Major Gábor

A PILÓTA NÉLKÜLI LÉGIJÁRMŰ RENDSZEREK HASZNÁLATA AZ ELEKTRONIKAI HADVISELÉSBEN

Napjaink társadalmában az információ, annak megszerzése és birtoklása a fennmaradás elsődleges záloga. Ezzel az értékkel jól kell gazdálkodni, ezt fontos tudatosan megosztani és felelősen őrizni, védeni. Minden információmorzsát valaki meg akar szerezni, bízva abban, hogy annak birtokában a konkurenciát, ellenfelet, netán az ellenséget meg tudja előzni, le tudja győzni. Ebben a „harcban" az kerekedhet felül, akinek fejlettebb eszközei vannak az adatok felderítésére, értelmezésére, vagy az, aki ezeket a fontos ismereteket megfelelő eszközökkel, eljárásokkal és módszerekkel álcázni tudja a kíváncsiskodó szemek elől. Az elektronika és a számítástechnika fejlődése egy sor olyan iparág kialakulását hozta magával, amelyek az ezekből adódó tudás leplezésére, valamint a megszerzésére szakosodtak. Ezeket az információs műveleteket nem csupán a hadiiparban, hadműveletekben „alkalmazzák", hanem a civil hétköznapokban, így például az ipari kémkedés világában is találkozhatunk velük. Az alábbi publikációban a szerző bemutatja az információs műveletek egy elemének, az elektronikai hadviselés és a drónok[1] közötti kapcsolódási lehetőségeket a témában megjelent, releváns hazai és külföldi publikációk segítségével, valamint tartalmazza a szerző egyéni következtetéseit is.

Kulcsszavak: pilóta nélküli légijármű rendszerek, drón, elektronikai hadviselés, információszerzés

BEVEZETÉS

„Ha az ellenség nyitva hagy egy kaput, rohanj be rajta!"
(Szun-ce[2]) [1]

Amióta ember él a Földön, mindig adódik ok arra, hogy háborúzzon valakivel. Minden esetben sikerült megfelelő, magyarázható célt „találni" ahhoz, hogy az aktuálisan szemben álló fél ellen az érdekeit erővel érvényesítse, mely lehet területszerzés, gazdasági erőforrások megszerzése/megtartása, vallási és/vagy politikai ideológia terjesztése.

Az ipari termelési korszakot felváltó információs termelési kor új társadalmi modellt hozott magával. Minden eddigi társadalmi modellnél gyorsabban változó és intenzívebben fejlődő társadalom körvonalazódott az elmúlt évtizedekben, létrejött az információs társadalom. Ebben a társadalomban az információ vált az egyik legfontosabb tényezővé, ahol már a mindennapi élet alapvető mozgatórugója, valamint társadalmi értéke az információ, a kommunikáció és a tudás [2].

Ebben a korszakban az információhoz történő mielőbbi hozzájutás az egyik, sőt talán a legfontosabb ok a „háborúzásra". Nem az a kérdés, hogy egy fontos, vagy annak tartott adatot ki birtokol, hanem az, hogy az érvényesülés érdekében ki és milyen gyorsan tudja azt megszerezni. Akinek van valamilyen értéke, az megtesz mindent annak érdekében, hogy ne kerüljön avatatlan kezekbe, akinek pedig szüksége van erre, az meg megragad minden lehetőséget, minden lehetséges eszközt „hadrendbe állít" a megkaparintására.

[1] A köznapi használatban a pilóta nélküli légijárművekre (UA – Unmanned Aircraft, ICAO Circular 328,) használt kifejezés.
[2] Ókori kínai hadvezér i.e. 544–i.e. 496.

Ezen fontos adatokhoz, leírásokhoz, „titkokhoz" való hozzájutást nagyban elősegíti, hogy az infokommunikációs technológia rohamosan fejlődik, amivel egyenes arányban növekszik az ezt használó rendszerek sebezhetősége is. Ezt mindenki megtapasztalhatja akár saját magán is, a számítógépek, okostelefonok és más, ma már elengedhetetlen, vagy a média útján a társadalomra erőltetett, elengedhetetlennek tűnő eszközök használata során. Az ilyen eszközökön a különböző biztonsági alkalmazások futtatása szinte már kötelező, ha nem akarunk áldozatává válni különféle rosszindulatú „ajánlattételeknek", megkereséseknek, vagy fenyegetéseknek. A „próbálkozások" számának növekedése, a megszerezhető információ érzékenységével exponenciális arányban növekszik, amely még fokozottabban igaz a gazdasági élet szereplőinek hálózataira, valamint az állami és önkormányzati szervek és intézmények által működtetett rendszerekre is. A különböző elemzések azt mutatják, hogy az infokommunikációs rendszerek ellen irányuló támadások száma növekszik, és e támadások következményeként felmerülő károk egyre nagyobb mértéket öltenek, amin csodálkozni dőreség lenne, hiszen szinte minden „értékünk" a virtuális világban létezik. Addig, amíg a gépeink, termőföldjeink, jószágaink kézzel fogható valóságban voltak, a fizető eszközeink az adás-vétel helyén léteztek tárgyiasult formában, a ház világító-, hűtő-fűtő és vagyonvédelmi berendezéseit kézzel, nem okos eszközön keresztük irányítottuk, kapcsoltuk, addig az ilyen elemzéseknek, okfejtéseknek nem volt alapja. Ám az információs társadalom kialakulása új kihívásokat teremt, mivel komoly probléma, hogy az információs rendszerek elleni támadások egyre kifinomultabbak, nehezebben érzékelhetők, kiterjedtebbek és a magánszférát, illetve a vállalati és kormányzati szektort egyaránt fenyegetik [3].

Mindezen változások maguk után vonják a biztonságkultúra kérdéseinek újszerű megközelítését mind a magán, mind pedig az állami szférában, a biztonsági cégek, a fegyveres erők és a titkosszolgálatok lehetőségeinek, alkalmazási módjainak, struktúrájának, vezetési és törzskultúrájának gyökeres megváltozását és az információs műveletek új fogalomrendszerének kialakulását [4].

A társadalom már-már túlzottan is „elfogadja" az infokommunikációs eszközök és rendszerek előnyeit, támaszkodik a mindennapok egyszerű tevékenysége során a megszokott virtuális rituálékra, mindeközben észre sem veszi, hogy valaki befolyásolja érzéseit, gondolatait és tevékenységét. Ez megtehető távolról számítástechnikai hálózatokon keresztül, de ha a célszemély olyan „távol" van, akkor közelebb kell menni hozzá a megfelelő hatás elérése érdekében. Ehhez egyre kifinomultabb, precízebb és okosabb eszközök „fejlődnek" mind a földön, mind pedig a levegőben történő alkalmazásra. Egy adott helyszínre a kijuttatás leggyorsabb, legegyszerűbb és talán a leginkább feltűnésmentes eszközei a légi eszközök, azok közül is a pilóta nélküli rendszerek. A napjainkban ismert repülőeszközök közül (az űreszközöket jelenleg ide nem sorolva), talán a legdinamikusabb fejlődés a pilótanélküli repülőgépeké.

