagyfelbontású topográfiai adatigény hatására az utóbbi évtizedekben az adatgyűjtés technológiai fejlődése rendkívül gyorsnak bizonyult, így váltak az eszközkészlet elemeivé többek között a földi és légi távérzékelő műszerek (pl. ALS/TLS lézerszkennerek, LiDAR), valamint hajó-alapú technológiák (pl. akusztikus Doppler-szenzorok, szonárok), amelyek gyors, hatékony és szinte autonóm topográfiai adatgyűjtést tesznek lehetővé (Wheaton, 2009). A technológiai fejlesztéseknek köszönhetően a fluviális geomorfológia egy új, "adat-gazdag" korszakba lépett (Piégay et al., 2015; Viles, 2016). A rendszeres időközönként ismétlődő topográfiai felmérés lehetővé teszi a geomorfológiai változások nyomon követését a folyórendszereken belül (Wheaton et al., 2009), és áramlási hidraulika és hordalékszállítás modellezésére útvonalvezetés (Lane et al., 1994; Marks és Bates, 2000), valamint a folyók helyreállítási projektjeinek értékelésére (Marteau et al., 2017), beleértve akár gátak eltávolításának hatását. Az elmúlt 10-15 évben a légi és földi LiDAR a geometriai pontosságuk és nagy felbontású méréseik miatt általánosan alkalmazott eszközökké váltak a folyók medertopográfiájának felmérésére és a medervándorlással kapcsolatos geomorfológiai változások számszerűsítésére (Jaboyedoff et al., 2012; Cook, 2017).

Az utóbbi években azonban a Structure-from-Motion (SfM) fotogrammetria megjelenése forradalmasította a topográfiai felmérést a földtudományokban (Smith et al., 2016). Ezt a költségcsökkentést a pilóta nélküli légi járművek (Unoccupied Aerial Systems/UAS, Uncrewed Aerial Vehicles/UAV), vagy hétköznapibb nevükön drónok használata tette lehetővé, amelyek hosszabb repülési időt tettek lehetővé. Az UAS-ok a megnövekedett stabilitás, megnövelt szenzorfelbontás és a fedélzeti GPS pontossága jóvoltából, kimagaslóan nagy felbontású felmérési eredményeket biztosítanak. Mindemellett arányait tekintve a hagyományos topográfiai felmérésekhez képest lényegesen nagyobb kiterjedésű területek is térképezhető az alkalmazásukkal. Ennek eredményeképpen a fluviális geomorfológiában való alkalmazásuk széles körűvé vált, beleértve a horizontális és vertiális mederváltozások felmérését, a hordalékokhoz kapcsolódó szemcseméret-elemzést, sőt a medertopográfiai (batimetriai) felmérést is (Carrivick és Smith, 2019). Az UAS-alapú térképezés alkalmazása lehetővé teszi olyan nagy kiterjedésű területek felmérését is, ahol a folyócsatorna megközelítése egyébként gyalog vagy csónakkal nehézkes.

Térképezés drónokkal folyóvízi környezetben

A távérzékelésben használt egyre növekvő számú és egyre szélesebb körű spektrális tulajdonságokkal rendelkező földmegfigyelési műholdak napjainkban már rendkívül rövid visszatérési idővel és kimagaslóan részletes térbeli felbontással rendelkeznek. Ennek ellenére a fluviális geomorfológiai folyamatok és formák, valamint a hidrológiai jelenségek nagypontosságú monitoringját még tovább-

ra sem teszik lehetővé (McGabe et al. 2017). A légi távérzékelés sokkal inkább alkalmas erre a feladatra, ugyanis a LiDAR-technológiával részletgazdagon térképezhetők a felszínformák, azonban jelenleg ez a technológia még alapvetően költséges (Manfreda et al. 2018). A fluviális geomorfológia területén az elmúlt években olyan folyamatok és formák elemzése során alkalmazták az UAV-SfM modellezést, mint a fonatos medrek avulziója (Javernick et al. 2013); általános ártéri állapotfelmérés (Dietrich 2016); villámárvizeket és extrém áradásokat követő kárfelmérés (Smith et al. 2014; Tamminga et al. 2015); ártéri törmelékkúpok és morénagátak épülése (Micheletti et al. 2014; Westoby et al. 2014); ártéri üledékek akkumulációja (Woodget et al. 2015) valamint a meanderező folyók parteróziója (Prosdocimi et al. 2015; Bertalan et al. 2018).

Az UAV eszközök, többnyire multirotoros vagy merevszárnyú platformok, által szállított szenzorok között egyaránt megtalálhatók a kisméretű akciókamerák, a tükörreflexes (SLR) vagy tükör nélküli cserélhető objektíves (MILC) fényképezőgépek, a multispektrális, valamint termális infrakamerák is (Nex et al. 2022). A Structure-from-Motion (SfM), mint új fotogrammetriai elemzési módszer, a felszín 3D rekonstrukcióját több, különböző perspektívából származó kép alapján valósítja meg (Eltner & Sofia, 2020). Az SfM nagy előnye a hagyományos sztereo-fotogrammetriai felszínrekonstrukcióval szemben abból adódik, hogy nem szükséges hozzá professzionális, kalibrált mérőkamera, hanem akár egy mobiltelefon beépített kamerája is alkalmas lehet a művelet végrehajtásához (Westoby et al. 2012). Ezen kívül a munkafolyamat egyes részei teljesen automatikusan, fotogrammetriai operátor nélkül futtathatók (Fonstad et al. 2013). Természetesen az SfM-feldolgozás geodéziai pontossága kizárólag akkor hozható a geomorfológiában elfogadott szintre, ha a hagyományos fotogrammetriában ismert elemekkel is kiegészítjük (James és Robson 2012). Ilyen elemek lehetnek a lencse torzulásából adódó elrajzolások által generált hibák korrekciója érdekében megadott kamera-kalibrációs adatok (Manfreda et al. 2019) valamint a modell georeferálása földi illesztőpontok (Ground Control Point – GCP) segítségével (Turner et al. 2012; Tonkin és Midgley 2016).

A munkafolyamat alapvetően négy fő lépésből áll:

1. Az algoritmus az egymással átfedő képsorozatokon homológ pontokat keres, majd azonosítja a képpont-képpár kapcsolatokat, végül elvégzi a képek összeláncolását.
2. A képpont-kapcsolatok felhasználásával megtörténik a képek térbeli helyzetének rekonstrukciója, majd ezek alapján a kapcsolópontok 3D koordinátáinak meghatározása iteratív tömbkiegyenlítés alkalmazásával. Létrejön a „ritka pontfelhő".

3. A képek helyzetének meghatározását követően a modellezés során meghatározott mértékben megtörténik a képek összes képpontjának térbeli rekonstrukciója. Létrejön a „sűrített pontfelhő".
4. A pontfelhő georeferálása elvégezhető, habár ez akár a 2. lépéssel egyidőben is végrehajtható. A sűrített pontfelhő alapján digitális domborzatmodellek generálása válik lehetővé.

Az SfM-alapú felszínrekonstrukció térbeli is időbeli léptéke az elérhető bemeneti adatoktól függően elég széleskörű lehet. Előbbi esetén a térbeli felbontás a szubmilliméterestől a kilométeres nagyságrendig, míg utóbbi esetén az időbeli lépték a szubmásodpercestől az évtizedes mértékig terjedhet (Eltner et al. 2016).

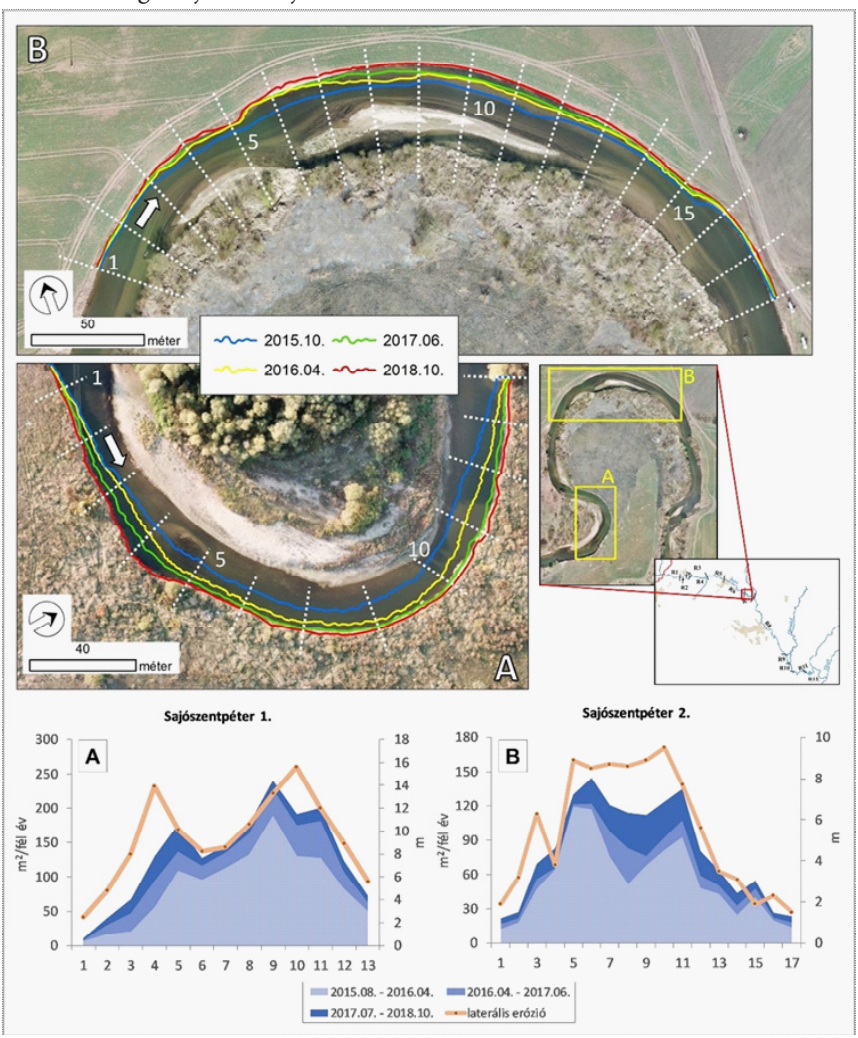
Drónok alkalmazása a Sajó hidromorfológiai elemzéséhez

Napjainkban a geoinformatika eszköztára, kiegészítve távérzékelési módszerekkel és terepi geodéziai mérésekkel gyors és pontos adatgyűjtést és -rendszerezést tesz lehetővé, melyekkel hatékonyan feltárhatók a horizontális mederfejlődés sajátosságai. A történeti térképek és a vízügyi tervezések felméréseinek leiratai további értékes forrásokat biztosítanak a múltbéli folyamatok elemzéséhez, azonban a térképi méretarányokban mutatkozó különbségek és a korabeli térképezési eljárások pontatlanságából adódóan a megbízhatóságuk jóval kisebb, továbbá a változások kvantifikációja is kevésbé részletesen lehetséges (Bertalan 2019).

