ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

BEREGI ALEXANDRA LILLA

A digitalizáció, mint a 21. század új biztonsági kihívása, különös tekintettel Magyarország kibervédelmére

Témavezető: Dr. Babos Tibor címzetes egyetemi tanár

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2022.10.03.

Szigorlati/komplex vizsga bizottság:

Elnök:

Prof. Dr. Rajnai Zoltán, egyetemi tanár

Tagok:

Dr. habil. Besenyő János, egyetemi docens

Prof. Dr. Szternák György Mihály, ny. egyetemi tanár

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Dr. Rajnai Zoltán, egyetemi tanár

Titkár:

Dr. Pető Richárd, adjunktus

Tagok:

Dr. Németh Gyula id.

Dr. Kollár Csaba PhD

Prof. Dr. Szternák György Mihály, ny. egyetemi tanár

Bírálók:

Dr. habil Remek Éva, egyetemi docens

Dr. Szűcs Endre PhD

Nyilvános védés időpontja

2023.

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK

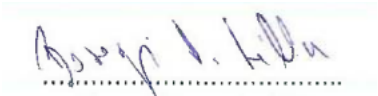
MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott Beregi Alexandra Lilla kijelentem, hogy a

A digitalizáció, mint a 21. század új biztonsági kihívása, különös tekintettel Magyarország kibervédelmére

című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2022.10.10.



Beregi Alexandra Lilla

TARTALOMJEGYZÉK

BEVEZETÉS

„A 3. évezred, az eddig ismert fizikai létünk mellett egy új, virtuális világot is nyitott számunkra.”

Babos Tibor

A tudományos probléma megfogalmazása

Az informatikai forradalom hatására jelentős változások indultak el a társadalomban, mert átformálta a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, logisztikai, energetikai, diplomáciai, nemzeti biztonsági és katonai rendszereket. [1 pp. 122-145] Ez a folyamat globális korszakváltást eredményezett.

A hidegháború a második világháború két nyertes nagyhatalmának ideológiai; kulturális; társadalmi; gazdasági és politikai összecsapásában mutatkozott meg. Már a hidegháború időszakában is jelentkezett a biztonság egyoldalú katonai értelmezésének átalakulása, amelyet azonban a hidegháború vége, vagyis az 1990-es évek elején megszűnő kétpólusú világrend hozott el. A biztonság szűkebb, katonai értelmezése már a hidegháború időszakának második felében elkezdett fellazulni, azonban a jelentős változás csak a bipoláris világrend végét követő időszakban jelentkezett. Az európai biztonsági környezet a hidegháborút követően, a 21. századra átalakult azért, mert a hidegháború alatti és az azt követő időszakban a biztonság szűkebb értelemben vett – kizárólagos – katonai értelmezése kibővült a biztonság gazdasági, politikai, társadalmi, környezeti és informatikai dimenziójának értékelésével is. [2 pp. 3-24]

A biztonság átalakulása a 21. század kezdetén, a korábbi évtized poszthidegháborús trendjeibe illeszkedve folytatódott. Az 1980-as évek végén, új globális stratégiai helyzet alakult ki Európában azért, mert a közép- és kelet-európai államokban megszűnt a régi politikai elvek támogatása. Ennek eredményeképp a posztszocialista államok a nyugati világrend felé fordultak. A régi – fegyverekkel vívott – hagyományosnak nevezhető biztonsági kihívásokat felváltották a (1) katonai; (2) gazdasági; (3) politikai; (4) társadalmi és (5) környezeti biztonsági szektorokban jelentkező új biztonsági kihívások, melyek közül az alacsony intenzitású biztonsági kockázati tényezők, a tömegpusztító fegyverek proliferációja, a nukleáris, vegyi, biológiai technológiák kontroll nélküli fejlesztése, a számítógépek tömeges felhasználásából adódó kiberfenyegetések már kiváltak. A hidegháború időszakában megjelenő biztonsági fenyegetettség és a Kelet-Nyugat ellentétének látszólagos eltűnésével új biztonsági tényezők kerültek előtérbe.

A hangsúlyok átrendeződtek oly módon, hogy megjelentek a kibertérben jelentkező, digitalizáción alapuló technológiai és informatikai kockázatok. A Nyugat technológiai fejlettsége új világot és végtelen sok lehetőséget nyitott, azonban az előnyök mellett számtalan problémát, kiszámíthatatlanságot és megoldásra váró helyzetet is teremtett a biztonság terén, például a kritikus infrastruktúrák védelme, az adatok- és adatvagyon védelme, kifejezetten az agrár- és banki adatok vonatkozásában.

A digitalizáció a globalizáció hatására egyre inkább áthatja a mindennapjainkat, egyre több területen jelenik meg új irányokkal, megoldásokkal és ezáltal új választ ad a gazdasági és társadalmi gyors és gyökeres változásokra. Gazdasági hatásait tekintve fokozódik a termelékenység, nő a hatékonyság és javulnak a termékek, szolgáltatások minőségi szintjei. Ennek a folyamatnak a társadalmi hatásai közt szerepel, hogy a digitalizáció terjedésének nincsen fizikai határa, ezért megteremti az információkhoz, javakhoz való közvetlenebb hozzáférést, így erősíti az esélyegyenlőséget. A digitalizáció lehetőséget ad a virtuális jelenlétre, az azonnali kommunikációra és adatcserére, továbbá hatással bír a fizikai mobilitásra, így a környezettudatossághoz is hozzájárul. [3] A digitalizáció tehát számos előnnyel jár, azonban ezek az előnyök ugyanúgy hátrányokat is hordoznak magukban.

Mindezek következtében kijelenthető, hogy a digitalizáció globális biztonsági kihívás, mert a 21. században végbemenő informatikai forradalom hatására megváltozott a politika, közigazgatás, gazdaság, ipar, mezőgazdaság, oktatás- és tudomány, egészségügy, közlekedés, logisztika, energetika, diplomácia, valamint átformálódtak a nemzeti biztonsági- és katonai rendszerek. E folyamat globális korszakváltásként jelentkezik, ezért szükséges vizsgálni, hogy a nemzetállamok hogyan adaptálódnak a technológiai forradalom kihívásaihoz. [4 pp. 147-155]

Az aktuális biztonsági folyamatokat, kihívásokat, változásokat és trendeket egyformán szükséges elemezni és értékelni ahhoz, hogy mind hazai mind nemzetközi viszonylatban sikeres biztonságpolitikát folytathassunk. A jelenlegi, instabil biztonsági környezetben a biztonságra ható tényezők és kockázatok, veszélyforrások szintén változnak. Ez azt jelenti, hogy a digitalizáció következtében szembe kell néznünk a technikai, informatikai rendszerek és ezzel együtt a kibertérbeli kockázatok növekedésével. A világban kialakuló hatalmi központok alapja az információs, technológiai, digitális, informatikai rendszerek aktív, célratörő és széles körű használatán alapszik. Jelenleg az egyik legfőbb kérdés, hogy a nemzetállamok és stratégiáik milyen módon kezelik, és kezelik-e az informatikai forradalom hatására kialakuló rohamosan fejlődő információs és technológiai haladást. A

digitalizációhoz és a digitális transzformációhoz hazánknak is csatlakoznia kell, és célszerű az élvonalba állnia, hiszen országunk tudományos, technológiai, informatikai és matematikai téren elért eredményei szilárd alapot biztosíthatnak a nemzetközi színtéren.

A politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, energetikai és egyéb polgári rendszereken túl a digitalizáció nagymértékben hatással van a védelmi, katonai, és nemzeti biztonsági rendszerekre is. A katonai biztonsági rendszerekért a Honvédelmi Minisztérium (a továbbiakban: HM) és a Magyar Honvédség (a továbbiakban: MH) és szervezetei, háttérintézményei felelnek.

Az értekezés a digitalizációt – a 21. század új biztonsági kihívását és annak kapcsán kialakult felzárkózási nehézségeket, a digitalizáció által létrejött veszélyforrásokat, kiszámíthatatlan tényezőket – vizsgálja különös figyelmet fordítva Magyarország kibervédelmére és a kiberbiztonságra.

A problémafelvetés tükrében a doktori disszertáció az alábbi kérdésekre keresi a választ:

- Milyen módon igazolható, hogy a 21. századi kihívások hatékony kezelése komplex nemzetközi együttműködéssel, ugyanakkor a védelmi szektor adaptív képességfejlesztésével, a honvédség modernizációjával, strukturális és eljárásrendbeli átalakításával érhető el?
- Milyen módon állapítható meg, hogy a digitalizáció az egyik leghangsúlyosabb biztonsági kihívás?
- Milyen módon igazolható, hogy a honvédelmi, katonai és nemzeti biztonsági rendszerek hazai digitális hálózatba való beágyazódása a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program (a továbbiakban: Zrínyi 2026) keretein belül a légierő- és a szárazföldi erők modernizálásával érhető el?
- Milyen súllyal és intenzitással jelenik meg az MH digitalizációja érdekében ajánlott tíz digitális platform?

Célkitűzések

Az értekezés első fejezetének célja, hogy vizsgáljam a 21. századi európai biztonsági környezetet; a digitalizációt; az információtechnológia jellemzőit; a haderőreform egyes szakaszait, általános képet adjak a hadviselés négy generációjáról, elemezzem és értékeljem a 21. századi műveleti környezetet és feltárjam a hadügyi forradalom négy hullámát a haditechnikai-katonatechnikai képességek mentén.

Annak érdekében, hogy bizonyítsam a hagyományos és az új típusú biztonsági kihívások közti összefüggéseket. Párhuzamot vonjak a hagyományos hadviselés és a negyedik generációs vagy hibrid hadviselés jellemzői között. Igazoljam, hogy az új biztonsági kihívások kezelése a hadviselés átalakításával, modernizációjával, digitális platformra állításával érhető el.

A disszertáció második fejezetének célja, hogy feltárjam a kibertér és kiberbiztonság alapvetéseit; elemezzem és értékeljem a kibertér vonatkozó hazai és nemzetközi doktrínáit ismertessem a kiberbiztonság, a kiberműveletek és a kibertérbeli fenyegetések általános jellemzőit, elemezzem a kiberbiztonság és kibervédelem magyarországi helyzetének katonai, honvédelmi vetületeit.

Annak érdekében, hogy vizsgáljam a digitalizáció kibertérre gyakorolt hatásait, igazoljam az állami, katonai, nemzeti biztonsági rendszerek digitális felzárkózásának szükségességét és a stratégiai dokumentumok felülvizsgálatát. Következtetéseket vonjak le a kiberfenyegetésekből és igazoljam a honvédség digitális képességfejlesztését a kiberbiztonság garantálása és kibervédelem kiépítése érdekében.

A harmadik fejezet célja, hogy vizsgáljam az MH feladatait az új biztonsági kihívások tükrében; általános képet adjak a Zrínyi 2026 célrendszeréről, elemezzem az MH és a HM tevékenységét a légierő és a szárazföldi haderőnem képességének modernizálása érdekében. A két haderőnem kapcsán fókuszáljak a már beszerzett és a még beszerzés alatt álló eszközökre, az eszközök és a katonák digitalizációjára, az elavult eszközök modernizálására, a nemzetközi együttműködések bemutatására, az infrastruktúrák korszerűsítésére és a digitális képességek kiépítésére.

Annak érdekében, hogy vizsgáljam az MH digitalizációját, vagyis az analóg rendszerek digitalizálását, az új digitális eszközök beszerzését, és a digitális képességek fejlesztését.

A negyedik fejezet célja tíz ajánlás megfogalmazása az MH digitalizációjának eléréséhez az alábbi platformok mentén (a továbbiakban: tíz platform):

(1) a nemzetközi hadiiparban való magyar részvétel;
(2) az 5G technológia;
(3) az okos fegyverek fejlesztése;
(4) a Digitális Katona Program;
(5) a Mesterséges Intelligencia (a továbbiakban: MI)
(6) a digitális képességek fejlesztése;
(7) a katonai kiképzési és oktatási rendszer;

(8) a nyilvántartási rendszerek digitalizációja;

(9) a magyar űrprogram;

(10) a katonai hírközlő és kommunikációs rendszer digitalizációja.

A téma kutatásának hipotézisei

Az értekezés hipotézise, hogy a digitalizációt irányító kormányzati szerveknek jobban, vagy tevékenyebben kellene befogadniuk a katonai tényezőket és a katonai kiberbiztonság szakterületeit és fordítva, a katonai kiberrendszereknek is jobban kellene kapcsolódniuk a kormányzati hálózatokhoz. Jóllehet a katonai rendszereknek külön, a többi kormányzati biztonsági rendszertől leválasztva is működniük kell, azonban békeidőben összekapcsolódhatnak a rendszerek kölcsönös fejlődése érdekében. A kormányzati rendszer platformja jóval nagyobb, mint a katonai, azonban utóbbi specifikusságában eltér az általánosabb kormányzatiétól. Ezért fontos, hogy ha a két rendszer már békeidőben jó gyakorlatot szerez egymásról, akkor különleges jogrendben valószínűleg hatékonyabban működhetnek együtt. A rész és egész elve alapján célszerű lenne, ha a katonai rendszerek a kormányzati biztonsági rendszer részeként, ugyanakkor különleges jogrend esetén pedig külön, leválasztva is működnének a Kormány infokommunikációs támogatása érdekében azért, mert

(1) Feltételezem, hogy a 21. századi biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel, vagyis multilateralizmussal, ugyanakkor a védelmi szektor adaptív képességfejlesztésével érhető el;

(2) Feltételezem, hogy a digitalizáció a biztonságpolitikai trendek közül, mint technológiai faktor, az egyik leghangsúlyosabb biztonsági kihívás.

(3) Feltételezem, hogy a Zrínyi 2026 mind a légierő mind a szárazföldi erők modernizálásával hozzájárul ahhoz, hogy a honvédelmi, katonai és nemzeti biztonsági rendszerek beágyazódjanak a hazai digitális hálózatba.

(4) Feltételezem, hogy az MH széles körű digitalizációja akkor érhető el, ha a Zrínyi 2026 keretein belül megvalósuló/megvalósult fejlesztéseken és beszerzéseken túl a tíz platform azonos súllyal és intenzitással jelenik meg.

Kutatási módszerek

Kutatásom során a kvalitatív kutatási módszert választottam, azon belül is a szakirodalom-feldolgozás módszertanát, melyet saját szakmai tapasztalatommal ötvözve jelenítettem meg az értekezésben. A tudományos munka céljának elérése érdekében az

optimálisság és szükségesség elvének betartásával dolgoztam fel a releváns nemzetközi és hazai szakirodalmakat. A forrásfeldolgozás kapcsán előnybe részesítettem a katonai folyóiratokat, a hadtudományi, hadügyi és biztonságpolitikai kiadványokat, tanulmányokat, a vonatkozó doktrínákat, ágazati stratégiákat, törvényeket, kormányhatározatokat, kormányrendeleteket. A téma elméleti kidolgozásához különös figyelmet fordítottam a hazai Nemzeti Biztonsági Stratégiában (a továbbiakban: NBS) a Nemzeti Katonai Stratégiában (a továbbiakban: NKS), a Nemzeti Kiberbiztonsági Stratégiában (a továbbiakban: NKBS), a Mesterséges Intelligencia Stratégiában (a továbbiakban: MIS) és a Nemzeti Digitális Stratégiában (a továbbiakban: NDS) foglaltakra. A nemzetközi forrásfeldolgozás kapcsán elsősorban az Európai Unió (a továbbiakban: EU) és az Észak-atlanti Szerződés Szervezete (a továbbiakban: NATO) jogi doktrínáit és nemzetközi kereteket biztosító szabályzók normáit, stratégiai dokumentumait részesítettem előnyben.

A téma aktualitása érdekében folyamatosan monitoroztam az MH, a HM és a Kormány *social media* platformjait. A források feldolgozása során módszertani alapelvem volt, hogy az elméleti vonatkozásokat a gyakorlati elemekre és tényekre építsem.

Az értekezés megalapozottságát alátámasztja a több, mint 5 éves közigazgatási tapasztalatom, amely során a Miniszterelnökségen és a Miniszterelnöki Kabinetirodán többek között HM kapcsolattartóként, majd a HM vezető kormánytisztviselőjeként végeztem munkámat, valamint számos biztonságpolitikai, hadtudományi kurzuson, képzésen és továbbképzésen, szemináriumon és konferencián szereztem szakmai és módszertani ismereteket. A disszertációm szakmaiságát a fentiek kapcsán végzett tevékenység, módszerek és személyes tevékenység tapasztalatai képezik. Az értekezés hitelességét az irodalomjegyzékben megjelenített 202 különböző tanulmányra, könyvre, releváns internetes forrásra való hivatkozás adja.

A kutató munkám során 2020-ban mozdultam el a digitalizáció irányába, ennek eredményeképp született meg a „*Magyar Honvédség digitalizációja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program tükrében”* c. tanulmányom, amellyel a Digitális biztonságpolitika tudományos kutatási pályázaton 3. helyezést értem el. A 2022. május 31. napi műhelyvitámra benyújtott és megvitatott „*A digitalizáció, mint a 21. század új biztonsági kihívása, annak katonapolitikai vetületei különös tekintettel a kiberbiztonságra”* c. értekezés-tervezetem kapcsán az Adatgazdaság digitalizációs összefüggései pályázaton szintén 3. helyezést értem el.

A kutatásomat 2022 márciusában lezártam, azonban a 2022. évi választások és a májusi Kormány átalakítás kapcsán érintett és a disszertációmban megjelenített minisztériumok és releváns szervezetek megnevezése frissítésre, feltüntetésre került.

1 TECHNOLÓGIAI ÉS INFORMÁCIÓS HADVISELÉS A 21. SZÁZADI BIZTONSÁGI ÉS MŰVELETI KÖRNYEZETBEN

A hidegháborút követően a korábbi, kizárólagos katonai biztonság átalakult. A biztonságot meghatározó tényezők átalakulása és kibővülése a technológiai fejlődés és a globalizáció hatására történik azért, mert a hidegháború előtti és a hidegháború korában a kizárólagos katonai dimenzióban megmutatkozott régi típusú biztonsági kihívásokat felváltották a hidegháború végével jelentkező új típusú biztonsági kihívások, amelyek a korábbi, kizárólagos katonai értelmezésen túl kibővültek a biztonság gazdasági, pénzügyi, vallási, környezeti, közbiztonsági, nemzeti, demográfiai, etnikai továbbá kultúrát és migrációt érintő dimenzióival. Az új dimenziók által újszerű, instabil helyzet alakult ki, ezért a biztonságra ható és a biztonságot formáló kockázatok, tényezők, fenyegetések és veszélyforrások új hangsúlyokat kaptak.

Az információs infrastruktúrák megjelenése és ezen infrastruktúrák regionálisból globális szintűvé válása változásokat hozott a háborús terekben. A klasszikus műveleti terek: szárazföld, levegő, tenger, űr kiegészültek egy új, információs hadszíntérrel. Ennek eredményeképp a klasszikus műveleti terek átformálódnak és információs technológia alapú digitális háborús terekké válnak. A hagyományos háborús terekben folyó küzdelem mellett és azokkal párhuzamosan zajlanak az információs műveletek az információs hadszíntéren, ez tehát az információs hadviselés.

A hagyományos háború háttérbe szorulása, a hidegháborús totális nukleáris hadviselés valószínűségét is nagyban csökkentette. A nukleáris háború nem lehet a 21. század politikai céljának eszköze, azonban az információs és technológiai fejlődés következtében kialakult új hadviselés globális és nemzetközi kezelést igényel különös tekintettel a fegyverrendszerek terjedésére, a szupertechnikai rendszerek felhasználására és az alkalmazási technológiák fejlesztésére.

A globalizációs folyamat, vagyis az információ, a tőke, a munkaerő, az áru, a szolgáltatások és a politikai elvek, ideológiák szabad és gyors áramlásával párhuzamosan lódult meg a technológiai fejlődés, tehát az elektronika, az informatika, a biogenetika, az űrkutatás, az MI és sok más műszaki tudományos terület robbanásszerű fejlődése. [5]

A problémafelvetés tükrében az első fejezetben az alábbi a kérdéseket vizsgálom:

- Milyen módon igazolható, hogy a hagyományos és az új típusú biztonsági kihívások összefüggenek egymással?
- Hogyan és milyen módon garantálható a hagyományos és az új típusú biztonsági kihívások leghatékonyabb kezelése?
- Az új biztonsági kihívások kezelése érdekében növeli-e a honvédség hatékonyságát a hadviselés átalakítása, a digitális képességfejlesztés és a modernizáció, digitális platformra állítás?
- Hogyan igazolható az, hogy a háborúk elsődleges célpontját az információs rendszerek és az információs infrastruktúrák adják?

Az első fejezet hipotézise, hogy ha a hagyományos és az új biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel, vagyis multilateralizmussal - ugyanakkor a védelmi szektor adaptív képességfejlesztésével érhető el, akkor a védelmi szektornak, ideértve a honvédségnek az országvédelmi, katonai feladatok ellátása mellett szükséges az új biztonsági kihívásokhoz alkalmazkodni. Ahhoz, hogy a hagyományos katonai feladatok ellátása mellett az információs hadviselés korában jelentkező új biztonsági kihívásokat a honvédség felismerje és megfelelően kezelje, szükséges a hadviselés átalakítása, modernizációja.

Az első fejezetben rámutatva a súlypontokra, vizsgálom a 21. századi európai biztonsági környezet kialakulását és jellemzőit; a digitalizációt, mint globális biztonsági kihívást; az információtechnológia jellemzőit a biztonságpolitikában és a hadügyben; a haderőreform egyes szakaszait a haderő átalakítása és a haditechnikai reformok kora mentén. Általános képet adok a hadviselés négy generációjáról, különös tekintettel a negyedik generációs vagy hibrid hadviselésre; vizsgálom a 21. századi műveleti környezet és az információs hadviselés jellemzőit az információs infrastruktúrák fókuszában, és bemutatom a hadügyi forradalom négy hullámát a haditechnikai-katonatechnikai képességek mentén.

1.1 A 21. századi európai biztonsági környezet kialakulása és jellemzői

A Hadtudományi Lexikon szerint Resperger István nyomán a biztonságpolitikai kihívások, kockázatok és fenyegetések *„azok... a veszélyt és fenyegetést magukban hordozó helyzetek és állapotok, amelyek általában negatívan befolyásolják az adott*

országban az átfogó biztonságot, annak egyes összetevőit, s gyengítik a belső és külső stabilitást." [6 p. 116]

Resperger István tehát elkülöníti egymástól a biztonsági kihívásokat, kockázatokat és fenyegetéseket, amelyeket a lehetséges veszélyek megnyilvánulási formáinak tekint. Fentiek hátrányosan befolyásolják a belső és külső stabilitást, így hatást gyakorolhatnak egy régió hatalmi viszonyaira. A három fogalom egymásra épül és feltételezik a növekvő feszültségi szint meglétét. Jellegüket tekintve kizárólag dinamikus folyamatokként értelmezhetjük őket, a gyakorlatban átfedésben, összemosódva jelennek meg. [7 pp. 5-17]

A hidegháborút követően a hagyományos biztonsági kihívásokat felváltották az új biztonsági kihívások. A hagyományos és az új típusú biztonsági kihívások összefüggenek egymással. A hidegháború utáni európai biztonsági környezetet ért változások hatására kialakult új típusú biztonsági kihívások meghatározzák hazánk jelenlegi biztonsági környezetét azért, mert ezek a változások, a Kelet-Nyugat nyitottságának köszönhetően a globalizáció által felgyorsult technológiai és digitalizációs forradalom következtében újabb lendületet kaptak.

A hidegháború 1947 és 1991 között zajlott, amelyet a két szuperhatalom, az Amerikai Egyesült Államok (a továbbiakban: USA) és a Szovjetunió közötti versengés jellemzett. A hidegháború a II. világháború két nyertes nagyhatalmának ideológiai; kulturális; társadalmi; gazdasági és politikai összecsapásában mutatkozott meg. Az európai biztonsági környezet meghatározása szempontjából fontos megemlíteni, hogy a propaganda mellett a hidegháború időszaka alatt a nukleáris fenyegetés; a fegyverkezési verseny és az űrverseny is előtérbe került. [8]

Fentiekből következik tehát, hogy már a hidegháború időszakában is jelentkezett a biztonság egyoldalú katonai értelmezésének átalakulása, amelyet azonban a hidegháború vége, vagyis az 1990-es évek elején megszűnő kétpólusú világrend hozott el. Az USA és a Szovjetunió bipoláris hatalmi versengésének megszűnésével világossá vált, hogy a nagyobb katonai erő önmagában nem garantál nagyobb biztonságot azért, mert a szovjet birodalom összeomlásához végül a fegyverkezési verseny miatt kialakult gazdasági és ennek következtében politikai válság vezetett. A biztonság szűkebb, katonai értelmezése tehát már a hidegháború időszakának második felében elkezdett fellazulni, azonban a jelentős változás csak a bipoláris világrend végét követő időszakban jelentkezett.

A mai felfogás szerint a biztonság értékelésének komplex rendszerében a biztonság fogalmi keretének átalakulásáról, értelmezési tartományának jelentős kibővüléséről beszélhetünk. [9]

A biztonság fogalmának átalakulását, kibővítését Barry Buzan és szerzőtársai, 1983-ban alkották meg a szektorális elmélettel, ezzel kibővítve az addigi hagyományos, katonai biztonság fogalmát. A szektorelmélet szerint a biztonság legalább az alábbi 5 szektorra osztható: (1) katonai; (2) gazdasági; (3) politikai; (4) társadalmi és (5) környezeti biztonságra. A szektorok gyakorlatban nem, csak elméletben választhatóak szét egymástól. [10 pp. 431-451]

A szektorelmélet szerint a fenti 5 szektor kapcsán az egzisztenciális fenyegetettség hiánya esetén garantált a biztonság. A 21. századi új típusú biztonsági kihívások viszont megjelennek a szektorokban, amely azt eredményezi, hogy a biztonság egyre inkább instabillá válik. [11 pp. 214-234]

Egyetértek azzal, hogy Gazdag Ferenc szerint az európai biztonsági környezet a hidegháborút követően, a 21. századra átalakult azért, mert a hidegháború alatti és az azt követő időszakban a biztonság szűkebb értelemben vett – kizárólagos – katonai értelmezése kibővült a biztonság gazdasági, politikai, társadalmi, környezeti és informatikai dimenziójának értékelésével is. [12 pp. 9-18]

A hidegháború időszakát követő európai biztonsági környezet jellemzői az alábbiak mentén alakultak ki. A biztonság átalakulása a 21. század kezdetén, a korábbi évtized poszthidegháborús trendjeibe illeszkedve folytatódott. Az 1980-as évek végén, új globális stratégiai helyzet alakult ki Európában azért, mert a közép- és kelet-európai államokban megszűnt a régi politika támogatása. Ennek eredményeképp a posztszocialista államok elfordultak a nyugati világrend felé. A régi, hagyományosnak nevezhető fegyveres konfliktusok kibővültek az új biztonsági fenyegetésekkel, kockázatokkal és kihívásokkal. Az egyenlőtlen társadalmi és gazdasági fejlődésből származó érdekellentétek vagy a nem állami szereplők, terrorcsoportok által szervezett támadások, mind-mind új, megelőző és védelmi természetű célrendszerek meghatározására késztetik az államokat, túlélésük jegyében. A napjainkra kialakult újszerű, biztonság szempontjából instabil helyzetben a biztonságra ható tényezők, veszélyforrások és kockázatok is átrendeződtek, újak jöttek létre. Ezért előtérbe kerültek a biztonság egyéb alkotóelemei: (1) gazdasági; (2) pénzügyi; (3) vallási; (4) környezeti; (5) közbiztonsági; (6) nemzeti; (7) demográfiai; (8) etnikai; (9) kulturális; (10) migrációs kérdések. [13]

Az európai biztonság átalakulási dinamizmusa stabilizálódni látszik, azonban kiszámíthatatlanabbá, bonyolultabbá és bizonytalanabbá vált a poszthidegháborút követő időkben. A hidegháború időszakában megjelenő biztonsági fenyegetettség és a Kelet-Nyugat ellentétének látszólagos eltűnésével új biztonsági tényezők kerültek előtérbe. A hidegháború korából ismert kölcsönös függőségek, a földrajzi közelség és az ideológiai és kulturális hasonlóság okán ismert politikai és gazdasági jellemzők azonossága, a határok nyitottsága, a piacok liberalizálódása mind teret engedett a korábban is ismert problémák felszínre törésének. Mindez azt eredményezte, hogy a nacionalizmusnak; a szeparatizmusnak; a gazdasági; kulturális aránytalanságoknak; az etnikai és vallási ellentéteknek; a tömegpusztító fegyverek proliferációjának; a terrorizmusnak; a nemzetközi szervezett bűnözésnek; a kábítószer, fegyver,- és emberkereskedelemnek; a migrációnak; a környezetszennyezésnek; az ipari,- és természeti katasztrófáknak; az ember által okozott mesterséges katasztrófáknak és a világjárványok terjedésének az országhatárok már nem szabnak gátat. A globális és az európai biztonsági kihívások is egyaránt mutálódnak, természetükre pedig az a jellemző, hogy térben kisebb kiterjedésűek, viszont sokrétűbbek és szerteágazóbbak, dinamikusabbak is, hatásuk könnyen globálissá válhat, és időben behatárolhatatlanok. [14 pp. 78-79]

A biztonságot meghatározó tényezők vizsgálatának szempontjából hangsúlyos a biztonságot alakító tényezőkre hatással bíró globalizáció és modernizáció. Ez azt jelenti, hogy párhuzamosan fokozódik a gazdasági és technológiai szabad verseny és a kulturális, vallási központok közti verseny. A nemzetközi rendet átalakítja a gazdasági struktúraváltás, a pénzügyek, a tudomány és az információ univerzalitása. A globális stratégiai javakat – amelyek többsége véges – behatároló nemzeti, gazdasági, politikai és katonai stratégiák közti ellentét a 21. század egyik biztonsági veszélytényezője. A globalizáció következtében a biztonsági kihívások univerzálódnak, ezáltal összemosódnak a bel- és a külbiztonságpolitika közötti különbségek. A biztonsági kockázatok, majd kihívások egyetemesen jelentkeznek, azonban azok eloszlása sem globális sem európai viszonylatban nem egyenletes. Európán belül a határok átjárhatósága miatt a transznacionális biztonsági kihívások térben és időben is gyorsabban terjednek. Az olyan aszimmetrikus biztonsági kockázati tényezők, mint a tömegpusztító fegyverek proliferációja vagy a terrorizmus nagyobb eséllyel jelennek meg a fejlettebb országokban. A világ stratégiai erőegyensúlyának átstrukturálódása a tömegpusztító fegyverek és a technológiák ellenőrizetlensége és proliferációja következtében történik.