Szinte nem telik el nap, de egy hét biztosan, hogy ezen eszközökkel végrehajtott feladatokról, újdonságokról, fejlesztésekről ne olvashatnánk a médiában. Igaz, a legfelkapottabb hírek a napozó szomszédot filmező, fotózó drónról, a csomagokat szállító UAV/UAS[3]-ról, a rablót üldöző pilóta nélküli légijárműről, a rendezvényeket felügyelő és az épületeket szkennelő távirányítású eszközökről szólnak, de a felsorolt tevékenységeknél sokkal többet tudnak ezek a rendszerek.

Ebben a publikációban bemutatom, hogy a „hétköznapi ember" számára megismert, szinte már a megunásig ismételgetett felhasználási lehetőségeken túl, mit tudunk még tenni ezekkel az eszközökkel, milyen kapcsolódási pontok vannak az információs hadszíntérben végrehajtott műveletek, és az ezek végrehajtása során alkalmazott, pilóta nélküli légijárművek között. Mielőtt a konkrét

[3] Unmanned Aerial Vehicle/Unmanned Aerial System – pilóta nélküli légijármű/ pilóta nélküli légijármű rendszer

UAV felhasználásról írnék, a magyar szakirodalmak segítségével tisztázom az elektronikai hadviselés helyét az információs műveletek rendszerében.

AZ INFORMÁCIÓS SZÍNTÉR ÉS AZ INFORMÁCIÓS MŰVELETEK

„Az információs hadviselés lesz a legösszetettebb típusú hadviselés a 21. században, és az információ fogja eldönteni, hogy ki nyeri meg és ki veszíti el a harcot."
(Mengxiong, Chang) [5]

Napjaink új típusú társadalmában a különféle információs tevékenységek az úgynevezett információs környezetben, vagy más kifejezéssel az információs színtéren zajlanak. Az információs környezet defníciójára többféle meghatározást is találhatunk, attól függően, hogy ki milyen szempontból vizsgálja azt és mit tart fontosnak hangsúlyozni. Például az USA összhaderőnemi információs műveletek doktrínájában olvashatjuk, hogy: „*az információs környezet mindazon egyének, szervezetek és rendszerek összessége, akik, és amelyek az információ gyűjtésével, feldolgozásával, szétosztásával foglalkoznak*". A definíció szerint az információs környezet magában foglalja annak valamennyi szereplőjét és erőforrásait, illetve tevékenységeit és folyamatait. Az információs környezetet tekintve beszélhetünk katonai információs környezetről, valamint globális információs környezetről, mely az információs társadalom kibontakozásával alakult ki és az információ világméretű gyűjtésével, feldolgozásával és elosztásával foglalkozó szereplők (egyének, szervezetek és rendszerek) összessége. Ennek az átfogó környezetnek a technikai-technológiai alapját az a globális információs infrastruktúra képezi, amely nem más, mint azoknak a vezetékes és vezetéknélküli távközlési rendszereknek, számítógép-hálózatoknak és egyéb információszerző, -feldolgozó és -szétosztó rendszereknek az összessége, amelyek az információcserét biztosítják. Az átfogó információs környezetnek a világ minden érintett globális, regionális és nemzeti szerve, intézménye és rendszere részét képezi [6].

Miután új társadalmi modell és környezet definiálódott, így törvényszerű, hogy a katonai műveletekben is újabb, az eddigi fizikai dimenziók mellé, egy nem földrajzi dimenzió kerüljön meghatározásra. A szárazföldi-, tengeri-, légi- és kozmikus hadszíntér mellett a hadviselés egy újabb tartománya jelent meg, amelyet katonai információs környezetnek, más szóval információs hadszíntérnek nevezünk.

Az információs hadszíntéren a szárazföldi-, légi-, tengeri- és kozmikus műveletek mellett, és azokkal szoros összhangban, egy újabb fajtájú katonai tevékenységet is folytatnak az egymással szembenálló felek az információ megszerzéséért, megtartásáért és hatékony felhasználásáért. E tevékenységeket összefoglalóan információs műveleteknek nevezik. Az információs hadszíntér kifejezésben az információs jelző azonban nemcsak a műveletekre utal. Azt is jelenti, hogy a hagyományos katonai műveleteket a korábbiaknál jelentősebben támogatják az információs korszak által biztosított infokommunikációs technológiák [7]. Ezáltal minőségileg új helyzet áll elő a katonai tevékenységek eddigi történetében, hiszen ha az egyik félnek egyre gyorsabban és pontosabban van lehetősége folyamatos információáramlással az adatok gyűjtésére, feldolgozására és továbbítására, miközben kihasználja, vagy megakadályozza az ellenség képességét ennek megtételére, akkor uralja az információs hadszínteret [8]. Az információs hadszíntér a háborús színtér egyik speciális vetülete, amelyben az információs küzdelem az információ megszerzéséért és a szembenálló félnél hatékonyabb felhasználásáért folyik. *„Az információs hadszíntér minden olyan valós és virtuális teret, helyet, eszközt, rendszert magába foglal, ahol az információ megszerzésével, előállításával, feldolgozásával, felhasználásával, tárolásával és védelmével foglalkoznak."* Az információs hadszíntér

kiterjedésében rendszerint túl mutat a valódi hadszíntéren, mivel a hadműveleti területen kívül magába foglalja a hátországi támogató katonai és polgári szervek infokommunikációs rendszereit és szervezeteit is [7].

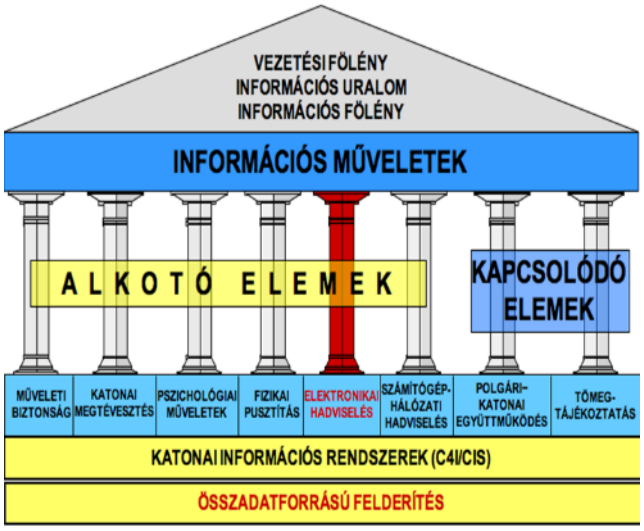
Ezen az információs hadszíntéren végrehatott mindennemű tevékenységet, műveletet, egyfajta értelmezés szerint, információs műveletnek nevezhetjük. *„Ezen eljárások a fizikai-, az információs-, és a tudati dimenzióban érvényesülő, koordinált tevékenységeket jelentik, amelyek a szembenálló fél információira, információalapú folyamataira és infokommunikációs rendszereire gyakorolt ráhatásokkal képesek befolyásolni a döntéshozókat a politikai és katonai célkitűzéseik elérésében úgy, hogy emellett a saját hasonló folyamatokat és rendszereket hatékonyan kihasználják és megóvják. Az információs műveletek – az információs fölény és a befolyásoló képesség elérése, valamint megtartása érdekében – minden szinten (például politikai, gazdasági, kulturális, katonai: hadászati, hadműveleti, harcászati) és minden időben (béke, válság, háború) alkalmazott információs képességek közötti integráló, szinkronizáló és koordináló tevékenység. Az információs műveletek célja az információs fölény, információs uralom és végső soron a vezetési fölény kivívásával a befolyásoló képesség fenntartása, továbbá a saját oldali vezetési ciklus számára az idő csökkentése, valamint a szembenálló fél vezetési idő ciklusának tekintetében pedig az idő növelés elérése, így ezek által a hadműveleti fölény elérésének elősegítése”* [6].