A Sajó hazai szakaszának horizontális mederdinamikáját a Debreceni Egyetem, Természetföldrajzi és Geoinformatikai Tanszékén már 2014 óta részletesen vizsgáljuk. Az elemzéseink egyik legfőbb eszköze az UAS-alapú medertérképezés. Terepi felméréseink alapján a korábban elérhető eredményekhez képest sokkal nagyobb térbeli-időbeli léptékben tártuk fel az intenzív parterózió által érintett rész-szakaszok geomorfológiai sajátosságait (1. ábra). A UAS-lerepülések során a hagyományos légitérképezésben alkalmazott módon szükséges a vizsgált területet felmérni. Az autonóm UAS-lerepüléseket 100-120 méteres repülési magasságból végeztük (egy-egy helyszínről 300-400 db légifotó készült). Az SfM-algoritmuson alapú feldolgozási folyamat eredményeképpen az elkészült ortofotók térbeli felbontása a felmérésekhez használt DJI Phantom 4, valamint DJI Mavic Pro UAS-eszközök esetén 3-4 cm volt.

A parterózió számszerűsítése érdekében az ortofotókon minden egymást követő évben vektorizáltam a kanyarulatok külső ívét, a kiindulási időszak meder-középvonalára merőlegesen 20 méterenként keresztszelvényeket szerkesztettünk. A keresztszelvények mentén először megmértük a meder oldalirányú elmozdulását (1. ábra térképei). Ezt követően az egymást követő partélek által bezárt poligonokat szerkesztettem, majd ezeket a keresztszelvények mentén feldaraboltam. A művelet során minden önálló poligon-szektort kódoltam attól

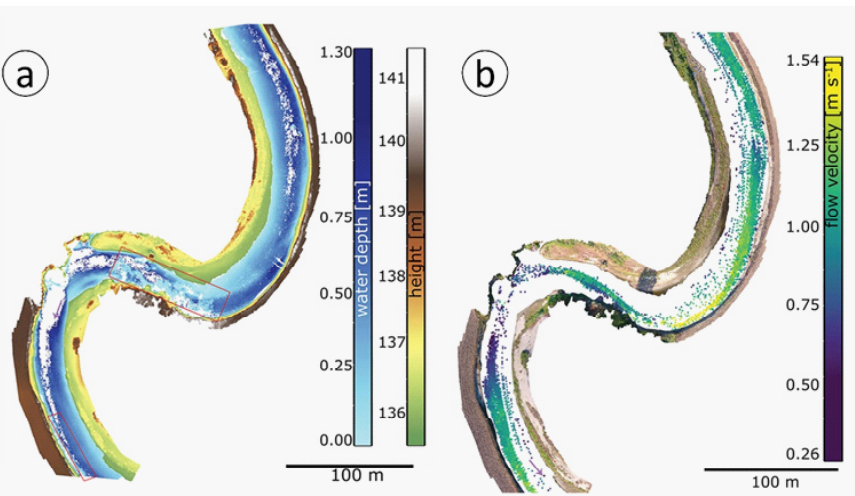
függően, hogy melyik időszak, melyik szektora; végül kiszámítottuk minden szektor területét. Annak érdekében, hogy az eltérő hosszúságú időszakok során végbement parteróziót összehasonlíthassuk, a szektorokban számított erodált területet m^2/félév formátumba számítottuk át. Az összesítés eredményét az 1. ábra alsó diagramjai mutatják.



1. ábra: Parteróziós intenzitása a Sajó két kanyarulata mentén Sajószentpéter határában (Bertalan 2019)

Az ábra alapján egyértelműen azonosíthatók a kanyarulat mentén a legintenzívebb eróziós szakaszok. Mindemellett kimutathatók az egyes vizsgált időszakok közötti eróziós ráták közötti különbségek is.

A Sajó hazai szakaszán kijelölt mintaterületeken továbbá olyan újszerű hidromorfológiai módszereket is fejlesztettünk, melyek lehetővé teszik a vízalatti medertopográfia 3D rekonstrukcióját (2/a ábra). A sekély medrű és kevésbé zavaros víztestek esetén ugyanis a fénytörés mértéke modellezhető, továbbá az UAS-eszközök nagypontosságú fedélzeti GPS-adatai alapján az SfM-algoritmusba implementálva a mederfenék mélységértékei és térbeli koordinátái korrigálhatók is. Az így előállított 3D modell kimagasló részletességgel hatékony alapadata lehet további hidrodinamikai modellezési eljárásoknak a Sajó mentén.

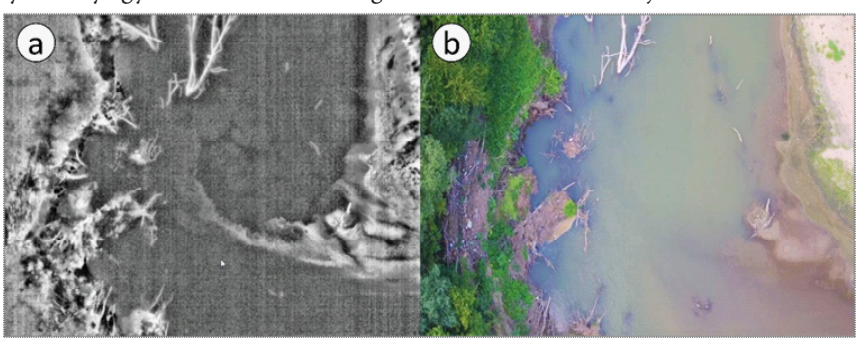


2. ábra: UAS-alapú nagyfelbontású hidromorfológiai adatok a Sajó nagycsécsi kanyarulatán: digitális felszínmodell a folyómeder peremén; 3D batimetriai modell; felszíni vízsebességek (Eltner et al. 2021).

A vízhozamok becslése érdekében szükség van a felszíni vízsebességek lokális becslésére is, ugyanis a hivatalos vízmércék gyakran csak nagy távolságban elérhetők, ezáltal a helyszíni adatok nem biztosítottak. Az UAS-eszközök kameráival kiváló minőségű és egyedülállóan stabilizált videofelvételek készíthetők. A Particle Tracking Velocimetry (PTV) algoritmusok segítségével a víztükrön azonosítható képelemek azonosíthatóvá válnak, az általuk megtett út és az eltelt idő meghatározása alapján közvetetten a felszíni vízsebesség vektorai is kiszámíthatók. Az általunk tesztelt eljárás segítségével (Eltner et al. 2021) a folyómeder felett kb. 50 méteres magasságból végzett videofelvétel segítségé-

vel egyedülálló módon, a teljes mederszakaszra vonatkozó sebesség-adatokat származtathatunk. Tekintve, hogy a mederkeresztmetszetek a 3D batimetriai modellből megszerkeszthetők, a vízsebességgel kiegészítve néhány százalékos eltéréssel vízhozam adatokat számíthatunk.

Végezetül fontos megemlíteni, hogy az UAS-eszközök fedélzetén napjainkban már az elektromágneses spektrum egyedi tartományaiban is érzékelni képes szenzorokat is alkalmazunk (Bertalan, L., Eltner, A., Maddock, I., Pizzaro, A., 2023: Monitoring of river channel dynamics by UAS. In: Ben-Dor, E. Manfreda, S. Eds.), Unmanned Aerial Systems for Monitoring Soil, Vegetation and Riverine Environments. Elsevier. pp. 271-292.). Többek között a termális infravörös szenzorok (hőkamerák) lehetővé teszik olyan hidrodinamikai folyamatok vizualizációját is, melyek az emberi szem számára látható tartományban nem azonosíthatók. A 3. ábrán a Sajó nagycsécsi szakaszán teszteltük a vízsebesség becslési módszerünket, azonban az RGB-felvételeken lekövethető képelemek hiányában nem sikerült a művelet. A DJI Matrice M210 RTK v2 UAS-eszközre szerelt Zenmuse XT2 radiometrikus hőkamera felvételein azonban egyértelműen azonosítottuk a kanyarulat belső íve felől a kanyarulat inflexiós pontja felé haladó fő áramlási pályát, mely egyaránt alkalmas a lebegtetett hordalék dinamikájának feltárására is.



3. ábra: A Sajó áramlási viszonyai hőkamerás (a), valamint látható tartományú (b) UAS-felvételeken

Összefoglalás

Az UAS-eszközök alkalmazása a fluviális geomorfológiai rendszerek térképezését egyedülálló perspektívából tett lehetővé a tudósok és vízügyi szervezetek számára. A legfontosabb fejlesztések a légi járművek által rögzíthető légi adatok megnövekedett térbeli és időbeli felbontására épültek. Ma már képesek vagyunk a hidromorfológia összetettebb folyamatait értékelni, akár egyetlen szemcse léptékében is, és a sekélyvízi batimetria rekonstruálására is lehetőség nyílik a vízfelszínnel való közvetlen érintkezés nélkül.

Köszönetnyilvánítás

A kutatást a Thematic Excellence Programme (TKP2020-NKA-04) of the Ministry for Innovation and Technology in Hungary támogatta.

Irodalomjegyzék

Bangen, S., Wheaton, J., Bouwes, N., Jordan, C., Volk, C., Ward, M.B., 2014.: Crew variability in topographic surveys for monitoring wadeable streams: a case study from the Columbia River Basin. Earth Surf. Process. Landforms 39, 2070–2086.

Bertalan, L., Szabó, G., Szabó, S., 2016.: Soil degradation induced by lateral erosion of a non-regulated alluvial river (Sajó River, Hungary), in: Zapletalová, J.; Kirchner, K. (Ed.), Aktuální Environmentálni Hrozby a Jejich Impakt v Krajiné (Current Environmental Threats and Their Impact in the Landscape Brno): Sbornik Abstraktu Z Mezinárodniho Workshopu. Ústav geoniky AV ČR, pp. 8–9.

Bertalan, L., Novák, T., Németh, Z., Rodrigo-Comino, J., Kertész, Á., Szabó, S., 2018a.: Issues of Meander Development: Land Degradation or Ecological Value? The Example of the Sajó River, Hungary. Water 10, paper 1613.

Bertalan, L. 2019.: A horizontális mederdinamikában bekövetkezett változások geomorfológiai, hidrológiai és ökológiai összefüggései a Sajó hazai szakaszán. Egyetemi doktori (PhD) értekezés. Debreceni Egyetem, 173p.