A fejlett világgal szembenálló országok, állami és nem állami szereplők aszimmetrikus eszközökhöz nyúlnak, amelyek relatíve olcsóak, azonban egyetemes hatást is elérhetnek.

Technológiai szempontból a legnagyobb fenyegetést a nukleáris, vegyi, biológiai technológia, a génmanipuláció, a tömegpusztító eszközök hordozóeszközei és az informatikai eszközök tömeges használata, valamint a különböző technológiák ellenőrizetlenül hagyása jelentik. [14 pp.79-85]

Egyetértek azzal, hogy Babos Tibor szerint napjaink legmeghatározóbb biztonság kihívásai: (1) a globalizáció; (2) a digitalizáció; (3) a globális felmelegedés (4) és a nyersanyagforrások kimerülése. [15 pp. 16-29]

A disszertációban a fenti 4 kihívás közül a digitalizációt, mint a 21. század új biztonsági kihívását elemzem és értékelem különös figyelmet fordítva a kiberbiztonságra és a kibervédelemre.

Összegzésképp megállapítom, hogy az új típusú biztonsági kihívások, amelyek a poszthidegháború korában jelentkeztek, a korábban hangsúlyos egyirányú, katonai dimenzió kibővülésével jöttek létre. Ez azt jelenti, hogy a biztonságot meghatározó tényezők a katonai dimenzió mellett kibővültek, átalakultak és újak jöttek létre. A hagyományos és új biztonsági kihívások gyakran összekapcsolódnak, ezáltal a fenyegetések egyértelműen összefüggenek egymással, hatnak egymásra, folyamatosan befolyásolva a stabilitás adott szintjét.

1.2 Digitalizáció, mint globális biztonsági kihívás

A technológia rohamos fejlődésének következtében új lehetőségek és kihívások jelennek meg, amelyek meghatározzák hazánk biztonságát, ezek közé tartozik a digitalizáció.

A digitalizáció az a folyamat, amikor egy fizikai mennyiséget számítógép segítségével feldolgozhatóvá alakítanak. A digitalizálás szó a digitális szóból ered, átalakítás digitális formátumúra jelentéssel. A fizikai, analóg dolgok számítógépek által feldolgozhatóvá tétele a digitalizálás. [16 pp. 8-14]

A digitalizáció a globalizáció hatására egyre inkább áthatja a mindennapjainkat, egyre több területen jelenik meg új irányokkal, megoldásokkal és ezáltal választ ad a gazdasági és társadalmi gyors és gyökeres változásokra. Gazdasági hatásait tekintve fokozódik a termelékenység, nő a hatékonyság és javulnak a termékek, szolgáltatások minőségi szintjei. Ez azt jelenti, hogy nagyobb mennyiséget, relatíve kedvezőbb áron és jobb minőségben tudunk előállítani. A társadalmi hatásai közt szerepel, hogy a digitalizáció

terjedésének nincsen fizikai határa, ezért megteremti az információkhoz, javakhoz való közvetlenebb hozzáférést, így erősíti az esélyegyenlőséget. Tekintettel arra, hogy a digitalizáció által lehetőség nyílik a virtuális jelenlétre, az azonnali kommunikációra és adatcserére, hatással bír a fizikai mobilitásra, így a környezettudatossághoz is hozzájárul.[3]

A digitalizáció és az okos városok következtében szinte minden könnyebben és gyorsabban elérhetőbbé válik a társadalom tagjai részére. Az információs társadalom nyújtotta digitális lehetőségekhez elengedhetetlen a társadalom információbiztonság tudatossága. A lakosság információbiztonság tudatosságának kiépítésén túl fontos a kibertérbeli kockázatok megfelelő kezelése.

A kibertérben elkövetett támadások sok esetben visszafordíthatatlan politikai vagy gazdasági károkat eredményeznek. A nemzetállamoknak, így Magyarországnak is rendelkeznie kell azzal a képességgel, hogy a kibertérbeli fenyegetéseket felismerje és kezelje, a kiberbiztonságot kiépítse, a kritikus információs infrastruktúra zavartalan működését biztosítsa, a támadásokat elhárítsa és a kibervédelmi feladatokat megfelelően elvégezze. A digitalizáció térhódítása azonban nemcsak a virtuális térben zajlik, hanem nagyban befolyásolja az alábbi globális közös tereket is, amelyek haderőnemi szempontból műveleti terek is egyben: (1) szárazföld; (2) tenger; (3) levegő; (4) világűr. [17 pp. 89-112]

Nemzetközi viszonylatban az Európai Bizottság (a továbbiakban: EB) által 2020 februárjában elfogadott stratégia az alábbiak szerint ad keretet a digitalizációnak és a digitális transzformációnak.

A következő öt érték mentén került meghatározásra a digitális transzformáció biztonságos fejlesztéséhez kapcsolódó stratégia: (1) nyitottság; (2) igazságosság; (3) változatosság; (4) demokrácia; (5) bizalom. [18]

A stratégia célja az emberközpontú technológiák fejlesztése, különös tekintettel a kutatás, fejlesztés (a továbbiakban: K+F) befektetésekre; a szakmai tapasztalat megosztására; a nemzetközi együttműködésekre a szuperszámítógépek és a micro-elektronika területén; és az 5G hálózatok fejlesztéseire.

A cél elérése érdekében a következő kulcsintézkedések megtétele szükséges valamennyi tagállamnak:

- a megbízható MI jogi keretrendszer lehetőségeit meghatározó Fehér Könyv megalkotása;

- az MI, a kiber-, szuper- és kvantumszámítás, kvantumkommunikáció és a blokklánc területén csúcstechnológiájú közös digitális kapacitások kiépítése, valamint telepítése;
- beruházások felgyorsítása az európai gigabites összeköttetésben;
- Közös Kiberbiztonsági Egység létrehozása;
- a digitális- és médiaműveltség, továbbá a kompetenciák növelése érdekében Digitális Oktatási Cselekvési terv létrehozása;
- Készségfejlesztési Menetrend és Ifjúsági Garancia akciótervek létrehozása a digitális készségek elsajátításához és megerősítéséhez;
- munkakörülmények javítása;
- a közigazgatásbeli biztonságos adatáramlás és szolgáltatás összehangolása és biztosítása. [19]

A digitalizáció kapcsán valamennyi országnak és ágazatnak szükséges lépéseket hoznia, ezt a folyamatot erősíti a koronavírus járvány hatásai okán kialakult válsághelyzet, amely kezelésében fő tényező a digitalizáció. A digitalizációs fejlesztések növelik a felhasználók jólétét, hozzájárulnak a nemzetgazdaság, a vállalkozások, a közigazgatás és a polgárok versenyképessége mellett a társadalmi esélyteremtéshez és a digitális jóléthez is. Hazánk digitális képességfejlesztésének központjában a digitális gazdaság, oktatás és a digitális közszolgáltatások állnak.

Az EU stratégiájával összhangban és annak megfelelve készült el az NDS 2020-ban, amely az alábbi pillérek mentén határozza meg hazánk digitális képességfejlesztéseit:
(1) digitális infrastruktúra; (2) digitális kompetencia; (3) digitális gazdaság; (4) digitális állam. Az NDS célja, hogy a gazdaság, az oktatás, a kutatás, fejlesztés, innováció (a továbbiakban: K+F+I) és a közigazgatás területén történő digitalizáció hozzájáruljon az ország versenyképességének javulásához és a polgárok jólétének biztosításához. [3]

A digitalizációt irányító kormányzati szervek közti együttműködést erősíti a 2021 nyarán megalakult Interdiszciplináris Technológiai Alkalmazások Bizottság (a továbbiakban: ITAB), amelynek célja, hogy összkormányzati – szakágazati és államigazgatási – és tudományos szinten kutassa a jövőben jelentkező digitális kihívásokat, a fejlődési irányokat és mérföldköveket továbbá, hogy vizsgálja ezeknek a hazai iparba, gazdaságba történő felhasználási és fejlesztési lehetőségeit. [20]

A politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, energetikai és egyéb polgári rendszereken túl a digitalizáció

nagymértékben hatással van a védelmi, katonai, és nemzeti biztonsági rendszerekre is. A katonai biztonsági rendszerekért a HM és az MH és szervezetei, háttérintézményei felelnek.

Az aktuális biztonsági folyamatokat, kihívásokat, változásokat és trendeket egyformán szükséges vizsgálni ahhoz, hogy mind hazai mind nemzetközi viszonylatban sikeres biztonságpolitikát folytathassunk. A jelenlegi, instabil biztonsági környezetben a biztonságra ható tényezők és kockázatok, veszélyforrások szintén változnak. Ez azt jelenti, hogy a gazdasági, pénzügyi, társadalmi, kulturális, vallási, környezeti, közbiztonsági, migrációs gondokon túl a digitalizáció következtében szembe kell néznünk a technikai, informatikai rendszerek és ezzel együtt a kibertérbeli kockázatok növekedésével.

1.3 Információtechnológia a biztonságpolitikában és a hadügyben

Ahhoz, hogy a 21. század információs hadviselési formáját elemezzem és értékeljem, szükséges az információtechnológia biztonságpolitikában és hadügyben elfoglalt helyét bemutatni.

A napjainkban végbemenő információs technikai és technológiai forradalom kapcsán okkal merül fel a kérdés, hogy vajon sérülékenyek-e annyira a rendszereink, hogy magukban hordozzák a támadhatóság esélyét? A válasz abból tevődik össze, hogy ezek a számítógépes digitális technikai alapú rendszerek nagyobb kockázatot és ennélfogva nagyobb sérülékenységet indukálnak. Ez a gyengepont azonban ellensúlyozható a rendszerek felkészítésével, technikai védőmechanizmusok kidolgozásával és megfelelő alkalmazásával. Biztonságpolitikai szempontból az információs rendszerek sérülékenységei azonban biztonsági kockázatot jelentenek. Ennek következtében az információbiztonság, mint a 21. század új biztonsági szektora, nem alaptalanul egészíti ki a katonai, politikai, gazdasági, társadalmi és környezeti szektorokat. A kiberműveleteket és a kiberhadviselést, mint a katonai és információbiztonsági szektorok kölcsönhatását tekinthetjük az egyik leghangsúlyosabb technológiai biztonsági kihívásnak. [21 pp. 37-42]

Fentiek okán elengedhetetlen a honvédség és a hadviselés átalakulásának vizsgálata, mert az információs kihívások a katonai információs rendszerek kapcsán is jelentkező veszélyforrások. A kérdés az, hogy hordoz-e magában akkora előnyt ezen rendszerek használata, hogy vállaljuk a rendszerek sérülékenységével járó kockázatot? A válasz egyértelműen igen, ugyanis kockázatok nélkül nincs győzelem. A modern technikai kor

eszközeinek és rendszereinek üzembe helyezése és alkalmazása a leginnovatívabb technikai és technológiai K+F által valósulhat meg, azonban rendkívül magas költséggel jár, amelyet – sajnos – nem minden szervezet, csoport vagy ország engedhet meg magának. Ezért ezek a rétegek egyéb eszközökhöz nyúlnak a céljaik elérése érdekében. Fenti folyamatot, vagyis amikor egy gazdaságilag fejlett, modern technikai és technológiai eszközökkel rendelkező országgal egy gazdaságilag fejletlenebb és eszközeit tekintve elavultabb technológiát alkalmazó ország áll szemben, aszimmetrikus hadviselésnek nevezzük, amelynek legismertebb színtere a terrorizmus. A fejletlenebb csoportok, szervezetek, országok a pusztításhoz és a figyelemfelkeltéshez a hagyományos eszközök mellett az információs technika és technológia eszközeit is használhatják. Az információs társadalmak, az információs infrastruktúrák és szolgáltatások függőivé váltak, ezért ezen infrastruktúrák támadása komoly veszélytényezőt jelent. Az aszimmetrikus támadások ellen megelőzéssel és a kritikus infrastruktúrák rendszerelemeinek védelmével, információszerzéssel, feldolgozással, nemzetközi információcserével és értékeléssel léphetünk fel. [22]

Mindent összevetve megállapítom, hogy az információ és az információszerzésért, - feldolgozásért, - elemzésért, - és értékelésért, valamint annak felhasználásáért felelős információs rendszerek a hadviselésben is egyre meghatározóbb elemmé váltak. A háborúk elsődleges célpontjait napjainkban az információs rendszerek és az információs infrastruktúrák adják. Éppen ezért fontos a honvédség átalakítása, képesség alapú fejlesztése, digitális platformra állítása.

1.4 A haderő átalakulása, haditechnikai reformok kora

A disszertáció következő részében elemzem és értékelem a haderő átalakulását a haditechnikai reformok korára jellemző súlypontok bemutatása mentén.

A haditechnikai reformok korának első időszaka a tömeges hadviselés kora, amely a francia forradalomtól a 20. század közepéig tartó időszak volt. Ebben az időszakban a katonai erő sorozott tömeghadseregből állt össze, vagyis azok voltak a legsikeresebbek a harctéren, akik nagyobb létszámú hadsereggel rendelkeztek. A tömeghadseregek kora azonban lejárt. Az iraki – a világ negyedik legnagyobb hadseregének csaknem teljes megsemmisítése 1991-ben is az előszele volt annak, hogy az elavult haditechnika a fejlett fegyverekkel felülmúlható. [23 pp. 59-66]

A 19-20. században az országok hadseregei azonos fegyverekkel rendelkeztek. Az első világháború korában már nagyobb különbségeket lehet felfedezni e téren: amíg a

szövetségesek tömeges harckocsi gyártásba kezdtek, addig a németek nem fejlesztették ezt a szárazföldi képességet. A második világháború során a kontraszt még jobban nőtt. Az USA és Nagy-Britannia ekkor fejlesztette ki a nehézbombázókat, ellenben ezt a példát sem az akkori Szovjetunió, sem az ellenségeik nem követték. Ennek ellenére a második világháborúban és a hidegháború idején a fegyverrendszerek alapvetően hasonlóak voltak. A nagy változás a 20. század végén kezdődött, ekkorra ugyanis rohamosan fejlődtek a fegyverek, amely a tényleges pusztító eszközök fejlődését, az egyedi fegyverkezési megoldások megjelenését és a haditechnika rendszereinek létrehozását jelentette. A haderő átalakulása során a világ legtöbb országában elhagyták a kötelező, sorkatonai szolgálatot ezáltal csökkentették a fegyveres erők méretét, és előtérbe kerültek a haditechnikai fejlesztések. A fejlettebb haditechnikával és a célszerűen kiképzett katonákkal együttesen az erőviszonyok megváltozásával akár 1:3 arányban is győzelmet lehet aratni egy nagyobb, ámde elavultabb technikákat alkalmazó haderő ellen. A minőség, amely a kiképzett katona és a technika együttese tehát legyőzi a mennyiséget.[24]

A „haderőreform”, vagyis a fegyveres erők változása állandó történelmi folyamat. A modern korban ez a folyamat költségvetési, fejlesztési és politikai kérdésként van jelen. A haderő átszerveződése a háborúkép változásaitól függ. A hadviselési mód az adott, a kifejlődött, vagy a fejlődés alatt álló haditechnika, a politikai érdekek és a gazdaság függvénye. Mindezen túl a geopolitikai helyzet és katonaföldrajzi pozíció is meghatározza a haderők paramétereit. A jelenlegi változékony biztonsági környezetben az új biztonsági kockázatok és kihívások kezelése az eddigiektől eltérő, más hadviselési elveken alapszik, ahol a mozgékonyság, a rugalmasság, a képességfejlesztés és a tudás funkcionális használata, vagyis a minőség kerül a mennyiség elé. Ezzel párhuzamosan jelentkezik a haditechnikai forradalom, az elektronikai és informatikai alapú hadviselés, vagyis az ember-gép arányának megváltozása. Jelen részfejezet tehát a fenti folyamat állomásait veszi sorra a hadsereg átalakításához vezető jelentősebb, közelmúlt eseményeit formáló mérföldkövek bemutatásával. [25 pp. 295-316]

A védelmi és katonai együttműködést nemzetközi keretek között szükséges megvalósítani, ami azt jelenti, hogy fontos a nemzetközi interoperabilitás. A NATO szövetségesi és EU-tagságunk tekintetében az MH-nak azon elemei és képességei korszerűek, modernek és hasznosak, amelyek országhatáron kívül is telepíthetőek, ezáltal nemzetközi környezetben is alkalmazhatóak. Ezért a haderőfejlesztés központját a fenti képességek elérése adja. Ennek következtében elképzelhető, hogy egyes időközben

szükségtelenné vált képességek teljesen eltűnnek és azokat újak, korszerűek váltják fel. Olyan hadsereg képzése a cél, amely nem a rendszerváltás előtti sorozásos, minden képességgel rendelkező „tömeghadsereg” elvén alapszik, hanem új és innovatív, technológiai és képességfejlesztés alapú.

A haditechnika állandóan változik, fejlődik. A hadügyi forradalom a változások együttes jelenlétén alapszik. A haditechnika evolúció-szerűen változik, kisebb-nagyobb ütemekben, hektikusan alakul át, vagyis egyenlőtlenül fejlődik. A fejlődés során egyes technikai újdonságok összefonódása nagyobb átalakulást indukál, míg más területek másodlagossá váltak (lásd: tömeges nukleáris képességek napjainkban).

A hadviselésben bekövetkező változások először az 1991-es Öbölháborúban jelentek meg, ahol megmutatkozott a nagy pontosságú fegyverek hatékonysága, megjelent egy sor támogató haditechnika és ez magával hozta a hadviselés alapjaiban történő változását. Az öbölháború sajátosságainak elemzése során megállapíthatjuk, hogy (1) a minőség a mennyiséggel szemben, (2) a katonai eszközök specializációja, (3) és a polgári fejlesztésű technológiák katonai alkalmazása adja azt a hármas fogatot, amely jellemzi a hadviselés új technológiai korszakát. [26]

Manapság már a vezető hatalmak közti fegyverrendszerek nem olyan kiegyenlítettek, mint a múltban. Az USA élen jár az olyan haditechnikai fejlesztések terén, mint a nehéz, nagy hatótávolságú lopakodó technológiát alkalmazó bombázó B-2. [27]

Ezt a technológiafejlesztést kevés ország képes követni, azonban számos ország képes ballisztikus rakéták fenntartására. Ez a folyamat arra enged következtetni, hogy az országok és nagyhatalmak közti fegyverkezési verseny aszimmetrikussá válik/vált.

A katonai fejlődést nagyban befolyásolja az átfogó rendszerek helyzete. Az USA haditengerészete együttműködő harcérintkezési képessége okán képes arra, hogy a rendszerben lévő adatok által kialakított közös képet egyszerre lássa és kezelje minden kötelékben lévő hajó. A világűr-vezetési rendszerek, amelyek használatával követhető minden Föld körüli pályán mozgó tárgy és összehangolhatóak a járművek mozgásai, elérhetővé válnak a katonai vezetés számára. Az USA és néhány európai ország kiemelkedő a repülő- és űriparfejlesztésben, amelyben Japán kevéssé sikeres, míg Kína és Oroszország vegyes eredményekkel rendelkezik. Magyarország részéről a külgazdasági és külügyminiszter a 2019-es sevillai Európai Űrügynökség (a továbbiakban: ESA) konferenciáján tett bejelentést az űrkutatással és űriparral kapcsolatos célokról, amely a nemzetközi űrkutatásában és űrprogramban való részvételen túl az önálló képességfejlesztést is magába foglalja.[28]

A rendszerintegrációt, azaz a komplex technológiák célirányos összeillesztését az USA-ban – követendő példát mutatva – a fegyverrendszerek és szenzorok összekapcsolásával fejlesztik annak érdekében, hogy ezek a rendszerek a folyamatosan változó környezetben is működhessenek. [29 pp. 33-41]

A polgári fejlesztésű technológiák katonai használata nem újszerű, hiszen a fejlesztések egy része mindig a civil szektorból származott. A polgári technikai eszközök alapvetően nagy hatást gyakoroltak a hadviselésre (vasút, távíró). A második világháborút követően azonban a technikai fejlődésben érdekelt országok nagy számban hoztak létre kutatóintézeteket, ennek következtében inkább a katonai fejlesztések kerültek át a civil szektorba (tranzisztor, sugárhajtómű). Hasonló megállapításra juthatunk az információs korszak kezdetekor megjelenő Advanced Research Projects Agency Network (a továbbiakban: ARPANET) kapcsán, amely az Egyesült Államok Védelmi Minisztériumának (a továbbiakban: DOD) által kifejlesztett „internet őseként" emlegetett – a nukleáris háború idején létrehozott – üzenetküldő- és fogadó hálózati rendszer. [30]

Manapság az információs korszak fordulópontjaként ismét a katonai szektor támaszkodik a civil szférában megjelenő fejlesztésekre. A civil technológia mutatja az utat a katonai alkalmazások tekintetében. A kormányzati és nem kormányzati, gazdasági, piaci szereplők egymásra utaltsága egyre jobban kerül előtérbe a technikai innovációk és fejlesztések tekintetében.

Az új haditechnika érvényesüléséhez idő kell. A modern hadseregeknek megterhelést jelent megküzdeni az információs forradalom kihívásaival. Az egyik legnagyobb kihívás a humán erő megtartása. Az ipari forradalom idején még nem kellett a civil szektorral, a magánvállalkozásokkal versenyezni. Az információs forradalomban azonban a civil-katonai szervezetek közti különbség egyre kiélezettebb. Sokkal nehezebb a kiképzett haderőt a honvédelmi pályán tartani egy olyan korban, ahol a civil szektor nagyobb szabadságot, jobb béreket és lehetőséget ajánl. Éppen ezért nagyon fontos a katonai életpálya fejlesztése. A technológiai fejlődés hatására más kihívással is szembe kell néznie a hadseregnek: a hadviselés, a kamerák és a műholdas kapcsolat keretei között zajlik. Ez azt jelenti, hogy a fegyveres összecsapásokra hatással lehet a kibertér, egyes harcok kibontakozhatnak a világhálón is, tehát a valós és virtuális csatatér elválaszthatatlan részei egymásnak. [31]

1.5 A hadviselés generációi, a negyedik generációs hadviselés

A Magyar Hadtudományi Társaság 2017-ben szervezett konferenciát *„A hadviselés generációi – Generációváltás a hadviselésben és ezek kihívásai, hatásai a Magyar Honvédségre”* címmel. A konferencia középpontjában a 21. század katonai, politikai és társadalmi kihívásai álltak. A konferencia egyrészt a nemzeti önerő és a honvédelem képességfejlesztését, másrészt a szövetségesi kötelezettségvállalások áttekintését tűzte ki célul, választ adva a negyedik generációs, vagy hibrid hadviselés korában jelentkező új biztonsági kihívásokra. [32 pp.75-76]

A hadviselés generációit négy időszak szerint különíthetjük el egymástól. A történelem során megismert első három generációt egészíti ki a jelenkor negyedik generációs hadviselése, vagyis a hibrid hadviselés. [33 pp. 15-51]

Az első generációs hadviselés korát az 1648-as vesztfáliai békekötéssel zárult 30 éves háború végétől számítjuk. Ebben az időszakban az élőerő segítségével vívták ki a győzelmet a harctéren. Éles határvonal választotta el a hadsereget, a civileket és az állami területeket, amelyek saját hadsereggel rendelkeztek. Ezért az állami hadseregek szabályozott és korlátozott háborúkat vívtak egymással, megkímélve ezáltal a polgárokat. A hadüzenetet követően, katonai manőverekkel lezajlott háborúkat a harc lezárásaként békekötés követte. Ebben a korban ugyanazok az államok vívták egymással felváltva a harcokat. A második generáció jellemzője a koncentrált tűzerő és az anyagcsata volt az első generációs élő erő fölényével szemben. Az I. világháború alatt indult meg – elsősorban a tüzérségnél – a tűzerő koncentrációja. A háború végére a géppuska mellett a géppisztolyt és a lángszórót is alkalmazták a harctéren. Az I. világháború végére megjelent a harmadik generációra jellemző gyalogság és a mélységbe csapást mérő koncentrált páncélosok. A harmadik generáció a mobil hadviselés és a villámháború kora. Az 1920-30-as évekre a technikai feltételek is rendelkezésre álltak a könnyen áttörhető védelemhez. Ebben a korban a totalitás volt az uralkodó eszme a hátország katonai célponttá tételével. A három generáció jellemzője, hogy egymásra épülnek, vagyis kiegészítik, nem pedig felülírják egymást. [34 pp. 3-17]

A hibrid hadviselés vagy negyedik generációs hadviselés kezdetét a 2001.09.11. napi terrortámadástól számítjuk azért, mert a klasszikus államok közti háborúk kora megrendült. Az al-Kaida – azzal, hogy a támadás nem kifejezetten katonai/állami célpont ellen, hanem a lakosság ellen irányult – felülírta az államiság kereteit, és ezzel kezdetét vette az aszimmetrikus hadviselés kora. Ezt a folyamatot erősítették meg az európai

fővárosok (Madrid 2004, London 2005) kritikus infrastruktúráival szemben mért terrortámadások. [35]

A negyedik generációs hadviselés jellemzője, hogy (1) térben és időben nem behatárolható, totális jellegű, ez azt jelenti, hogy egy ilyen típusú összecsapás bárhol jelentkezhet, azonban kisebb területre összpontosít, mint a hagyományos hadviselés; (2) a „kemény" katonai célpontokat felváltják a „puha" civil célpontok; (3) az ellenség nem rendelkezik reguláris hadsereggel; (4) jellemző a beazonosítható vezetési pontok és a katonai infrastruktúra hiánya; (5) feltétele a támadást támogató állam megléte. [36 pp. 4-12]

A negyedik generációs hadviselés módszerei: (1) a terrorizmus; (2) a kiberhadviselés; (3) a kritikus infrastruktúrák elleni szabotázs. Az okozott kár hatásait tekintve széles körű lehet, viszont életveszélyt csak korlátozott időben és térben tud okozni a szűkös és katonai infrastruktúrát nélkülöző erőforrások miatt. [37 pp. 10-18]

A 21. századi infokommunikációs eszközök, rendszerek és szolgáltatások olyannyira áthatják a mindennapjainkat, hogy életünk létfontosságú elemeivé válnak. Ezért fontos az informatikai rendszerek biztonságának garantálása. Ez a folyamat azonban változást indít el a hadviselésben is. A negyedik generációs hadviselés korában tudjuk azt, hogy egy ország megtámadásához nem szükséges átlépni annak fizikai határait. Az információs rendszerekbe történő behatolás, kártevés vagy akár megsemmisítés a világ bármelyik pontjáról kivitelezhető. A hadviselés tehát ennek megfelelően éppúgy változik, mint ahogy az a generációk során az előzőekben bemutatásra került. A nagy technikai felfedezésekhez hasonlóan a kibertérbeli infokommunikációs eszközös és rendszerek is változást hoznak a hadviselési eljárások terén. [38 pp. 119-137]

1.6 A 21. századi műveleti környezet jellemzői

A 21. századi műveleti környezet az új biztonsági kockázatok és kihívások és a rohamos technikai, technológiai fejlődés hatására változásokon ment keresztül. Mindez azt jelenti, hogy a műveleti környezet elemzése és értékelése során a helyzet és körülmények vizsgálata ugyanolyan súllyal jelenik meg, mint korábban azonban tartalmi és minőségi szempontból új feladatok hárulnak mind a parancsnokra, mind a törzsre.