Megszerzésének és megtartásának két azonos fontosságú oldala van, úgymint: kihasználni és megvédeni a saját információs képességeket, illetve gyengíteni az ellenség információs lehetőségeit. Mindezek érdekében adott szervezetek béke, válság és konfliktus időszakában információs műveleteket hajtanak végre [9].

Az információs műveletek más megfogalmazásban: *„Az információs fölény kivívása a szemben álló fél információi, információs folyamatai és információs rendszerei befolyásolására, illetve a saját információk, információs folyamatok és információs rendszerek védelmére irányuló tevékenységek összessége.”* [10]

Az ilyen tevékenységek az 1. ábrán látható felosztásban alkotják az információs műveleteket, melyek a már korábban is létező és a katonai műveletekben alkalmazott információs tevékenységek közötti összhangot teremti meg.

Az 1. ábrán látható, szemléletesen összefoglalt műveleti elemek közül, számos tevékenységi körben nagy biztonsággal és sikeresen alkalmazhatók a pilóta nélküli légijárművek, ám ennek az írásnak nem célja minden egységet részletesen kifejteni, példával ábrázolni. Ezért az információs technológián alapuló hadviselésének egyik fontos elemét, az elektronikai hadviselést kiválasztva haladok tovább a bevezetőben célként kitűzött kapcsolat (elektronikai hadviselés és a drónok) megjelenítése felé.



1. ábra Az információs műveletek elemei [9]

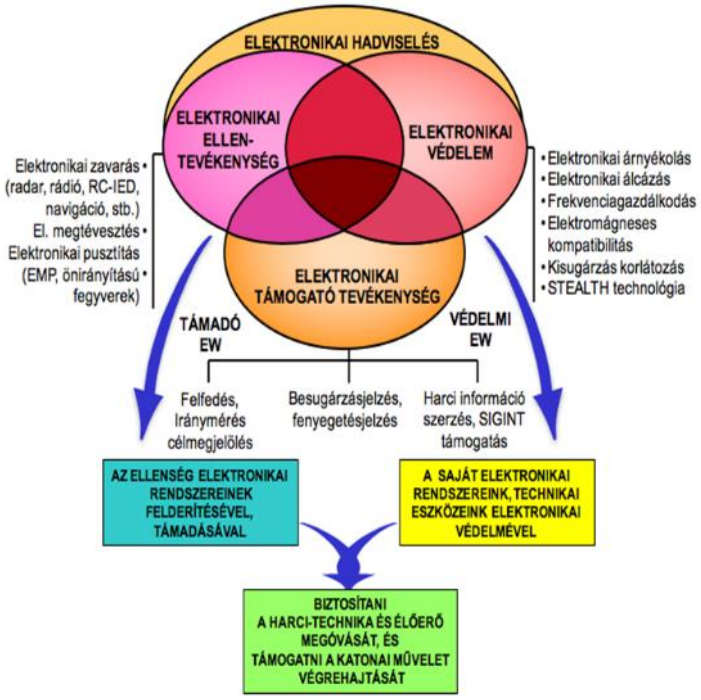
Az elektronikai hadviselés

Olyan harci képességeket foglal magában, amelyek kiegészítik más fegyverrendszerek hatását [18]. Más megfogalmazásban az elektronikai hadviselés olyan katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza a frekvenciaspektrum ellenség részéről történő használatát és biztosítja annak a saját csapatok általi hatékony alkalmazását. Területei (2. ábra) az elektronikai támogató tevékenység, az elektronikai ellentevékenység és az elektronikai védelem. Az elektronikai támogató tevékenység az elektronikai hadviselés azon része, amely magába foglalja – a fenyegetés azonnali jelzése érdekében – az elektromágneses kisugárzások felkutatására, elfogására és azonosítására, valamint a források helyének meghatározására irányuló tevékenységeket. Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és irányítható energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát. Az elektronikai ellentevékenység egyik területe az elektronikai zavarás, amely az elektromágneses energia szándékos kisugárzását, vissza sugárzását vagy visszaverését jelenti azzal a céllal, hogy megakadályozzuk az ellenség elektronikai eszközeinek vagy rendszereinek hatékony működését. Az elektronikai védelem az elektronikai hadviselés azon része, amely biztosítja az elektromágneses- és egyéb spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére [11].

A továbbiakban az elektronikai védelem és az elektronikai támogató tevékenység halmazába is beilleszthető tevékenységgel foglalkozok, mivel a jelen írás terjedelme nem teszi lehetővé, hogy az elektronikai hadviselés teljes spektrumát, minden egyes elemét feldolgozzam. Abban az esetben, amikor a saját csapataimat kívánom védelmezni az ellenség hatékony elektronikai felderítésétől, több módszer mellett az eszközeim kisugárzásának korlátozására van szükség. Ám amennyiben információval szeretnék gazdagodni a szemben álló fél műveleteiről, akkor a SIGINT[4], MASINT[5],

[4] Signals Intelligence – jelhírszerzés, amerikai katonai rövidítés a rádiós és rádióelektronikai hírszerzésre
[5] Measurement and Signature Intelligence – különböző típusú mérőműszereket felhasználó, technikai jellegű hírszerzés, amely észleli, beméri, követi, azonosítja és leírja a célforrásra jellemző egyedi tulajdonságokat, mint

IMINT[6], HUMINT[7], OSINT[8] és a RINT[9] hírszerzési tevékenységek állnak rendelkezésre. Az imént említett eljárások közül a publikáció további részeiben a nem szándékos kisugárzás felderítési tevékenységgel, az elektronikus biztonsággal és az ehhez kapcsolható UAV tevékenységekkel foglalkozok, így közelebb kerülve és bemutatva a pilóta nélküli rendszerek által megoldható egy-egy feladatot.



2. ábra Az elektronikai hadviselés összetevői [6]

Ha a felhasználó akaratán kívül kisugárzott adatokhoz szeretnénk hozzájutni, abban az esetben úgy kell a rendszerünket hangolni, hogy az ellenség elektronikai eszközeinek nem szándékos elektromágneses kisugárzásait keresse a felderítő eszközünk. Ezek a mechanikai- (szeizmikus-, akusztikai-, hidroakusztikai), elektromágneses (rádióhullámok, optikai-, infra-, lézer-, ultraibolya sugárzások) és/vagy részecske sugárzások, keletkezhetnek az adóberendezések, antennák, tápvonalak sérüléseiből a berendezések helytelen üzemeltetésből, sávon kívüli melléksugárzásokból, esetleg a számítógép monitorok normál működése közbeni kisugárzásból.