Bertalan, L., Rodrigo-Comino, J., Surian, N., Šulc Michalková, M., Kovács, Z., Szabó, S., Szabó, G., Hooke, J., 2019.: Detailed assessment of spatial and temporal variations in river channel changes and meander evolution as a preliminary work for effective floodplain management. The example of Sajó River, Hungary. J. Environ. Manage. 248, 109277.

Carrivick, J.L., Smith, M.W., 2019.: Fluvial and aquatic applications of Structure from Motion photogrammetry and unmanned aerial vehicle/drone technology. WIREs Water 6, e1328.

Cook, K.L., 2017.: An evaluation of the effectiveness of low-cost UAVs and structure from motion for geomorphic change detection. Geomorphology 278, 195–208.

Das, A.K., Sah, R.K., Hazarika, N., 2012.: Bankline change and the facets of riverine hazards in the floodplain of Subansiri-Ranganadi Doab, Brahmaputra Valley, India. Nat. Hazards 64, 1015–1028.

Dietrich, J.T., 2016.: Riverscape mapping with helicopter-based Structure-from-Motion photogrammetry. Geomorphology 252, 144–157.

Eltner, A., Kaiser, A., Castillo, C., Rock, G., Neugirg, F., Abellán, A., 2016.: Image-based surface reconstruction in geomorphometry - merits, limits and developments. Earth Surf. Dyn. 4, 359–389. https://doi.org/10.5194/esurf-4-359-2016

Eltner, A., Bertalan, L., Perks, M., Grundmann, J., Lotsari, E. 2021.: Hydro-morphological mapping of river reaches using videos captured with unoccupied aerial systems. Earth Surface Processes and Landforms, 46, 2773–2787.

Eltner, A., Mader, D., Szopos, N., Nagy, B., Grundmann, J., Bertalan, L. 2021.: Using thermal and RGB UAV imagery to measure surface flow velocities of rivers. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 43, 717–722.

Eltner, A., Sofia, G. 2020.: Structure from motion photogrammetric technique. Developments in Earth Surface Processes, 23, 1–24.

Fonstad, M.A., Dietrich, J.T., Courville, B.C., Jensen, J.L., Carbonneau, P.E., 2013.: Topographic structure from motion: A new development in photogrammetric measurement. Earth Surf. Process. Landforms 38, 421–430.

Jaboyedoff, M., Oppikofer, T., Abellán, A., Derron, M.-H., Loye, A., Metzger, R., Pedrazzini, A., 2012.: Use of LIDAR in landslide investigations: a review. Nat. Hazards 61, 5–28.

James, M.R., Robson, S., 2012.: Straightforward reconstruction of 3D surfaces and topography with a camera: Accuracy and geoscience application. J. Geophys. Res. Earth Surf. 117, F03017.

Javernick, L., Brasington, J., Caruso, B., 2014.: Modeling the topography of shallow braided rivers using Structure-fromMotion photogrammetry. Geomorphology 213, 166–182.

Konsoer, K.M., Rhoads, B.L., Langendoen, E.J., Best, J.L., Ursic, M.E., Abad, J.D., Garcia, M.H., 2016.: Spatial variability in bank resistance to erosion on a large meandering, mixed bedrock-alluvial river. Geomorphology 252, 80–97.

Lane, S.N., Richards, K.S., Chandler, J.H., 1994.: Developments in monitoring and modelling small-scale river bed topography. Earth Surf. Process. Landforms 19, 349–368.

Manfreda, S., McCabe, F.M., Miller, E.P., Lucas, R., Pajuelo Madrigal, V., Mallinis, G., Ben Dor, E., Helman, D., Estes, L., Ciraolo, G., Müllerová, J., Tauro, F., de Lima, I.M., de Lima, L.J., Maltese, A., Frances, F., Caylor, K., Kohv, M., Perks, M., Ruiz-Pérez, G., Su, Z., Vico, G., Toth, B., 2018.: On the Use of Unmanned Aerial Systems for Environmental Monitoring. Remote Sensing 10(4), paper 641.

Manfreda, S., Dvorak, P., Mullerova, J., Herban, S., Vuono, P., Arranz Justel, J.J., Perks, M., 2019.: Assessing the Accuracy of Digital Surface Models Derived from Optical Imagery Acquired with Unmanned Aerial Systems. Drones 3, paper 15.

Marks, K., Bates, P., 2000.: Integration of high-resolution topographic data with floodplain flow models. Hydrol. Process. 14, 2109–2122.

Marteau, B., Vericat, D., Gibbins, C., Batalla, R.J., Green, D.R., 2017.: Application of Structure-from-Motion photogrammetry to river restoration. Earth Surf. Process. Landforms 42, 503–515.

McCabe, M.F., Rodell, M., Alsdorf, D.E., Miralles, D.G., Uijlenhoet, R., Wagner, W., Lucieer, A., Houborg, R., Verhoest, N.E.C., Franz, T.E., Shi, J., Gao, H., Wood, E.F., 2017.: The future of Earth observation in hydrology. Hydrol. Earth Syst. Sci. 21, 3879–3914.

Micheletti, N., Chandler, J. H., Lane, S. N., 2014.: Investigating the geomorphological potential of freely available and accessible structure-from-motion photogrammetry using a smartphone. Earth Surf. Proc. Land., 40, 473–486.

Mičijovský, J., Šulc Michalková, M., Petyniak, O., Máčka, Z., Trizna, M., 2015.: Spatial-temporal evolution of the unique preserved meandering system in central Europe - The Morava River near Litovel. Catena 127, 300–311.

Nex, F., Armenakis, C., Cramer, M., Cucci, D. A., Gerke, M., Honkavaara, E., Kukko, A., Persello, C., Skaloud, J. 2022.: UAV in the advent of the twenties: Where we stand and what is next. ISPRS Journal of Photogrammetry and Remote Sensing 184, 215-242.

Piégay, H., Mathias Kondolf, G., Toby Minear, J., Vaudor, L., 2015.: Trends in publications in fluvial geomorphology over two decades: A truly new era in the discipline owing to recent technological revolution? Geomorphology 248, 489–500.

Prosdocimi, M., Calligaro, S., Sofia, G., Dalla Fontana, G., Tarolli, P., 2015.: Bank erosion in agricultural drainage networks: new challenges from structure-from-motion photogrammetry for post-event analysis. Earth Surf. Process. Landforms 40, 1891–1906.

Smith, M. W., Carrivick, J. L., Hooke, J., Kirkby, M. J., 2014.: Reconstructing flash flood magnitudes using "Structure-fromMotion": A rapid assessment tool, J. Hydrol. 519, 1914–1927.

Tamminga, A. D., Eaton, B. C., and Hugenholtz, C. H., 2015.: UAS-based remote sensing of fluvial change following an extreme wood event, Earth Surf. Proc. Land. 40, 1464–1476

Viles, H., 2016.: Technology and geomorphology: Are improvements in data collection techniques transforming geomorphic science? Geomorphology 270, 121–133.

Westoby, M.J., Brasington, J., Glasser, N.F., Hambrey, M.J., Reynolds, J.M., 2012.: "Structure-from-Motion" photogrammetry: A low-cost, effective tool for geoscience applications. Geomorphology 179, 300–314.

Wheaton, J.M., Brasington, J., Darby, S.E., Sear, D.A., 2009.: Accounting for uncertainty in DEMs from repeat topographic surveys: improved sediment budgets. Earth Surf. Process. Landforms 35.

Woodget, A. S., Carbonneau, P. E., Visser, F., Maddock, I.P., 2015.: Quantifying submerged fluvial topography using hyperspatial resolution UAS imagery and structure from motion photogrammetry. Earth Surf. Proc. Land. 40, 47–64.

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

A jövő nagy kihívása: kiberbiztonság és kiberhadviselés

Az Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar és a
Magyar Természettudományi Társulat
konferenciasorozata – 3.

BITCOIN ÉS BLOCKCHAIN

A konferencia-sorozat szervezői:
Prof. Dr. Rajnai Zoltán, PhD, dékán (Óbudai Egyetem)
és Dr. Tardy János, PhD, üv. elnök (MTT)

A MAGYAR TUDOMÁNY ÜNNEPE

HELYSZÍN
Internet (Zoom)

IDŐPONT
2021. november 30., 14:00 óra

PROGRAM

1. **Rajnai Zoltán:** ***Mi a kriptovaluta, hogyan "bányásszák?***
2. **Nagy Attila:** ***Bitcoin-blockchain***
3. **Ujváry Patrik Richárd:** ***Blokklánc és DeFi***
4. **Sándor Barnabás:** ***Blockchain technológia alkalmazhatóságának vizsgálata okosvárosok kialakításánál***

Mi a kriptovaluta, hogyan „bányásszák"?

Prof. Dr. Rajnai Zoltán egyetemi tanár, dékán
Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
rajnai.zoltan@bgk.uni-obuda.hu

A Blockchain technológia

A blokklánc (blockchain) lényegében digitális műveletek során végrehajtott, és a résztvevő ügyfelek között megosztott tranzakció, vagy digitális esemény rekordjainak (nevezhetjük nyilvános főkönyvnek is) elosztott adatbázisa. A nyilvános főkönyv minden tranzakcióját a rendszer résztvevőinek többsége konszenzussal ellenőrzi. És miután beírta az információkat, soha nem lehet törölni. A blokklánc tartalmaz egy bizonyos ellenőrizhető nyilvántartást minden egyes valaha végrehajtott tranzakcióról. A Bitcoin, a decentralizált peer to peer digitális valuta a legnépszerűbb példa, amely blokklánc-technológiát használ. Maga a Bitcoin digitális valuta rendkívül ellentmondásos, de a mögöttes blokklánc-technológia hibátlanul működött, és széles körű alkalmazásokat talált mind a pénzügyi, mind a nem pénzügyi világban.

A fő hipotézis az, hogy a blokklánc létrehoz egy rendszert a digitális online világ **konszenzusának** megteremtésére. Ez lehetővé teszi a részt vevő entitások számára, hogy biztosan tudják, hogy egy digitális esemény történt azáltal, hogy megcáfolhatatlan rekordot hoznak létre egy nyilvános főkönyvben. Óriási lehetőségek rejlenek ebben a forradalmi technológiában, és a forradalom ezen a téren még csak most kezdődött. A cikkben szeretnénk bemutatni a blokklánc-technológiát és néhány konkrét alkalmazást mind a pénzügyi, mind a nem pénzügyi szektorra, majd ezután bemutatjuk az előttünk álló kihívásokat és az üzleti lehetőségeket ebben a technológiában, amely készen áll digitális világunk forradalmasítására.