Az elmúlt évek során a globális technológiai környezetet érintő változások alapjaiban változtatták meg a hadviselés szabályait és eljárásrendjét. A civil és a védelmi szféra területén olyan eszközökkel és technológiákkal találkozhatunk, mint az MI-vel rendelkező robotok; drónok; ember-robot koalíció; automatizált döntéshozatalt támogató

technikák; 3D nyomtatás; kibertér műveletek; irányított energiájú fegyverek; autonóm csapásmérő eszközök. A 21. századi műveleti környezetben megjelenik a kisebb létszámú és fejlett technológiát alkalmazó hadsereg. [39]

A hadviselés fejlődésével látjuk, hogy az idők során a fegyverrel vívott harc előkészítése és lebonyolítása összetettebbé és sokoldalúbbá vált. Amíg az ókorban és a középkorban a parancsnokot a megérzései, a tapasztalata és a felkészültsége vezérelte a győzelemig, addig a fegyverrel vívott harcok változásai, a fegyvernemek létrejötte, a harckiszolgáló- és támogató feladatok kialakulása és fejlődése miatt a parancsnok segítségére kialakult egy tanácsadói, támogató csoport, azaz a törzs. Napjainkban a törzs feladatai közé tartozik a műveleti környezeti körülmények elemzése, értékelése és ezek alapján javaslattétel a parancsnok számára.

A műveleti időszak változása az alkalmazott harceljárások változását hordozza magában, ez azt jelenti, hogy a hangsúly a gerilla harcmodorra és a partizán hadviselésre tevődik. A lehetőségek és képességek csökkenésének, a precíziós fegyverek alkalmazásának következtében a polgári, civil lakosság is bekerül a harc résztvevői közé, sok esetben ártatlan emberek halálával humanitárius katasztrófákat okozva.

Az idők során a mennyiségi fölény nem feltétlen hozott garantált sikert, azonban egy új fegyver, vagy technika megjelenése meghatározó hatással bírhat a harc kimenetelére. A 21. századra a tömeghadseregeket felváltották a speciálisan képzett és kiképzett mozgékony erők. Itt megjegyzendő, hogy kivételt képez a kínai haderő, mert a mennyiségi mellett a minőségi változást és a modernizációt egyszerre alkalmazzák a haderőfejlesztés érdekében. A technikai és tudományos fejlődés következtében átalakultak a fegyverek, a taktikák, és mindez hatást gyakorol a szállítóeszközökre, a logisztikai rendszerekre, a gyógyszerekre és a kommunikációra.

Napjainkban a katonai erők ugyanúgy részt vesznek a békeidőben jelentkező feladatokban és a békeműveletekben, mint a háborús helyzetekben. A hadszíntér kiterjedése és a hátország fogalma, feladatai mára megváltoztak. A műveleti terület megnövekedése következtében a katonai erőkön túl a lakosság, a humanitárius szervezetek, kormányzati szervek, a nem kormányzati szervezetek, a nemzetközi szereplők, vallási csoportok, a konfliktusövezetben élő lázadók, felkelők és semleges erők is a harcok résztvevőivé váltak, ezért a műveleti környezet szempontjából meghatározó elem a tervezés és a pontos elemzés.

A mai haderőt a modern fegyveres erő és a professzionális képzettség, kiképzettség és a modern technika alkalmazása jellemzi. A fegyveres erők sokrétű alkalmazása adja a

választ a 21. századi megváltozott biztonságpolitikai körülményekre. A haderőfejlesztés célja a megváltozott műveleti környezethez való tökéletes alkalmazkodás. A modern haderő képes a többnemzeti környezetben gyorsan, hatékonyan és eredményesen a nemzetközi erőkbe integrálódni. A katonák felkészítése kapcsán kiemelendő, hogy a sorozásos hadkötelezettséget felváltotta a szerződéses, professzionális haderő, azonban a felkészítés továbbra is a klasszikus elveket követve – egyéni, szak, kötelék felkészítés – történik.

A jelenlegi negyedik generációs hadviselés korában a hibrid hadviselés jelenik meg leginkább a harctéren. A különféle harceljárásokra különféleképpen kell felkészülni és reagálni, ilyen új elem például modern fegyverrel vívott harc során a pilóta nélküli eszközök szakszerű használta. A modern hadviselés jellemzői közt említendőek a hatásalapú műveletek, ami annyit tesz, hogy bármelyik fél vesztesége kihat a veszteséget elszenvedett fél további tevékenységére is.

Az informatikai hadviselés jellemzője, hogy a hangsúly az informatikai eszközök zavarásán, lefogásán, megsemmisítésén és a saját eszközök védelmén van. A kibertérben elkövetett események nagyban befolyásolják a harc kimenetelét. Egy sikeres kritikus infrastruktúra támadás következtében megszüntethető a fegyveres erők támogatottsága. A fegyveres küzdelmek során éppen ezért kiemelt hangsúlyt kell fektetni az informatikai eszközök védelmére és a működésükre, vagyis a kiberbiztonságra és a kibervédelem széles körű kiépítésére.

A műveleti környezet vallási és etnikai összetételének ismerete kulcsfontosságú a 21. századi katonai műveletek végrehajtása során. A modern haderő feladata a konfliktus zónákban élő lakosság kulturális szokásainak vizsgálata és tisztelete, mert ez is nagy mértékben hozzájárulhat a műveletek sikeres végrehajtásához. Fontos elem a vallási vezetők műveleti bevonása, mert ezáltal a helyi lakosság támogatása is elérhetővé válik a katonák számára.

Napjainkra jelentősen megváltozott a műveleti célok jellege és tartalma. A nagy kiterjedésű katonai műveleteket egyre inkább felváltják a speciális, kisebb támadó csoportok tevékenységei. A tartalmi változást tekintve előtérbe kerültek a kritikus infrastruktúrákat biztosító műveletek. [40 pp. 63-77]

1.7 Az információs hadviselés jellemzői

A 21. században olyan új hadviselési formák jelentek meg, mint (1) az információs műveletek; (2) információs hadviselés; (3) hálózat központú hadviselés; (4) hatás alapú műveletek.

Az információs hadviselés mellett megjelent a hibrid hadviselés is, amely a hagyományos hadviselés során alkalmazott eszközöktől eltérően, vagy azok kiegészítéseként alkalmazza a kiberműveleteket és az információs hadviselési elemeket. A 2000-es évek előtt a katonai vezetésben alkalmazott információs technológia számítógépes információs rendszerekre épült. Az információs műveletekkel megjelent egy új hadviselési mód, a Hálózat Központú Hadviselés, így a rendszerbe kötött információk már több felderítési forrásból is eljuthatnak a végrehajtóhoz. [41 pp. 22-28]

A következő rész azt a célt szolgálja, hogy átfogó képet adjak az információs társadalomról és hadviselésről, továbbá az információs infrastruktúrákat fenyegető veszélyekről.

Az információs társadalom biztonságos működése függ az információs infrastruktúrától és az információs rendszerektől. Ezeken keresztül fizikai, elektronikai és informatikai támadásokat lehet indítani egy fejlett ipari ország politikai, gazdasági és kulturális élete ellen. Egy sikeres információs támadással olyan károkat lehet okozni, amely szükségtelenné teszi a tényleges katonai támadást, válsághelyzet fennállása esetén pedig megbéníthatóvá válhatnak általa a csapásmérő erők, a korai előrejelző rendszerek, az azonnali és gyorsreagálású erők. Az információs támadások előrevetítik egy információs infrastruktúráktól függő, iparilag fejlett ország rövid időn belüli gazdasági és társadalmi hanyatlását. Ez pedig azt jelenti, hogy az információs támadások egyaránt érintik a civil lakosságot és a katonaságot is. [42]

Az információs infrastruktúrák komplex rendszerek, amelyek egymásra épülnek, egymást feltételezik és egymást kölcsönösen támogató infrastruktúrák halmazából tevődnek össze. Az információs társadalom függ a funkcionális információs infrastruktúráktól és a támogató infrastruktúrák folyamatos működésétől. Ezért, ha ezt a komplex infrastruktúrarendszert támadás éri, az befolyással bír a többi infrastruktúra zavartalan működésére is. Az infrastruktúrák között tehát kölcsönös a függőség. Az információs társadalom információs infrastruktúráinak működésében lehet zavart vagy kárt okozni, azonban ezek az infrastruktúrák a károkozással teljes egészében megsemmisíthetővé is válhatnak. Az információs infrastruktúrák működésének fenntartása egyaránt fontos a vállalatok, kormányzati intézmények, szervezetek

szempontjából. Az infokommunikációs rendszerek globális elérhetősége azonban egyben lehetőséget ad globális sebezhetőségükre is. A veszélyek és fenyegetések származhatnak személyektől, jogosulatlan felhasználóktól, terroristáktól, nemzetközi szervezetektől, külföldi hírszerzőktől vagy katonai szervezetektől. A fenyegetések motivációja általában (1) politikai; (2) gazdasági; (3) pénzügyi; (4) katonai; (5) szociális; (6) kulturális; (7) ipari; (8) etnikai; (9) regionális; (10) vagy egyéni érdekeltségű lehet. [43]

A fentiek alapján a fenyegetések a következő módokon történhetnek:

- illetéktelen adatbevitellel, információ hozzáféréssel;
- rosszindulatú szoftverek és vírusok rendszerbe való bevitelével;
- adatbázis lerontással, módosítással, megsemmisítéssel;
- az információs rendszer adatainak ellopásával;
- elektronikai támadásokkal mind a katonai mind a polgári kommunikációs, felderítő, rendszerek ellen;
- katonai vezetési, kommunikációs, fegyverirányító rendszerek és polgári rendszerek katonai célokra használható elemeinek a megsemmisítésével, pusztításával. [44]

Békeidőben a leggyakoribb információs tevékenység az informatikai hálózatokba való behatolás, ezáltal lehet felmérni a rendszer gyengepontjait, így válságidőszakban, vagy háborúban több közvetlen támadással lehet számolni. A katonai cselekmények megkezdését vagy kibontakozását összehangolt információs tevékenységgel képesek támadni. Az információs rendszerek elleni támadóeszközök közé tartoznak a pilóta nélküli eszközök, a műholdak és a GPS. A polgári és katonai információs infrastruktúrák és infokommunikációs rendszerek elleni támadások képezik az információs hadszíntér elsődleges célpontjait. [45]

Az információs hadviselés kapcsán kialakult kiberterrorizmus globális veszély, ezért minden országnak fel kell készülnie az információs társadalom rejtette veszélyekre. Napjainkban kiszámíthatatlan, hogy mikor melyik országból és milyen célpontra indítanak kibertámadást. Egy kibertámadást indító ország, vagy terrorszervezet számára kedvező, ha költséghatékony információs támadásokkal tud sújtani egy célország stabilitására és nemzetközi tekintélyére, különösen, ha ezt rejtve, az azonosság felfedése nélkül tudja megtenni. [46 pp. 659-671]

Következtetésképp megállapítom, hogy az információs támadások és agressziók ugyanolyan veszélyforrások, mint a nemzetközi, globális, regionális vagy nemzeti érdekeket ért kihívások, kockázatok és veszélytényezők. Ezért elhárításuk érdekében és a küzdelemben minden országnak cselekednie kell.

1.8 A hadügyi forradalom hullámai

A 21. század kezdetére változásokon ment keresztül a hadviselés, évszázadokon át fejlődtek az új technikai eszközök, a hadszíntéren új alkalmazási elvek jelentek meg, ezt a folyamatot jelen fejezetben a hadügyi forradalom négy fejlődési hullámának elemzésével mutatom be.

Az információs forradalom hatására alakult ki az új hadügyi forradalom (Revolution in Military Affairs), [47] amely kapcsán az információs, tudományos és számítógépes forradalom vívmányait használják fel a haderő korszerűsítésére és a 21. századi haderőmodell átalakítására az információs társadalom védelme érdekében. Az USA-ban az Army Transformation Programs [48] keretein belül zajlik a haderő átalakítási programja, míg Magyarországon a Zrínyi 2026 adja a képességfejlesztések keretét. [49]

A haderőfejlesztési, haderő-átalakítási programok összhangban vannak az információs korszak és az információs társadalom fejlődésével. Ez a folyamat fejlődési szakaszokban bontakozik ki, amelyek egymást hullámszerűn, magasabb teljesítményt produkálva követik. Ezekben a hullámokban új katonai, technikai eszközök és képességek jelennek meg az információs társadalom fejlődését elősegítő hadsereg számára. A fejlődési szakaszokban létrejövő új katonai képességekkel és fegyverrendszerekkel párhuzamosan új hadászati, hadműveleti és harcászati elvek, módszerek jönnek létre.

A hadügyi forradalom hullámait az alábbi négy időszak szerint különíthetjük el egymástól:

- első hullám (1950-2010);
- második hullám (2010-2030);
- harmadik hullám (2030-2050);
- negyedik hullám (2050-2100). [50 pp. 12-28]

A fejezet a továbbiakban a súlypontokat kiemelve elemzi az egyes hullámok legfőbb jellemzőit.

1.8.1 A hadügyi forradalom első fejlődési hulláma

Az első fejődési hullám az informatikai és tudományalapú technikai forradalomhoz kapcsolódik, különös tekintettel a precíziós fegyverek és a számítás, - szoftver, - hálózat, - távközlés, - vezérlés, - irányítástechnika kifejlesztésére.

A hadügyi forradalom első fejlődési hulláma alatt jelentek meg az első generációs légi és földi robotok és a miniatürizált atomfegyverek. Az új eszközök harctéren való bevetése lehetővé teszi az aszimmetrikus és terrorista cselekmények hatékonyabb leküzdését, ezáltal az atomfegyverek mérete és bevetésének mértéke csökken. [51]

Az első hullám főbb katonatechnikai képességei a következőek:

- a tudomány eredményeinek hadügyi felhasználása;
- csúcstechnikai-haditechnikai eszközök megjelenése;
- intelligens rakétafegyverek, integrált fegyverrendszerek megjelenése;
- miniatürizált atomfegyverek prototípusainak megjelenése;
- nagy kapacitású bombák és rakéták, légnyomással és tűzzel pusztító robbanófejek fejlesztése;
- személyzet nélküli, távvezérelt/programozott légi és földi felderítő és harci robotok első generációs megjelenése;
- nagy teljesítményű, precíziós hálózatos felderítőrendszerek megjelenése;
- összhaderőnemi vezetés kialakulása;
- csapatok manőverezőképességének növekedése;
- műholdas felderítő, navigációs és híradórendszerek harci felhasználása;
- kis valószínűséggel felderíthető harc- és híradóeszközök használatának bevezetése;
- globális információs környezet, információs hadszíntér, digitális harctér, digitális katonák megjelenése;
- digitális jelfeldolgozás, híradás, vezérlés kiépítése és használata;
- hálózatalapú vezetési rendszerek fejlesztése;
- harci számítógépek, harcászati internet, komplex katonai számítógépes hálózatok fejlesztése és használata;
- korszerű, számítógépes információs, vezetési és komplex felderítőrendszerek (C4ISR) kiépítése; [52]
- információs műveletek, információs hadviselés, vezetési hadviselés jelenléte. [53 pp. 194-201]

A hagyományos termelési korszak gépesített-motorizált, analóg-rendszerű hadseregeit felváltják az új típusú tudományos eredményeket hasznosító, digitális hadseregek, amelyek digitális vezetési fölénnyel és precíziós tűzfölénnyel rendelkeznek. A digitális haderők harctere a digitális harcmező, ahol információs műveleteket folytatnak. [54 pp. 141-157]

1.8.2 A hadügyi forradalom második fejlődési hulláma

A hadügyi forradalom második fejlődési hulláma alatt azok a fegyverek és fegyverrendszerek jelennek meg, amelyeket az első hullámban prototípusként fejlesztettek ki. Ennélfogva a digitális hadsereg tovább fejlődik, létrehozva ezzel a digitális, precíziós és hálózatközpontú hadsereget. Ezáltal a hadviselés átalakulása nagy mozgékonyságú- és tűzerejű, légi úton szállítható harceszközök felé irányul. [55]

A második hullám katonatechnikai jellemzői az alábbiak mentén csoportosíthatóak:

- digitális és precíziós hadseregek megjelenése a fejlett országokban;
- első generációs fejlesztésű, pilóta nélküli harci repülőgépek és földi robotrendszerek megjelenése; második generációs robotok fejlesztése;
- cirkálórakéták lopakodó technológiával való készítése;
- légi, űr- és földi lézerfegyverek megjelenése;
- elektromágneses impulzusfegyverek, mikrohullámú, lézer-és infrazavaró berendezések, navigációs műholdakat zavaró eszközök megjelenése;
- hatodik generációs, lopakodó technológiával készült, háromszoros hangsebességű többcélú légi harci robotrepülőgépek megjelenése;
- hiperszonikus repülőgépek tesztelése (NASA); [56]
- hetedik generációs hangvezérlésű kísérleti repülőgépek fejlesztése;
- többcélú légi harci robotrepülőgépek rendszeresítése;
- kisméretű légi harci robotokat szállító légi robotanyahajók fejlesztése;
- fejlett vegyi, biológiai, géntechnikai, lélektani hadviselési eszközök elterjedése;
- precíziós fegyverek továbbfejlesztése;
- távolból indítható precíziós fegyverek használatának növelése;
- precíziós, multi- és hiperspektrális, felügyelet nélküli felderítő szenzorrendszerek megjelenése;

- hadszíntéri, földi, légi, tengeri, kozmikus-támadó harci robotok rendszeresítése;
- hangvezérlésű harceszközök megjelenése;
- híradórendszerek és eszközök korszerűsítése multimédiás adatátvitel, hang-és mozgókép átvitel, harcászati internetkapcsolat hálózatos harcvezetés céljából;
- hipersebességű technikai eszközök megjelenése;
- a nem összefüggő harctéren folytatott hadviselés, új felfogású városharc, hálózatközpontú hadviselés, hatásalapú műveletek, információs műveletek továbbfejlesztése;
- hálózatos katona program fejlesztése, amely a haderő digitalizálásának komplex programját alkotja. [44]

A második fejlődési hullám központi elemét képezi a hálózatos, Digitális Katona Program kialakítása, a nemzetközi terrorizmus információs támadásainak kivédése különös tekintettel az információs infrastruktúrák és a számítógép-hálózatok védelmére. Ebben a fejlődési hullámban a digitális, hálózatos, precíziós hadsereg vezetési és technikai fölényt képez, ami azt jelenti, hogy arányaiban akár három-hatszor hatékonyabb, mint egy hagyományos hadsereg. [57 pp. 49-64]

1.8.3 A hadügyi forradalom harmadik fejlődési hulláma

A hadügyi forradalom harmadik fejlődési hullámában nagy valószínűséggel megjelennek majd a többcélú, második generációs robotok és a vegyes összetételű, robot és ember alkotta hibrid hadseregek. Az első generációs hibrid hadsereg előreláthatóan nagyobb részt élő erőből és kisebb hányadban robotokból fog állni. [41 pp. 22-28]

1.8.4 A hadügyi forradalom negyedik fejlődési hulláma

A hadügyi forradalom negyedik fejlődési hullámának várható jellemzője lesz, hogy a hibrid hadseregben a robotok és emberek aránya fele-fele, vagy a robotok javára nagyobb arányban fog megoszlani. Egyre nagyobb befolyása lesz a tudományos eredményeknek a haditechnikai fejlesztésekre. A harceszközök a nano, -bio, - és géntechnológiák, míg a haditechnikák a molekuláris számítógépek alkalmazásával fejlődhetnek majd a hadügyi forradalom negyedik fejlődési hulláma alatt.

Ezáltal kialakul a nanotechnológia alapú hibrid hadsereg, amely tudományos és katonai fölényt képviselhet. [58 pp. 36-48]

Az előzetesen ismertetett hadügyi forradalom hullámai kapcsán kialakult/kialakuló képességek elsajátítására (elvileg) minden információs társadalom képes, ezért kiélezett képességiverseny kialakulására lehet számítani. A fejlődési hullámok általános jellemzője, hogy szorosan összefüggenek egymással, épülnek egymásra és kapcsolódnak egymáshoz, mert az egyes képességek, eszközök, rendszerek már az előző szakaszokban jellemzően megjelennek, így azokat a korábbi periódusokban már kipróbálhatták. Ezek a változások azt eredményezik, hogy új katonai doktrínák alakulnak ki, az alakulatok mérete csökken, az alkalmazási területek száma nő és a pusztító erő mértéke megsokszorozódik.

1.9 Részösszefoglalás

Az első fejezet hipotézise az volt, hogy ha a hagyományos és az új biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel, vagyis multilateralizmussal - ugyanakkor a védelmi szektor adaptív képességfejlesztésével érhető el, akkor a védelmi szektornak, ideértve a honvédségnek az országvédelmi, katonai feladatok ellátása mellett szükséges az új biztonsági kihívásokhoz alkalmazkodni. Ahhoz, hogy a hagyományos katonai feladatok ellátása mellett az információs hadviselés korában jelentkező új biztonsági kihívásokat a honvédség felismerje és megfelelően kezelje, szükséges a hadviselés átalakítása, modernizációja.

A hipotézis igazolása érdekében e fejezetben megvizsgáltam a 21. századi európai biztonsági környezetet; a digitalizációt, mint globális biztonsági kihívást; az információtechnológia jellemzőit a biztonságpolitikában és a hadügyben. Elemeztem és értékeltem a haditechnikai forradalom egyes szakaszait, átfogó és általános képet adott a haderőreform történelmileg jelentős pontjairól. Vizsgáltam a hadviselés generációit, különös tekintettel a negyedik generációs, vagy hibrid hadviselésre. Kifejtettem a 21. század műveleti környezeti és az információs hadviselés jellemzőit különös tekintettel az információs infrastruktúrák tulajdonságaira. A hadügyi forradalom hullámait négy fejlődési szakaszban elemezte a haditechnikai-katonatechnikai képességek mentén.

Összességében megállapítottam, hogy az új típusú biztonsági kihívások, amelyek a poszthidegháború korában jelentkeztek, a korábban hangsúlyos egyirányú, katonai dimenzió kibővülésével jöttek létre. Ez azt jelenti, hogy a biztonságot meghatározó tényezők a katonai dimenzió mellett kibővültek, átalakultak és újak jöttek létre. A hagyományos és új biztonsági kihívások gyakran összekapcsolódnak, ezáltal a

fenyegetések egyértelműen összefüggenek egymással, hatnak egymásra, folyamatosan befolyásolva a stabilitás adott szintjét.

A globalizáció és a technológiai forradalom hatásai előbb-utóbb minden nemzethez elérnek. Az információs társadalmak fejlődésének hatására az új fenyegetések nem ismernek országhatárokat, ezért a hagyományos és az új biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel és a védelmi szektor adaptív képességfejlesztésével érhető el. Egyre nő az esélye a kiberbűnözésnek, a terrorizmusnak, a migrációnak, a katasztrófahelyzeteknek. Nagy veszélyt hordoz magában az aszimmetrikus hadviselés és a tömegpusztító fegyverek proliferációja. Az új biztonsági kihívások kezelésére minden országnak fel kell készülnie, ezért szükséges a védelmi szektornak az országvédelmi, katonai feladatok ellátása mellett az új kockázati tényezők mentén kialakult/kialakuló biztonsági fenyegetésekhez a honvédség digitális képességfejlesztésével, a hadviselés átalakításával, modernizációjával alkalmazkodni.

A háborúk elsődleges célpontjait napjainkban az információs rendszerek és az információs infrastruktúrák adják. Az információs támadások és agressziók ugyanolyan veszélyforrások, mint a nemzetközi, globális, regionális, vagy nemzeti érdekeket ért kihívások, kockázatok és veszélytényezők. Éppen ezért fontos a honvédség átalakítása, képesség alapú fejlesztése, digitális platformra állítása.

2 A KIBERTÉR JELLEMZŐI A KIBERBIZTONSÁG ÉS A KIBERVÉDELEM TEKINTETÉBEN

A digitalizáció fő színtere a kibertér. A kibertérben elkövetett támadások nemcsak az egyének, vagy civilek ellen irányulhatnak, hanem sok esetben visszafordíthatatlan politikai, vagy gazdasági károkat okozó cselekményeket rejtenek magukban. A kibertér – és az elektromágneses tér – a szárazföld, a tengerek, a levegő és a világűr mellett ma már külön műveleti térnek számít. [1 pp. 122-145]

Napjaink kiberfenyegetései a terrorizmushoz hasonlóan nem ismernek határokat, és a globalizáció hatására egyre inkább terjednek. A számítástechnikai rendszerek működtetik a társadalmakat, a tudomány és technológia valamennyiünk részére elérhetővé válik, ezért számolnunk kell a váratlan, kibertérben történő támadásokkal. Megfelelő módon szükséges védekezni a kibertérben bekövetkező támadások ellen, mint például az információs és kommunikációs rendszerek, vagy a kormányzati gerincháló rendeltetésszerű működésének megzavarása, blokkolása vagy túlterhelése. A nemzeti biztonság és honvédelem fejlesztése mellett kiemelkedő hangsúlyt kell fektetni a kibervédelemre és a nemzetközi kritikus infrastruktúra biztosítására.

Előnyei mellett új kockázatként azonosítható tehát az informatikai robbanás. A kibertámadások, mint országokat, nemzetközi és világszervezeteket, a kormányzatot és a gazdasági élet szereplőit ért támadások, a 21. század legjelentősebb technológiai biztonsági kihívásai közt szerepelnek. [59]

Egyetértek azzal, hogy napjaink legmeghatározóbb biztonsági kihívásai (1) a globalizáció elmélyülése; (2) a digitalizáció terjedése; (3) a globális felmelegedés állandósulása; (4) és a nyersanyagforrások kimerülésének fokozódása. [60] Ezek a globális és Európát érintő biztonságpolitikai trendek meghatározzák Magyarország biztonságpolitikai kihívásait, törekvéseit és céljait.

A disszertációban a digitalizációt, mint a 21. század új biztonsági kihívását kutatom, ehhez azonban elengedhetetlen a kibertér, a kiberbiztonság és a kibervédelem átfogó elemzése és értékelése.

A fentiek tükrében második fejezetben az alábbi kérdéseket vizsgálom:

- Hogyan igazolható az, hogy a digitalizáció következtében nőnek a technikai, informatikai rendszerek és a kibertérbeli kockázatok?
- Fokozódik-e a kiberbiztonsággal foglalkozó szervezetek tevékenysége a kiberbiztonsági kihívások növekedésével párhuzamosan?

- Melyek a 21. század leghangsúlyosabb kibertérbeli fenyegetései?
- Milyen súllyal jelenik meg Magyarország vonatkozásában a hazai szabályozás és nemzetközi szerepvállalás a kiberbiztonság kiépítése érdekében?
- Milyen feladatok jelennek meg a honvédelem rendszerében a kibertérbeli fenyegetések felismerése, a kiberbiztonság és a kibervédelem kiépítése és fenntartása érdekében?