Ez a tevékenység nem csupán harci körülmények között kívánatos eljárás, hanem az üzleti élet, a magánszféra és az állami, önkormányzati szektor bizonyos adatainak, eljárásainak, rendszeradatainak, üzleti-, állam-, vagy magántitkok felderítése esetén is.

Ezen „titkok” megóvása érdekében számos technikai jellegű, írott és íratlan szabály létezik, melyek folyamatosan frissítésre is kerülnek, így ezek betartása a károk minimalizálásában jelentősen segíthet mindaddig, amíg a felderítési lehetőségek tárházának bővülése nem kerül lépéselőnybe.

például egy meghatározott repülő eszköz radarjele vagy a levegőből vett minta vegyi összetétele. Más szóval minden olyan technikai hírszerzés, ami nem sorolható a SIGINT és az IMINT kategóriába

[6] Imagery Intelligence – képanyagok elemzésén alapuló hírszerzési módszer

[7] Human-Source Intelligence – humán hírszerzés, emberi erőforrások felhasználásával folytatott hagyományos hírszerzés, kémkedés

[8] Open Source Intelligence – a nyílt forrású hírszerzés nemzetközileg is elfogadott angol nyelvű rövidítése

[9] Radiation Intelligence – kisugárzás felderítés

Az elektronikus biztonság

A témával foglalkozó jogszabályok, rendeletek és előírások útvesztője nem könnyíti meg a dolgát az egyszerű felhasználónak, de a következő néhány gondolatban összegyűjtöttem a legfontosabb ismereteket ezzel kapcsolatosan.

Az országgyűlés az állami és a közfeladatok ellátásának biztosítása érdekében, a közérdekű adatok megismerésének alkotmányos jogából, illetve e jog kizárólag **szükséges és arányos** mértékű korlátozásának lehetőségéből kiindulva, a minősített adat védelméről megalkotta a 2009. évi CLV. törvényt. Ezt követően az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól alkotott rendeletet a kormány 92/2010. (III. 31.) számon. Majd ugyanebben a jogalkotási ciklusban megszületett a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 161/2010. (V. 6.) számú kormányrendelet. Ebben kerül pontosításra az elektronikai hadviselés szempontjából is egy fontos fogalom, mint a **kompromittáló kisugárzás**, amely olyan elektromos vagy elektromágneses jel, amelynek vétele és feldolgozása lehetővé teszi az arra illetéktelen személy vagy szerv számára az elektronikusan kezelt minősített adat kinyerését és megismerését. Ennek a rendeletnek a tanulmányozását folytatva ismerhetjük meg a kisugárzás csökkentésének jogszabályi követelményeit, melyet a **TEMPEST**[10] követelmények fogalom alatt egységesítették. A megfogalmazás szerint a „Titkos!" és „Szigorúan titkos!" minősítési szintű nemzeti minősített adat, valamint a „Bizalmas!", vagy magasabb minősítési szintű külföldi minősített adat bizalmasságának védelme érdekében kialakított biztonsági intézkedések – amelyek kiterjednek az elektromos és adatkábelek vonalvezetésére, a rendszer környezetében alkalmazható berendezésekre, árnyékolástechnikai megoldásokra, valamint csökkentett kisugárzású eszközökre – együttese, amelyet a rendszer valamennyi eleme vezetett és elektromágneses kompromittáló kisugárzásának csökkentése érdekében alakítottak ki. A jogszabály a követelmények érvényesítésével is foglalkozik a későbbi (49§-51§) paragrafusok között, melyben pontosításra kerül, hogy a TEMPEST követelmények kiterjednek a rendszer környezetében alkalmazható berendezésekre, elektromos árnyékolástechnikai megoldásokra, csökkentett kisugárzású hardver eszközök alkalmazására, az építészeti, épületgépészeti, épületvillamossági, valamint a rendszerhez tartozó vagy a rendszer környezetében található fém berendezések földelésére. A rendelet alapján az NBF feladata meghatározni a minősített rendszer telepítési helyének TEMPEST zóna besorolását, kivéve, ha az NBF által kijelölt szerv, a NATO, az EU vagy tagországaik TEMPEST hatósága által elfogadott vagy kiadott zóna besorolással rendelkezik az adott szervezet, ebben az esetben további vizsgálatok nélkül is elfogadható az érvényes besorolás [24].

Néhány gondolat erejéig talán érdemes foglalkozni azzal, hogy mi is az a TEMPEST, ugyanis a jogszabályok tanulmányozásával (számomra) még nem sikerült megtudni, csupán azt, hogy a kompromittáló kisugárzás megelőzésére, vagy legalábbis a csökkentésére milyen bürokratikus

[10] Vihar, förgeteg (főnévként, de átvitt értelemben is) [14] Minden elektromosan működő eszköz bocsát ki magából elektromágneses jeleket. Ez a fizikai jelenség lehetővé teszi, hogy megfelelő eszközök alkalmazásával a kisugárzott jelekből reprodukálható legyen az eszközön kezelt eredeti adat. Minősített adat elektronikus úton történő kezelése esetén a kompromittálódás elleni fő feladat a minősített adatot tartalmazó kisugárzás minimális szintre való csökkentése, ami megakadályozza az adat reprodukálhatóságát, annak illetéktelen kezekbe való jutását. E módszer szabályait TEMPEST összefoglaló néven említik.[26]

teendői vannak a rendszert üzemeltetőnek és a felhasználónak. A kutatásaim során a következő leírásokkal találkoztam a teljesség igénye nélkül:

- a TEMPEST egy vizsgálat fedőneve volt, amely során a különböző elektronikai adatfeldolgozó egységek kisugárzását elemezték. Ezen vizsgálatok során megállapították, hogy minden elektronikai berendezés kibocsát bizonyos rezgéseket, amelyeket elfogva, és különböző eljárásoknak alávetve, az adatok kinyerhetők. Megállapították továbbá, hogy a kisugárzás lehet akusztikus, elektromos vagy mágneses és az adatok visszanyerhetősége miatt, fontos nemzetbiztonsági tényezőként könyvelték el ezt a fizikai tényt (bizonyos rendszereknél akár fény kisugárzás is lehetséges). A laboratóriumi tesztek bebizonyították, hogy a tökéletes információ védelmet, csak a fizikai közeg átalakítása, valamint a háttérzaj létrehozásával érhetik el. A vizsgálatok szerint, az elektromágneses hullámok sokszorosításával, minél több „fals" rezgés mesterséges indukálásával, már szinte lehetetlen az adatvisszafejtés, amennyiben ehhez pedig egy megfelelő árnyékoló környezet társul, a belső visszhang miatt lehetetlenné válik a dekódolás. Fontos tudnunk, hogy ez a jelenség nem sugárzás, hanem kisugárzás. Tehát az információáramlás, a feldolgozás során az elektronikai vagy mechanikai berendezések által keltett hullámok. A TEMPEST jelzést gyakran használják, illetve említik úgy, hogy Kisugárzás Biztonság vagy Biztonságos Sugárzás (EMSEC)[11]. A TEMPEST kezdetét a 60'-as és korai 70'-es évekre vezethetjük vissza, amikor is az NSA[12], ezt fedőnévként használta, a különböző elektronikai berendezések által kibocsátott jelek elfogására, és azokból való értelmezhető adatvisszafejtésre tett kísérleteire. Kezdetben ezek a távközlési berendezésekre irányultak, mára azonban igen kiszélesedett ezen adatvédelmi technológia alkalmazása [12];
- a TEMPEST megoldások, többszintű védelmi rendszerrel igyekeznek az elkerülendő kisugárzásokat megakadályozni. A leghatékonyabb védelmi stratégia, az aktív és passzív védelem együttes használata. Az I/O kapukra kriptográfiai egységek felszerelésével, az adatok immár nem szabványos átvitele, jócskán megnehezíti a visszafejtést. Ezt követően az árnyékolástechnológia szab gátat a sugárzásnak, így minden információ, csak a hardvereszközökben marad. A következő védelmi pont, a hardverelem hozzáférhetőségének korlátozása. És az utolsó szakasz, egy esetleges zavaróegység beépítése.