Bevezetés

A blokklánc tartalmaz egy bizonyos ellenőrizhető nyilvántartást minden egyes valaha végrehajtott tranzakcióról. Egy hasonlattal élve: könnyebb ellopni egy süteményt egy sütis tálról, amelyet félreeső helyen tartanak, mint ellopni a süteményt egy olyan sütis tálról, amelyet egy piactéren több ezer ember figyel.

A Bitcoin a legnépszerűbb példa, amely szervesen kötődik a blokklánc-technológiához. De egyben a legvitatottabb is, mivel segít lehetővé tenni a névtelen tranzakciók több milliárd dolláros globális piacát, kormányzati ellenőrzés nélkül. Ezért számos, a nemzeti kormányokat és pénzügyi intézményeket érintő szabályozási kérdéssel is foglalkoznia kell.

A kriptovaluta olyan *digitális eszköz*, amely csereeszközként vagy manapság fizetőeszközként is funkcionál. *Kriptográfiát* (titkosítást) használ a tranzakciók biztonságossága érdekében.

A legtöbb kriptovaluta közös jellemzője a *decentralizáció*, azaz a központi felügyelet nélküli működés

Az irántuk fennálló bizalom megroppanása esetén gyors bukás lehet a sorsuk, ezért piramisjátékhoz hasonlítanak.

További *súlyos bírálat* éri a kriptovalutákat *energiaigényük* miatt, ami már magasabb egyes *közepes országok* energiafogyasztásánál is. Ezért kritikusai szerint a kriptovaluták nagyon drága megoldást jelentenek egy nem létező problémára.

Maga a Blockchain technológia azonban nem vitatott, az évek során hibátlanul működött és sikeresen alkalmazzák ma is mind a pénzügyi, mind a nem pénzügyi világ alkalmazásaiban. Tavaly Marc Andreessen, a Szilícium-völgy kapitalistáinak doyenje a blokklánc **elosztott konszenzusos modelljét** az internet óta a legfontosabb találmányként sorolta fel. Johann Palychata a BNP Paribas-tól azt írta a Quintessence magazinban, hogy a Bitcoin blokkláncát, a digitális valuta működését lehetővé tevő szoftvert úgy kell tekinteni, mint a gőz- vagy belső égésű motort, amely képes átalakítani a pénzügyi világot – és azon túl is.

A jelenlegi digitális gazdaság egy bizonyos megbízható hatóságra való támaszkodáson alapul. Minden online tranzakciónk alapja, hogy megbízunk valakiben, aki elmondja nekünk az igazat – ez lehet egy e-mail szolgáltató, amely azt mondja nekünk, hogy az e-mailjeinket kézbesítették; de lehet egy tanúsító hatóság is, amelyik igazolja, hogy egy bizonyos digitális tanúsítvány megbízható. De lehet ez egy közösségi hálózat is, mint a Facebook, amely azt mondja nekünk, hogy az eseményeinkkel kapcsolatos bejegyzéseinket csak barátainkkal osztottuk meg. A helyzet azonban az, hogy bizonytalanul éljük az életünket a digitális világban azáltal, hogy egy harmadik entitásra támaszkodunk digitális biztonságunk és adatvédelmünk érdekében. Az ma már elfogadott tény, hogy ezek a harmadik féltől származó források feltörhetők, manipulálhatók vagy veszélyeztethetők.

Ebben a viszontagságos helyzetben jön jól a blokklánc-technológia, amelyik képes forradalmasítani a digitális világot azáltal, hogy lehetővé teszi a **megosztott konszenzust**, ahol minden egyes múltbeli és jelenlegi online tranzakció digitális eszközöket érint, és ezek a jövőben bármikor ellenőrizhetők. Ezt anélkül teszi, hogy veszélyeztetné a digitális eszközök és az érintett felek identitását. Az **elosztott konszenzus** és az **anonimitás** a blokklánc-technológia két fontos jellemzője.

A Blockchain-technológia előnyei meghaladják a szabályozási kérdéseket és a technikai kihívásokat. A blokklánc-technológia egyik legfontosabb felhasználási esetei az "intelligens szerződések". Az intelligens szerződések alapvetően olyan számítógépes programok, amelyek automatikusan végrehajthatják a szerződés feltételeit. Ha a részt vevő entitások közötti intelligens szerződés előre konfigurált feltétele teljesül, akkor a szerződéses megállapodásban részt vevő felek műveletei automatikusan teljesíthetők és a szerződés átlátható módon működik

Az intelligens tulajdon egy másik kapcsolódó fogalom, amely egy ingatlan vagy eszköz tulajdonjogának blokkláncon keresztüli ellenőrzésére vonatkozik intelligens szerződések segítségével. Itt meg kell jegyezni, hogy még a Bitcoin sem igazán valuta – a Bitcoin a pénz tulajdonjogának ellenőrzéséről szól. A blokklánc-technológia számos területen talál alkalmazásokat **pénzügyi** és **nem pénzügyi** területeken egyaránt.

A **pénzügyi** intézmények és a bankok már nem tekintik a blokklánc-technológiát a hagyományos üzleti modellek fenyegetésének. A világ legnagyobb bankjai valójában innovatív blokklánc-alkalmazások kutatásával keresik a lehetőségeket ezen a területen. Egy nemrégiben készült interjúban Rain Lohmus, az észt LHV bank munkatársa elmondta, hogy a Blockchain technológiát találták a leginkább tesztelhetőnek és biztonságosnak egyes banki és pénzügyi vonatkozású alkalmazások esetében.

A Bitcoin rövid története

2008-ban egy Satoshi Nakamoto néven író egyén vagy csoport közzétett egy tanulmányt "Bitcoin: A Peer-To-Peer Electronic Cash System" címmel. Ez a dokumentum az elektronikus készpénz peer-to-peer változatát írta le, amely lehetővé tenné, hogy az online fizetéseket közvetlenül az egyik féltől a másikhoz küldjék anélkül, hogy a pénzügyi intézmény beavatkozna. A Bitcoin volt ennek a koncepciónak az első megvalósítása. Napjainkban a kriptovaluta az a címke, amelyet az összes olyan hálózat és csereeszköz leírására használnak, amely kriptográfiát használ a tranzakciók biztosítására azokkal a rendszerekkel szemben, ahol a tranzakciók egy központosított megbízható entitáson keresztül kerülnek továbbításra.

Az első blokk megalkotója névtelen akart maradni, ezért mind a mai napig senki sem ismeri Satoshi Nakamoto-t. Az ő nevéhez fűződik egy nyílt forráskódú program, amely megvalósította az új protokollt, amely az 50 érméből álló Genesis blokkal kezdődött. Bárki telepítheti ezt a nyílt forráskódú programot, és ezzel a Bitcoin peer-to-peer hálózat részévé válhat. Az a technológia azóta egyre népszerűbb.

2008

- ***Augusztus 18.*** "bitcoin.org" domain név regisztrálása
- ***Október 31.*** megjelent a Bitcoin tervezési papírja
- ***November 09.*** Bitcoin projekt regisztrált SourceForge.net

2009

- ***Január 3.*** Genesis blokk megalapítása 18:15:05 GMT
- ***Január 9.*** A Bitcoin v0.1 megjelent és bejelentették a kriptográfiai levelezőlistán
- ***Január 12.*** Az első Bitcoin tranzakció, a 170-es blokkban Satoshi-tól Hal Finney-ig

A Bitcoin népszerűsége azóta sem szűnt meg, a mögöttes Blockchain technológia most új alkalmazásokat talál a pénzügyeken is túl.

A Bitcoinnak nincs egy centralizált rendszere, amely jóváhagyná a tranzakciókat. Ezt a munkát a Bitcoin bányászok végzik, és munkájuk folyamán jutalmul új Bitcoinokat hoznak létre!

Bányászat = óriási munkabefektetést és energiát igényel annak érdekében, hogy egy rendkívül értékes eszköz álljon elő. *A Bitcoin egy teljesen digitális eszköz, ezért a bányászatais a virtuális világban történik.*

Gazdasági szempontból akkor van értelme a Bitcoin bányászatnak, amikor a Bitcoin bányászattal kapcsolatos költségek (elektromosság, számítógépes teljesítmény) kisebbek a bányászattal kapcsolatos jutalom értékénél.

A kriptovaluta bányászat az a folyamat, amely során a *felhasználók közötti tranzakciókat ellenőrzik és hozzáadják a blokklánc* nyilvános főkönyvéhez. A bányászati folyamat feladata az *új érmék bevezetése* a forgalomban lévő készletbe. Az elosztott számítógépek hálózata és a bányászat teszi lehetővé, hogy a kriptovaluták *peer-to-peer* decentralizált hálózatként működjenek egy harmadik fél központi irányítása nélkül.

Blockchain technológia: hogyan működik?

A blokklánc fogalmát azzal magyarázzuk el, hogy bemutatjuk a Bitcoin működését, mivel a kettő szervesen kapcsolódik egymáshoz. Ugyanakkor a blokklánc-technológia minden online cserélt digitális eszköztranzakcióra alkalmazható.

Az internetes kereskedelem kizárólag azokhoz a pénzintézetekhez kötődik, amelyek megbízható harmadik félként szolgálnak, és amelyek bármilyen elektronikus tranzakciót feldolgoznak és közvetítenek. A megbízható harmadik fél szerepe a tranzakciók érvényesítése, védelme és megőrzése. A csalások bizonyos százaléka elkerülhetetlen az online tranzakciók során, és ehhez pénzügyi tranzakciókkal történő közvetítésre van szükség. Ez magas tranzakciós költségeket eredményez.

A Bitcoin kriptográfiai bizonyítékot használ a harmadik félbe vetett bizalom helyett két hajlandó fél számára, hogy online tranzakciót hajtsanak végre az interneten keresztül. Minden tranzakciót digitális aláírás véd, és minden tranzakciót a küldő "privát kulcsával" digitálisan aláírt fogadó "nyilvános kulcsára" küldünk. A pénz elköltéséhez a kriptovaluta tulajdonosának bizonyítania kell a "privát kulcs" tulajdonjogát. A digitális valutát fogadó szervezet ellenőrzi a digitális aláírást – így a megfelelő "privát kulcs" tulajdonjogát – vagyis a tranzakción a feladót. Minden tranzakciót a Bitcoin hálózat minden csomópontjára szétküldenek, majd az ellenőrzés után a nyilvános főkönyvbe rögzítik. Minden egyes tranzakció érvényességét ellenőrizni kell, mielőtt rögzítenék a nyilvános főkönyvben. A csomópont ellenőrzésének két dolgot kell biztosítania a tranzakciók rögzítése előtt:

1. A Spender tulajdonában van a kriptovaluta – a tranzakció digitális aláírásának ellenőrzése.

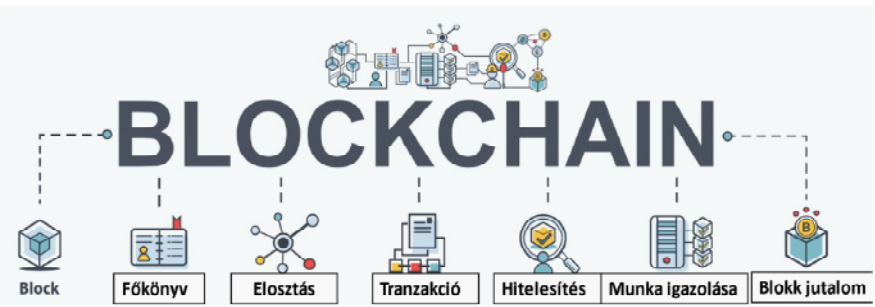
2. A Spender számláján elegendő kriptovaluta van: minden tranzakció ellenőrzése a Spend számlájával ("nyilvános kulcs") a főkönyvben, hogy megbizonyosodjon arról, elegendő egyenleggel rendelkezik a számláján.