A problémafelvetés tükrében az értekezés második fejezetének hipotézise az, hogy ha a digitalizációt, mint technológiai faktort vizsgálom, akkor ez az egyik leghangsúlyosabb biztonsági kihívás azért, mert leginkább ez kapcsolódik az emberhez és ez van hatással leginkább a mai modern világ fejlődésére, Európa, és benne Magyarország biztonságára, hiszen a gazdasági, technológiai fejlődés mellett erre épülnek a haditechnikai, katonai fejlesztések is. [61 pp. 81-93] Ennek következtében nőnek a technikai, informatikai rendszerek és kibertérbeli kockázatok is. Ezért Magyarországnak képesnek kell lennie a kibertérbeli fenyegetések felismerésére és kezelésére, a kiberbiztonság kiépítésére, a kritikus információs infrastruktúra zavartalan működésének biztosítására, a támadások elhárítására és a kibervédelmi feladatok ellátására. Az infokommunikációs rendszerek elleni támadások száma folyamatosan nő, így szükséges azok védelmének erősítése, valamint a felhasználók információbiztonsági szintjének növelése. [62]

A hipotézis igazolása érdekében a fejezetben kutatom a kibertér és kiberbiztonság alapvetéseit; elemzem és értékelem a kibertér vonatkozó hazai és nemzetközi doktrínáit különösképpen a NATO megközelítéséből; áttekintem a kiberbiztonság, a kiberműveletek és a kibertérbeli fenyegetések általános jellemzőit, különös tekintettel a kiberbűnözésre, a hacktivizmusra, a kiberkémkedésre, a kiberhadviselésre és a kiberterrorizmusra; végül feltárom a kiberbiztonság és kibervédelem magyarországi helyzetének katonai, honvédelmi vetületeit.

2.1 A kibertér és kiberbiztonság alapvetései

A kibertér fogalma kapcsán számos definíció született már kutatók, intézetek és nemzetközi szervezetek megfogalmazásában. A kibertér általános megfogalmazása szerint a számítógépek, számítógéphálózatok, kommunikációs csatornák, alkalmazások és adatok által együttesen alkotott virtuális tér.

A DOD katonai terminológiai szótára szerint a kibertér „*Az információs környezet egy globális tartománya, amely tartalmazza az informatikai infrastruktúrák, a bennük tárolt*

adatok egymással összefüggő hálózatát, beleértve az internetet, a távközlési hálózatokat, a számítógép rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket" [63 p. 55]

Magyarország tekintetében az NKBS szerint *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információsrendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."* [64 I/3]

A fenti meghatározások szerint a kibertér az összekapcsolt elektronikus információs rendszerek és hálózatok összessége.

A 21. század biztonsági kihívásai közül kiemelt figyelmet szükséges fordítanunk az információs társadalom nyújtotta, digitális alapú kihívásokra. A kiberbiztonság kérdése már az 1970-es évekre nyúlik vissza, amikor is a kártékony programok önreprodukciójuk tekintetében megjelentek az ARPANET számítógépein. [30]

A kibertérben jelentkező globális kihívások azonban több tényezőből adódnak össze, amelyek az alábbiak:

(1) a kibertérbeli dinamikus kihívások;
(2) a rohamos technológia fejlődés;
(3) a felhasználók tudatosságának alacsony szintje;
(4) a kibertérben bekövetkezett károk nagysága. [65 pp.341-356]

A kiberbiztonság a kibertér működéséből és használatából adódó biztonsági dimenziókkal foglalkozó terület. Az alapfogalom a kibertér és a biztonság fogalmak közti összefüggésekből alakult ki. A kiberbiztonság fogalmára nem találunk általános definíciót. A DOD, az EU, az ENSZ-hez kapcsolódó Nemzetközi Távközlési Egyesület, International Telecommunication Union (ITU), az EU-s Kiberbiztonsági Ügynökség, European Union Agency for Cybersecurity (a továbbiakban: ENISA) és a NATO mind, más definíciót használnak a kiberbiztonságra.

Katonai szempontból vizsgálva az USA meghatározása szerint a kiberbiztonság egy tágabb, stratégiai nézőpontot előtérbe helyező fogalom, amely a kibervédelem és a kiberháború fogalmakon alapszik. A kiberbiztonság a számítógépek, az elektronikus rendszerek, szolgáltatások és a vezetékes-elektronikus kommunikáció sérüléseinek prevencióját, védelmét és a tárolt információk visszaállítását jelenti. A NATO meghatározása a védelem és a kiber kifejezéseket helyezi előtérbe, miszerint a

kibervédelem olyan képesség, amellyel egy műveleti kommunikációs és információs rendszer szolgáltatásai megvédhetők egy rosszindulatú kibertérből érkező támadással szemben. [66 pp. 69-79]

Az ENISA az alábbi területeket vizsgálja a kiberbiztonság meghatározásakor: (1) a kommunikáció biztonsága; (2) a működés biztonsága; (3) az információ biztonsága; (4) a fizikai biztonság; (5) közbiztonság és/vagy nemzeti biztonság. [67] A kiberbiztonsági definíciók közti eltérések szervezetektől és intézményektől függően eltérőek. A legtöbb ország azonban saját terminológiát, egyedi meghatározást alkalmaz.

Magyarország kiberbiztonságát a szövetségesi dokumentumokkal összhangban az NKBS határozza meg, mely szerint *„A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."* [64 I/5]

A fenti fogalmak kapcsán kijelenthető, hogy a kiberbiztonság egyfajta állapot, amelyet az adatok, az információk bizalmassága, integritása, valamint rendelkezésre állása határoz meg.

A kiberbiztonságnak speciális a helye és viszonya a többi biztonsági kihíváshoz képest, mert minden kihívással van közös keresztmetszete és valamennyi biztonsági kihívás rendelkezik kiberbiztonsági tényezővel. A kiberbiztonság különösen érinti a fegyveres konfliktusokat és a nemzeti biztonsági kérdéseket. A tengerbiztonság és az egészségügyi rendszer digitalizációja is kiemelt területet képvisel a kiberbiztonság terén. A szervezett bűnözés klasszikus formái digitalizáltan jelennek meg, ezzel kihívások elé állítva a szervezett bűnözés ellen fellépő hazai és nemzetközi szerveket, szervezeteket. A kiberbiztonsági kihívások következtében olyan károk keletkezhetnek, amelyek veszélyeztethetik a gazdaság biztonságát. [68 pp. 251-260]

A kiberbiztonsági támadásokat motivációjuk szerint az alábbi kategóriákba sorolhatjuk:

(1) politikai, ideológiai;
(2) pénzügyi/gazdasági;
(3) hírszerzési/kémkedési;
(4) hacktivista;

(5) destruktív indíttatású.

A digitalizáció következtében a társadalmi folyamatok jelentős részéhez használjuk a kiberteret, ennek következtében a kiberbiztonsági kihívások dinamikus és folyamatos növekedése tapasztalható. Fentiek és a biztonsági kihívások dinamikus volta miatt a kiberbiztonsággal és kibervédelemmel foglalkozó szervezetek tevékenysége is fokozódik, ezzel hozzájárulva a kihívások mielőbbi felismeréséhez és az ellenük történő eredményes fellépéshez. [69 pp. 93-116]

2.2 Kiberdoktrínák

A kibertér átfogó értelmezéséhez szükségszerű a hazai és a vonatkozó nemzetközi kiberdoktrínák vizsgálata. Jelen részfejezetben ezért a jelentősebb kiberdoktrínák – a szabályozók létrejöttét kiváltó biztonsági események tükrében – kerülnek elemzésre és értékelésre különös tekintettel a NATO normákra.

Az infokommunikációt érintő rohamos technológiai fejlődés következtében a társadalom valamennyi területét érintő változás áll be. A modern állam, szervezetei és állampolgárai egyre nagyobb körben válnak az elektronikus infrastruktúrák és az elektronikus információs rendszerek felhasználóivá. Az infokommunikációs eszközök és technológiák egyrészt új lehetőségeket jelentenek az innováció és a fejlődés területein, másrészt a terrorizmus és a kiberbűnözés tekintetében is. Mindezek alapján kijelenthető, hogy a fenti lehetőségek terjedésével egyre nagyobb energiát és figyelmet szükséges fordítani a kiberbiztonsági és kibervédelmi kérdésekre, amelyeket szakértők, állami és nem állami-piaci szereplők együttes bevonásával transznacionális szinten kell kialakítani.

Hazánk kiberbiztonsága szempontjából a 2013-ban elfogadott Információbiztonsági törvény [70] (a továbbiakban: Ib. törvény) mellett az NKBS jelenti az alapkövet.[64] Az Ib. törvény lehetőséget ad egy olyan jogszabályi környezet megteremtésére, amely biztosítja az állami, közigazgatási infokommunikációs rendszerek tekintetében működő kiberbiztonsági szervezetek kialakítását, azonban inkább erősíti a kiberbiztonság civil szféráját a honvédelmi platform hiányával. A kiberbiztonság irányítását a civil szervezetek közül a Belügyminisztérium, még a katonai szervezetek közül a Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) mellet az MH irányítja. Tekintettel arra, hogy az értekezésnek a honvédelem a központi a témája, az egyéb szervezetek jogi szabályozását, szervezeteit és tevékenységeit részleteiben nem tárgyalja.

Az NKBS a kibertér létrejöttének következtében meghatározza a kiberbiztonság megteremtését és biztosítását, és kimondja, hogy Magyarországnak szükséges a kibertér védelmével kapcsolatos feladatokat nemzeti keretek között és nemzetközi együttműködéssel felelősséggel ellátnia. Az NKBS célja a szabad és biztonságos kibertér kialakítása; a nemzeti szuverenitás védelme a nemzeti és nemzetközi környezetben, a nemzetgazdaság és a társadalom szabad tevékenységének és biztonságának garantálása, az innovatív technológia adaptálása a gazdasági növekedése érdekében és a nemzetközi együttműködések kialakítása. Magyarország elsődleges célja a megelőzés útján kialakítani hatékony védelmi rendszerét, biztosítani a kibertérbeli fenyegetések és kockázatok kezelését és az ehhez nélkülözhetetlen kormányzati koordináció kiépítését. A stratégiában kiemelt hangsúlyt kap az információbiztonság alappilléreinek megteremtése; a rendelkezésre álló eszközök, szervezetek és tudás felhasználása és továbbfejlesztése és a kibertér biztonságos és innovatív kialakítása.

Az NKBS a célok elérése érdekében az alábbiakat határozza meg:

(1) kormányzati szervezeti rendszer és koordináció létrehozása;
(2) operatív együttműködés kialakítása a civil, gazdasági és tudományos területek bevonásával a megalapozott kormányzati döntéshozatal érdekében;
(3) szakosított intézményekkel való együttműködés biztosítása;
(4) nemzeti kooperáció növelése;
(5) a civil, a gazdasági és tudományos élet szereplőivel közös kiberbiztonsági szabályozás megalkotása;
(6) Az EU, NATO, ENSZ, Európai Biztonsági és Együttműködési Szervezet (a továbbiakban: EBESZ) kiberbiztonsági együttműködéseiben való fokozott jelenlét biztosítása és fenntartása;
(7) a kiberbiztonsági tudatosság növelése különös tekintettel az egyéni felhasználók és a kis- és középvállalkozások (a továbbiakban: KKV) tekintetében;
(8) az oktatás és a K+F korszerűsítése kiemelt figyelmet fordítva a köznevelésre és a felsőoktatásban tanulókra, a kormányzati tisztviselők képzéseire, a szakmai továbbképzésekre és az informatikai oktatásra;
(9) a gyermekvédelem erősítése kifejezetten a gyermekeknek és fiataloknak szóló online tartalmak tekintetében;
(10) a gazdasági szereplők motiválása a kiberbiztonság fokozása érdekében. [64]

Az NKBS által elsőként került meghatározásra a magyar kibertér gazdasági és társadalmi szerepe a globális térben. Ennek kapcsán kezdődött meg a kibertérbeli fenyegetések, kockázatok tudatos jogi szabályozásának előkészítése, a kormányzati, piaci és társadalmi szereplők bevonásával. [71 pp. 351-354]

Hazánk kiberbiztonsága és kibervédelme szempontjából szintén mérföldkőnek tekinthető a 2018-ban elfogadott hálózati és információs rendszerek biztonságára vonatkozó stratégia, amely Stratégia pontosítja az NKBS-ben meghatározott kibertér fogalmát. [72]

A Stratégia szerint a kibertér *„globálisan összekapcsolt, decentralizált, folyamatosan változó elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti”*. [73 p. 4]

A Stratégia célja Magyarország tekintetében:

(1) a biztonságos, szabad és innovatív kibertér kialakítása;
(2) a versenyképesség növelése;
(3) a digitalizált állami, kormányzati, gazdasági területeken az innovatív technológiai megoldások biztonságos bevezetése és adaptálása;
(4) biztonságosabb E-közigazgatás létrehozása;
(5) az állami szolgáltatások fejlesztése;
(6) a kiberbiztonság és az információtudatosság növelése.

A Stratégia az NKBS-ben meghatározott célokkal összhangban az új kihívásokra és fenyegetésekre választ adva, az új lehetőségek és célok meghatározásával erősíti a hálózati információs rendszerek védelmét a modern kor kihívásainak megfelelően. [73]

A jelenlegi és jövőbeli kiberbiztonsági kihívások eredményes kezeléséhez szükséges a nemzeti kiber-irányítási rendszer hatékony működése, amely a NATO és az EU által meghatározott védelmi kötelezettségvállalásoknak történő megfelelés, az európai és nemzetközi együttműködés megállapodásainak és a hazai vonatkozó szabályzók összhangjának kiépítésével érhető el.

Magyarország kiberbiztonsága szempontjából számottevő lépés volt, hogy az Európa Tanács (a továbbiakban: ET) 2001-ben, Budapesten fogadta el a Számítástechnikai bűnözésről szóló egyezményt, amelyet Magyarország 2004-ben írt alá. [74] Az egyezmény az első olyan fontos jogi doktrína, amely szerint az EU és az egyezményt

aláíró tagországok felismerték, hogy a kiberbűnözés ellen való fellépés a nemzetközi színtéren a legeredményesebb. Nemzetközi viszonylatban a NATO a 2007-es Észtország elleni kiberincidens óta fordít kiemelt figyelmet a kiberbiztonságra és a kiberpolitikára.

Az informatikailag kiemelkedően fejlett észt főváros ellen elkövetett kibertámadások során a bankokat és a kormányzati rendszereket sújtották a támadások, amely hatására a NATO 2007-ben úgy döntött, hogy a tagállamok kibervédelmi törekvéseit egységesíteni kell.

2008-ban fogadta el a NATO az új kibervédelmi irányelvét, amelyben először került hivatalos megfogalmazásra az informatikai biztonság kérdése, ugyanebben az évben hozták létre a NATO Kooperatív Kibervédelmi Kiválósági Központját, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), amely a szervezet kutatási és oktatási központjaként működik. [75 pp. 76-83]

A NATO 2010 novemberében Lisszabonban megrendezett csúcsértekezletén adta ki az új stratégiai koncepcióját, amelynek célja, hogy a NATO képességek megbízhatóbb védelmet nyújtsanak a modern kihívásokkal szemben. Ennek értelmében a hibrid fenyegetések elleni fellépés, az informatikai rendszerek védelme és az elektronikus hadviselés került a képességfejlesztés központjába. [76 pp. 79-86]

A 2011. szeptember 11. napi terrortámadásokat követően a terrorizmust nyilvánították az egyik legfontosabb veszélyforrásnak, a támadások elemzésének következtében világossá vált, hogy az információ korunk egyik leghangsúlyosabb tényezője. Az események bekövetkezése miatt az információszerzés, - összegyűjtés, - feldolgozás, - elemzés, - és értékelés azonban komoly hiányosságokat mutatott. A NATO tagországok 2011-ben hagyták jóvá a NATO új kibervédelmi politikáját, melynek részeként indult el a NATO kiberincidens-kezelési képességének (NCIRC) kialakítása. [77]

Végül a 2016-os varsói csúcson a NATO önálló műveleti térré nyilvánította a kiberteret. [78 pp. 97-101] Ezzel egyidőben a tagországok megállapodtak a kibervédelmi képességeik fejlesztésében, ez az úgynevezett *Cyber Pledge* vagyis Kibervállalás, amelyet a NATO évente ellenőriz továbbá segítséget ad a tagállamoknak a – nemcsak katonai, hanem össztársadalmi – kiberképességek kialakításához. [38 pp. 119-137]

Fentiek jegyében indult el a *Global Common* vagyis a „globális közös terek” projekt, amely a tengerek és az óceánok, a légtér, a világűr és a kibertér alapos vizsgálatát tűzte ki célul. Ezek a közös dimenziók összefüggésben állnak egymással, mert mindenki használja őket, lehetővé teszik az információ, az áru és a szolgáltatások áramlását. A globalizáció hatására ezek a terek mindenki számára elérhetőek és ezáltal ugyanúgy

használhatóak jó célokra, mint ártó szándékkal, ezért e terek stratégiai jelentősége nő. A NATO célja, hogy tagországai politikai, diplomáciai és katonai lépésekkel egyaránt felvehessék a küzdelmet a közös dimenziókban okozott károk ellen. A dimenziókban rejlő folyamatosan változó és újszerű biztonsági kihívások jelentősége katonai szempontból igen magas, mert a hadsereg aktívan használja a tengereket és óceánokat katonai csapatok, egységek szállítására, a légteret és a világűrt navigációra, felderítésre és vezetés-irányításra, valamint a kiberteret kommunikációra. [79 pp. 34-46]

A biztonsági kihívások szemszögéből a kibertér vizsgálata a leghangsúlyosabb, mert egyértelműen nem körülírható, nem körülhatárolható és a technológiai fejlődés következtében egyre több feltérképezetlen lehetőség adódik a kibertér széles körű használatára. A kibertér fizikai szempontból függ azoktól a fizikai eszközöktől, amelyek működtetik: számítógépek, modemek, kábelek, műholdak. Ezáltal fizikailag lekövethetővé válik a kibertér elsődleges támadói, a hackerek tevékenysége. Annak ellenére, hogy a négy nagy tér összekapcsolódik és egymással összefüggésben áll, a kibertér mégis különbözik a többitől abban, hogy az információ-bázisa és infrastruktúrája jórészt nem állami tulajdonban van, azaz civil cégek, gazdasági szereplők határozzák meg a biztonságot és a fejlesztéseket, ezáltal az állam kontrollszerepe gyengül. Fentiek okán fontos, hogy az állami szereplők kibertérbeli befolyásoltságát erősítsük, annak érdekében, hogy a nemzeteket, állami rendszereket ért támadásokat észlelhessük és rendelkezzünk a megfelelő eszközökkel, képességekkel azok leküzdése céljából. [80 pp. 65-90]

A NATO a *Global Common* projekt keretében közel 20 éve felismerte azt, hogy a hadsereg digitalizációja és fejlesztése elengedhetetlen az új biztonsági kihívásokkal való szembenézés sikeressége érdekében. Az állami, katonai, nemzeti biztonsági rendszereknek ezért szükséges digitálisan felzárkózniuk, a nemzetállamoknak pedig a stratégiai dokumentumaikat szükséges az új biztonsági kockázatokhoz mérten felülvizsgálniuk.

2.3 Kiberbiztonság, kiberműveletek

A korábbiakban már említett, Barry Buzan-féle szektorelmélet szerint a biztonságot alapvetően öt szektorra lehet felosztani: katonai, politikai, gazdasági, társadalmi és környezeti biztonságra. [10 pp. 431-451] A 21. században a biztonság az információbiztonsággal, mint új szektorral egészült ki. Ennek oka, hogy a 20. század végére, a 21. század elejére az információ meghatározó erőforrássá vált. Az információbiztonság és a kibertér elválaszthatatlan részei és egészei egymásnak, mert az

információ, információs rendszereken át áramlik, amely rendszerek létrehozzák a kiberteret. Katonai értelemben az a tér, ahol az információs folyamatok mennek végbe, az információs hadszíntér. Ezen a hadszíntéren zajlanak az elektronikai rendszerek elleni támadások. A kiberhadszíntér csakúgy, mint az általánosságban vett kibertér jóval több a számítógépes hálózatok összességénél és az internet nyújtotta platformnál. Katonai értelmezésben egyszerre a kibertér a harctéri elektronikai eszközök (rádió, radar, navigációs eszköz, harctéri azonosító eszköz) és a számítógépek hálózatai által alkotott közös működési környezeti komplex rendszer. A kibertér a hadviselés hagyományos dimenzióival egyenértékű tartománya. [22]

A kiberbiztonság megteremtéséhez számos tevékenység összehangolt működésének kell megvalósulnia, idetartoznak az aktív kibervédelmi műveletek is. A kiberbiztonság garantálásához azonban a védelmi célú kiberműveleteken túl szükséges az offenzív kiberműveletek alkalmazása is.

Az offenzív kiberképességek nem azonosíthatóak tisztán a kibertámadások képességével. A kibertámadás egy infokommunikációs rendszerbe történő, jogtalan és nem engedélyezett informatikai eszközökkel történő behatolás. Az offenzív kiberképességek ennél többet foglalnak magukban, pontosabban az alábbi területekre oszthatóak fel: (1) információszerző-és feldolgozó képesség; (2) kibertámadási képesség; (3) a hatások értékelésével foglalkozó képesség. Az offenzív kibertérműveletek nemcsak a saját rendszereink védelmét erősítik, hanem képesek az ellenfél infokommunikációs rendszereinek a lefogására, működésük akadályozására, azokból információk kinyerésére és ezáltal más műveletei terekben zajló tevékenységek támogatására. [81 pp. 187-204]

A kiberképességek fejlődése magával hozza a hadviselésben bekövetkező változást is. A kibertérben zajló tevékenységeket két csoportra oszthatjuk. Az első csoportba tartoznak az önálló kiberműveletek, amelyek békeidőben következnek be, a tevékenység során a cél, a konfliktus háborúsküszöb alatt tartása. Az ilyen kiberműveletek a hibrid műveletekkel párhuzamosan vagy azok részeként zajlanak. A második csoportba tartoznak azok a kiberműveletek, amelyek a kinetikus műveletek, vagyis a hagyományos műveletei terekben végbemenő katonai műveletekkel párhuzamosan történnek egy fegyveres konfliktus során. A többdimenziós műveletek célja az ellenfél vezetési rendszerének megzavarása, működésének akadályozása. Multitér műveleteknek nevezzük az azonos időben, de több dimenzióban végbemenő műveleteket, melynek a lényege, hogy egy időben több egymást támogató művelet zajlik más műveletei területeken történő végrehajtással: szárazföld, levegő, víz, űr, kibertér. [81 pp. 187-204]

A fent kifejtett multitér műveletek a 2022. február 24-én kezdődött és jelenleg is zajló orosz-ukrán háborúban is megmutatkoznak tekintettel arra, hogy a konfliktusok párhuzamosan történnek a hagyományos műveleti tereken és a kibertérben egyaránt.
Korunk leghangsúlyosabb biztonságpolitikai kihívásai közé soroljuk a kibertérbeli kihívásokat, fenyegetéseket és veszélyeket, melyek egyre nőnek és az élet egyre több területén jelentkeznek. Az információs társadalom természetessége, hogy a kibertérben elérhető adatok és információk dinamikusan növekednek, azonban kevésbé van jelen ezen adatok és információk védelme, vagyis az információtudatosság. Az infokommunikációs technológiai fejlődés következményeként számos társadalmi folyamat zajlik le a kibertérben. Ezekhez az információkhoz pedig egyre többféle eszközzel és különféle módon férhetünk hozzá. Az elmúlt években a kiberbiztonság mind egyénileg, nemzetileg, regionálisan és globális szinten is átalakult. A kibertérbeli szolgáltatások bővülése, az okos eszközök rendelkezésre állása, a rosszindulatú felhasználók és módszereik terjedése okán a kibertámadások ma már sokkal szélesebb kört érintenek. Ezzel párhuzamosan a kiberbiztonsági tudatosság fejlesztésére és terjesztésére is nagyobb igény mutatkozik. A kibertérbeli szabályok másként jelentkeznek, mint az offline világban, tekintettel arra, hogy itt nincsenek államhatárok, a nemzetállamok nem egyeduralkodók és a társadalom tagjai széles körben a kibertér részesei az egyéni állampolgároktól kezdve, a multi cégeken át a kormányzati szereplőkig. A kibertér sajátosságaiból adódóan a nemzetállamok és kormányaik ráeszméltek, hogy önállóan nem képesek szabályozni a kiberbiztonságot. Az együttműködési szabályozók és szövetségek a kiberbiztonsági trendek kapcsán alakultak ki. [82 pp. 191-214]

2.4 Kibertérbeli fenyegetések

A kibertérből érkező fenyegetések számos szempont alapján csoportosíthatóak, melyek közül szerintem a leghangsúlyosabbak: a kiberbűnözés, a hacktivizmus, a kiberkémkedés, a kiberhadviselés és a kiberterrorizmus. Jelen fejezetben külön hangsúlyt fektetek a kiberhadviselésre és kiberterrorizmusra.

A kibertámadásokkal egyre gyakrabban kell szembenéznünk, a kiberfenyegetések komplexebbé és nagyobb volumenűvé válnak és egyre több (szélsőséges)csoport és szervezet használja a kiberteret saját ideológiájuk terjesztésére. A kiberbűnözés célja a gazdasági, politikai befolyásolás mellett a személyes és pénzügyi adatok eltulajdonítása és az elektronikus szolgáltatásokban történő célzott károkozás; kéretlen levelek,

kártékony kódok és robothálózatok előállítása. A kibertérben végrehajtott támadások javarészt anyagi haszonszerzés céljából következnek be. Az elkövetők a hagyományos bűnelkövetői csoportok tagjai, akik felvásárolják az informatikai és technológiai tudást biztosító szakembereket, eszközöket. A kiberbűnözés célpontjait az egyének alkotják, azonban az egyéni felhasználókon keresztül könnyen elérhetővé válnak a bankok, pénzintézetek is. A kiberbűnözést alapvetően két kategóriára különíthetjük el: az első kategóriába tartozik az, amikor számítógép segítségével követnek el bűncselekményt, vagyis a számítógépet eszközként használják, a második kategóriában pedig a számítógépek és az általuk alkotott hálózat ellen követnek el bűncselekményt, vagyis adatlopást, adatmódosítást, manipulálást vagy adattörlést. [83 pp. 3-16]

A hacktivizmus digitális eszközök illegális használatát jelenti politikai célok elérése érdekében. A hacktivizmus és a kiberterrorizmus fogalmilag különálló tevékenység, azonban céljaikat és eszközrendszereiket tekintve azonosak. Az informatikai bűncselekményeket általában kisebb, decentralizált csoportok ellen hajtják végre azzal a céllal, hogy minél nagyobb médiahatást keltsenek. [84 pp.142-151] A két fenyegetést külön csoportba sorolom. A hacktivizmus az 1990-es évek óta van jelen az információs társadalomban, a hacktivista tevékenységek mögött általában valamilyen ideológiai megfontoltság, cél közvetítése áll, továbbá gyakran reagálnak politikai eseményekre is. Módszerük általában a weboldalakat megbénító túlterheléses támadás. [85 pp. 179-202]

A kémkedés elsősorban katonai információk megszerzésére irányul, azonban a kiberkémkedés célja az ipari, pénzügyi, diplomáciai információk megszerzése és felhasználása, kifinomult és rejtett támadások végrehajtása, információs rendszerekben tárolt adatok megszerzése állami és piaci szereplők ellen. [73]

A társadalom valamennyi tagja számára elérhető digitális technológia nyújtotta lehetőségek kiberbiztonsági kockázatot jelentenek, mert a kibertérbeli fenyegetések zavarják az infokommunikációs rendszerek és a kormányzati gerinchálók működését továbbá veszélyeztetik a kritikus infrastruktúra elemeit és a nemzetállamok információs vagyonát.