Az USA és a NATO TEMPEST három szintet határozott meg: [13]

1. NATO SDIP-27 Level A (régebben AMSG 720B) és az USA-ban ***NSTISSAM I. Szint*** *„Egyezményes Laboratóriumi Test Kisugárzási szint"* Ez a „stricteszt" mondhatni rövidtávú szint, azon egységeknek feleltethető meg, ahol az információ elnyelő, nevezzük támadónak, szinte közvetlenül hozzáfér az adatokhoz, azaz a kisugárzást közvetlen közelről rögzíti. (maximum **1 m-es távolság**ig megengedett ezen szintben a támadó) NATO Zóna 1 szint.
2. NATO SDIP-27 B Szint (régebben AMSG 788A) és az USA-ban ***NSTISSAM II. Szint*** "*Laboratóriumi Próba Szabvány Gyengén Védett Berendezésekre*" Ez egy némileg lazább szabvány, ami NATO Zóna 1 egységeknél az működik. A szabvány szerint adott egy támadó, aki a kisugárzó berendezéshez **maximum 20 m-es távolság**ba tud csak közel jutni. A szabvány szerint a támadó számára a fizikai kontaktus lehetetlen. (a 20 m-es táv mérésében, fizikai közeg nem játszik szerepet, így az építőanyagok, vagy páncélzat sem).

[11] Emissions security - sugárzás biztonságtechnika

[12] National Security Agency (Nemzetbiztonsági Ügynökség) az Amerikai Egyesült Államok rádióelektronikai, jelhírszerzéssel foglalkozó hírszerző szervezete

3. NATO SDIP-27 Szint C (régebben AMSG 784) és az USA-ban *NSTISSAM III. Szint "Labor Próba Szabvány, Taktikai Mobil Berendezés / Rendszerek esetében"* Ez a szint, még inkább lazább szabvány, amely NATO Zóna 2 egységekben működik. A szabványban a támadó **maximum 100 m-re** tudja megközelíteni a kisugárzás forrását.

Pótlólagos szabvány:

1. NATO SDIP-29 (régebben AMSG 719G): *"Üzembe helyezése Villamos Berendezésnek a Feldolgozása Titkos Információnak"*. Ez szabvány meghatározza az elektronikai berendezések üzembe helyezésének követelmények például, hogy milyen az alap összetétele, milyen távolságra legyenek a kábelek, milyen borításúnak kell lennie a berendezésnek;
2. AMSG 799B: NATO Övezetekre Osztási Eljárási Szabvány. Ezen szabvány rendelkezik a különböző övezetekre vonatkozó feltételekről, és egyértelműen leírja, hogy az egyes titokvédelmi követelményeknek miként kell megfelelni.

A tanulmányom eddigi részeiben írtam az információs társadalomról, az információs hadszíntérről, azt is bemutattam, hogy mik azok az információs műveletek és milyen elemei vannak, majd bemutattam az elektronikai hadviselés alkotó elemeit, valamint a kompromittáló kisugárzással kapcsolatban a TEMPEST jelentését és annak jogi hátterét is körbe jártam, de hogy miként kapcsolhatók a pilóta nélküli légijárművek ehhez a témához, erre még nem adtam magyarázatot. A következő pár bekezdésben erre mutatok lehetőségeket, elképzeléseket.

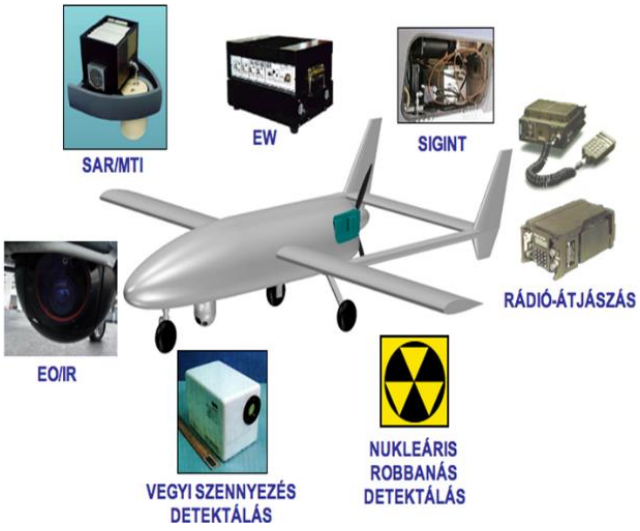
AZ UAV FELHASZNÁLÁSÁNAK LEHETŐSÉGEI AZ ELEKTRONIKAI HADVISELÉSBEN

A drónok lehetőségeit tekintve a XXI. század elején, a technikai fejlődés eredményeinek köszönhetően, egyre gyakrabban találkozunk a repülésben a hagyományos repülő eszközök mellett a pilóta nélküli repülőgépekkel. Feladatukat és rendeltetésüket tekintve számtalan helyen és célra alkalmazhatjuk ezeket az eszközöket, akár katonai, akár polgári vonatkozásban.

Tipikus katonai légi tevékenységek, mint például megelőző csapások, vagy légiharcok, felderítési manőverek megvívása folyamán az ember által vezetett és a személyzet nélküli repülőgépek együttes alkalmazása biztosíthatja az alkalmazott eszközök hatékonyabb felhasználását és a saját erők fokozottabb megóvását. Például a pilóta által vezetett légijármű előtt repülő UAV-ken helyezik el a felderítő és csapásmérő eszközöket – amelyeket a hajózó saját fedélzeti rendszere részeként üzemeltet (drónok és repülőgépek hálózatos, rajban történő üzemeltetése) [15].