A Bitcoin megoldotta ezt a problémát egy olyan mechanizmussal, amelyet ma népszerűen Blockchain-technológiának nevezünk. A Bitcoin-rendszer úgy rendeli meg a tranzakciókat, hogy blokkoknak nevezett csoportokba helyezi őket, majd ezeket a blokkokat összekapcsolja az úgynevezett blokkláncon keresztül. Az egyik blokkban lévő tranzakciók egyidejűleg történtek. Ezek a blokkok megfelelő lineáris, időrendi sorrendben kapcsolódnak egymáshoz (mint egy lánc), és minden blokk tartalmazza az előző blokk hash-ét.

A Bitcoin egy matematikai „rejtvény" bevezetésével oldja meg ezt a problémát: minden blokkot elfogadnak a blokkláncban, feltéve, hogy választ tartalmaz egy nagyon különleges matematikai problémára. Tövét "munka bizonyítékának" is nevezik – a blokkot generáló csomópontnak bizonyítania kell, hogy elegendő számítási erőforrást tett egy matematikai rejtvény megoldásához. Például egy csomópontnak meg kell találnia egy "nonce"-t, amely tranzakciókkal és az előző blokk kivonatának alkalmazásával bizonyos számú hash-t hoz létre. Az átlagos szükséges erőfeszítés exponenciális a szükséges nulla bitek számában, de az ellenőrzési folyamat nagyon egyszerű.

Ezt a matematikai rejtvényt nem triviális megoldani, és a probléma összetettsége úgy állítható be, hogy átlagosan nagyjából tíz percet vegyen igénybe a Bitcoin hálózat egy csomópontján, hogy helyesen generáljon egy blokkot. Nagyon kicsi a valószínűsége annak, hogy egy adott időpontban egynél több blokk jön létre a rendszerben. Az első csomópont a probléma megoldásához továbbítja

a blokkot a hálózat többi részéhez. Időnként azonban egynél több blokkot oldanak meg egyszerre, ami több lehetséges ághoz vezet. A megoldás matematikája azonban nagyon bonyolult, ezért a blokklánc gyorsan stabilizálódik. Azokat a csomópontokat, amelyek számítási erőforrásaikat adományozzák a rejtvény megoldására és blokkok generálására, "bányász" csomópontoknak nevezik, és erőfeszítéseikért pénzügyileg erősítik őket.



A hálózat csak a leghosszabb blokkláncot fogadja el érvényesnek. Ezért szinte lehetetlen, hogy egy támadó csalárd tranzakciót vezessen be, mivel nem csak blokkot kell generálnia egy matematikai rejtvény megoldásával, hanem ugyanakkor matematikailag versenyeznie kell a jó csomópontokkal, hogy létrehozza az összes további blokkot annak érdekében, hogy más csomópontok elfogadják a tranzakcióját. Ez a feladat még nehezebbé válik, mivel a blokklánc blokkjai kriptográfiailag kapcsolódnak egymáshoz.

A piac

A blokklánc-technológia mind a pénzügyi, mind a nem pénzügyi területeken olyan alkalmazásokat talál, amelyek hagyományosan egy harmadik megbízható online szervezetre támaszkodtak az online tranzakciók validálásában és a digitális eszközök védelmében.

Volt egy másik "Smart Contracts" alkalmazás is, amelyet 1994-ben Nick Szabo talált ki. Nagyszerű ötlet volt a részt vevő felek közötti szerződések automatikus végrehajtására, ez azonban nem talált felhasználást, amíg a kriptovaluták vagy a programozható fizetések fogalma nem jött létre. Most két program, a blokklánc és az intelligens szerződés együtt működhet a kifizetések elindításában, amikor egy szerződéses megállapodás előre programozott feltétele aktiválódik.

Az intelligens szerződések olyan szerződések, amelyeket a számítógépes protokollok automatikusan érvényesítenek. A blokklánc-technológia használatával sokkal könnyebbé vált az intelligens szerződések regisztrálása, ellenőrzése és végrehajtása. Az olyan nyílt forráskódú eljárások, mint az Ethereum és a Codius lehetővé teszik az intelligens szerződéseket a blokklánc-technológia használatával. Számos Bitcoin és blokklánc-technológiával működő eljárás támogatja az intelligens szerződéseket.

Az Ethereum sok izgalmat keltett programozható platformképességei miatt. Az Ethereum lehetővé teszi bárki számára, hogy saját kriptovalutát hozzon létre, és ezt felhasználja az intelligens szerződések végrehajtására, fizetésére. Magának az Ethereumnak is van saját kriptovalutája (éter), amelyet a szolgáltatások fizetésére használnak. Az Ethereum már a korai alkalmazások széles skáláját hajtja végre olyan területeken, mint az irányítás, az autonóm bankok, a kulcs nélküli hozzáférés, a közösségi finanszírozás, a pénzügyi derivatívák kereskedése és elszámolása intelligens szerződésekkel.

Ezenkívül számos blokklánc létezik még, amelyek az alkalmazások széles skáláját támogatják, nem csak a kriptovalutát. Jelenleg három megközelítés létezik az iparban más alkalmazások támogatására és a Bitcoin blokklánc észlelt korlátainak leküzdésére:

1. Az **alternatív blokkláncok** egy olyan rendszer, amely a blokklánc algoritmust használja egy adott digitális eszközzel kapcsolatos megosztott konszenzus elérésére. Megoszthatják a bányászokat egy olyan szülőhálózattal, mint a Bitcoin – ezt hívják egyesített bányászatnak. Azt javasolták, hogy olyan alkalmazásokat valósítsanak meg a fájltárolásra, mint a DNS, az SSL hitelesítésszolgáltató.

2. A **Colored Érmék** egy nyílt forráskódú protokoll, amely leírja azokat a módszereket, amelyekkel a fejlesztők digitális eszközöket hozhatnak létre a Bitcoin blokklánc tetején a digitális pénznemen túlmutató funkcióinak felhasználásával.

Az oldalsávok alternatív blokkláncok, amelyeket a Bitcoin támogat a Bitcoin szerződésen keresztül – ugyanúgy, ahogy a dollárokat és a fontokat korábban az arany támogatta. Lehet, hogy több ezer oldalsáv "van rögzítve" a Bitcoinhoz, amelyek mindegyike különböző jellemzőkkel és célokkal rendelkezik – mindegyik kihasználja a hiányt és a Bitcoin blokklánc által garantált rugalmasságot. A Bitcoin blokklánc viszont iterálhat, hogy támogassa a kísérleti oldalsávok további funkcióit – miután kipróbálták és tesztelték őket.

A ***bányászok üzemeltetik*** a kriptovaluták hálózatán történő ***tranzakciókat***, valamint ***ellenőrzik*** azok hitelességét. Ehhez bonyolult matematikai feladatokat oldanak meg a sz.gépeik segítségével (blokk lezárása), amiért cserébe ***digitális valutában részesülnek***. Vagyis erős számítógépes hardvert és elektoromos áramot biztosítanak, amiért cserébe digitális valutában részesülnek. (Bitcoin, Ethereum stb.)

Amikor a Bitcoin először indult, ***blokkonként 50 Bitcoint*** adtak jutalmul a bányászoknak. Minden 210.000 blokk bányászása után (körülbelül 4 évente) a blokk-jutalom feleződik, és addig fog feleződni, amíg a blokkonkénti jutalom 0 lesz (körülbelül 2140-ig). Jelenleg a blokk jutalom blokkonként 6,25 ₿ és blokkonként 3,125 érmére csökken a felezés után.

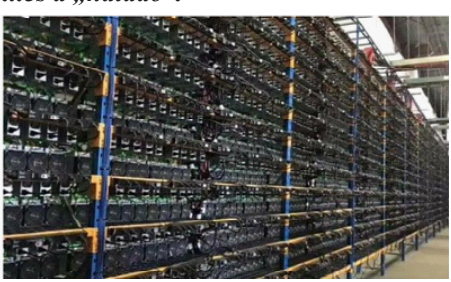
Mivel bányászhatunk?

Kezdetben:

...ma már...

A „kezdő" bánya:

...és a „haladó".



Következtetések

Összefoglalva: a Blockchain a Bitcoin technológiai gerince. Az elosztott főkönyvi funkció a Blockchain biztonságával párosulva nagyon vonzóvá teszi a technológiát a jelenlegi pénzügyi és nem pénzügyi üzleti problémák megoldására. Ami a technológiát illeti, a kriptovaluta alapú technológia vagy a felfújt elvárások lefelé lejtőjén, vagy a kiábrándultság mélypontján van Óriási az érdeklődés a Blockchain alapú üzleti alkalmazások iránt, és ezért számos induló vállalkozás dolgozik rajtuk. Alkalmazásának mindenképpen erős ellenszéllel kell szembenéznie, amint azt korábban is leírtuk. A nagy pénzügyi intézmények, mint például a Visa, a Mastercard, a bankok, a NASDAQ stb., befektetnek a jelenlegi üzleti modellek Blockchain-en történő alkalmazásának feltárásába, és valójában néhányan közülük új üzleti modelleket keresnek a Blockchain világában.

Blokklánc és DeFi

Ujváry Patrik Richárd, doktorandusz
Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
ujvary.patrick@gmail.com

Kivonat

A digitális aranytól a blokklánc-technológián át a DeFi-ig, hogyan működik a jövő „világunkat megváltoztató" technológiája a jelenben. Az okos szerződések megalkotása a hiányzó darabka a decentralizált pénzügyek megvalósítása és mindennapossá válása felé. Hitelezés, fizetés, derivatívák, váltás, tőkeáttét és stablecoin-ok mind részei a DeFi-nak nevezett kripto-forradalomnak.