Az államilag támogatott kibertámadások jelentik napjaink egyik leghangsúlyosabb biztonsági kihívását. A kiberhadviselés előzménye az elektronikai hadviselés. A kiberhadviselésben a klasszikus ország-ország elleni háborús modellt felváltják az egyéni vagy kiscsoportos informatikai támadások. Ebben a hadviselési formában az egyéni elkövetők sikeres támadást tudnak véghez vinni akár egy régió, ország ellen, aránytalanul nagy károkat és veszteséget okozva. A jövőre vonatkozóan a kibertámadások mellett

továbbra is számolhatunk fizikai támadásokkal a klasszikus műveleti területeken, azonban egyre dominánsabbak lesznek a kibertérben zajló információs konfliktusok. A két hadviselési forma párhuzamos jellege azért veszélyes, mert egy összehangolt fizikai és kibertérbeli támadás teljesen megbéníthatja egy fejlett ország közigazgatását, energiaszolgáltatási rendszerirányítását, a pénzügyi és gazdasági életben zajló kommunikációt. [86 pp. 131-148]

A fentiek okán érdemes vizsgálni a kibertérben zajló konfliktusok katonai biztonság vetületeit is. Alapvetően az információs és a fizikai térbeli hadviselés is ugyanazon az elven működik, vagyis a cselekményt megelőzi egy klasszikus felderítő munka, az adat-információszerzés, majd az információfeldolgozás- és értékelés. A kibertérbeli célpontok kijelölése jóval több időt vesz igénybe, mint a konkrét támadás, amely nagyon rövid idő alatt zajlik le. A kiberfegyverek olyan eszközök, amelyek informatikai vagy információs sérülékenységet képesek okozni.

A kibertérben zajló támadások legtöbbször a kiberterrorizmusban nyilvánulnak meg. Ahhoz azonban, hogy ezt elemezzük szükséges párhuzamot vonnunk a hagyományos és kiberterrorizmus között. A hagyományos terrorizmus, vagyis az öngyilkos merénylők, nemzetközi terrorszervezetek, és az általuk végrehajtott terrorcselekmények, valamint a kiberterrorizmus között számos azonosság van és párhuzamosságuk aránytalanul nagy károkat tud okozni. A hagyományos terrorizmus először az 1970-es években jelent meg, majd a 2001. szeptember 11. napi terrortámadások újra felhívták a figyelmet a fontosságára. Ekkor vált egyértelművé, hogy a hidegháborút követően a nagyhatalmak szembenállása mellett a legnagyobb veszély a nemzetközi színtereken megjelenő terrorizmus. A terrorizmus célja az erőszak és a pánikkeltés, éltetője pedig a média, kulcseleme a nyilvánosság. Minél több *social media* platformot ér el egy-egy terrorakció, annál nagyobb félelmet tud kelteni a lakosságban. A terrorista csoportok és terrorszervezetek is használják és alkalmazzák az információtechnológia eszközeit, platformjait. A terroristák az internet segítségével, titkosított csatornákon, vagy titkosított üzenetváltással tudják megszervezni a támadásokat. A terrorszervezetek az interneten toboroznak tagokat a csoportjaikhoz, továbbá az internetes keresőprogramokkal számtalan házi-készítésű terrorfegyverként alkalmazható eszköz videója is elérhető számukra. A *social media* platformok – a lakosság információ-tudatosság hiánya miatt – mindenki számára könnyen és nyíltan elérhető információkat adnak az esetleges célpontokról. [87 pp. 51-68]

A kiberterrorizmus fogalma a szeptember 11. napi terrortámadásokat követően került meghatározásra. Kovács László nyomán Denning szerint *„a kiberterrorizmus számítógép alapú támadást vagy fenyegetést jelent, amelynek célja, hogy megfélemlítsék, vagy kikényszerítsék a kormányok vagy a társadalmak részéről az adott terrorszervezet politikai, vallási, vagy ideológiai céljainak elérést."* [22 p. 26]

A kiberterroristák az elérni kívánt cél alapján két csoportra oszthatók. Az első csoportba tartozók a propaganda tevékenység, toborzás és adatszerzés céljából használják az információtechnológia adta lehetőségeket, ők a *soft* vagyis puha típusú kiberterrorizmus képviselői. A második csoportba tartozók pedig a *soft* tevékenységeken túl erőszakos, vagyis *hard* tevékenységeket is végrehajtanak az internet segítségével, ez azt jelenti, hogy az interneten túl azok a kritikus információs infrastruktúra rendszerek is a terroristák célpontjai közé tartoznak, amelyek információtechnológiai és/vagy fizikai támadásokkal sújthatóak. A kiberterroristák – a kiberbűnözőkhöz hasonlóan – rosszindulatú programokat és egyéb informatikai támadási módszereket használnak. [88]

Mindent összevetve, kiberbűnözés, a hacktivizmus, a kiberkémkedés, a kiberhadviselés és a kiberterrorizmus valós fenyegetésként van jelen, és a rohamos technológiai fejlődés következtében egyre szélesebb körben terjed a kibertérbeli támadásokhoz szükséges tudás, és az eszközök elkészítéséhez szükséges forrás az infokommunikációs eszközök használatával.

2.5 Kiberbiztonság és kibervédelem Magyarországon

Az emberiség technológiai szintje rohamos fejlődésének következményeként új lehetőségek és kihívások jelennek meg, amelyek meghatározzák hazánk biztonságát, ilyen a kiberbiztonság. A kibertámadások, mint országokat, nemzetközi és világszervezeteket, a kormányzatot és a gazdasági élet szereplőit ért támadások, a 21. század legjelentősebb biztonsági kihívásai közt szerepelnek. A digitalizáció következtében minden elérhetőbbé válik a társadalom tagjai részére. Napjainkban komoly igény mutatkozik arra, hogy a városok és falvak intelligensebbek legyenek, és képessé váljanak arra, hogy hatékonyan kezeljék az urbanizáció kihívásait, valamint sikerrel alkalmazkodjanak az új helyzetekhez és a felmerülő kérdések kapcsán adekvát válaszokat adjanak. Ezért a DJP 2.0-ban külön hangsúllyal szerepel az Okos Város (Smart City) fejlesztések témaköre azzal a céllal, hogy a települések mindennapi életébe olyan okos megoldások épüljenek be, amelyek könnyebbé, élhetőbbé és biztonságosabbá teszik az ott élő emberek életét. Egy település vezetésének is alapvető feladata mind a településen

élők és környezetük biztonságának megteremtése, mind az irányítása alatt működő intézmények, vállalatok vagyonának megőrzése. Az okos biztonsági rendszerek kiépítésével mindezen célok megvalósíthatóak. A rendszerek összekapcsolásának és kiépítésének alapvető feltétele a hálózatok biztonságának garantálása. A kibertérben elkövetett támadások sok esetben visszafordíthatatlan politikai vagy gazdasági károkat okozó cselekmények. [89]

Magyarországnak képesnek kell lennie a kibertérbeli fenyegetések felismerésére és kezelésére, a kiberbiztonság kiépítésére, a kritikus információs infrastruktúra zavartalan működésének biztosítására, a támadások elhárítására és a kibervédelmi feladatok ellátására. Az infokommunikációs rendszerek elleni támadások száma folyamatosan nő, így szükséges azok védelmének erősítése, valamint a felhasználók információbiztonsági szintjének növelése. [90 pp. 205-217]

A kiberbiztonság a terrorizmushoz hasonlóan nem ismer határokat, és a globalizáció hatására egyre inkább terjed. A számítástechnikai rendszerek működtetik a társadalmakat. A tudomány és technológia mindenki részére elérhetővé válik, ezért számolnunk kell a váratlan, kibertérben történő támadásokkal. Megfelelő módon szükséges védekezni a kibertérben bekövetkező támadások ellen, mint például az információs és kommunikációs rendszerek, vagy a kormányzati gerincháló rendeltetésszerű működésének megzavarása. Kiemelkedő hangsúlyt kell fektetni a kibervédelemre és a nemzetközi kritikus infrastruktúra biztosítására. [91 pp. 302-311]

2020 tavaszán jelent meg az új NBS, amely az alábbiak szerint rendelkezik az új biztonsági kihívásokkal való fellépésről, különösképpen a digitalizáció és a kibertér vonatkozásában: [62]

Magyarország biztonsági helyzete stabil, melyet a NATO és EU tagságunk tovább növel, azonban az új kihívások negatív hatást gyakorolnak a biztonsági környezetünkre. kihívások fő elemei közé tartozik a globális közjavak újraelosztása, a klímaváltozás, a migrációt kiváltó okok és következmények, a túlnépesedés, az erőforrások szűke, a szélsőséges vallási irányzatok, a terrorizmus, a technológiai forradalom, a fokozódó digitális és pénzügyi sérülékenység. A globalizáció következtében egyre nagyobb teret kap az aszimmetrikus és hibrid hadviselés, amely során állami és nem állami szereplők katonai és nem katonai eszközök alkalmazásával érvényesítik érdekeiket. A hatalmi vetélkedés a globális közjavakat is érinti: a nemzetközi vizek és erőforrásaik, az északi sarkvidék, a világűr, a kibertér vonatkozásában fokozódik a küzdelem. A globális technológiai fejlődés következtében a digitalizáció, a tömeges adat, az 5G, az

űrtechnológia és az MI alkalmazása olyan új lehetőségeket és kihívásokat jelent, amely hatással van az ország biztonságára.

A nemzetközi, politikai, gazdasági és legfőképp a technikai és technológiai változások hatására a biztonság jelenti az országok és a szövetségek számára az egyik legfontosabb tényezőt. Az információ továbbá az információszerzés, rendszerezés, feldolgozás és elosztás kapcsán érdekelt (kritikus) információs infrastruktúrák a 21. században a legfőbb meghatározói a biztonságnak. Mindezek alapján a kritikus infrastruktúrák védelme és biztonságos üzemeltetése jelenti a legnagyobb és legfontosabb kihívást az országok, nemzetek számára. [92 pp. 15-22]

Az információs infrastruktúrák (közműszolgáltatások, gazdasági élet, közigazgatás) a kritikus infrastruktúrák részeként áthatják a mindennapjainkat. Az információs infrastruktúrák védelme mára már nemzetközi kérdés, mert az információs társadalom kiépítése és fejlesztése jelen van számos országban, régióban, kontinensen egyaránt. Az információs infrastruktúrák rendszere alapvető feladatokat lát el: nélkülözhetetlen javak előállítása, szállítása, szolgáltatások folyamatos biztosítása. Ezek a rendszerek összeköttetést és együttműködést teremtenek és biztosítják a közbiztonságot, fenntartják az ország külső biztonságát. Az MH és a HM feladatai közé tartozik a kritikus infrastruktúrák kiépítése és védelme. Éppen ezért nemzeti és nemzetközi szinten is érdemes vizsgálni a hadseregek feladatát a kritikus infrastruktúrák védelme és a kiberbiztonság kiépítése során. [93]

A hibrid támadásokkal szemben a honvédelmi és a rendvédelmi erők a civil infrastruktúrával együttesen képesek felvenni a küzdelmet. Az új biztonsági kockázatok, köztük a kiberhadviseléssel és az információ áramlást elősegítő technológiai fejlődéssel szemben úgy tudunk védekezni, ha adaptáljuk a megfelelő rendszereket és fejlesztjük az eszközeinket. Ezáltal elérhetőek a kapacitásfejlesztések – a Kormány támogatásával – hazánk kiberbiztonsága érdekében. A technikai fejlesztések és felzárkózás kiemelten fontosak tekintettel arra, hogy a technológiai fejlődés következtében rohamosan nő az infokommunikációs rendszerek elleni támadások száma, amely veszélyt a felhasználók információbiztonsági tudatosságának alacsony szintje csak tovább eszkalál. Fentiek okán nemcsak az eszközeink, képességeink fejlesztése, hanem a felhasználói tudatosság növelése is szükséges. [94]

A kibertér mellett a nemzetközi vizek és erőforrásaik, az északi sarkvidék és a világűr feletti dominanciáért is folynak a hatalmi harcok. A kibertér ma már az óceánok és tengerek, a légtér és a világűr és a szárazföld mellett külön műveleti térnek számít. Nagy

valószínűséggel a jövő konfliktusai egyre inkább a kibertérben fognak kicsúcsosodni. [95 pp. 101-108]

A stratégiai közös terekben a digitalizáció és globalizáció hatására olyan új kihívásokkal kell szembe néznünk, mint az 5G által megjelenő technológiai és forradalmi fejlesztések és az űrtechnológia. Azért fontos, hogy a nemzeti biztonsági és katonai rendszereink a növekedés ütemében folyamatosan felzárkózzanak és az élen járjanak az új biztonsági kockázatok azonosításában, mert az ilyen léptékű fejlesztések hatással vannak/lehetnek a társadalmunkra és a gazdaságunkra egyaránt. [96 pp. 2665-2674]

A nemzetközi biztonságpolitikát ért változások, mint a nem állami szereplők: szervezett bűnözői csoportok; nemzetközi terrorszervezetek; kiberbűnözői szervezetek; szélsőséges vallási közösségek; magántulajdonban lévő biztonsági cégek; és egyéb nem kormányzati szereplők súlyának növekedése mind hatással vannak hazánk biztonságpolitikájára. Ez azt jelenti, hogy a kiberteret kritikus adatok megszerzésére és károkozásra egyaránt használják különböző államok és nem állami szereplők. [97 pp. 140-150]

A globalizáció hatására növekvő technológiai fejlődés a digitalizáción alapszik. Az információs rendszerek sérülékenysége új biztonsági kihívásként van jelen. A kibertérben elkövetett rossz szándékkal vezérelt cselekmények száma egyre növekszik, módszerüket tekintve kifinomultabbak és egyre nagyobb károkat okoznak. Nagy kockázatot rejt magában az információk tömeges rendelkezésre állása, amelyek információtechnológiai kihívásként jelentkeznek, azonban az információkhoz való hozzáférés hazánk számára is egyelőre csak részlegesen biztosítható. Ezért a gépi tanulás által támogatott folyamatok bevezetése nem várat tovább magára. [98 pp.55-66]

Az űrtechnológia rohamos fejlődése által a technológiákat jelentősen alkalmazók és a felzárkózók között egyre nagyobb technológiai rés képződik. Hazánknak kiemelt szerepet szükséges betöltenie az űrtechnológiák ismeretében és alkalmazásában, mert ezek használata meghatározóvá válhat a fejlettségi, gazdasági mutatók, valamint a politikai érdekérvényesítés kapcsán. [99 pp. 153-165]

Az új biztonsági kihívások következtében keletkező kiszámíthatatlanságot tovább fokozza a tömegpusztító fegyverek és hordozóeszközeik proliferizációja. Terrorszervezetek, terroristacsoportok és különböző bűnszervezetek is birtokolnak és alkalmaznak tömegpusztító fegyvereket. Az ilyen eszközökkel kezdeményezett támadások elhárítása hagyományos módszerekkel többnyire eredménytelen, ezáltal kiemelt veszélyforrásként szükséges kezelni őket. [53 pp. 194-201]

Magyarországnak érdeke a hibrid hadviselés elleni küzdelem mind nemzeti, mind szövetségesi kereteken belül. A kibertámadó képességek célja lehet a stratégiai elrettentés. A nyilvánosságra hozott képességek azonban veszélyt hordozhatnak magukban, ezért a kibertámadó képességek stratégiai dokumentumban történő megjelenítése bizonyul az elrettentés színterének. [81 pp. 187-204] Az NBS-ben megfogalmazott elrettentés szerint hazánk a kárt okozó és biztonságot fenyegető kiberképességeket fegyvernek, azok alkalmazását agresszióként értelmezi, ennélfogva lehetségesnek tartja – a bevonásra kerülő kormányzati szervek jóváhagyásával és előzetes egyetértésével – a fizikai térben történő válaszadást. Kiemelt figyelmet fordítunk a K+F-re, különös tekintettel a kibervédelem, az MI, az autonóm rendszerek és a biotechnológia terén, mert hazánk stratégiai kérdésként kezeli a forradalmi technológiák fejlesztését. [62]

Magyarország biztonsági kihívásaiként azonosíthatjuk a kormányzati rendszerek, az E-közigazgatás, a kritikus infrastruktúra és kritikus információs infrastruktúra valamennyi eleme, az állami és nem állami cégek és szervezetek rendszerei ellen irányuló kibertámadásokat. [100]

Ahhoz, hogy hazánk képes legyen felvenni az új biztonsági kihívásokkal a küzdelmet különös tekintettel a kibertérre szükséges a honvédségnek jól felszerelt és megfelelően kiképzett erőkkel, hatékony, telepíthető és fenntartható képességekkel rendelkeznie a mennyiségi helyett a minőségi képességfejlesztés jegyében. Ez azt jelenti, hogy a honvédség hagyományos feladatai kiegészülnek az olyan új biztonsági kihívásokkal, mint a koronavírus járvány, a tömeges irreguláris migráció, a terrorveszély, a hibrid támadások és a katasztrófa helyzetek kezelése. Mindezek tükrében a haderőfejlesztését úgy kell véghez vinni, hogy rendelkezzen valamennyi hadszíntéren jelentkező kihívás leküzdéséhez szükséges képességgel. A fegyveres erők szempontjából fontos a haderő műveleteinek kibertérbeli támogatása, ezért szükséges a honvédség kibervédelmi és kiberműveleti erőinek tervszerű fejlesztése. [39]

A kibervédelmi feladatok kezelésére, a kiberbiztonság fenntartására és a kritikus infrastruktúra megfelelő működésének biztosítására hazánk a következőképpen intézkedik:

- kibertérben megjelenő kihívások, kockázatok és fenyegetések azonosítása és nyomon követése;
- a kormányzati koordináció összehangolása;
- a kibertér jogi szabályozásának fejlesztése;

- a felhasználói tudatosság erősítése;
- a kormányzati infokommunikációs rendszerek, a nemzeti kritikus információs infrastruktúra, a nyílt- és minősített adatok információvédelme és a nemzeti adatvagyon védelmének erősítése, valamint a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése;
- hazai bázisú K+F erősítése;
- partnerség kialakítása az állami és nem állami szereplők, valamint az oktatási-tudományos intézmények és felhasználók között;
- A hibrid támadások elleni küzdelmet a megelőzés, a felderítés, a hírszerzés és az elhárítás eszközeit az állami szereplők együttműködésére alapozva szükséges alkalmazni;
- A kibertérbeli kockázatok azonosításához és a kihívások kezeléséhez szükséges a nemzetközi együttműködésben aktívan részt vennünk. [62]

Magyarország kiberbiztonságának kiépítése céljából azonban nemcsak a hazai, hanem a nemzetközi szerepvállalásainkat is szükséges megemlíteni.

Magyarország alapító tagként vesz részt az állandó strukturált együttműködés, Permanent Structured Cooperation (a továbbiakban: PESCO) [101] projektjében, amelynek egyik első lépése a Kiber és Információs Domain Koordinációs Központ, Cyber and Information Domain Coordination Center (CIDCC) létrehozása. [102] A PESCO az EU egyik állandó együttműködési keretrendszere, aminek részeként alapvetően védelmi típusú projekteket, kezdeményezéseket támogatnak. Az Európai Védelmi Ügynökség, European Defence Agency (EDA) szervezésében számos ilyen projekt működik már. A PESCO-projekt legfontosabb célja egy olyan kiber- és információs tér, információmegosztó központ felállítása, amely az EU-s katonai műveletek helyszínén, illetve annak térségében egy közös kiber-helyzetképet állít elő. Ehhez a kezdeményezéshez alapító tagként csatlakoztunk. [103 pp.71-84]

Magyarország elkötelezett aziránt, hogy 2030-ra Európa öt és a világ tíz legbiztonságosabb országához tartozzon. A fenti cél elérése érdekében kiemelt hangsúlyt fektetünk a közbiztonság garantálására és a korszerű haderőfejlesztésre, az exportképes hazai védelmi ipar bevonásával. A haderőfejlesztés hozzájárul alapvető értékeink és érdekeink védelméhez és az euroatlanti biztonság jövőbeni hozzájárulásához. A biztonsági tényezők megállapításánál a NATO és az EU stratégiai dokumentumai az irányadóak. Valamennyi kihívás hatékony kezeléséhez többnemzeti és globális

együttműködés szükséges. A globális és európai ügyeket meghatározó biztonsági együttműködése fórumok, így az ENSZ, az EBESZ és az ET hazánk nemzeti érdekérvényesítésének elsődleges és kulcsfontosságú szereplői. Az MH az ország szuverenitását és területi integritását biztosítja, nemzetközi szerepvállalásainak köszönhetően pedig a külpolitika jelentős intézménye. az MH biztosítja a haza védelmét, hozzájárul a transzatlanti kapcsolatok és az európai biztonság erősítéséhez. [62]

Összegzésképp megállapítom, hogy a kiberbiztonság és kibervédelem kiépítése céljából Magyarország szempontjából ugyanolyan súllyal jelenik meg a hazai szabályozás, mint a nemzetközi szerepvállalás.

2.6 Részösszefoglalás

A problémafelvetés tükrében az értekezés második fejezetének hipotézise az volt, hogy ha a digitalizációt, mint az egyetlen technológiai faktort vizsgálom, akkor ez az egyik leghangsúlyosabb biztonsági kihívás azért, mert leginkább ez kapcsolódik az emberhez továbbá ez van hatással leginkább a mai modern világ fejlődésére, ez van hatással Európa, és benne Magyarország biztonságára, hiszen a gazdasági, technológiai fejlődés mellett erre épülnek a haditechnikai, katonai fejlesztések is. Ennek következtében nőnek a technikai, informatikai rendszerek és kibertérbeli kockázatok is. Ezért Magyarországnak képesnek kell lennie a kibertérbeli fenyegetések felismerésére és kezelésére, a kiberbiztonság kiépítésére, a kritikus információs infrastruktúra zavartalan működésének biztosítására, a támadások elhárítására és a kibervédelmi feladatok ellátására. Az infokommunikációs rendszerek elleni támadások száma folyamatosan nő, így szükséges azok védelmének erősítése, valamint a felhasználók információbiztonsági szintjének növelése. [62]

A hipotézis igazolása érdekében a második fejezetben vizsgáltam a kibertér és kiberbiztonság alapvetéseit; elemeztem és értékeltem a kibertér vonatkozó hazai és nemzetközi doktrínáit különösképpen a NATO megközelítéséből; áttekintettem a kiberbiztonság, a kiberműveletek és a kibertérbeli fenyegetések általános jellemzőit, különös tekintettel a kiberbűnözésre, a hacktivizmusra, a kiberkémkedésre, a kiberhadviselésre és a kiberterrorizmusra; végül feltártam a kiberbiztonság és kibervédelem magyarországi helyzetének katonai, honvédelmi vetületeit.

Összegzésképp megállapítottam, hogy a jelenlegi, instabil biztonsági környezetben a biztonságra ható tényezők és kockázatok, veszélyforrások változnak. Ez azt jelenti, hogy a gazdasági, pénzügyi, társadalmi, kulturális, vallási, környezeti, közbiztonsági,

migrációs gondokon túl a digitalizáció következtében szembe kell néznünk a technikai, informatikai rendszerek és ezzel együtt a kibertérbeli kockázatok növekedésével. A digitalizáció hatására a társadalmi folyamatok jelentős részéhez használjuk a kiberteret, ennek következtében a kiberbiztonsági kihívások dinamikus és folyamatos növekedése tapasztalható, ezért a kiberbiztonsággal foglalkozó szervezetek tevékenysége is fokozódik, ezzel hozzájárulva a kihívások mielőbbi felismeréséhez és az ellenük történő eredményes fellépéshez.

A NATO a *Global Common* projekt keretében közel 20 éve felismerte azt, hogy a hadsereg digitalizációja és fejlesztése elengedhetetlen az új biztonsági kihívásokkal való szembenézés sikeressége érdekében. Az állami, katonai, nemzeti biztonsági rendszereknek ezért szükséges digitálisan felzárkózniuk, a nemzetállamoknak pedig a stratégiai dokumentumaikat szükséges az új biztonsági kockázatokhoz mérten felülvizsgálniuk.

A kiberbűnözés, a hacktivizmus, a kiberkémkedés, a kiberhadviselés és a kiberterrorizmus valós fenyegetésként van jelen, és a rohamos technológiai fejlődés következtében egyre szélesebb körben terjed a kibertérbeli támadásokhoz szükséges tudás, és az eszközök elkészítéséhez szükséges forrás az infokommunikációs eszközök használatával.

Ahhoz, hogy hazánk képes legyen felvenni az új biztonsági kihívásokkal a küzdelmet különös tekintettel a kibertérre szükséges a honvédségnek jól felszerelt és megfelelően kiképzett erőkkel, hatékony, telepíthető és fenntartható képességekkel rendelkeznie. A fegyveres erők szempontjából fontos a haderő műveleteinek kibertérbeli támogatása, ezért szükséges a honvédség kibervédelmi és kiberműveleti erőinek tervszerű fejlesztése.

A kiberbiztonság kiépítése céljából Magyarország szempontjából ugyanolyan súllyal jelenik meg a hazai szabályozás, mint a nemzetközi szerepvállalás. A digitalizáció és a digitális átalakulás a globalizáció hatására jelen van az egész világban, ezért Magyarországnak és az MH-nak is rendelkeznie kell azzal a képességgel, hogy a kibertérbeli fenyegetéseket felismerje és kezelje, a kiberbiztonságot kiépítse, a kritikus információs infrastruktúra zavartalan működését biztosítsa, a támadásokat elhárítsa és a kibervédelmi feladatokat – alaptörvényi kötelezettségének megfelelően – maradéktalanul elvégezze.

3 AZ MH DIGITALIZÁCIÓJA A ZRÍNYI 2026 TÜKRÉBEN

Az értekezésben megállapított, Európát és ezáltal Magyarországot is fenyegető új biztonsági kihívások új megoldásokat, kezelési lehetőségeket indukálnak. Véleményem szerint a digitalizáció napjaink legmeghatározóbb technológiai biztonsági kihívása.

A digitális robbanás időszakában az új biztonsági kihívásokkal való sikeres fellépés érdekében elengedhetetlen a hadsereg modernizációja, amelyet a Zrínyi 2026 keretében a HM az MH-val szorosan együttműködve 2017-ben kezdett el megvalósítani. [49]

A Zrínyi 2026 célkitűzései között szerepel az MH áttérése és felzárkózása az informatikai, digitális- és hálózatalapú katonai rendszerekhez.

Az értekezés harmadik fejezete a következő kérdések vizsgálatának eredményét rögzíti:

- Az új biztonsági kihívások következtében szükséges-e az MH modernizációja? Milyen fejlesztésekkel, átalakításokkal, modernizációval, képességekkel szükséges a honvédség feladatainak kibővítése?
- Mely beszerzések és képességfejlesztések valósultak meg a légierő- és a szárazföldi erők modernizálása érdekében? Hogyan definiálhatjuk a további célokat?
- A Zrínyi 2026 beszerzései hozzájárulnak-e a honvédség digitalizációjához és digitális platformra állításához?

A problémafelvetés tükrében a harmadik fejezet hipotézise, hogy ha a honvédelmi, katonai és nemzeti biztonsági rendszerek hazai digitális hálózatba beágyazódnak, akkor a békeidőben megfelelően működő katonai informatikai, digitális- és hálózatalapú rendszerek képesek lesznek önállóan működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő különleges jogrendben is. [1 pp.122-145]

A Zrínyi 2026 fejlesztési és modernizációs törekvéseinek összehangolása elengedhetetlen az MH digitalizációjával. A problémafelvetés tükrében a harmadik fejezetben vizsgálom az MH feladatait az új biztonsági kihívások tekintetében, azokat a haderőfejlesztési és digitális platformokat, amelyek mentén a Zrínyi 2026 lefekteti az MH digitalizációja és modernizációja érdekében tett cél- és eszközrendszerét. Elemzem és értékelem a légierő és a szárazföldi erők modernizálása érdekében már beszerzett és a még beszerzés alatt álló eszközöket, képességeket és digitális fejlesztéseket.