A légi eszközünk képességeit tekintve folyamatos „fejlődést" figyelhetünk meg. Számos területen bevonásra kerülnek, mint például rendvédelmi felhasználásban, ahol néhány országban megjelentek a paintball lövedékekkel felszerelt, tömegoszlatásra alkalmas UAV-ok. Indiában paprikaspray-vel felszerelt eszközökkel kísérleteznek a rendvédelmi szervezetek fejlesztői. Egyre nagyobb népszerűségnek örvendenek a képrögzítésre alkalmas eszközökkel rendelkező, pl. események rögzítésére használható eszközök. A szórakoztatás mellett külön cégeket alapítottak (alapítanak) események filmezésére, terepfelmérésre, térképezésre, hő- és infrakamerás felvételek készítésére, továbbá nehezen megközelíthető helyek felderítésére is. Másik alkalmazási terület, amivel a német posta is kísérletezik az a csomagszállítás, melynek keretében az Északi-tengeren található egyik szigetre indítottak gyógyszer kézbesítő pilóta nélküli repülőgépes szolgáltatást. A közel jövőbeni tervek között szerepel, hogy a Facebook közösségi portált üzemeltető vállalat,

pilóta nélküli repülőgépekkel szeretne földközeli, műhold szerű Internetes lefedettséget biztosító szolgáltatást nyújtani az elmaradott országokban vagy nehezen megközelíthető helyeken tervek szerint napelemes UAV-al. További lehetőségként adódik nagyméretű mezőgazdasági területek megfigyelésére is. A drónokra szerelt nagy felbontású kamerákkal a különböző spektrumokban felvett képekkel egyszerűen és költséghatékonyan megállapítható az egyes területeken telepített növényzet fejlődése és betegsége egyaránt. A katasztrófavédelmi szervezeteknél is hatékonyan használhatók a kárfelmérésére, a kutató-mentő műveletek támogatására, esetleg gyógyszerek, mentő eszközök helyszínre juttatására, valamint az alkalmazásuk kiterjedhet tűzfelderítés, tűzoltás körére is. A katonai alkalmazásokat nem kihagyva szükséges megemlíteni, hogy az USA a különleges műveleti erők támogatására (információs műveleti támogatás) is be kívánja vetni ezeket az eszközöket. A válságkörzetek területén is sikerrel bevethetők légi megfigyelő tevékenység végrehajtására az UAS-ok. Segítségükkel a légi megfigyelés során a nemzetközi szervezetek munkatársai távolról figyelhetik meg az eseményeket, ezzel minimálisra csökkentve a személyi sérülés lehetőségét a körzetben. Az Európai Biztonsági és Együttműködési Szervezet (EBESz) szintén alkalmaz Ukrajna területén UAS eszközöket felderítési, megfigyelési feladattal [16].



3. ábra Az UAV lehetséges alkalmazásai [22]

Az ebben a fejezetben eddig leírt, felsorolt lehetséges bevetési módok mellett, közeledve a címben említett elektronikai hadviselést megvalósító UAS eszközünkhöz, a pilóta nélküli légijárművön elhelyezett függesztményeket tekintve a 3. ábrán rendkívül szemléletesen kerül bemutatásra néhány lehetséges megvalósítási mód, amivel „harcba" küldhetők az UAV-k. Ezt a megoldási repertoárt tekintve, az eszközünk képes az egyszerű rádió-átjátszásra, a nukleáris robbanás és a vegyi szennyezés detektálásra, infravörös tartományú (EO/IR)[13] felderítésre, térképezésre, mozgó célpont indikálására (SAR/MTI)[14]), elektronikai hadviselési (EW)[15] és rádió felderítési (SIGINT) feladatok elvégzésére.

A XXI. század információs társadalmában rendkívül nagy teret kapott a számítógép, mely minden háztartásban és munkahelyen nagy számban megtalálható. Ezen keresztül bonyolítjuk

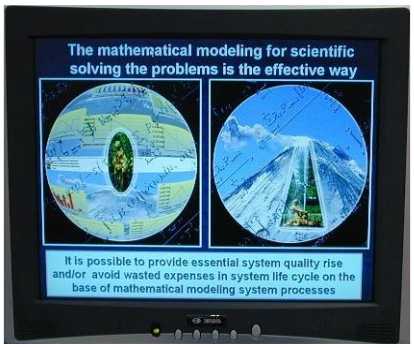
[13] Electrooptical/infrared – elektrooptikai/infravörös
[14] Synthetic Aperture Radar/Moving Target Indicator
[15] Electronic Warfare – elektronikai hadviselés

levelezéseinket, olvassuk a híreket, kapjuk a munkahelyi feladatokat, intézzük a vásárlásainkat, és mindeközben talán nem is gondolunk arra, hogy veszélynek lehetünk kitéve.

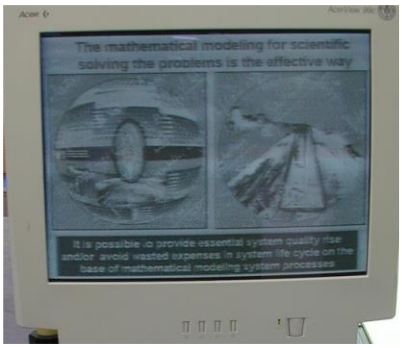
A hálózatba kötött informatikai eszközök elleni támadások és az ellenük történő védekezés számos publikációban elérhető. Ebben az írásban a számítástechnika még szűkebb szegmensét vizsgálom, ami az egyedül álló gépekről történő „adatlopások" megvalósíthatóságával hozható kapcsolatba, amelyek kivitelezéséhez segítségünkre lehet a megfelelően paraméterezett és felkészített UA eszközünk. Az egyik esetben a Wim Van Eck nevéhez köthető lehallgatási technikát16 említeném, melyet a holland számítástechnikus 1985-ben dolgozott ki [25]. Ezen eljárás során a lehallgató, egy informatikai eszköz, például a monitor elektromágneses sugárzását figyeli meg. Van Eck ezzel a módszerrel eredetileg a katódcsöves (CRT) monitorokat vizsgálta, ám később kifejlesztésre került a hasonló elven működő lehallgatási módszer az LCD képernyőkre is, amely a mai napig használható, működtethető eljárás. Az ilyen monitorok képét a képernyő belső felületére felvitt foszfor felvillanásai adják, amelyeket egy elektronsugár gerjeszt. Az elektronsugár, amelyet elektromágneses tekercsek térítenek el a megfelelő irányba, másodpercenként néhány tucatszor végig pásztázza a képernyőt. A tekercseket vezérlő magasfeszültségű jel, amely a képernyőn megjelenő összes információt tartalmazza, elektromos kisugárzást gerjeszt. A jelet nagyfrekvenciás antennákkal fogva és szinkronizálva akár relatíve nagy távolságról is kiolvasható belőle az eredeti kép, melyet a 4. ábrán szemléltetek. Ehhez a kiolvasáshoz mind a CRT, mind pedig az LCD képernyőket célzó eszköz viszonylag olcsó, könnyen beszerezhető alkatrészekből állítható össze. Az UA szerepe ott jelentkezik, amikor a TEMPEST követelményeknek megfelelni kívánó felhasználó a NATO zóna 1. szintnek megfelelően kiépíti a védelmet, így joggal gondolhatná, hogy teljes biztonságban van. Ám a pilóta nélküli eszközök rohamos fejlődése a miniatürizálást is beleértve, ezt a szabályzót is képes felülírni.