Bevezető

A DeFi a decentralized finance, vagyis magyarul a decentralizált pénzügy rövidítése. Példaképpen a Bitcoin egy olyan pénzforma, amelyet egyetlen központi bank vagy kormány sem irányít. Értéket képvisel és bárkinek közvetlenül elküldhető a világ minden tájáról, bank vagy pénzintézet nélkül. A Bitcoin decentralizált pénz, megértése, használata viszonylag egyszerű [1].

A pénz utalása azonban csak az egyik a sok építőelem közül az egész pénzügyi rendszerben. Az egymásnak való pénzküldés mellett számos szolgáltatást használunk manapság. Például a hitel, megtakarítás, biztosítás, tőzsde mind olyan szolgáltatás, amelyek a pénz köré épülnek, és együtt alkotják a pénzügyi rendszerünket.

Központosított pénzügyi rendszer és a DeFi kapcsolata

Ma a pénzügyi rendszer és minden hozzá kapcsolódó szolgáltatás teljesen központosított. A bankoknak, tőzsdéknek, biztosítótársaságoknak és minden pénzügyi intézménynek van valamilyen felelőse, legyen az egy vállalat vagy egy személy, aki kínálja ezeket a szolgáltatásokat vagy épp felügyeli őket. Ennek a központosított pénzügyi rendszernek, melyet röviden CeFi-nak[1] nevezünk megvannak a saját kockázatai – a rossz gazdálkodás, a csalás vagy akár emberi hiba.

A gyors technológiai fejlődés miatt gyakran még az internet megjelenése előtt tervezett vagy megalkotott rendszerek használatosak, pedig a technológia révén már sokkal hatékonyabbak is léteznek.

A DeFi által az egész jelenleg központosított pénzügyi rendszer ugyanúgy decentralizálható, ahogy a Bitcoin tette ezt a pénzzel [1]. A DeFi kifejezés olyan pénzügyi szolgáltatásokra vonatkozik, amelyek felett nincs központi hatóság vagy felügyeleti szerv. A decentralizált pénz – mint amilyen néhány kriptopénz is – programozható, automatizálható. Segítségével tőzsde, hitelezési szolgáltatás, biztosítók és egyéb szervezetek készíthetőek, melyeknek nincsen hagyományos értelemben vett tulajdonosa és nem irányítja senki – az irányítást programkód végzi. Nem hibázik, nem kérdez, kiszámítható.

DeFi és Dai

Egy decentralizált pénzügyi rendszer létrehozásához először is egy alap infrastruktúrára van szükség a programozáshoz és a szolgáltatások futtatásához. Ma a leginkább elterjedt ilyen infrastruktúra az Ethereum hálózata[2]. Az Ethereum a platformot biztosítja decentralizált programok írásához és futtatásához [2].

Az Ethereum használatával automatizálhatóak a pénzügyi műveleteket, úgynevezett okosszerződéseket lehet írni. Meghatározhatók a szabályok egy bizonyos szolgáltatás pontos és kiszámítható működéséről, és az okosszerződés létrejötte után az végleg megváltoztathatatlanná tehető. Többé senki nem írhat hozzá, nem vehet el belőle, nem veszítheti el, a központosított rendszerek legtöbb hibája így kiküszöbölhető [2]. Természetesen ezzel együtt új problémaforrások is megjelennek.

A decentralizált alkalmazások létrehozásához szükséges infrastruktúrát felhasználva egy teljes decentralizált pénzügyi rendszer felépíthető egyes építőelemekből. Minden pénzügyi rendszernek szüksége van pénzre. A Bitcoin bár valóban decentralizált, de alig alig programozható [1]. Ezzel szemben az Ether nagyon jól programozható [2], ugyanakkor rendkívül nagy az értékének a volatilitása a hagyományos pénzekhez képest.

[1]centralized finance

[2]és a hozzá hasonló EVM-kompatibilis blokkláncok, L2 hálózatok

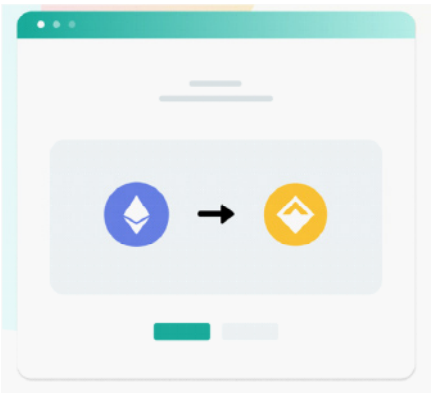
Ahhoz, hogy olyan megbízható pénzügyi szolgáltatásokat lehessen építeni, melyeket az emberek használni akarnak, stabilabb pénzre lesz szükség. Ezért jöttek létre az úgynevezett stablecoin-ok. A stablecoin-ok olyan kriptopénzek, melyek egy hagyományos eszköz értékéhez vannak kötve, általában valamilyen nagy pénznemhez, például az amerikai dollárhoz. Léteznek centralizált és decentralizált stablecoin-ok [3].

Központosított stablecoin-oknál egy hagyományos cég egy hagyományos bankszámlán banki átutalással fogad pl. amerikai dollárt, majd cserébe kripto-dollárt bocsát ki[3]. A kibocsátott kripto-dollár fedezetét a hagyományos bankban lévő „igazi" dollár jelenti, arra bármikor visszaváltható. Ezzel az a probléma, hogy megjelent a rendszerben egy olyan központi szereplő, akiben feltétel nélkül meg kell bízni – éppen ennek elkerülése volt a kriptopénzek alapgondolata [1].

A DeFi hoz tehát olyan stablecoin-t szeretnénk használni, amely nem igényel hagyományos pénztartalékot a háttérben, mivel ehhez valamilyen központi szervre lenne szükség. Ezért jött létre a Dai decentralizált kriptopénz, amelynek értéke az amerikai dollár értékéhez van kötve, ami azt jelenti, hogy egy Dai egy amerikai dollárnak felel meg. Más népszerű stablecoin-októl eltérően, amelyek értékét közvetlenül amerikai dollár tartalékok adják, a Dai fedezetét kriptoeszközök adják, mely fedezet bárki által nyilvánosan megtekinthető a blokkláncon. Ezt úgy lehet elképzelni, mint amikor egy bank hitelt nyújt jelzálogjogért cserébe. Minden Dai mögött több a fedezet, mint 1 dollár, vagyis ha valaki letétbe helyez 1 dollár értékű Ethert, 66 cent értékű Dai-t kölcsönözhet. Vagyis a Dai túlfedezett[4]. Ha vissza akarja kapni a zárolt Ether-t, csak vissza kell fizetni a kölcsönzött Dai-t, és a fedezet felszabadul. Fedezetként zárolható kriptopénz hiányában Dai egyszerűen vásárolható a tőzsdén is. Mivel a Dai túlfedezett, még akkor is, ha a fedezetül szolgáló mögöttes kriptotermék ára csökkenne, a fedezet valószínűleg továbbra is értékesebb, mint a forgalomban lévő Dai. Végsősoron ha a fedezet értéke a Dai értéke alá csökkenne (vagyis 1 Dai nem érne 1 dollárt), az okosszerződés automatikusan aukción eladja a fedezetként szolgáló eszközöket Dai-ért cserébe. Az így befolyt Dai-t „elégeti", ezzel csökkenti az összes Dai stablecoin mennyiségét és mindig visszaállítja az eredeti 1 Dai = 1 USD árat. Mindezt önműködően, emberi beavatkozás nélkül [3].

[3]megj.: ezzel a tevékenységgel kapcsolatban szabályozási-felügyeleti kérdések is felmerülnek

[4]over-collateralized



1. ábra: Ether-ből Dai [4]

A Dai stablecoin működését is okosszerződések biztosítják, működésük bárki számára elérhető, megtekinthető, ellenőrizhető. Nincs szükség bankárokba, kereskedelmi bankokba, jegybankokba vetett bizalomra, csak a kód működésében kell bízni, melyet a blokklánc garantál. Nem lehet egyszerűen leállítani vagy cenzúrázni.

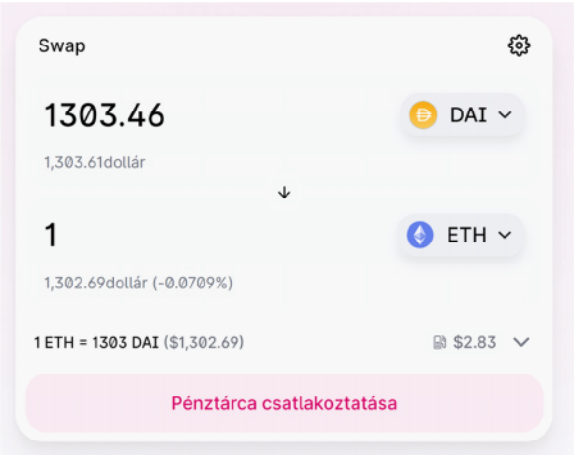
Decentralizált alkalmazások

A decentralizált pénzügyi rendszer a stabil pénz mellett további szolgáltatások nyújtására is alkalmassá tehető.

A decentralizált pénzváltók, vagy röviden DEX-ek[5], olyan szabályok, vagyis okosszerződések szerint működnek, melyek lehetővé teszik a felhasználóik számára kriptopénzek vásárlását, eladását vagy kereskedelmét. Szintén központi felügyeleti szerv nélkül működnek [5].

Egy DEX használatakor nincsen tőzsdei bróker, regisztráció, személyazonosság-ellenőrzés és nincs pénzfelvételi díj sem. Ráadásul nem a beutal-átváltkiutal modell szerint működnek, hanem egyidőben történik a két kriptopénz cseréje – nincs egy olyan időpillanat sem, amikor a felhasználó már nem rendelkezik a régi felett, de még az új felett sem. Hasonlóképpen a kriptopénz küldéséhez, atomi műveletek vannak a pénzváltásnál is: vagy mindkettő megtörténik, vagy egyik sem [5].

[5]decentralized exchange



2. ábra: A Uniswap DEX felülete [6]

Az okosszerződés betartja a szabályokat, ügyleteket hajt végre, gyorsabb, biztonságosabb, átláthatóbb és bizalommentes.

A decentralizált pénzügyi szolgáltatások köre azonban nem ér véget. Okosszerződések használatával létrehozhatóak decentralizált pénzpiacok – olyan szolgáltatások, amelyek összekötik a hitelfelvevőket a hitelezőkkel.