3.1 Az MH feladatai az új biztonsági kihívások tükrében

A 21. századi műveleti környezet változásainak következtében, a negyedik generációs vagy hibrid hadviselés kora a honvédség számára is új kihívásokat generál, melynek következtében az MH szerepe a honvédelem rendszerében új feladatokkal bővült ki, amelyeket a 2021 nyarán elfogadott új NKS az alábbiak mentén határoz meg. [104]

A cél, hogy az MH a kor követelményeihez igazodva, szemléletben, szervezeti kultúrában és haditechnikát tekintve megújult, szervezett, a nemzeti hagyományokat és értékeket szem előtt tartva, önállóan és nemzetközi szövetségesi keretek közt alkalmazható, önkéntes tartalékos rendszerrel rendelkező haderővé váljon, ezáltal képes legyen – az új biztonsági környezet kihívásaihoz alkalmazkodva – a nemzetközi válságkezelő, békefenntartó hadműveletekben való részvételre, így biztosítva hazánk önerőn és kollektív szövetségesi kapcsolatokon alapuló védelmét. A honvédségnek korszerű felszereléssel, megfelelően kiképzett katonákkal, rugalmas alkalmazkodókészséggel, hatékony, telepíthető és fenntartható képeségekkel kell rendelkeznie. A korszerű haderő kialakításához szükséges a védelmi ipar fejlesztése. A fenti célok eléréséhez a Zrínyi 2026 járul hozzá. [39]

Az MH-nak igazodnia kell az új biztonsági fenyegetésekhez, kockázatokhoz és kihívásokhoz, a klasszikus katonai képességek megtartásával együtt. Jelen fejezet meghatározza a körülményeket, amelyek az új biztonsági kihívások kezelése érdekében újraértelmezik és kibővítik az MH feladatait.

Az új feladatok végrehajtása érdekében a Zrínyi 2026 keretein belül az MH létrehozza a katonai erőt és kialakítja a nemzeti önerő fenntartásához szükséges hadiipari körülményeket. A honvédelmi és haderőfejlesztési program és a változékony biztonsági környezetben kialakuló új biztonsági kihívások hatására megváltozik a 21. századi műveleti környezet. Az új kihívások és új műveleti terek új képességek elsajátítását igénylik, amelynek elengedhetetlen részét képezi a hadiipar kapacitásfejlesztése.

A megújuló MH különös figyelmet fordít a meglévő képességek fejlesztésére és az új képességek kialakítására az ország szuverenitásának, területének és állampolgárainak védelme érdekében. A haderőfejlesztés következtében fokozódik a nemzeti önerő, ugyanakkor az önvédelmi és az elrettentési képesség fenntartása érdekében továbbra is hatékonyan hozzá kell járulnunk a regionális, európai és transzatlanti biztonsági erőfeszítésekhez. Hazánk biztonságának sarokköve a NATO által biztosított kollektív védelem, amelyhez szintén elengedhetetlen a nemzeti önerőnk fejlesztése.

Az NKS kitűzött célja, hogy az MH 2030-ra a NATO tagjaként képessé váljon az ország biztonságának garantálására, az agressziók elrettentésére, a katonai és nem katonai jellegű kihívások és fenyegetések elleni összkormányzati védekezés támogatására és a szövetségesi és EU-s tagságból fakadó feladatai ellátására. A célok megvalósításához a Zrínyi 2026 biztosítja a keretet. Az ország katonai biztonságának garantálása több pilléren nyugszik. Az egyik pillért a nemzeti önerő fejlesztése, a másik pillért a NATO által garantált kollektív védelem, az EU által biztosított kölcsönös segítségnyújtási klauzula, az ENSZ és az EBESZ keretein belüli együttműködés adja. Az ország védelmét a katonai, gazdasági, politikai, társadalmi környezeti, kiber és információs dimenziók alkotják. A biztonsági kihívások hatékony kezelése összkormányzati együttműködést igényel. Az NKS-ben kifejtésre kerülnek azok a célok és eszközök, amelyek mentén az MH korszerű, fenntartható, rugalmas és hatékony képességekkel, korszerű struktúrával rendelkező haderővé válhat. [39]

Az MH műveleti részvételei hozzájárulnak a Magyarország és szövetségesei közti biztonság erősítéséhez. A magyar katonai hozzájárulás nemzetközi felhatalmazás alapján a közös értékek és érdekek mentén történik.

A honvédségnek rendelkeznie kell azzal a képességgel, hogy egy esetlegesen bekövetkező fegyveres támadást elrettentsen, annak bekövetkezése esetén pedig az ország védelmét biztosítsa akár önállóan is, a szövetségesi segítség megérkezéséig. Magyarországnak és az MH-nak készen kell állnia a szövetségesi vagy EU-s feladatok ellátására külföldön és belföldön egyaránt. A honvédség vezetési-irányítási rendszerének megzavarása esetén a károkozó ellenséges kiberképességeket fegyvernek, és alkalmazásuk esetén fegyveres támadásnak tekintjük, ezért a katonai válaszadás lehetősége biztosított. A hazánkat és/vagy a környező országokat sújtó tömegpusztító fegyverek alkalmazása esetén szükséges a honvédség képességeinek bevetése. A hazánkat esetlegesen érő hagyományos, nukleáris és kettősképességű rakétarendszerek által indított támadásokkal szembeni védelem szövetségesi keretek között biztosított. Az új biztonsági kihívásokból eredő fenyegetettségek ellen a honvédség – önállóan vagy koalíciós keretek közt – védelmet nyújt az alábbi színtereken: válságkezelési műveletekben való részvétel; radikális ideológiák és az Európában terjedő terrorizmus elleni küzdelem; irreguláris migráció tömeges megjelenése elleni fellépés, koronavírus járvány kezelése; klímaváltozás hatására kialakuló természeti katasztrófák és egyéb ipari katasztrófák kezelése. [105]

A 21. századot érintő globális folyamatok, és az ezekből eredő új biztonsági kihívások következtében az MH szerepvállalása felértékelődik. Az új biztonsági kihívások: a regionális konfliktusok; tömegpusztító fegyverek és hordozóeszközeik elterjedése, a terrorizmus, a pénzügyi biztonság, a kiberbiztonság; az energiabiztonság; a globális éghajlat- és környezetváltozás; a természeti és ipari katasztrófák; a szervezett bűnözés, a kábítószer-kereskedelem, és a migráció Magyarországot is elérik. A honvédségnek képesnek kell lennie a hagyományos és hibrid fenyegetések elleni fellépésre, a nemzeti ellenálló képesség növelésére, a honvédelmi szempontból kiemelt létfontosságú rendszerelemek, létesítmények őrzés-védelmére, a civil és rendvédelmi szervek támogatására és a velük való együttműködésre. Fokozott figyelmet kell fordítani a katonai hírszerzés és elhárítás működése hazai és szövetségesi keretek között. A biztonság nem katonai jellegű fontossága egyre nő, de ez nem jár a katonai tényezők szerepének csökkenésével. Magyarország haderejének így a hagyományos és az új kihívásokkal is szembe kell néznie, mert a globális biztonsági környezet dinamikus változásaiból következően nem zárható ki, hogy egy regionális konfliktus kezelése során Európa térségében, így hazánknak is katonai erőt kell bevetni. Ugyanakkor az új biztonsági kihívásokat egyéni, kormányzati, nem kormányzati és transznacionális szinten is kell kezelni, így ez a folyamat összkormányzati együttműködést igényel.

A 21. századi nem állami szereplők által jelentkező kihívások kezeléséhez az MH a konfliktusok keletkezési helyén, a válságkezelési műveletekben történő részvétellel járul hozzá. Ilyen fenyegetést jelentenek az Európa-szerte terjedő radikális ideológiák és terrorizmus, a forradalmi technológiák illetéktelenekhez való kerülése következtében végrehajtott nemzeti biztonság elleni támadások és terrorcselekmények. A tömeges, irreguláris migráció ellen az MH a rendvédelmi szervekkel karöltve lép fel. Az ilyen jellegű migrációt kiváltó okok kezelése nemzetközi koalíciós keretek között történhet. A COVID-19 járvány és a klímaváltozás okán kialakuló természeti katasztrófák kezelésében és enyhítésében az MH a továbbiakban is kulcsfontosságú szerepet tölt be. [106]

Az új biztonsági kihívások globalizációja következtében a gyakran változó biztonsági helyzet miatt a katonai hírszerzés és az elhárítás szerepe felértékelődik, a fokozott műveleti tempó és a műveleti igénybevétel csökken. A média közvetítésével a műveleti döntések politikai jellegűek lehetnek. Az aszimmetrikus kihívások – amelyek halálos áldozattal nem járnak, de nagy anyagi károkat képesek előidézni – következtében felülíródott a háború és a támadás fogalmának jelentése. A technológia fejlődésének

következtében új képességek és fegyverrendszerek jelennek meg, amelyek átalakítják a korábbi hadviselés jellegét. Egy nem fegyverrel elkövetett támadás azonban képes akkora kárt okozni, mint egy fegyverrel elkövetett klasszikus támadás. Az MH-nak ezért fel kell készülnie a kinetikus és nem kinetikus támadásokra és a hibrid fenyegetésekre is. Ennek érdekében elengedhetetlen a nemzeti reziliencia fenntartása és további biztosítása. A hagyományos és hibrid fenyegetések elleni fellépés, a nemzeti ellenállóképesség növelése, a honvédelem szempontjából érintett kritikus rendszerelemek és objektumok, létesítmények őrzés- védelme, a civil szervezetekkel való együttműködés és a rendvédelmi szervek munkájának támogatás és a katonai hírszerzés és elhárítás működése mind a honvédség új feladatait képezik. [107 pp. 104-118]

Az MH megfelelő működéséhez szükséges az anyagi- és a humán erőforrások megfelelő biztosítása. Korunk új biztonsági kockázataival szemben akkor tudunk eredményesen fellépni, ha a nemzeti önerő fejlesztését a honvédek képzése, kiképzése, fizikai és pszichikai állóképességük fejlesztése határozza meg. Az MH korszerűsítéséhez hozzájárul a katonák nemzetközi műveletek által szerzett tapasztalatainak felhasználása. A Magyarországon működő önkéntes tartalékos rendszer szintén segíti a képességek növelését. Az MH képességeit az Alaptörvény, a származtatott törvények, valamint a szövetségesi erők és a működési környezet összefüggései együttesen határozzák meg. A honvédségnek képesnek kell lennie a szövetségesekkel együttműködve olyan haderőként működni, amelynek szervezete biztosítani tudja az ország fegyveres védelmét, és az alapképességek fejlesztését a rendelkezésre álló nemzetgazdasági forrásokból. [39]

A jövő hadereje egy korszerű, magas fokú mobilitással és reagáló képességgel felvértezett szervezet, amely képes a folyamatos fejlődésre és innovációra, feladatait önállóan és szövetségesi keretek közt is magas szinten tudja végrehajtani. A honvédség képességei modulárisan épülnek fel, ami azt jelenti, hogy a kötelékek alkalmasak az egymással és a szövetségesekkel való teljes körű együttműködésre. A nemzeti képességfejlesztések jegyében kulcsfontosságú az állampolgárok elérése és bevonása. A nemzetközi és nemzeti képességfejlesztésekkel egy szövetségesi rendszerbe megfelelően illeszkedő, a nemzeti önerejére is támaszkodni képes MH jöhet létre. [108 pp. 3-21]

A képességfejlesztések célja, hogy a honvédség megfelelően tudjon alkalmazkodni a jelen és jövő kihívásaihoz, rugalmasan tudjon reagálni a változó körülményekhez és megfelelően kezelje a kihívásokat. A rohamos technológiai fejlődés, a változó társadalmi, gazdasági és hadműveleti környezet miatt követelmény az MH folyamatos transzformációja, amely a műveletek fejlesztését, a szervezet modernizációját, az új

képességek integrációját, a koncepciók és szabályozók kidolgozását továbbá a képzési-kiképzési és felkészítési rendszer hatékonyságának növelését jelenti. A honvédségnek olyan integrált képességekkel kell rendelkeznie, amelyek biztosítják a műveleti fölényt. A jelenkori és a jövőbeli hadviselés jellege már túlmutat a hagyományos, fegyverrel vívott harcokon, sokkal inkább kerülnek előtérbe az olyan új műveleti terek, mint az elektromágneses tér, a kibertér és a világűr. A 21. századbéli magyar haderő a haderőfejlesztés tekintetében képessé válik a szimmetrikus és az aszimmetrikus hadviselés folytatására. [39]

Összegzésképp megállapítom, hogy az MH-nak megújult, szervezett, önállóan működő és szövetségi szinten alkalmazható – önkéntes tartalékos rendszerrel szervezett – haderőként kell működnie. Ehhez szükséges egy megfelelően képzett és kiképzett, korszerű, modern és digitális eszközökkel felszerelt, nemzetközi tapasztalatokkal rendelkező állomány, amely képes az ország szuverenitásának védelmére, így lehetővé téve a szövetségesi műveletben történő érdemi segítségnyújtást. Ezáltal érvényesítve mind a nemzeti önerő fejlesztését, mind a szövetségesi szerepvállalást az ország biztonságának kialakításáért és fenntartásáért.

3.2 A Zrínyi 2026 bemutatása és célrendszere

A honvédség digitalizációjához elengedhetetlen az elavult képességek és technikák fejlesztése. Az MH szárazföldi- és légierő eszközei, képességei modernizációra szorulnak. A fentiek érdekében a Zrínyi 2026 meghatározza azokat a modernizációs, honvédelmi és haderőfejlesztési képességeket és tevékenységeket, amelyek hozzájárulnak a honvédség digitalizációjához.

2017 januárjában vette kezdetét a Zrínyi 2026, amelynek célja, hogy biztosítsa a honvédség számára a mai kornak és kihívásoknak megfelelő technikai eszközöket, képességeket és személyi feltételeket. Egy hadseregnek folyamatos felkészülésre, képességekre és fejlett technikai eszközökre van szüksége ahhoz, hogy eredményesen helytálljon honvédelmi feladatainak végrehajtásában, megvédje a hazát – a szövetségesi együttműködés mellett – a nemzeti önerő képességének fenntartásával és fejlesztésével oly módon, hogy az állampolgárok hazafiasságra való nevelése, a haza védelmében való részvétele is megvalósuljon. [49]

A Zrínyi 2026 az elmúlt 30 év legnagyobb és legátfogóbb haderőfejlesztési programja. A program részét képezi:

(1) a növekvő költségvetés az MH átfogó fejlesztése és modernizációja érdekében;
(2) a biztos életpálya a kiszámíthatóság, tervezhetőség és biztonság megteremtése érdekében;
(3) a honvédelmi program a biztos utánpótlásért az Önkéntes Területvédelmi Tartalék, az Önkéntes Honvédelmi Előképzés és a Honvédelmi Sportszövetség létrehozásával;
(4) az Önkéntes Tartalékos Rendszer kiépítése a sorkatonai szolgálat és az általános hadkötelezettség hiánypótlásaként;
(5) a katonacsaládok pénzbeli és természetbeni támogatása;
(6) a honvédelmi táborok országos szintű kiépítése a honvédség feladatainak ismerete céljából;
(7) a honvédelmi ösztöndíjprogram a középfokú és felsőoktatásban résztvevők számára;
(8) a fiatalok a honvédségért, honvédelmi nevelési program népszerűsítése a Honvéd Kadét Program keretében;
(9) a korszerű kiképzés az MH képességeinek megőrzése és fejlesztése okán a személyi állomány továbbképzésével, a korszerű haditechnikai eszközök alkalmazhatósága érdekében;
(10) az I. és II. világháborús hősök előtti tisztelgés a Katonahősök Emlékezete Program és a Magyar Katona Áldozatvállalása a Nagy Háborúban Program keretein belül;
(11) haderőfejlesztés a digitalizáció útján. [109]

A Zrínyi 2026 több pilléren nyugszik, ezek közül a leghangsúlyosabb a haderőfejlesztés, a hadsereg modernizációja, a képességek korszerűsítése, fejlesztése és digitalizációja. A fejlesztési és modernizációs program egyaránt átfogja a szárazföldi haderőnem és a légierő területét. A program keretein belül azonban modernizáción megy keresztül a logisztikai, a katonai-egészségügyi és a vezetési rendszer egésze is. A haderőfejlesztés célja a katonák egyéni harcászati felszerelésének megújítása, a helikopterflotta, a tüzér- és páncéltörő tüzérképességek modernizálása, a honvédség merev- és forgószárnyas légiszállító képességének korszerűsítése, a radarok modernizálása, a légvédelmi rakétaegységek megújítása, a honvédség híradó-

informatikai és tábori vezetési rendszerének modernizációja, valamint a különleges műveleti képességek továbbfejlesztése és a hibrid hadviselésen belül a kibervédelem fejlesztése korunk új biztonsági kockázatainak és kihívásainak eredményes leküzdése érdekében. A komplex haderőfejlesztés a missziós feladatok és a katonai műveletek végrehajtását, valamint a katasztrófavédelmi helyzetek szakszerű kezelését, esetlegesen a polgári segítségnyújtást szolgálják. [110]

A jelenlegi, 2022. évi statisztikák alapján a NATO elvárását, miszerint minden tagországnak kötelessége 2024-ig a GDP legalább 2%-át a védelmi költségvetésre fordítania, Magyarország már 2023-ra teljesíteni fogja. Az MH törekvése, hogy a NATO ajánlásaival összhangban 2024-ig a védelmi költségvetés legalább 20%-át fejlesztésekre és modernizálásra fordítsa. [111]

A Zrínyi 2026 egyik alappillére a magyar hadiipar fejlesztése is. A Kormány a magyar védelmi ipar szereplői mellett a nemzetközi piacot is bevonva kötött együttműködési megállapodásokat a hadiipar fejlesztése érdekében. A fejlesztések következtében Magyarország a Rheinmetall céggel kooperálva, Rheinmetall Hungary Zrt. néven hoz létre egy zalaegerszegi üzemet Lynx KF41 lánctalpas gyalogsági harcjárművek gyártása céljából és egy kaposvári üzemet a Gidrán 4x4-es meghajtású, valamint egy következő generációs 8x8-as meghajtású gumikerekes harcjárművek gyártása céljából. A Rheinmetallal való együttműködés kapcsán épül a szintén magyarországi telephelyű lőszergyár Várpalotán, azzal a céllal, hogy a Zrínyi 2026 kapcsán már beszerzett és még beszerzés alatt álló eszközök számára is kompatibilis lőszereket állítsanak elő. A Rheinmetall-hoz kapcsolódik továbbá egy nyírteleki székhelyű vegyesvállalat létesítése is, amely hadiüzem csúcstechnológiás rádiólokátorokat fog gyártani. A Hirtenberger Defence System Magyarországon, szintén Várpalotán épít egy aknavetőgránátokat előállító gyáregységet. Az Airbus Gyulán épülő helikopter-alkatrészgyára, az Airbus Helicopters Hungary Kft. vegyesvállalat biztosítja a magyar légiipar alapjait. Az Arzenál Zrt. égisze alatt működő kiskunfélegyházi fegyvergyár termelése is fokozódik tekintettel arra, hogy a hazai igények mellett export tevékenység ellátását is biztosítja. [112],[113]

A hadiipar fejlesztése és az infrastrukturális körülmények megteremtése szükséges az új eszközök megfelelő elhelyezéséhez, üzembe helyezéséhez és karbantartásához. A Zrínyi 2026 keretein belül beszerzett eszközöket a teljesség igénye nélkül a légierő és a szárazföldi erők modernizálása mentén mutatja be a fejezet.

A Zrínyi 2026 kapcsán már megkezdődött a katonák egyéni felszerelésének és ruházatának megújítása, továbbá különféle kialakítású terepjáró tehergépjárműveket, személygépkocsikat és speciális gépjárműveket is beszerzett a honvédség.

A védelmi ipar fejlesztésének keretében 100 db moduláris, modern autóbusz gyártása is megtörtént. [114] Ezenfelül megvalósult a vállról indítható páncéltörő képesség fejlesztése és a tüzéroptikai eszközök rendszeresítése is. Megkezdődött a légvédelmi rakétarendszer, a légvédelmi rakéták és a Gripen szoftverek megújítása is. [115]

Az MH kecskeméti légi bázisán a Zrínyi 2026 keretében a felújítások részét képezi a kifutópálya, a fénytechnikai eszközök, az üzemi területek és az infrastruktúra fejlesztése is. A harckocsi és önjáró tüzér, valamint helikopter képesség megteremtéséhez szükség volt Tatán és Szolnokon az infrastrukturális fejlesztésekre, továbbá az érintett laktanyák, mint Hódmezővásárhely esetében az épületek korszerűsítésére. [109]

3.3 A légierő képességének modernizálása

A Zrínyi 2026 beszerzései következtében a 21. század követelményeinek megfelelő páncélosok és lövészpáncélosok, önjáró lövegek, valamint többcélú moduláris járművek kerültek és kerülnek beszerzésre és elhelyezésre a honvédség szervezeteihez. A szárazföldi erők fejlesztésével párhuzamosan indult meg a légierő és a légvédelem átalakítása, modernizálása is a modern kor kihívásaihoz alkalmazkodó eszközökkel.

A légierő képességeinek megújítása, a légi szállítás, mint katonai képesség megtartása stratégiai fontosságú az MH számára. A katonák felkészítése, kiképzése a műveleti és missziós feladatokra, a külszolgálathoz szükséges felszerelés és eszközök szállítása, utánpótlása és a humanitárius katasztrófa elhárítási tevékenységben való részvétel a gépek megújításával, modernizálásával és új típusú digitális műszerekkel felszerelt helikopterek beszerzésével érhető el. A légiszállító-képesség súlyos baleset, természeti katasztrófa, terrortámadás, vagy fegyveres konfliktus következtében, illetve tömeges baleset esetén szállításra is bevethető képesség.

A légierő képességének modernizálása érdekében a Mi-17-es szállító és a Mi-24-es harci helikopterek nagyjavításokon estek át, lezajlott a Jak-52-es kiképző repülőgépek új Zlin típusú gyakorló- és felderítő gépekre történő lecserélése. A Mi-24-es helikopterek átestek az utolsó nagyjavításokon egyfajta technológiai hidat képezve és folyamatosságot biztosítva az új helikopterek megérkezéséig. A javítások következtében a Mi-24-esek már teljes hatékonysággal tudják átvenni a tűztámogatási-harctámogatási feladatokat. [116]

Első körben 2019 novemberében érkeztek meg Szolnokra a Zrínyi 2026 keretében beszerzett Airbus H145M könnyűhelikopterek. Az MH a helikopterekhez logisztikai programot is biztosít, amely által a pilóták kiképzése már megtörtént és az új gépek ellátása is biztosított.

A helikopterek fegyverzete tartalmazza a 20 milliméteres gépágyút, és a nem irányított rakétákat, de lézeres irányítású páncéltörő rakétákkal is felszerelhetők. [117] 2020 júniusában további 3 db Airbus H145M típus helikopter érkezett meg az MH 86. Szolnok Helikopter Bázisra. Az újonnan beszerzett helikopterek közül kettő már rendelkezik kutató-mentő felszereltséggel is. [118] 2020 decemberére összesen 16 db Airbus H145M érkezett meg Szolnokra. [119]

2021 márciusában 2 db HForce-fegyverrendszerrel felszerelt Airbus H145M típusú könnyű, többcélú helikopter, 2021 novemberében pedig az utolsó előtti Airbus H145M is átlépte a magyar határt. Az utolsó, és egyben a 20. forgószárnyas, 2021 decemberében került végleges helyére a szolnoki laktanyában. [120]

A honvédség összesen 20 db Airbus H145M típusú helikopter beszerzését hajtotta végre 2021-ig. A korszerű, modern felszereléssel, digitalizált műszerekkel és digitális, hálózati alapú fegyverekkel felszerelhető helikopterek használatát a szolnoki helikopter bázison tudják elsajátítani a magyar katonák. A nagyteljesítményű kamerával és elektronikus védelmi rendszerrel ellátott könnyű, többcélú helikopterek egyben rendelkeznek a kiképző helikopter, a kutató-mentő helikopter és a fegyveres-tűztámogató helikopter valamennyi tulajdonságával. [121]

A H145M típusú gépeken túl további 16 db Airbus H225M közepes katonai helikopter beszerzése van folyamatban, amelyek előreláthatólag 2023-2024-ben szintén a Zrínyi 2026 keretében érkeznek meg Magyarországra. [122]

A H225-ös helikopterek kiválthatják a Mi-8-as és Mi-17-es típusokat, amelyek a nagyjavításokat követően 8 évig maradhatnak üzemben, így 2024-2025-re kifutják üzemidejük tartalékát. Ekkorra az új H225-ös beszerzések is teljes számban megérkeznek hazánkba, továbbá a pilóták kiképzése is megtörténik. Az új Airbus H225-ösök katasztrófahelyzetben árvízi mentésnél, tűzoltásnál szintén bevethetők lesznek. A helikopterek tekintetében a számos fejlesztés mellett kiemelten a digitalizációé a fő szerep. Amellett, hogy a hajtóművek teljesen digitális vezérlésűek, a pilótafülkében is a számítógépeken van a fókusz, mert a műszerfalon színes LCD kijelzők kerültek kialakításra és a gép alapfelszereltségébe tartozik a navigációs rendszerrel együttműködő mozgótérkép is. [123]

Első körben azok a szállító repülőgépek kerültek beszerzésre, amelyek a katonákat képesek elszállítani bárhová, míg az új beszerzések az anyagszállításban és az utánpótlás biztosításában lesznek érdekeltek. Ennek érdekében a 2018-ban beszerzett, többnyire személyszállításra használt 2 db Airbus A319 és a 2 db Dassault Falcon 7X repülőgépeken túl tervezetten 2023-2024-ben érkeznek meg Magyarországra a KC-390-esek, amelyek a nagyméretű terhek hadszíntéri célba juttatását szolgálják majd, ezzel biztosítva a honvédség légiszállítási, kimenekítési, légideszant és légiutántöltő képességének fejlesztését. A A319 csapatszállító repülőgépek vonatkozásában a légi egészségügyi kiürítési képesség, Medical Evacuation (a továbbiakban: MEDEVAC képesség) alkalmazhatóságának feltételei, valamint mind az A319-esek mind a Falcon 7X futárgépek kapcsán önvédelmi képességek kerültek kialakítására. Ezekkel a képességekkel olyan logisztikai műveletek is végrehajthatók, mint a személy- és utánpótlás szállítás, amelyek sikeres elsajátítása érdekében Bren 2-es típusú gépkarabélyokkal felfegyverzett különleges műveletei erők kiképzése is megtörtént. [124]

A csaknem 40 éve üzembe helyezett és szolgálatot ellátó szállító repülőgépek cseréjének érdekében kerülnek beszerzésre a brazil gyártmányú KC-390-esek. A KC 390-es hadszíntéri szállító repülőgépek beszerzésével az MH légierő képessége rámpás szállítógépekkel kerül felszerelésre, amelyekkel műveleti körülmények között is meg lesz a képesség a nagyméretű terhek, katonai felszerelések, járművek és személyi állomány 23 tonnáig történő szállítására. Az új beszerzésű gépek nemcsak a betonozott repülőtéri, hanem a rosszabb minőségű terepen történő le- és felszállásra, valamint ejtőernyős műveletek kiszolgálásra is alkalmasak. A vészhelyzeti kimenekítés és a nagyobb létszámú beteg- és sebesültszállítás végrehajtása is a feladataik közé tartozik. A honvédség tehát új légierő képességgel nő a beszerzések kapcsán. Ezzel a beruházással kiszolgáljuk a NATO igényeit is, hiszen ez a képességfejlesztés – Portugália mellett – nálunk egyedülállóan jelenik meg a régióban.

A 2020-ban kölcsönösen aláírt megállapodás értelmében megvalósult – a kezdeti alkatrészcsomag, a kiegészítő felszerelések biztosításán túl – a hajózó-repülőműszaki állomány átképzése és az integrált logisztikai támogatása is. A gépek megérkezését követően 1 év időtartamban kapott kiképzést az állomány a szakmai ismeretek elmélyítésének érdekében. A KC 390-es beszerzésével a honvédség a közép-európai régió legmodernebb hadszíntéri szállítórepülőgép-képességet birtokolja. [125]

A légierő képességének fejlesztése érdekében a Zrínyi 2026 által sugárhajtású kiképző repülőgépek kerülnek beszerzésre, amely beszerzés hozzájárul a pilótaképzés fejlesztéséhez. Ezenkívül a Gripenek MS20 Block 2 képességfejlesztése, vagyis a fegyverzeti rendszerének modernizálása, MISTRAL M2 kis hatótávolságú rakéták fejlesztése és további kis- és közepes hatótávolságú rakétakomplexumok beszerzése is tervben van. A MISTRAL légvédelmi rakétarendszer korszerűsítése 2017-ben kezdődött, mely kapcsán nagyobb lőtávolsággal, jobb zavarvédelemmel és hosszabb üzemidővel rendelkező MISTRAL M3 rakéták és MATIS MP3 hőkamerák, gyakorló berendezések, alkatrészek és akkumulátorok is beszerzésre kerültek. [109]

A légierő képességfejlesztése azonban nemcsak az eddig áttekintésre került új eszközök beszerzésével valósul meg. A légvédelem és a légtérvédelem szintén fontos szerepet tölt be a hadsereg modernizációjában.