Mivel a nagyfrekvenciás vevő eszköz elvi felépítése adott, az a megoldandó feladat, hogy ez olyan kisméretű legyen, ami a lehallgatásra szánt eszköz közelébe történő juttatásra alkalmas drónunkra biztonságosan felhelyezhető legyen. Minél védettebb adatokkal dolgoznak az adott munkaállomáson, a számítástechnikai rendszer védelme annál magasabb szintű, így annál kisebb, precízebb pilóta nélküli szállító eszköz kell az észrevétlen megközelítéshez és a lehallgatás ideje alatti az észrevétlen pozíció tartáshoz. A nanotechnológia korában a nanorobotok egyre több, információ szerzésre képes nanoszenzort tudnak magukkal vinni, amelyekkel megszerezhetővé válnak a szenzitív adatok is. A hordozó eszköz, amely esetünkben egy nanodrón, a mesterséges intelligenciával felvértezve, képes megtalálni a rést, amelyen át bejut az őrzött helyiségbe. Az adatok felderítését, rögzítését követően önállóan megkeresi a kijutási lehetőséget, ám amíg nem mutatkozik lehetőség a távozásra, addig a saját energiaellátó rendszerét tartja karban az eszköz. Kihasználva a falban futó vezetékek, valamint különböző elektromos eszköz körül gerjesztett mágneses teret, vezeték nélküli töltéssel „gondoskodik" a maximálisan elérhető energia szintről. Azt hihetnénk, hogy ez a módszer az LCD monitorok, notebookok korában elavulttá vált. Ez azonban nem igaz, mivel az eljárás „él és virul" napjainkban is, ami felértékeli az UAV-k szerepét ennek a precízebb végrehajtásában.

[16] A lehallgatás az információ titokban való megszerzésének - általában - etikátlan módja.



Eredeti Power Point prezentáció



25 m távolságban elhelyezett lehallgató eszközön megjelent információ

4. ábra Monitor kisugárzás lehallgatása [19]

Egy másik módszer, amivel akár jelszavakat is lehet „lopni" a számítástechnikai eszközünkről, az a számítógép házában található hűtőventilátor manipulálása. Biztonsági kutatók igazolták, hogy a ventilátor gyorsításával és lassításával adatok továbbíthatók egy közeli hangrögzítő eszközre. Egy különálló számítógépből történő adatlopásnak erre a módszerére eddig a gyanútlan felhasználó nem is gondolt, hiszen még a letiltott USB portok sem akadályozzák meg a lehallgatást. Az izraeli Ben-Gurion Egyetem mérnökei igazolták, hogy egy elszigetelt gépről is kinyerhetők a szükséges adatok, ha egy kártevő segítségével ráveszik az eszközt, hogy zajt adjon. Mivel a digitális adatok nullákból és egyesekből állnak, így nem is meglepő, hogy a ventilátor gyorsulása zajt kelt, amit a feldolgozó egység egyesnek, a lassulást pedig nullásnak dekódol. Így a gyorsítás és lassítás ciklusaival egyesek és nullák közvetíthetők. Mivel a mai modern eszközök hűtő elemei igazán csendesek, így a zajt vevő egységnek, a megfelelő érzékelés miatt, nagyon közel (kb. egy m-es távolságon belül) kell tartózkodni az adatnyerés idejére. Ennek megvalósításához az előző módszernél is említett miniatürizálás fejlődése elengedhetetlen, mivel a cél ventilátor mellé fixen telepített eszköz akár feltűnő is lehet. Ellenben drónt használva, megfelelő időpontban elvégezhető a berepülés, majd a megfelelő mennyiségű adat megszerzését követően pedig feltűnés nélkül távozhat az eszközünk, akár az előző felhasználási lehetőségnél leírt módszerrel, amikor a mesterséges intelligenciával ellátott NUAV[17] önállóan felderíti a zsilip nyitásának pillanatát, majd berepül a célzónába. A másik lehetőség a nano eszközt tekintve, amikor a védett helyiségbe maga a kezelő „szállítja be" az eszközt a ruhájának redőjében, vagy akár a táskájának oldalára tapadva [20][21].

KÖVETKEZTETÉS

Az írásom elején célként fogalmaztam meg, hogy kapcsolódási pontokat keresek és mutatok be a hagyományos hadviselés fizikai hadszíntere mellett megjelent, információs hadszíntérben végrehajtott műveletek és az ezek végrehajtása során alkalmazott, pilóta nélküli légijárművek között.

Számos fórumon olvasható, hogy a világ modern hadseregeiben eddig is, ezután pedig egyenesen elengedhetetlen a fejlett technológiák alkalmazása, legyen az akár az „egyszerű" lőfegyver, a repülőgép és annak pilóta nélküli változata vagy korunk mindennapi használati eszköze, a számítógép. Mindennapi életünkre jellemző (nem csupán a hadviselésre), hogy nagymértékben alkalmaz kisugárzó elektronikai eszközöket is. Ez a tény támasztja alá azon figyelmeztető hangokat,

[17] nano UAV

melyek arra ösztönzik a mérnököket, jogalkotókat, hogy az elektronikai hadviselés minden területével érdemes foglalkozni, és nem csupán a szemben álló hadseregek "játszmájában".

A publikációmban elhelyeztem az újkori hadviselés térképén az információs műveleteket, bemutattam ennek a hadviselési fajtának az alkotó elemeit. Ezt követően az elektronikai hadviselésről írtam, részletesebben a kompromittáló elektromágneses kisugárzás elleni védelmet, annak felderítését taglalva, melynek a magyar jogszabályi környezetét is megjelenítettem. Majd ezek után kísérletet tettem arra, hogy összefüggést találjak a drónok és az újonnan definiált információs hadszíntér között.

Az írásom időszerűsége azért releváns, mivel az információs társadalom nagyon fejlett, nagyon hatékony, ugyanakkor meglehetősen sebezhető társadalmi, gazdasági rendszer. Sebezhetőségének objektív alapját az adja, hogy ennek a társadalomnak működése szorosan kapcsolódik a globális, nemzeti, regionális és lokális környezethez. Ennek következtében igen erősen függ az információs környezet fejlett, ám erősen korlátozható, vagy sebezhető integrált információs infrastruktúráitól, például a távközlési hálózatoktól és a nagy teljesítményű számítógép hálózatoktól. Ezt az ártó szándékú egyének, csoportok, terroristák és az ellenségek is jól tudják, amit kihasználva, a lehetőségeikkel élve, mindent elkövetnek annak érdekében, hogy az információs társadalom felgyorsult és lüktető életritmusát lecsökkentések, vagy átmenetileg beszüntessék, amivel pánikot, riadalmat keltenek [7].