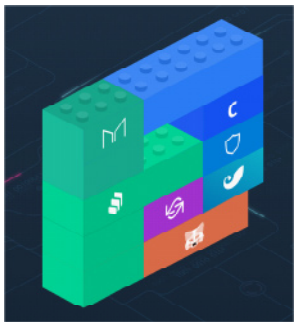
Ilyen rendszer többek között a Compound is, mely egy szintén Ethereum alapú hitelfelvételi és kölcsönzési app, ami azt jelenti, hogy bárki a fentebb említett korlátozások nélkül kölcsönadhatja kriptopénzét, és kamatot kaphat rá [7]. A másik oldalon pedig a kriptopénz zárolásának fejében kölcsönt lehet rá felvenni, mely kölcsön fedezeteként a letétbe helyezett kriptopénz szolgál. A Compound platform automatikusan összehozza a hitelezőket a hitelfelvevőkkel, érvényesíti a kölcsön feltételeit és kamatot fizet. Szintén okosszerződések működtetik.

Decentralizált stablecoin, tőzsde és pénzpiac mellett létrehozható decentralizált biztosítás is. Az új pénzügyi (kripto)termékek természetesen bizonyos kockázatokkal járnak, melyek egy részére biztosítás köthető a blokkláncon. Ez is decentralizált módon köti össze a biztosításért fizetni hajlandókat, az őket biztosítókkal egy biztosítási díj ellenében [8]. Miközben minden önműködően történik anélkül, hogy egy biztosítótársaság vagy ügynök állna a háttérben, vagy közvetítene.

Összefoglalás

A DeFi szolgáltatások együttműködnek, lehetséges a különböző szolgáltatások tetszőleges keverése, egymásra építése is, ezért szokás a DeFi szolgáltatásokra a „pénzügyi legók” kifejezést használni.

Tagadhatatlan azonban, hogy kockázatok is vannak. A legnagyobb kockázat, hogy a DeFi még korai fázisában jár és előfordulhat, hogy a dolgok rosszul sülnek el. Voltak például hibásan megírt okosszerződések, amikor nem határoztak meg bizonyos esetekre vonatkozó szabályokat, és hackerek kreatív módszerekkel kihasználták a sérülékenységet és elvitték az összes pénzt az okosszerződésből [10]. Ezzel és hasonló kockázatokkal érdemes tisztában lenni és csak ezek ismeretében kipróbálni az újdonságokat.



3. ábra: „pénzügyi legók" [9]

A DeFi forradalom túl van a legelső szakaszán, az elkövetkező évek során elválik, hogy sikerül-e eljutnia emberek tömegéhez. Kétségtelen, hogy a DeFi az emberiség nagy részének hasznára válhat.

Források

[1] *S. Nakamoto:* Bitcoin: a Peer-to-Peer Electronic Cash System, Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] *V. Buterin:* Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. By Vitalik Buterin (2014), 2014. [Online]. Available: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

[3] The Dai Stablecoin System Whitepaper By the Maker Team, 2017. [Online]. Available: https://makerdao.com/whitepaper/DaiDec17WP.pdf

[4] *MakerDAO:* Infographic, Blog, 2020. https://blog.makerdao.com/wp-content/uploads/2020/12/Infographic-English-1.pdf

[5] *H. Adams, N. Zinsmeister, and D. Robinson:* Uniswap v2 Core, 2020. [Online].

Available: https://uniswap.org/whitepaper.pdf

[6] Uniswap Interface, app.uniswap.org. https://app.uniswap.org/ (accessed Oct. 17, 2022).

[7] Compound: The Money Market Protocol, 2019. [Online]. Available:

https://compound.finance/documents/Compound.Whitepaper.pdf

[8] *H. Karp and R. Melbardis:* NEXUS MUTUAL A peer-to-peer discretionary mutual on the Ethereum blockchain. [Online]. Available:

https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf

[9] *Totle:* Building with Money Legos, Medium, Feb. 15, 2020. https://medium.com/totle/building-with-money-legos-ab63a58ae764

[10] A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency, The New York Times, Jun. 17, 2016. [Online]. Available: https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html

Bitcoin-blockchain: Blokklánc-technológia és a szemtelen Bitcoin

Nagy Attila, doktorandusz
Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

Bevezető

A kriptovaluta világában mindenkinek ismert az álnéven futó Satoshi Nakamoto, mivel a Bitcoin blokkláncot ő készítette el 2008-ban. [1] Satoshi Nakamotoról keveset lehet tudni, az sem biztos, hogy egy létező személyről van szó lehetséges, hogy egy csoport vagy szervezet tevékenysége áll a Bitcoin blokklánc megalkotása mögött. Az első blokklánc-technológia mégsem Satoshi Nakamotohoz fűződik. Vissza kell tekintenünk egész 1991-ig amikor is Stuart Haver és W. Scott Stonetta belekezdtek az első blokklánc fejlesztésbe. Az ő céljuk az volt, hogy egy olyan technológiát alkossanak meg ami azt eredményezi, hogy ne lehessen úgy adatokat változtatni, hogy annak ne maradjon nyoma, időbélyegezték az összes változást. [2]

Satoshi Nakamoto erre a technológiára építette a bitcoint azért, hogy lehessen pénzt küldeni és fogadni úgy, hogy a pénzügyi intézmények szolgáltatásait ne kelljen igénybe venni. [1] Az első Bitcoin (BTC) vásárlás 2010-ben történt meg, akkor még 0.003 dollárba került. [2] [3] Amikor ez a tanulmány készül a BTC ára 65 ezer dollár felett van (2021.11.08.).

A kriptovaluták világában a Bitcoin a legismertebb és legelfogadottabb. 2013-tól egész 2021-ig több mint 7500 különböző kriptovaluta került a piacra. [4] A top 10-es listába a következő kriptovaluták kerültek:

- Bitcoin (BTC)
- Ethereum (ETH)
- Binance Coin (BNB)
- Cardano (ADA)
- Tether (USDT)
- Solana (SOL)
- Ripple (XRP)
- Polkadot (DOT)
- Dogecoin (DOGE)
- USD Coin (USDC) [5]

A Bitcoin blokklánc-technológia azon felül, hogy sok embert gazdaggá tett, magával hozott sok olyan negatív eseményt is min a haszontalan áramfelhasználás vagy csalások sorozatát. A tanulmányban érintjük, hogy mi a blokklánc, milyen különbségek vannak blokklánc és adatbázis között. Átvesszük a lehetséges támadási felületeket, és kitérünk arra, milyen negatív hatásokkal kell, hogy megbirkózzon a társadalom a Bitcoin blokklánc-technológia miatt.

Blokklánc

A blokkláncok blokkokból (adathalmazokból) épülnek fel. A blokkok időrendben egymásra vannak fűzve, ebből ered a blokklánc elnevezés, mivel láncot képeznek az adatok. Minden egyes blokk időbélyeggel van ellátva. A blokkláncok sima lapoknak felelnek meg, melyek sorrendbe vannak rakva, és a sorrendet nem lehet megváltoztatni. Ebből ered a biztonság. Megkülönböztethetünk nyitott vagy privát megosztott főkönyvtárakat. [6]

A blokklánc-technológia széles körben kezd ismertté válni, mert:

- leredukálja az időt;
- a blokkláncokat nem lehet változtatni;
- megbízható;
- biztonságos és
- decentralizált. [7]

Blokklánc és adatbázis összehasonlítása

A blokklánc tulajdonképpen adatbázisnak is felfogható. Információt tárolunk az úgynevezett blokkokon.

	Blokklánc	Adatbázis
1.	A blokklánc decentralizált mivel nincs rendszergazda vagy felelős.	Az adatbázis centralizált mivel van rendszergazdája és felelőse.
2.	Nem szükséges engedély.	Szükséges az engedély.
3.	A blokklánc lassú.	Az adatbázis gyors.
4.	A blokkláncok visszanézhetőek.	Az adatbázis nem nézhető vissza.
5.	A bizalmassági kritériumnak megfelel.	Az adatbázis nem teljesen bizalmas.
6.	A blokkláncot nem lehet megváltoztatni.	Az adatbázisban lehet adatot módosítani.
7.	Masszív (robosztus) technológia.	Nem minden értelemben masszív (robosztus) technológia.
8.	Nincs közvetítő.	Van közvetítő.
9.	Aki a feltételeknek megfelel írhat a láncra.	Csak a felhatalmazott olvashat és írhat.
10.	Nem rekurzív.	Az adatbázis rekurzív.

Táblázat 1. (saját szerkesztés) [7]

A táblázatban jól láthatóak a különbségek. A blokklánc decentralizált, ellentétben az adatbázissal, ami centralizált. A blokklánc használatához nem szükséges engedély, bárki képes használni. Az adatbázis használatához szükséges a jogosultság. A blokklánc lassú, az adatbázis gyors. A blokkláncok esetében a keletkezését vissza lehet nézni, az adatbázisban nem lehet visszanézni, hogy mikor lett feljegyezve az adat. A blokklánc teljesen megfelel a bizalmassági kritériumoknak, míg az adatbázis nem teljesen, hanem részben. A blokkláncokat nem lehet megváltoztatni, nem lehet közéjük egy új blokkot hozzáadni, míg az adatbázisnál lehet újat hozzáadni, törölni, módosítani. A blokkláncoknál nincs közvetítő, pl. egy tranzakciónál, az adatbázisnál szükséges a közvetítő. Ha a felhasználó megfelel a feltételeknek, akkor hozzáadhat új blokkot, akárki is ő, az adatbázisnál csak a felhatalmazott olvashatja és írhatja át az adatokat. A blokklánc nem rekurzív, ami azt jelenti, hogy nem lehet ugyan azt a feladatot megismételni ellentétben az adatbázisnál, ott többször is meg lehet ugyan azt a feladatot ismételni.

A blokklánc hackelhető?