Ennek érdekében 2018-ban rendelte meg a honvédség az Airbus által kifejlesztett számítógép- és hálózatalapú légvédelmi rakéta vezetési rendszert. A Légvédelmi Rakéta Műveleti Központ, Surface to Air Missile Operations Centre (a továbbiakban: SAMOC) 2021 nyarán került telepítésre az MH 12. Arrabona Légvédelmi Rakétaezredhez.

A SAMOC képes megvalósítani a nemzeti és a szövetségi rendszerben alárendelt légvédelmi rakétaerők stratégiai és műveleti szintű integrációját, harc- és tűzvezetését. A SAMOC telepített és mobil komponensből áll. A telepített változat egy olyan statikus vezetési pont, amely kiképzési feladatok végrehajtására, kiértékelésére és szimulációra is egyaránt alkalmas. A konténerbe telepített, szállítható változat, arra alkalmas kommunikációs csatornák használatával akár 1000 km-en túli távolságból is tud kapcsolódni a telepített SAMOC-elemhez és az elöljáró vezetési ponthoz is. A munkahelyek rugalmas konfigurációs lehetőségei egyrészt biztosítják a nem valós idejű harcvezetést és a valós idejű tűzvezetési funkciók gyakorlását is. A telepített és mobil változat közös használata által biztosítható a légvédelmi rakétarendszer maximális használata. [126]

2020 novemberében írta alá az MH a norvég Kongsberg és az USA-beli Raytheon cégek által fejlesztett közepes hatótávolságú hálózatalapú légvédelmi rakétarendszer, National Advanced Surface to Air Missile System (a továbbiakban: NASAMS) földi telepítésű légvédelmi rakétarendszerek beszerzéséről szóló szerződést. A megállapodás értelmében az MH képességrendszere 2023-tól a világ egyik legkorszerűbb, földi telepítésű légvédelmi rakétarendszerével fog bővülni. [127]

Az új, földi telepítésű légvédelmi rakétarendszer beszerzése mérföldkőnek tekinthető, mert a csaknem 40 éve hadrendben lévő, orosz 2K12 KUB analóg rakétarendszer leváltását eredményezi. A légvédelmi rendszerhez további 120 db AMRAAM-C7 és 60 db AMRAAM-ER közép hatótávolságú, aktív lokátoros önirányítású légiharc rakéta is beszerzésre került. Ennek eredményeképp a honvédség légvédelmi képessége a 21. század kihívásaihoz mérten bővül a legmodernebb haditechnikai eszközökkel. A magyar légtér egyben NATO-légtér is, Magyarország pedig szövetségesként a légtérvédelem komplex rendszeréért felel, ezért fontos, hogy a honvédség a modern harcászati repülőgépek mellett a légtérvédelemhez elengedhetetlen radarokkal és a földi telepítésű légvédelmi rakétarendszerekkel is rendelkezzen. Magyarországnak 2024-től teljesítenie kell a szövetségesi rakétavédelmi képességekhez való hozzájárulásból adódó NATO követelményt, amit a NASAMS raktérandszerrel sikeresen tudunk megvalósítani. Ez a komplex és modern rendszer képes a kijelölt légtér ellenőrzését végrehajtani, a kijelölt zónát, objektumot, terepszakaszt megfelelő módon védeni, továbbá a légi célokat felderíteni, elfogni, azonosítani és megsemmisíteni. Ezenfelül a felderített, azonosított és megsemmisítésre kijelölt repülő eszközöket megsemmisíteni. [116]

2020 decemberében született szerződés 11 db ELM-2084 radar beszerzéséről. A radarok NATO kompatibilitását a Rheinmetall Canada vállalat közreműködésével fogja végrehajtani a honvédség. A radarok tervezetten két ütemben, 2022-ben és 2027-ben állnak majd szolgálatba, összeszerelésükről és karbantartásukról a nyírteleki hadiüzem fog gondoskodni. Az első ütemben beszerzésre kerülő 5 db nagy hatótávolságú légtérellenőrző az ország légterének forgalmát fogja figyelni és ellenőrzi, a második ütemben 6 db mobil közepes hatótávolságú radar és tüzérségi radar kerül beszerzésre.

Az ELM-2084 beszerzésével a honvédség célja a régi szovjet P-37, PRV-17 és SZT-68U típusú rádiólokátorok leváltása. Az új, 3D-s radarok teljes rendszerbe állásáig zajlik az állomány felkészítése.

Az ELM-2084 multimissziós, mobil radar biztosítja a 3D-s, valós idejű légihelyzetkép rendelkezésre állását. A lokátor képes a folyamatos, 360 fokos légi felderítésre, 470 km maximális felderítési távolságra és csaknem 1100 légi cél adatainak feldolgozására. Ezenkívül bevethető különféle rakétavédelmi, légvédelmi rendszerek elfogóinak irányítására.

Az ELM-2084 tüzérségi felderítő radarként is alkalmazható, így 120 fokos lefedettség biztosítása mellet akár 100 km-ig képes az eltérő gránátok, tüzérségi lövedékek, rakéták becsapódási pontjának és indítás helyének meghatározására. [128]

2021 decemberében született szerződés a német Diehl vállalattal, az IRIS-T kis hatótávolságú légiharc rakéták beszerzéséről. Az új rakéták az AIM-9L Sidewinder rakétákat váltják majd a Gripenek arzenáljában. Az új rakétafegyverzet beszerzésével és a Gripen vadászgépek modernizációjával teljesül a 21. századi repülőharcászati követelményeknek való megfelelés. [129]

Az új Airbus H145M és H225M típusú helikopterek, a sugárhajtású kiképző repülőgépek beszerzésével, továbbá a Gripenek modernizálásával, az A319-es MEDEVAC képességfejlesztésével és a Dassault Falcon 7x és a KC 390-esek beszerzésével, a MISTRAL légvédelmi rakétarendszer korszerűsítésével, valamint a SAMOC légvédelmi rakéta vezetési rendszer és a NASAMS földi telepítésű légvédelmi rakétarendszer, az IRIS-T rakéták és az ELM-2084 radar beszerzésekkel új dimenzióba került a honvédség légierő képességének modernizálása és ezen keresztül megnyílt az út a légierő képességek digitalizációja előtt. A fentiekben bemutatott eredmények és megfogalmazott célok mind egy-egy lépéssel közelebb hozzák a honvédség digitális platformra történő átállítását.

3.4 A szárazföldi erők modernizálása

A honvédségnek rendelkeznie kell azzal az elrettentő erővel és azokkal a katonai képességekkel, amelyek birtokában képes hatékonyan fellépni a biztonságot fenyegető veszélyekkel szemben. Ehhez szükséges a légierő fejlesztése mellett a honvédség szárazföldi erőinek modernizálása is, ezért a Zrínyi 2026 keretében sor kerül az MH szárazföldi képességeinek fejlesztésére és digitalizációjára is.

A katonák egyéni harcászati felszerelésének modernizálása már kezdetét vette a 2015M mintájú gyakorlóruha rendszeresítésével. Az egyéni harcászati felszerelés békeidőben a napi munkavégzéshez és a kiképzési feladatok végrehajtásához szükséges eszközöket tartalmazza, háborúban pedig a feladatellátás biztosítása mellett növeli a katonák túlélőképességét. A Zrínyi 2026-on belül elindult a Digitális Katona Program, amelynek célja, hogy a katonák technológiai és humánképességeik tekintetében eredményesen készüljenek fel a jövőbeli feladataik végrehajtására. A Digitális Katona Program az alábbi két részből áll: (1) a technológiai eszközpark biztosítása; (2) a fizikai, kognitív és mentális képességeket érintő fejlesztési programok kidolgozása.

Tekintettel arra, hogy a katonáknak az új kor kihívásaihoz kell alkalmazkodniuk, folyamatban van az analóg technológián alapuló rendszerek modernizálása, digitális eszközökre történő cseréje. Ezen túlmenően az új kihívásokhoz és a digitális kor

elvárásaihoz való alkalmazkodásban segít a komplex humán fejlesztési program. A fenti feladatok, valamint az új technológiák honvédségen belüli koordinálására jött létre 2019-ben az MH Modernizációs Intézete (a továbbiakban: MH MI), amely összekötő szerepet tölt be az MH és külsős ipari, egyetemi, kutatóintézeti partnerek között. [130]

A szárazföldi erők modernizálása érdekében strukturális átalakítások is megvalósulnak. Ennek keretein belül kerül sor a háromdandáros fejlesztésre, amely a nehéz, közepes és könnyű lövészdandár-szervezet létrehozását jelenti. A háromdandáros fejlesztés elemei összhangban állnak majd a szövetségesi elvárásokkal is, ezáltal a NATO követelményrendszere mellett az országvédelmi feladatok is megvalósulhatnak. A dandárok modern felszerelésének és fegyverzetének beszerzése szintén a Zrínyi 2026 által lesz biztosítva. A koncepció megvalósításával párhuzamosan kerül kialakításra a dandárok korszerű katonai vezetési, irányítási és kommunikációs rendszerének telepítése, amely lehetővé teszi az információk és a vezetés új, digitális platformra helyezését. [109]

A tüzér- és páncéltörő tüzérképesség fejlesztése és modernizálása érdekében új eszközök, valamint a hordozóplatformok és kiegészítő eszközök beszerzése és a honvédség műszaki csapatainak felzárkóztatása, a műszaki eszközök korszerűsítése, a közepes lánctalpas úszó gépjárművek és a hadihidak modernizálása szintén a hazai védelmi ipar bevonásával jön létre.

A világot és egyben Európát érintő új biztonsági kihívások közül a digitalizációs- és hálózati rendszerek szempontjából kiemelt figyelmet szükséges fordítani a kibertámadásokra és a kibervédelemre. A hibrid hadviselés elleni küzdelemmel szemben a honvédség egy olyan kibervédelmi rendszer létrehozását kezdte meg, amely ellenáll a vezetési- és irányítási rendszerekbe történő külső fél behatolásainak és képes felfedni a hálózat elleni támadásra utaló tevékenységet. A kibertérben jelentkező fenyegetések elhárításához, a katonák naprakész oktatására van szükség, ennek érdekében 2019 júniusában került átadásra az MH Kiber Képzési Központja (a továbbiakban: MH KKK). [131] 2022 év elején alakult meg az MH Kiber- és Információs Műveleti Központ (a továbbiakban: MH KIMK), amely a Budapest Helyőrségdandár Elektronikus Eseménykezelő Főközpont és a Civil-katonai Együttműködési és Lélektani Műveleti Központ egyesítésével jött létre. A nem kinetikus műveleti lehetőségek integrációjával megalakult szervezet célja egy új képesség létrehozása a hibrid környezetben történő gyorsabb, hatékonyabb és eredményesebb feladatvégrehajtás érdekében. Az újonnan létrehozott MH KIMK feladatai közé tartozik a HM elektronikus információs rendszerének védelme és a kibertéri fenyegetések folyamatos elhárítása. [132]

Az új és modernizált eszközök szakszerű elhelyezéséhez elengedhetetlen a korszerű logisztikai, elhelyezési és tárolási rendszer, amely a laktanya rekonstrukciós program keretében valósul meg. A laktanyák, lő- és gyakorlóterek modernizációja és az infrastruktúra-fejlesztés mind szerves részét képezik a szárazföldi haderőnem modernizációjának. A Zrínyi 2026 tervei között szerepel továbbá egy olyan tábori kórház felállítása és az ehhez szükséges eszközök beszerzése, amely a harctéren az életmentésen túl sebészeti beavatkozásokra és diagnosztikai vizsgálatokra is alkalmas. [109]

2019-ben a dezintegráció részeként megalakult az MH Parancsnoksága (a továbbiakban: MHP). Ennek megfelelőképpen létrejött az alábbi öt szemlélőség is: (1) szárazföldi; (2) légierő; (3) különleges műveleti; (4) logisztikai; (5) kibervédelmi. A szemlélőségek mutatják az MH fejlesztési irányait is, ez azt jelenti, hogy a fenti területek határozzák meg a Zrínyi 2026 által fejlesztendő területeket. A haderőnemek fejlesztése azonban több összetevős folyamat, egy új képesség kialakításához szükséges a személyi állomány, a technikai eszközkészlet, a kiképzés és a vezetési rendszer egyensúlya.

A szárazföldi erők modernizálása érdekében az alábbiakban a beszerzett és beszerzés alatt álló eszközök kerülnek áttekintésre.

2018-ban 12 db modulárisan átalakítható ultrakönnyű taktikai járművet helyezett el a honvédség Szolnokon. A Polaris MRZR-4-es „homokfutók” több célra is használhatók: felderítésre, kisebb csoportok ellenséges területre való bejuttatására és kivonására, sebesültszállítására és határvédelemre. A járművek felszerelhetők géppuskával, gránátvetővel és páncéltörő rakétával is, ezért harctámogató szerepben is bevethetőek.[133]

A szárazföldi erők modernizálása érdekében kötött szerződést a honvédség és a Krauss-Maffei Wegmann vállalatcsoport, amelynek eredményeképp 2020 decemberében beszerzésre került 12 db Leopard 2A4 lízingelt harckocsi, amelyet további 44 db Leopard 2A7+ nehéz harckocsi beszerzése várhatóan 2023 és 2025 között követ. [134]

Az új Leopardok beszerzésével leválthatóak lesznek a régi orosz gyártmányú T-72-esek. A Leopard 2A4-esek és a régi orosz T-72-esek között számos különbség van. A németek előtérbe helyezték a kezelőszemélyzet túlélőképességét, védelmét és kényelmét is. Ennek kapcsán különbséget lehet felfedezni a két eszköz technikája, használata továbbá kiszolgálása között. A Leopard A4-es felépítése merőben más, mint a T-72-esé, a mérete nagyobb és sokkal erősebb motorral lett felszerelve ennélfogva erősebb is. A botkormányokat leváltották a digitalizált eszközök, a kis méretű kormány és a modern érzékelőkkel ellátott műszerfal. A Leopard biztonságosabb is elődjénél, mert a beépített

szenzorrendszernek köszönhetően képes leállítani magát túlhevülés, vagy a motorolaj kifogyása esetén, a T-72-esnél viszont a vezetőnek figyelnie kell az olajnyomásra, olajhőmérsékletre, vízhőmérsékletre és váltónyomásra is egyaránt. A vezetői pozícióban is különbség van a két eszköz között, még a szovjet modellben a vezető középen ül, addig a német harckocsiban jobb oldalon. Az új eszközből való célzást a fedélzeti ballisztikai számítógép segíti, ennek köszönhetően sokkal pontosabb lövést lehet a harckocsiból az ellenség felé küldeni akár álló, akár mozgó helyzetben is. A Leopardok a lánctalpban elhelyezett speciális kialakítású aszfaltkímélő gumibetéteknek köszönhetően képesek a közúton való közlekedésre is. [135]

Ezenfelül 24 db PzH 2000 önjáró löveg érkezik, melyeket tervezetten két ütemben szállítanak le a tatai MH 25. Klapka György Lövészdandár 101. Tüzérosztály részére. Ezzel a képességgel eleget teszünk a NATO által követelt nehézdandár képesség kialakításának, a tüzérség modernizálásának. A PzH 2000-esek jelenleg a legmodernebb és legkorszerűbb nyugati eszközök. A lánctalpas fűtőművek úton és terepen is nagy mozgékonyságot biztosítanak az önjáró lövegeknek, amely képesség a páncélzattal kiegészítve növeli az eszközök és a katonák túlélőképességét. Az önjáró lövegeken található 155 milliméter űrméretű tarackágyú több 10 km-re képes akár speciális tüzérségi lövedék célba juttatására is. [136]

Az MH szárazföldi képessége kibővítésre kerül még 3 db Leguan 2 típusú hídvető harckocsi készlettel és 5 db Wisent 2 harckocsi vontatóval is. A harcjárműveken túl beszerzésre kerülnek azok a nehézgép-szállító szerelvények, amelyek a járművek szállítását teszik lehetővé; a tüzérképességhez szükséges meteorológiai lokátorok, és a karbantartáshoz, valamint javításhoz nélkülözhetetlen speciális szerszámok és bevizsgáló eszközök, szerszámkészletek továbbá tartalék alkatrészek is. [137]

2019-ben kerültek beszerzésre a svéd SAAB Bofors Dynamics Carl Gustaf M4 hátrasiklás nélküli lövegek elvén működő többfunkciós gránátvetők.

A Carl Gustaf gránátvetők beszerzésével is hozzájárult a honvédség az egyéni harcászati felszerelések megújításához. Az új gránátvetők rendszeresítésével, a korábbi RPG 7-esek kerültek leváltásra. Az M4-esek páncélátütő képessége kétszerese, hatótávolságuk nagyobb, mint az RPG 7-eseké, továbbá különböző típusú gránátok is használhatóak hozzájuk, ezenkívül helyiségharc során is bevethetőek. [138]

2020-ban kezdte meg működését a 2017 óta épülő kiskunfélegyházi fegyvergyár, melyben a magyar katonák egyéni felszerelésében található pisztolyokat, géppisztolyokat és gépkarabélyokat szerelnek össze. A legmodernebb eszközökkel felszerelt fegyvergyár

beindításának elsődleges célja az volt, hogy Magyarország rendelkezzen a saját fegyvert gyártó kapacitás képességével, továbbá a hazai termelés mellett megjelenjen a nemzetközi piacon is. A színvonalas fegyvergyártásnak köszönhetően a bajor Unique Alpine AG TPG-3 A4 típusú mesterlövészfegyver és az AR-10 és AR-15 elnevezésű gépkarabély is a Kiskunfélegyházán található magyar fegyvergyárban kerül előállításra. Az MH számára gyártott CZ-fegyvercsalád: a CZ Bren 2 karabély, a CZ P-09 és a CZ P-07 pisztoly, valamint a CZ SCORPION EVO 3 A1 géppisztoly licenszét adó cseh vállalat, és a belga FN Herstal is érdekelt a magyar fegyvergyár képességeinek kiaknázásban.[139]

A szárazföldi haderőnem fejlesztése jegyében a támogató harcjárművek beszerzése is elkezdődött. 2021 februárjában érkeztek meg Tatára a Gidránok. A 10 db Ejder Yalçın többcélú, moduláris jármű a Nurol Makina által került – a magyar igényekhez mérten átalakítva és felszerelve – fejlesztésre és legyártásra. Az első 10 db Gidránon túl további 40 db járművet rendelt a honvédség a törökországi gyártótól. Az új eszközök azonban a licenc alapján, Kaposváron kerülnek majd összeállításra, amely során beépítésre kerülnek az európai fegyverrendszerek is. A Zrínyi 2026 keretein belül a gyártási és K+F tevékenység német-magyar koalícióban fog megvalósulni. A Gidrán, egy modern, robbanásvédett külső-belső kialakítású, jó terepjáró képességű páncélozott jármű. A gyártó tájékoztatása alapján az Ejder Yalçınból csapatszállító, páncéltörő, légvédelmi, felderítő, tűztámogató, vegyivédelmi, önjáró aknavető, robot hordozására kialakított tűzszerész, aknamentesítő, parancsnoki, műszaki és mentő változat is beszerezhető, azonban a kaposvári összeszerelésnek köszönhetően a Gidránok képességeit a honvédség alakíthatja ki a felmerülő feladatok tekintetében. [140]

A Kormány 2020 augusztusában kötött megállapodást a német Rheinmetall céggel, amelynek köszönhetően német-magyar vegyesvállalat került létrehozásra Zalaegerszegen, Lynx típusú gyalogsági harcjárművek előállítása céljából. A honvédség és a Rheinmetall között 2020 szeptemberében kötött szerződés értelmében 218 db Lynx KF41 családhoz tartozó harcjárművet kap az MH, amelyből az első 46 db német gyártású harcjármű leszállítása tervezetten 2022-ben valósul meg és a további 172 db a zalaegerszegi gyárban kerül legyártásra. A német partnerrel kötött hosszú távú megállapodás a gyártáson túl a harcjárművek tesztelésére és fejlesztésére is kiterjed. [141]

A magyar Lynxeket a Rheinmetall Strike Shield rendszerével fogják felszerelni, amely egy hard-kill aktív védelmi rendszert képez. Erre azért van szükség, mert a védelmi rendszer képes az ellenséges páncéltörő lövedékek semlegesítésére, ezáltal biztosítva a mai tudás szerinti leghatékonyabb biztonságot a harcjárműveknek. A Strike Shield

megóvja a katonákat, ezzel lehetővé téve a 21. századi hadviselési viszonyok közti feladatok teljesítését. A magyar Lynxek hibrid páncélzattal kerülnek felszerelésre, amely egyszerre ad passzív páncélvédettséget és aktív védelmet. Magyarország vállalta a NATO felé annak a nehézdandárnak a fejlesztését, amelynek a leghangsúlyosabb fegyverrendszerét a Lynx-harcjárművek teszik majd lehetővé. [142]

A fenti beszerzések, fejlesztések, a harckocsik, az önjáró lövegek és a gyalogsági harcjárművek létrehoznak egy új fegyvernemet, a páncélos gyalogságot, amelynek a nehéz- és közepes dandár adja majd az alapját, ezzel támogatva a Zrínyi 2026 egyik fő célját, a nehézdandár kialakítását.

A hazai kézifegyverek további gyártása, a katonák egyéni harcászati felszerelésének fejlesztése, a kiberképesség fejlesztésének folytatása és az új eszközök fogadásához szükséges infrastrukturális feltételek megteremtése képezik a szárazföldi haderőnem további fejlesztéseit. A szerződések megkötését követően a honvédség kiemelt feladata a humán állomány kiképzése, továbbképzése és alkalmassá tétele az új digitális alapú eszközök szakszerű használata érdekében. A katonák képességfejlesztéséhez elengedhetetlen a nemzetközi környezet biztosítása, ugyanis szövetségesi elvárás az interoperabilitásnak való megfelelés, ami azt jelenti, hogy a katonáknak valamennyi NATO tagország katonájával kell tudnia együttműködni. A cél tehát a beszerzett eszközök és a katonák összekapcsolása. A katonákat ezért fel kell készíteni – a hagyományos analóg ismeretek mellett – a digitális eszközök, digitális technológián alapuló kezelésére. A NATO tagországok mind a digitális platformra való átállás felé haladnak, ezért is szükségszerű az MH felzárkózása, amelyet a fenti beszerzések és képességfejlesztések tesznek lehetővé. [143]

A katonák egyéni harcászati felszerelésének modernizálásával, a 2015M mintájú gyakorlóruha rendszeresítésével, az MH MI létrehozásával, a kiberképességek fejlesztésével, az MH KKK és az MH KIMK megalakulásával, továbbá az olyan új eszközök honvédségnél történő rendszeresítésével, mint a Polaris MRZR-4-es „homokfutók”; a Leopard 2A4 és Leopard 2A7+ harckocsik; PzH 2000 önjáró lövegek, Carl Gustaf M4 gránátvetők; hazai gyártású lőfegyverek; Gidránok és Lynxek a szárazföldi haderőnem digitalizációja és modernizációja is kezdetét vette, ezzel biztosítva a honvédség digitális platformra történő átállását.

A Zrínyi 2026 tehát mind a légierő mind a szárazföldi erők modernizálása által hozzájárul ahhoz, hogy a honvédség áttérjen az informatikai, digitális- és hálózatalapú katonai rendszerek széles körű alkalmazására. Mindez alátámasztja a hipotézist, amely

alapján a fejlesztések megvalósulásának következtében a honvédelem egésze digitális platformra állítható át, ezzel biztosítva azt, hogy a védelmi, katonai, nemzeti biztonsági rendszerek önállóan, más rendszerektől leválasztva is képesek legyenek működtetni a közigazgatást, fenntartani az ország vezetését békeidőben és a békétől eltérő különleges jogrendben is.

3.5 Részösszefoglalás

A problémafelvetés tükrében az értekezés harmadik fejezetének hipotézise az volt, hogy a honvédelmi, katonai és nemzeti biztonsági rendszerek hazai digitális hálózatba való beágyazódása szükséges annak érdekében, hogy a békeidőben megfelelően működő katonai informatikai, digitális- és hálózatalapú rendszerek képesek legyenek önállóan működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő különleges jogrendben is. [1 pp. 122-145]

A hipotézis igazolása érdekében a fejezetben megvizsgáltam az MH feladatait az új biztonsági kihívások tekintetében és a Zrínyi 2026 cél- és eszközrendszerét. Elemeztem és értékeltem a légierő és a szárazföldi erők modernizálása érdekében már beszerzett és a még beszerzés alatt álló eszközöket, képességeket és digitális fejlesztéseket.

Összegzésképp megállapítottam, hogy az új biztonsági kihívások megfelelő kezeléséhez szükséges az MH strukturális, eljárásrendbeli, hadviselési és modernizációs átalakítása, amely a Zrínyi 2026 indulásával vette kezdetét. Az MH képességfejlesztési irányait tekintve a 21. századbéli magyar haderő a haderőfejlesztés tekintetében képessé válik a szimmetrikus és az aszimmetrikus hadviselés folytatására. Az MH-nak megújult, szervezett, önállóan működő és szövetségi szinten alkalmazható – önkéntes tartalékos rendszerrel szervezett – haderőként kell működnie. Ehhez szükséges egy megfelelően képzett és kiképzett, korszerű, modern és digitális eszközökkel felszerelt, nemzetközi tapasztalatokkal rendelkező állomány, amely képes az ország szuverenitásának védelmére, így lehetővé téve a szövetségesi műveletben történő érdemi segítségnyújtást. Ezáltal érvényesítve mind a nemzeti önerő fejlesztését, mind a szövetségesi szerepvállalást az ország biztonságának kialakításáért és fenntartásáért.

Az új Airbus H145M és H225M típusú helikopterek, a sugárhajtású kiképző repülőgépek beszerzésével, továbbá a Gripenek modernizálásával, az A319-es MEDEVAC képességfejlesztésével és a Dassault Falcon 7x és a KC 390-esek beszerzésével, a MISTRAL légvédelmi rakétarendszer korszerűsítésével, valamint a SAMOC légvédelmi rakéta vezetési rendszer és a NASAMS földi telepítésű légvédelmi

rakétarendszer, az IRIS-T rakéták és az ELM- 2084 radar beszerzésekkel új dimenzióba került a honvédség légierő képességének modernizálása és ezen keresztül megnyílt az út a légierő-képességek digitalizációja előtt. A fentiekben bemutatott eredmények és megfogalmazott célok mind egy-egy lépéssel közelebb hozzák a honvédség digitális platformra történő átállítását.

A katonák egyéni harcászati felszerelésének modernizálásával, a 2015M mintájú gyakorlóruha rendszeresítésével, az MH MI létrehozásával, a kiberképességek fejlesztésével, az MH KKK és az MH KIMK megalakulásával, továbbá az olyan új eszközök honvédségnél történő rendszeresítésével, mint a Polaris MRZR-4-es „homokfutók”; a Leopard 2A4 és Leopard 2A7+ harckocsik; PzH 2000 önjáró lövegek, Carl Gustaf M4 gránátvetők; hazai gyártású lőfegyverek; Gidránok és Lynxek a szárazföldi haderőnem digitalizációja és modernizációja is kezdetét vette, ezzel biztosítva a honvédség digitális platformra történő átállását.

A Zrínyi 2026 tehát mind a légierő mind a szárazföldi erők modernizálása által hozzájárul ahhoz, hogy a honvédség áttérjen az informatikai, digitális- és hálózatalapú katonai rendszerek széles körű alkalmazására.

4 AZ MH DIGITALIZÁCIÓJA ÉRDEKÉBEN AJÁNLOTT DIGITÁLIS PLATFORMOK

Az előző fejezetekben a technológiai és információs hadviselés 21. századi jellemzői, a kiberbiztonság és kibervédelem honvédelmi dimenziói és a Zrínyi 2026 kapcsán a honvédelem digitalizációja került elemzésre és értékelésre. Mindhárom fejezet igazolja azt, hogy a digitalizáció áthatja a honvédelmi rendszereket, szervezeteket, képességeket és eszközöket is. Ahhoz, hogy az MH az információs hadviselés korában is helytálljon szükséges alkalmazkodnia az új kor biztonsági kihívásaihoz, trendjeihez.