Napjainkban az ellenérdekelt titkosszolgálatok mellett a bűnözői körök, vagy akár a szolgálatok számára célként megjelenő csoportok és személyek is védik, védhetik titkosítással adataikat, rendszereiket. Mindezek jelentősen megnehezítik, vagy akár lehetetlenné teszik az értelmezhető információkhoz való hozzáférést, amelyek felértékelik a szervezetek rejtjelezéssel, információbiztonsággal, illetve az ellenfél rejtjelezett anyagainak megfejtésével foglalkozó technikai és tudományos területek jelentőségét. A rendelkezésre álló, közvetlenül értékelhető információkká történő átalakítás képessége és lehetősége így alapjaiban kihat a technikai forrásokhoz kapcsolódó információgyűjtő területek eredményeire, eszközeire és jövőbeli fejlődési irányaira. Tisztában kell lenni ugyanakkor azzal is, hogy a SIGINT-et, mint tudományos és technikai módszerekkel és eszközökkel folytatott rádióelektronikai felderítő tevékenységet az ellenség, illetve ellenérdekelt fél is alkalmazza velünk szemben. Az eszközeinkhez kapcsolódó kisugárzott jelekből és kommunikációból levonható következtetések és megállapítások a másik fél számára is értékes információkat eredményezhetnek. [17]

A cikkben leírtakból látható, megállapítható és elgondolkodtató az, hogy napjainkban robbanásszerű fejlődést mutató pilóta nélküli légijárművek, légijármű rendszerek egyre inkább ezen a területen is teret "kérnek" és kapnak a végrehajtandó feladatokból maguknak. Miután a felhasználó igényeinek és az elérendő célnak legjobban megfelelő szenzor elkészül, már "csak" a rendszert szállító felépítményt kell "alárakni" és a siker szinte garantált. A szellemi, ipari kapacitás készen áll erre a "kihívásra", már csupán a jogi háttér hiányzik, amely egyértelműsíti, keretekbe foglalja a ki, mit, mikor, hol kérdések megválaszolását nagyban elősegítő autonóm eszközök használatát.

FELHASZNÁLT IRODALOM

[1] Szun-ce: A háború művészete. Cartaphilus Kiadó, Budapest, 2006. p. 74.
[2] Hausner Gábor-Padányi József: Kutatások a hadtudományok és a katonai műszaki tudományok területén, Nemzeti Közszolgálati Egyetem, Budapest, 2013. ISBN 978-615-5305-17-7 p. 17.
[3] Haig Zsolt: Információ, társadalom, biztonság. Nemzeti Közszolgálati Egyetem, Budapest, 2015. ISBN 978-615-5527-08-1. p. 9.
[4] Várhegyi István – Makkay Imre: Az információs hadviselés alapjai, egyetemi jegyzet, ZMNE, Budapest, 2000. p. 7.
[5] Mengxiong, Chang: Kínai nézetek a jövő háborújáról. Negyedik rész: A 21. század katonai harci fegyvereinek forradalma. http://www.au.af.mil/au/awc/awcgate/ndu/chinview/chinapt4.html
[6] Haig Zsolt-Kovács László-Ványa László-Vass Sándor: Elektronikai hadviselés, Nemzeti Közszolgálati Egyetem, Budapest, 2014. ISBN 978-615-5305-87-0 p. 9, 17, 34, 157.
[7] Haig Zsolt-Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. p. 156, 69.
[8] George Seiferth: Hatásalapú információs műveletek. Nemzetvédelmi Egyetemi Közlemények, 9. évf. 4. sz., ZMNE, Budapest, 2005. pp. 17-23.
[9] Dr. Haig Zsolt: Számítógép–hálózati hadviselés rendszere az információs műveletekben, Bolyai Szemle 2006. 1. szám, ROBOTHADVISELÉS 5. Tudományos Konferencia kiadványa http://uni-nke.hu/downloads/bsz/bszemle2006/1/06_Haig_Zsolt.pdf
[10] Munk Sándor: Az információs műveletek típusai és modelljei. Hadtudomány, XII. évfolyam 1. szám, 2002. március http://www.zmne.hu/kulso/mhtt/hadtudomany/2002/1/z-02/chapter1.htm
[11] Horváth József: Elektronikai hadviselés a magyar honvédségben, Hadmérnök, 2014. március, IX. évfolyam 1. szám. p.177. http://hadmernok.hu/141_17_horvathj.pdf
[12] A TEMPEST meghatározása: http://www.tempest.hu/index.php?option=com_content&view=article&id=65:mi-is-az-a-tempest-&catid=11:cikk&Itemid=1
[13] A TEMPEST szabványok: http://hubel.net/index.php?option=com_content&view=article&id=23&Itemid=87
[14] Országh László: Angol-Magyar kéziszótár, Akadémiai Kiadó, Budapest, 1998. p.908. ISBN 963 05 6906X
[15] Dr. Palik Mátyás: A pilóta nélküli légijárművek katonai alkalmazása, In: Pilóta nélküli repülés profiknak és amatőröknek, Palik Mátyás (szerk.), Nemzeti Közszolgálati Egyetem, Budapest, 2013. ISBN:9789630869232 pp. 281-297.
[16] Vránics Dávid-Üveges András: Pilóta nélküli légi járművek fejlődése, Felderítő szemle, 2015. ISSN 1588-242X pp.129-132.
[17] Dr. Dobák Imre (szerk.): A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest, 2014. ISBN 978-615-5305-49-8 p. 168.
[18] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány. p. 3.
[19] Haig Zsolt-Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, tanulmány, Nemzeti Közszolgálati Egyetem, 2012. p. 241. TÁMOP 4.2.2/B-10/1-2010-0001 http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf
[20] Now Fan Noise Can Be Used To Steal Data From Air-Gapped Computers http://www.tech-worm.net/2016/06/now-fan-noise-can-used-steal-data-air-gapped-computers.html
[21] Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf
[22] Az UAV lehetséges alkalmazásai (http://hhk.uni-nke.hu/uploads/media_items/infoops-i.original.pdf
[23] TEMPEST A 318/2015. (X. 30.) Korm. rendelet 1. §-ával megállapított szöveg.
[24] Nemzeti Biztonsági Felügyelet: http://www.nbf.hu/jogszabalyok.html
[25] Van Eck Phreaking: https://www.techrepublic.com/blog/it-security/wim-van-ecks-legacy/
[26] TEMPEST meghatározás: http://www.nbf.hu/tempestmer.html

THE USE OF UNMANNED AIRCRAFT SYSTEMS FOR ELECTRONIC WARFARE

Nowadays, the information, its acquisition and possession is the primary key to survival. This value should be managed well. It is important to share it consciously and protect responsibly. Every piece of information is wanted to acquire by someone, trusting that in their possession he can overcome, or defeat his competitors, opponents, perhaps enemies. In this "battle" those can overcome whose assets are more advanced to reconnoitre and interpret data or who has adequate tools, techniques and methods to disguise this important knowledge from prying eyes. The electronics and computer science development brought a number of industries which are specialized to disguise and to acquire this knowledge. These information operations are not only "applied" in the war industry, or in operations but also in civil everyday life. We can see them in the industrial espionage as well. *In the following publications, the author presents a piece of information operations, a possible link between electronic warfare and drones, through relevant domestic and foreign publications given out in this subject, and the author's individual conclusions are included as well.*

Keywords*: unmanned aircraft systems, drones, electronic warfare, information intelligence*

Major Gábor	Gábor Major
tanársegéd	Assistant lecturer
Nemzeti Közszolgálati Egyetem	National University of Public Service
Hadtudományi és Honvédtisztképző Kar	Faculty of Military Science and Officer Training
Katonai Repülő Intézet	Institute of Military Aviation
Fedélzeti Rendszerek Tanszék	Department of On-Board Systems
major.gabor@uni-nke.hu	major.gabor@uni-nke.hu
orcid.org/0000-0003-2927-127X	orcid.org/0000-0003-2927-127X

http://www.repulestudomany.hu/folyoirat/2017_3/2017-3-22-0490_Major_Gabor.pdf