A blokklánc látszólag rendkívüli módon biztonságos, és a benne levő információ változtathatatlan. Sokan gondolják azt, hogy nincs rajta fogás. Azonban a behatolás tesztelők (hackerek) mégis találtak néhány módszert. A módszerek a következők:

- 51%-os támadás;
  Az új blokkok hozzáadása a lánchoz engedélyhez van kötve. Azok a számítógépek engedélyezik, melyek már a hálózatra vannak csatlakoztatva. Ha egy behatolás tesztelőnek sikerül a számítógépek 51%-án átvenni az irányítást, akkor képes az adatok módosítására. Így átveszi a hálózat irányítását egymaga. Ez a sérülékenység igen veszélyes. Az olyan kriptovaluták hálózatán, amikre még nincs sok számítógép csatlakoztatva, egyszerűbb az ilyen sérülékenységet kihasználni;
- tervezési hiba;
  A blokklánc keletkezésekor léphet fel biztonsági hiba. Ha ezt a hibát a hackerek kihasználják, akkor a felhasználó akaratán kívül el lehet tulajdonítani a hozzá tartozó kriptovalutát;
- hiányos biztonság;
  Ha nem a blokkláncra, akkor számos támadás a váltóirodákra irányult. A felhasználók a váltóirodákon keresztül tudnak kriptovalutákkal kereskedni (venni és eladni). Ha a váltóirodáknak nincs megfelelő védelme, akkor könnyedén hozzáférhetünk az adatokhoz és a kriptovalutákhoz egyaránt. [8] [9] [10]

Számos váltóirodát támadtak meg sikeresen, melyek a következők:

- Mt.gox (2014) 8,750 milliárd dollár
- Coincheck (2018) 500 millió dollár
- Bitfloor (2012) 250 ezer dollár
- Bitfinex (2016) 77 millió dollár
- BitGrail (2018) 187 millió dollár
- Binance (2019), 40 millió dollár [11]

Negatív hozadék

- **Áram**

  A 21. században a társadalmak törekszenek a zöld energiafelhasználásra. A Bitcoin bányászásához az áramfelhasználás 2017-ben 10 TWh volt évente. 2021-ben 129 TWh-ra nőtt a szükséglet, ami azt jelenti, hogy Hollandia éves áramfelhasználásától is több kell a Bitcoin bányászáshoz. Vannak olyan cryptovaluták amelyek tranzakcióihoz nem szükséges ilyen nagy teljesítmény (XRP). Jelenleg a leghatékonyabb, ha bankkártyán keresztül végzünk átutalásokat, az kerül a legkevesebbe a Földnek. [12] [13] [14]

	Kilowatt	CO2 Emissions	Gallons of Gas
Bitcoin	951.58 kWh/tx	4.66-7 Mt/tx	75.7 gal/tx
Ethereum	42.8633 kWh/tx	2.73-8 Mt/tx	2.3867 gal/tx
XRP	0.0079 kWh/tx	4.5-12 Mt/tx	0.00063 gal/tx
Visa	0.0008 kWh/tx	4.6-13 Mt/tx	0.00006 gal/tx
Mastercard	0.0006 kWh/tx	5.1-13 Mt/tx	0.00005 gal/tx
Paper Currency	0.0440 kWh/tx	2.32-11 Mt/tx	0.00350 gal/tx

Táblázat 2. [13]

A 2. táblázatban látható, hogy mennyi áram, széndioxid és gáz kell egyes kirptovaluták vagy banki szolgáltatások igénybevételéhez. [13]

- **Csalás** (adathalászat és cryptojacking)

  Adathalászat

  Az adathalász támadások a manipulációra építenek. A felhasználó megtévesztésére alkalmazzák. A kiberbűnözők e-maileken, különböző csevegő szolgáltatásokon keresztül (facebook, discord) tömegesen küldenek ki hamisított weboldalakat abban a reményben, hogy a felhasználó nem veszi észre a módosított weboldalt és megadja a saját adatait. A kriptovilág sem kivétel. Itt is rengeteg csalóval lehet találkozni, akik hamisított weboldalakat üzemeltetnek. [15]

  Kíváncsiságból november 4-én regisztráltam egy csevegő szolgáltatásra (discord). Érdekelt, hogy hány adathalász próbálkozást kapok. A discordon belül csatlakoztam 13 olyan szerverre, melyek a kriptovalutákkal foglalkoznak. Most november 10-e van és eddig 12 olyan üzenetet kaptam, amiben az szerepel, hogy nyertem egy bizonyos összeget és lépjek be az oldalra, aktíváljam a kódot és máris az enyém a nyeremény. Ha ki szeretném venni az összeget, amit nyertem, akkor viszont meg kell adnom a saját adataimat és még fizetnem is kell nekik. Ami nagyon megtévesztő, hogy a böngésző zöld lakatja azt írja, hogy biztonságos a kapcsolat, pedig nem.

  Cryptojacking

  A cryptojacking vagy más néven kriptobányászás (cryptomining) az ENISA 2018-as jelentésében került be első ízben a top 15 fenyegetettség sorába [16]. A cryptojacking a kiberbűnözők egy újabb támadási típusa. A kiberbűnöző a a cryptojacking kártevő szoftverrel eléri, hogy más felhasználók erőforrásait (számítógép, mobiltelefon) felhasználva magának bányássza a kriptovalutákat. A kriptovaluták széleskörűen kezdenek ismertté válni, és emiatt a cryptojacking is nagyobb figyelmet kap a bűnözők világában [17]. Ezzel a támadással jelenleg a törvény nem foglalkozik kellőképpen. A szervezetek észrevehetik, hogy az áramfogyasztás nagyobb lett, a dolgozók produktivitása leromlott, mivel le van terhelve a munkaállomás. [18] A szervezetek gépi tanulási módszerekkel az új típusú behatolás érzékelőkkel védhetik a rendszerüket. A rendszer felismeri a hálózati forgalomban a nem oda illő adatfolyamot. Így a cryptojacking támadás is elhárítható.

- **Disztópia** (Ez a rész csak a képzelet szüleménye, kérem úgy olvassa!)

  Úgy látom, hogy az embernek az idő a legértékesebb. Ha az ember idejét lefoglaljuk, akkor kevesebb ideje marad a családra, fejlődésre. Az Orwelli 1984-es disztópiához pont illik a kriptovilág. Tételezzük fel, hogy egy

nemzet (ország) elfogadja a kriptovalutát, mint fizetőeszközt, mondjuk egy nagyhatalom akarata miatt. Ha már elfogadták a kriptovalutát, akkor már nem egyfélét, hanem többfélét is elfogad. Ha szeretnék egy bizonyos plázában vásárolni, akkor egy adott kriptovalutával vagyok csak képes fizetni. Ha ki szeretném fizetni az áramszámlát, vízszámlát stb. akkor ezt csak egy másik valutával tehetem meg. A külföldről jött multicégek saját kriptovalutájukat kérik el a saját portékájukért cserébe. Egy fizetőeszköz helyett tíz különböző kriptovalutára kell koncentrálni. Ha csak fél órát kell naponta ilyen dolgokkal foglalkozni, az is sok egy ember életében. A 24 óra érték! A 21. században észlelni lehet a történelemhamisítást, a százféle társadalmi igény nyomulását, a nem normális normálissá tételét, akkor ez miért ne lenne lehetséges!?

Szerencsejáték

Számtalan kripto-tőzsdeoldal létezik már. Az oldalakon lehet kereskedni a kriptovalutákkal akár 150-szeres szorzókkal [19].

Lehetséges, hogy a kritpovilág a 21. század legnagyobb szerencsejátéka. Azt lehet tudni, hogy a kaszinók 51%-ban nyernek, a játékosok 49%-ban. Ez az 1% pedig több millió dolláros hasznot hoz a kaszinóknak. A kriptovilág is ugyanilyen elven működik, mindig a ház nyer, ebben az esetben a tőzsdeoldalak működtetői. De a 49% pont elég, hogy terjedjen a kriptovaluta jóhíre a világban. Ha a blokklánc-technológiát nem fogadják el, mint fő fizető eszközt, feltételezésem szerint, mint szerencsejáték megmarad.

Összegzés

Ha informatikus szemmel nézem a blokklánc-technológiát és viszonyítom az adatbázishoz, akkor nehéz megérteni, hogy milyen sokat ér a Bitcoin. Kiberbiztonsági szemmel pedig több problémát is észre lehet venni. Ha egy országban sok bányászó van, akkor az ország kiberterében megnövekszik a sérülékenységek száma. A cryptojacking az erőforrásokat nyeli el. Az adathalászok a személyes adatok mellett a pénzt is eltulajdonítják. A váltóirodák is úgy működnek, hogy a személyes adataidat meg kell adni. Szerintem az is egy gond, ha egy másik ország megszerez több százezer személyes adatot. Mindent összevetve a Bitcoin és társai több gondot okozhatnak, mint jót a világon. Ha már az ember hajlandó rengeteg információt megtanulni a kriptovilágról, akkor megfontolandó, hogy a ráfordított energiát máshova is lehetne irányítani és ott is pénzt keresni.

A jövőt tekintve a kvantumszámítógép lehet, hogy megállítja a Bitcoin őrületet, de ez még odébb van. Sejteni lehet, hogy a Bitcoin akármekkorára is ugrik fel, úgy le is fog esni…

Irodalomjegyzék

[1] Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf

[2] History of blockchain technology: A detailed guide https://101blockchains.com/history-of-blockchain-timeline/#prettyPhoto

[3] https://www.google.com/search?q=bitcoin+price+2010&oq=bitcoin+price+2010&aqs=chrome..69i57.5408j0j1&sourceid=chrome&ie=UTF-8

[4] Number of cryptocurrencies worldwide from 2013 to November 2021 https://www.statista.com/statistics/863917/number-crypto-coins-tokens/#:~:text=How%20many%20cryptocurrencies%20are%20there,might%20not%20be%20that%20significant.

[5] Coinmarketcap https://coinmarketcap.com/

[6] Blokkláncok http://hadmernok.hu/172_18_ambrus.pdf

[7] Difference between blokchain and database https://www.javatpoint.com/blockchain-vs-database

[8] https://www.epiqglobal.com/en-us/resource-center/articles/blockchain-can-be-hacked

[9] https://cipher.com/blog/how-blockchain-can-be-hacked-the-51-rule-and-more/

[10] https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

[11] https://cryptopro.app/history-of-cryptocurrency-exchange-hacks/

[12] Bitcoin energy consumption worldwide from February 2017 to October 19, 2021 https://www.statista.com/statistics/881472/worldwide-bitcoin-energy-consumption/

[13] Green Currency Interactive Tool https://xrpl.org/carbon-calculator.html?c1=GAW_SE_NW&source=INTL_SUST&cr2=search__-__intl__-__sustainability--crypto__-__xrpl__-__mod&kw=_PLUS_cryptocurrency__PLUS_energy__PLUS_consumption&cr5=469427170019&cr7=c&utm_source=GAW_SE_NW_INTL_SUST&utm_medium=cpc&utm_campaign=search__-__intl__-__sustainability--crypto__-__xrpl__-__mod&utm_term=_PLUS_cryptocurrency__PLUS_energy__PLUS_consumption

[14] Bitcoin Uses More Electricity Than Many Countries. How is that possible? https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html#:~:text=But%20first%2C%20consider%20this%3A%20The,nation%20of%20about%205.5%20million.

[15] *Muha Lajos, Krasznay Csaba*: Az elektronikus információs rendszerek biztonságának menedzselése

[16] ENISA Threat landscape report 2018 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[17] ENISA Threat landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[18] ENISA Threat landscape 2020 Cryptojacking https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking

[19] Binance https://www.binance.com/en