Hazánk biztonsági helyzetének stabilitását azonban csak akkor tudjuk garantálni, ha a honvédelem digitális pályára áll át. Ennek érdekében megfogalmazok tíz digitális platformot, amelyek mentén az MH digitalizációja megvalósítható.

A negyedik fejezetben a következő kérdéseket vizsgálom:

- Mely platformok mentén ajánlott a honvédségnek átállnia a digitalizációra?
- Milyen súllyal és intenzitással jelenik meg az MH digitalizációja érdekében megfogalmazott tíz digitális platform?

Annak érdekében, hogy valamennyi műveleti területen országunk a digitalizáció következtében kialakult új biztonsági kihívások ismeretével és ezek leküzdéséhez szükséges képességekkel rendelkezzen, a honvédségnek új szemléletű, digitális platformra szükséges átállnia. A negyedik fejezet hipotézise, hogy az MH széles körű digitalizációja akkor érhető el, ha a Zrínyi 2026 keretein belül megvalósuló/megvalósult fejlesztéseken és beszerzéseken túl az alábbi platformok azonos súllyal és intenzitással jelennek meg a honvédelem rendszerében:

(1) A nemzetközi hadiiparban való magyar részvétel.
(2) Az 5G technológia alkalmazása a katonai, műveleti, vezetési- és irányítási, hírközlési, hadiipari és haditechnikai fejlesztések terén.
(3) Okos fegyverek fejlesztése, különös tekintettel a kézifegyverek, önvezérlő fegyverrendszerek, bombák, rakétarendszerek digitalizációjára, önvezérlő katonai járművek: tehergépjárművek, páncélozott járművek, páncélozott szállítójárművek, harcjárművek, repülőgépek, helikopterek modernizálása, digitális műszerekkel való felszerelése.

(4) Intelligens katonai felszerelés fejlesztése különös tekintettel az intelligens ruha és digitális szenzorrendszer kialakítására, digitális katonai térkép és navigációs rendszer fejlesztése.
(5) Az MI alkalmazása a harctéren.
(6) A katonák és civilek átfogó felkészítése digitális kompetenciákkal, képzések és tanfolyamok biztosítása a digitális eszközök ismeretének és szakszerű felhasználásának céljából.
(7) A katonai kiképzési és oktatási rendszer, a védelmi igazgatási, a katonai igazgatási rendszer digitális- és hálózatalapú képességekkel való kiegészítése.
(8) A személyi nyilvántartási rendszerek, a katonai logisztika és hadtáp nyilvántartási rendszer kiegészítése és átállítása digitális- és hálózatalapú platformra.
(9) A magyar űrprogram digitális fejlesztése, magyar műhold fejlesztése és pályára állítása.
(10) A komplex hálózatalapú és digitalizált vezetési, irányítási, katonai hírközlő és kommunikációs rendszer fejlesztése. [1 pp. 122-145]

A hipotézis igazolása érdekében a fenti ajánlások – számos esetben nemzetközi példák alapján – kerülnek részletes kifejtésre.

4.1 A nemzetközi hadiiparban való magyar részvétel

A hazai védelmi ipar fellendüléséért többek között a HM, a Technológiai és Ipari Minisztérium (a továbbiakban: TIM, jogelődje: Innovációs és Technológiai Minisztérium, a továbbiakban: ITM) és a Védelmi Beszerzési Ügynökség Zrt. (a továbbiakban: VBÜ) együttesen felel. Azonban a Kormány védelmi ipari fejlesztéseibe az ütemesebb és eredményesebb fejlődés érdekében a KKV-k, valamint a *start up* cégek bevonása is szükséges lehet. Kiemelt cél a hazai védelmi ipar fejlesztése és a világ élvonalába tartozó befektetők Magyarországra vonzása, mint például az Airbus, amely a világ vezető repülés- és űrtechnikai vállalatai közé tartozik. Az Airbus magyarországi tervei közt a gyulai alkatrészgyártáson túl a légi ipari klaszter létrehozása is szerepel.[144] 2020 szeptemberében a HM, az MH és a Wizz Air együttműködési megállapodást írtak alá, annak érdekében, hogy a Wizz Air legmodernebb tréningprogramjának segítségével készülhessenek fel az Airbus A319-esek flottájának pilótái és légiutas-kísérői. A megállapodás keretein belül a honvédség kecskeméti repülőtere, taktikai kitérő

repülőtérként biztosítja majd a Wizz Air gépek részére az időjárási körülmények miatti kényszerleszállást. [145]

Magyarország nemzetközi hadiiparban való részvétele azonban nemcsak a légierő, hanem a szárazföldi haderőnem képességfejlesztése miatt is érdekelt. A Kormány 2020 augusztusában kötött megállapodást a német Rheinmetall céggel annak érdekében, hogy Zalaegerszegen egy német-magyar vegyesvállalat – Rheinmetall Hungary Zrt. – épüljön. A hosszú távú K+F megállapodás keretein belül kezdődhet meg a Lynx gumikerekes harcjármű, továbbá a haditechnikai eszközök, rendszerek, fegyverek fejlesztése és gyártása. A szerződés továbbá magába foglalja Várpalotán két hadiipari üzem létrehozását. Az egyik cég elsősorban hazai érdekeltségű, és tervezetten európai országokat is ellátó robbanóanyag gyár, míg a másik a nagy kaliberű lőszergyártás beindítója lesz. Az utóbbi cégbe kerül integrálásra a Hirtenberger cég aknagránát gyártó képessége. A Magyar Kormány 2020 októberében vásárolta fel a brit-osztrák Hirtenberger Defence Systems fegyvergyárat, amely így a magyar tulajdonú HDR Védelmi Ipari Kft. tulajdonába került. A Hirtenberger fegyvergyára csaknem 160 éve foglalkozik tüzérségi eszközök, valamint lőszerek fejlesztésével és gyártásával. [141] 2021 őszén kezdődött meg Kaposváron a Rheinmetall Hungary Zrt. hadiipari gyárának építése, amely szintén a német-magyar együttműködési megállapodás keretein belül jött létre. A termelés az indulást követően 1 éven belül fog beindulni, amely során harcászati, rádiótechnikai, elektronikai eszközökkel szerelik fel a törökországi járműveket, majd a Gidránok gyártása is hazánkban lesz biztosított. A gyártás fő profilját éveken belül azonban a NATO-n belüli K+F program fogja alkotni, amelynek célja a jövő technikájának megfelelő járművek előállítása. [146]

A magyar hadiipari fejlesztések egyrészt az MH modernizációja érdekében történnek, másrészt a NATO általi követelmények teljesítése és az új biztonsági kihívásokra adott válaszreakció összességét jelentik. A Magyarországon felépülő gyárak nemcsak a hazai piacra, hanem a nemzetközi profitra is fókuszálnak azért, mert jelentős gazdasági fellendülést, piaci profitot hozhatnak a neves nemzetközi partnerekkel létrehozott magyarországi székhelyű vegyesvállalatok. Az export országok alapvetően a NATO által meghatározott kritériumoknak megfelelően kerülnek kiválasztásra. A fejlesztések következtében Magyarország védelmi ipari stratégiája is felülvizsgálatra szorul, amelyben az iparfejlesztés és a vagyonkezelés mellett a K+F tevékenységek is szerepelnek. A stratégia aktualizálása 2021-től a HM, az ITM (jogutódja: TIM), valamint az állami vagyonkezelő szervek koordinálásában zajlik, és a fejlesztések irányvonalát a

védelmi ipari fejlesztésekben érdekelt nagyvárosok környéke, Békés, Somogy, Zala és Veszprém megye, továbbá Jász-Nagykun-Szolnok, Borsod és Heves megye adják.

A nyilvános stratégia-tervezet szerint az alábbi hat klaszter kerül létrehozására, az ország védelmi iparának kiépítése érdekében:

(1) harcjármű fejlesztés (Zalaegerszeg, Kaposvár)
(2) légi védelmi ipar klaszter az Airbus vegyesvállalat közreműködésével (kelet-magyarországi régió, Gyulán helikopteralkatrész-gyártó üzem létrehozásával, és a békéscsabai repülőtér továbbá a Békéscsabai Szakképzési Centrum átalakításával);
(3) Rheinmetall európai védelmi vállalattal együttműködve lőszer- és aknavetőgránátokat előállító üzemek klaszterközpontja (Várpalota);
(4) fegyvergyártási központ (Kiskunfélegyháza és a szegedi lézerközpont);
(5) hírközlés, telekommunikáció- és kiberrendszerek fejlesztésének központja (Budapest);
(6) a szenzorok klaszterközpontja (Északkelet-Magyarország, Nyírtelek).[147]

A K+F tevékenységek és a gyárak telepítésének koordinálása, összehangolása érdekében került létrehozásra 2021-ben a Védelmi Ipari Kutatóintézet, amelynek célja, hogy az MH-n belül működő MH MI katonai profilját kiegészítse egy civil kutatói csapattal. [148]

A védelmi ipar fejlesztését jelentős mértékben támogatja a *high-tech* magyar ipar kiépítésében jelenlévő kormányzati támogatás, vagyis:

(1) a járműipar fejlesztése;
(2) a kutatási rendszer reformja;
(3) az 5G-s mobilhálózat kiépítése;
(4) az MI projektek felkarolása;
(5) és az ipar 4.0 program. [147]

A fentiekben áttekintett koalíciók igazolják azt, hogy mind a légierő mind a szárazföldi haderőnem fejlesztése érdekében köttetnek nemzetközi együttműködések, amelyek

egyaránt hozzájárulnak a magyar hadiipar fejlesztéséhez és a honvédség modernizációjához, digitalizációjához.

4.2 Az 5G technológia

Az új biztonsági kihívások következtében az országok, régiók közti hatalmi vetélkedés egyre inkább kiéleződik a globális közjavak irányába is. Ez azt jelenti, hogy a nemzetközi vizek és erőforrásaik; az északi sarkvidék; a világűr; és a kibertér ellenőrzéséért és dominanciájáért egyaránt folyik a küzdelem. A technológiai fejlődés következtében egyre nagyobb hangsúlyt kap a digitalizáció, az 5G vezeték nélküli hálózat és az űrtechnológia. Az információs társadalom fejlődése, a digitalizáció és a globalizáció következtében új technológiai kihívások jönnek létre, amelyek befolyásolják hazánk biztonságát. [62]

Az 5G mobilhálózatra való átállással egy technológiai korszakváltás veszi kezdetét a világban. Az 5G hálózat jóval gyorsabb, mint a 4G mobilhálózat, ezáltal lehetővé teszi a gyorsabb adatátvitelt és a reakcióidők csökkentését. Az 5G-re való átállás hasznosítható az autóiparban, a közlekedésben, a feldolgozóiparban, a mezőgazdaságban, az egészségügyben, az energiagazdálkodásban, a kereskedelemben, a szórakoztatóiparban és a médiában. Az 5G által minimálisra csökkentett reakcióidő és szinte valós idejű kommunikáció hozzájárul az intelligens közlekedés, az önvezető gépjárművek és az e-egészségügy létrehozásához és/vagy fejlődéséhez. [149]

Az 5G hálózat kiépítésében történő állami szerepvállalás kapcsán Magyarország vezető szerepet tölthet be az európai fejlesztésekben, valamint a hálózat kiépítése is gyorsabban, a párhuzamosságokat elkerülve történhet, a piaci szektorral karöltve. Az új hálózat kiépítését az USA mellett Nagy-Britannia, Németország, Svájc, Kína, Dél-Korea és Ausztrália is szorgalmazza. [150]

2016-ban döntött a Kormány a ZalaZone tesztpálya létrehozásáról. A tesztpálya azzal a céllal épült, hogy tevékenyen részt vegyen az autóipar K+F tevékenységében. A zalaegerszegi tesztpályán a vezetésre és a menetstabilitásra fókuszáló tesztpálya jellemzőket K+F infrastruktúra elemekkel valósítják meg. A tesztpályán található ún. „bizonyító talaj" egyaránt alkalmas a hagyományos járművek dinamikai tesztjeinek biztosítására és az autonóm- és elektromos járművek validálási tesztjeinek végrehajtására.[151]

2018-ban az *„Autonóm on- és offroad járművek katonai alkalmazhatóságának lehetőségei"* címmel tartottak tudományos konferenciát a zalaegerszegi tesztpályán, ahol megvizsgálták az autonóm on- és offroad járművek katonai alkalmazhatóságának

elméleti kérdéseit, egy gyakorlati tesztelésre kialakított tesztpálya környezetben (Smart City Zone-okos város), amely az önvezető járművek fejlesztéséhez elengedhetetlen 5G hálózattal került kiépítésre. A konferencia keretein belül elhangzott, hogy a ZalaZone a hadiipari fejlesztésekre is alkalmas járműipari tesztpálya, mert biztosítani tudja a haditechnikai fejlesztésekhez szükséges környezetet mind a vezető nélküli harcjárművek tesztelése mind az offroad pálya biztosítása tekintetében. [152]

A honvédség modernizációjához, digitális képességfejlesztéséhez nem elég kizárólag az új eszközök beszerzése, hanem egyrészt szükséges a személyi állomány felkészítése az új gépek megfelelő kezelése érdekében, másrészt nélkülözhetetlen az újonnan beszerzett, modern eszközöket a megfelelő infrastruktúrával felszerelt környezetben tárolni. Mindez azt jelenti, hogy a Zrínyi 2026 több pilléren nyugvó fejlesztései magukba foglalják a személyi állomány 21. századi infrastrukturális körülmények közti elhelyezését és a kiképzési objektumok fejlesztését is. Ennek érdekében felújításra kerülnek a helyőrségi, központi gyakorló- és lőterek is. Az analóg gyakorlóterek helyére digitális gyakorlóterek épülnek – az újonnan beszerzésre kerülő, és már beszerzett haditechnikai eszközöknek – azért, hogy a kötelékben mozgó harcjármű csoportok tesztelése is megvalósulhasson. Ehhez szükséges az 5G technológia és a szimulátorok alkalmazása. [143]

A honvédség szempontjából a digitális műszerek 5G hálózathoz való csatlakozásával nemcsak a harctéren való alkalmazhatóságot, hanem a képzést és kiképzést is fejleszthetnénk. Az 5G technológiai alkalmazása a katonai, műveleti, vezetési- és irányítási, hírközlési, hadiipari és haditechnikai fejlesztések terén biztosítja a honvédség digitális platformra állítását.

4.3 Az okos fegyverek fejlesztése, önvezérlő gépjárművek, robotok

Az USA 2019-ben kezdte meg az okos fegyverek hadsereg számára történő fejlesztését és tömeges gyártását. Az elképzelés alapján a jövő kézi fegyverei külön operációs rendszerrel rendelkeznek. Az új technológiájú kézi fegyverek megváltoztatják a fegyverkezelés- és használat rendjét és növelik a hadsereg hatékonyságát. Az intelligens fegyverek működését illetően, az az elképzelés, hogy a fegyverekbe épített operációs rendszernek köszönhetően megakadályozható az illetéktelenek eszközhasználata, továbbá az alkalmazások segítségével pontosabb célzás valósítható meg. Mindez nemcsak átalakítja, de meg is könnyíti a katonák jövőbeli kiképzését. A fegyverek operációs rendszerrel való felszerelésével és digitalizációjával azonban megnő a hacker

támadások esélye, amely eshetőségre a kiberbiztonsági rendszer megerősítésével szükséges felkészülnie a kormányzatnak. [153]

A nemzetközi fejlesztések közül érdemes megemlíteni:

(1) a robot/autonóm fegyvereket;
(2) a hősugár fejlesztését;
(3) a lézerfegyvereket [An/SEQ-3 Lézer Fegyverrendszer];
(4) az okos gránátvetőt [XM 25];
(5) az „Acélvihar" vagy „Metal Storm" fejlesztését;
(6) a CornerShot fegyverkiegészítőt;
(7) a számítógépes mesterlövészpuskát;
(8) az elektromágneses ágyút;
(9) az Adaptiv technikával kialakított „láthatatlan" harckocsit;
(10) a hiperszonikus rakétákat [Dongfeng-21; Dongfeng-26].

Ezeket az okos fegyvereket egyelőre kísérleti jelleggel és/vagy korlátozottan alkalmazzák a nemzetközi harctereken, ezért részletes bemutatásukra – empirikus tapasztalat hiányában – az értekezés nem tér ki.

Az okos fegyverek fejlesztésében a katonai nagyhatalmak, köztük az oroszok is érdekeltek. 2021-ben az Egyesült Arab Emírségek fővárosában, az International Defence Exhibition konferencia keretein belül mutatta be a világ egyik legnagyobb fegyvergyártója, a Kalashnikov, az okos shotgunt. Az okos fegyver, amely világszínvonalú, egyedi fejlesztésű, az MP-155 Ultima nevet kapta, és beépített GPS-szel, kamerával, WiFi-vel és Bluetooth-szal szerelték fel, mindemellett a shotgunnal mért adatok okos telefonnal is szinkronizálhatóak. [154]

Az USA a rakétavédelmi képességek fejlesztésének keretében vizsgálja az F-35 II JSF lopakodó vadászgép új alkalmazási opcióit. A fejlesztés célja, hogy az F-35 szenzorait, adatkapcsolati rendszereit kihasználva képessé váljon az interkontinentális ballisztikus rakétákat akár már az indítási fázisban detektálni vagy megsemmisíteni. A fejlesztésekben érdekelt Kína és Észak-Korea is. [155]

2020. január 8-án Irán 18 db rövid hatótávolságú ballisztikus rakétát indított az Irakba települt amerikai erők bázisai ellen. Erbílben csaknem 200 magyar katona szolgált, akik a rakétatámadás kapcsán nem szenvedtek sérülést. A támadásokat követően azonban Irán

minden USA-val szövetségben álló országra ellenségként tekintett és célpontul szolgáltak számukra. [156]

A 2022. február 24-én kezdődött orosz-ukrán háború kapcsán is felmerültek hírek arról, hogy az oroszok hiperszonikus fegyvereket vetettek be az ukránok ellen, azonban a hírportálok ezt nem tudták teljes bizonyossággal megerősíteni. Az egyszerre több hadszíntéren párhuzamosan folyó háború kapcsán ugyanis a propagandának, és az álhírkeltésnek kiemelt szerepe van. [157]

A fenyegetettség növekvő tendenciája miatt a védelmi rendszer képességeinek bővítése nem odázható tovább. Ennek következtében a szövetséges tagállamoknak, köztük hazánknak szükséges a legmodernebb technológia védelmi képességeire koncentrálni.

Egyre inkább elterjedt a robotok harctéri alkalmazása a katonák munkájának megkönnyítése érdekében. Találkozhatunk kerekes, lánctalpas vagy lábakkal ellátott miniatűr katonai robotokkal, de léteznek nagyobb robotok is, amelyek nagy teherbírásúak, ezáltal képesek több tonnányi katonai felszerelést szállítani. Ezenkívül a háborús hadszíntereken megtalálhatóak a levegőben felderítő, vagy csapásmérő feladatot ellátó távolról vezérelt repülőgépek és improvizált robbantótest semlegesítő tűzszerész robotok is. Az aknamentesítő, robbanótest hatástalanító robotokat és a fegyverekkel felszerelt távirányítású robotokat a jövőben olyan fejlesztéseknek vetik alá, hogy képesek legyenek az előre meghatározott terület járőrözésére, és az ellenség kiiktatására. [158 pp. 3-21]

A robotizálás nemcsak az újonnan kifejlesztett MI hasznosításával, hanem a már meglévő járművek, repülőgépek autonóm működésének átépítésével is elérhető. Az USA haditengerészete így alkalmazza az MQ-8C távolról irányított helikoptert, amely a Bell 407-es helikopter átalakított változata. Oroszországban a BMP-3 típusú gyalogsági harcjármű átépítéseként számítógépek kerültek a kezelők helyére. Az orosz Uran-6 típusú tűzszerész robot, a horvát MV-4 DOK-Ing továbbfejlesztése, amely nagyméretű lánctalpas aknamentesítő rendszer. Kínában 2014-ben mutatták be a Sharp Claw 1 UGV, pilóta nélküli szárazföldi járművet, amely egy gumikerekes könnyű páncélozott terepjáró jármű segítségével önállóan tudja megközelíteni az ellenséges területet. A robotjárműnek saját felderítő- és fegyverrendszere van, az utóbbi használatához katona szükséges. A jármű egyszerre képes a levegőben és a földön is felderítést végezni tekintettel a kis hatótávolságú quadrocopterre. Az USA és Oroszország már elkezdte a tengeralattjáró

vadász, hadihajó tesztelését, az USA haditengerészete pedig a hajókon és tengeralattjárókon kialakuló tűz oltására alkalmas robotok fejlesztését. [159]

4.4 A Digitális Katona Program

Az intelligens katonai felszerelés ötletével elsők között az USA állt elő az 1990-es évek végén. A fejlesztések során a lézer alapú technikát, a beépített számítógépként működő digitális taktikai térképet és a saját- és csapathelyzetet megjeleníteni képes sisakképernyős rendszert alakítottak ki. Kifejlesztették az elődjénél jóval könnyebb lövedékálló kevlár sisakot, amelyre olyan speciális kijelző erősíthető, amelyen egy másik katona fegyverére szerelt kamera képe, vagy akár az ellenség helyzete és a harctéren történő események is elérhetőek. A jövő tervei szerint a felcsatolható gázmaszkkal együtt légmentesen záródó sisak 3D-s kijelzőkkel és 3D-s audió rendszerrel kerülne kibővítésre, mely technológia segítségével az ellenség már messzebbről észlelhetővé válna a katona számára. Az USA hadseregében a katonák olyan védőmellényt kaptak, amely egyaránt védi a felsőtestet, a combot és a felkart is. A hosszú távú cél, a jelenleginél súlyban könnyebb és hatékonyabb védelmet biztosító páncélkialakítás titán kompozit védőpanelek alkalmazásával, amely képes akár a közelről kilőtt géppuskalövedék megállítására is. [55]

A katonai egyenruháknak alkalmazkodniuk kell a különböző éghajlati övekhez. A modern technológia miatt azonban az egyenruhák nagy volumenű fejlesztése tapasztalható, egyre alkalmazkodóbbak és kényelmesebb, praktikusabb viseletet biztosítanak a katonáknak, ezáltal hozzájárulnak a harctéri teljesítmény növeléséhez. A jövőbeli elképzelés szerint az egyenruhák megfelelően szellőző, víztaszító, ellenálló anyagokból készülnek majd, a speciális éghajlati övekhez alkalmazkodva hűtő- és fűtőfunkcióval ellátva. A jelenleg is használatban lévő hűtőmellényekben egy olyan kristályos anyag van, amely vízzel érintkezve gél állagúvá válik, így biztosítja a hűtő funkciót. Ezt a technikát már a 2000-es évek közepén az iraki övezetben harcoló katonáknál sikerrel alkalmazták. [160]

Az USA hadseregének ruházat- és felszerelés mintája többgenerációs fejlődésen ment keresztül. A terepszínű egyenruhákat felváltotta a digitalizált minta. Az új pixeles Canadian Disruptive Pattern (CADPAT) nevű álcázó mintát először 1996-ban használta a kanadai hadsereg, majd ezt felváltotta az USA tengerészgyalogsága által 2001-ben használt Marine Pattern (MARPAT) mintája és végül az USA hadserege 2005-ben hadrendbe állította a Universal Camouflage Pattern (UCP) nevű pixeles mintát, amely

mára számos hadseregnél elterjedt. Az USA kutatja annak a lehetőségét, hogy a digitalizált egyenruha milyen módon tudná kaméleon módjára felvenni a háttér színeit, illetve az öltözék hogyan lenne képes teljesen azonosulni a mögötte lévő táj képével. [161]

Az USA a Land Warrior, az Objective Force Warrior és a Future Force Warrior programok keretein belül fejlesztette az intelligens katonai egyenruhát és a digitális katonai felszereléseket. A digitális hadviselés célja, hogy minden katona rendelkezzen olyan adóvevővel, amely képes hangot, adatot és képet is közvetíteni a harctéren lévő katona és a parancsnokság között. Az elképzelések alapján a rádiórendszer, a számítógép és az elektromos rendszerek kábelei a hámban és ruházatban kerülnének elhelyezésre, ezáltal biztosítva a katona zavartalan mozgását. [162]

A Future Force Warrior koncepciója olyan technológiák radikális alkalmazását irányozta elő, mint a nanotechnológia, a motoros exoskeletonok és a magnetoreológiai folyadék alapú testpáncélok. [163]

A nemzetközi fejlesztések vonatkozásában, dél-koreai kutatók egy olyan speciális bőrt dolgoztak ki, amely viselése során képes láthatatlanná tenni a katonákat. A különleges anyag speciális képességekkel bír, azaz nem látható sem emberi szemmel, sem infravörös éjjellátó kamerával. A kutatások szerint a bőr önálcázó képességgel rendelkezik és a környezetet érzékelve képes lehűteni vagy felmelegíteni magát, ezáltal észrevehetetlenné válik a hőkamerák számára. A speciális anyag színváltozásra alkalmas különálló pixelekből áll, amelyek termokróm folyadékkristályokat tartalmaznak, ez azt jelenti, hogy az eszköz érintésre fel tudja venni a környezete színpixeleit. A kutatók jövőbeli célja, hogy az eszköz képes legyen szélsőséges időjárási körülmények között is automatikusan, önállóan működni, mely fejlesztést egy mikrokamera beépítésének segítségével érnének el. [164]

A Central Research Institute for Precision Machine Building haditechnikai mérnökeinek legújabb fejlesztése egy orosz katonák számára tervezett páncél, amely lövedék-és repeszálló, a sisakjába pedig beépített kijelzőt építettek. A páncél egy úgynevezett exoskeleton, amely viselése során, mesterséges vázként erősebbé teszi a katonákat. Az exoskeleton elődje a szintén orosz fejlesztésű Sotnik nevű ruházat, melybe éjjellátó és egy olyan szűrő került beépítésre, amellyel a ruhát viselő katona képes ivásra alkalmas víz előállítására. [165]

Az USA kutatói már hosszú évtizedek óta dolgoznak olyan exoskeletonok fejlesztésén, amelyek képesek egyfajta külső csontvázként megnövelni a katonák erejét, vagy akár

páncélként védeni őket. Franciaország egy saját szuperkatona-programon dolgozik, amely keretein belül implantátumokat és egyéb technológiai eszközöket tesztelnek. A jövő katonai védőeszközeit már nanotechnológiás repeszálló mellények, sisakok és megszilárdulni képes folyékony páncélok alkothatják. Ezek a fejlesztések már az előszelei lehetnek a jövő hadseregének, amelyben a katonák és a robotok az MI segítségével együtt harcolhatnak. A brit hadsereg lépéseket tesz afelé, hogy 2030-ra a hadsereg negyedét a katonák munkáját segítő robotok alkossák. Úgy vélik, hogy az Európa-szerte jelentkező humán erőforráshiány ily módon lenne pótolható. Mindezekre való tekintettel 2050-re kialakulhat egy olyan harctér, ahol autonóm robotok és génmódosított szuperkatonák állnak majd harcban. [166]

A 21. században fontos, hogy a magyar katona is olyan elektronikai eszközökkel rendelkezzen, amely hangot, szöveges- és képüzeneteket tud fogadni, vagy küldeni egy védett alapú kommunikációs csatornán. Ezért a nemzetközi fejlesztésekkel összhangban a Zrínyi 2026 keretein belül Magyarország is elindította a Digitális Katona Programot, amelynek központjában a katona áll. A program célja az új, korszerű harcászati felszerelés: ruházat, bakancs, repeszálló mellény, málhamellény, sisak, hátizsák és egyéni fegyverzet biztosítása a kiképzési idő tartamára és a terepen lévő katonák számára. [167]

Mivel az USA által kifejlesztett digitalizált ruha hazai terepen nem rejt túl jól, a Digitális Katona Program első fázisában a régi sötétebb színű gyakorlókat leváltották a világosabb színű, infrasugarakat elnyelő gyakorló ruhák. A magyar katonák egyéni fegyverzete a kiskunfélegyházi fegyvergyárban készül, ahol pisztolyok, géppisztolyok és gépkarabélyok gyártására kerül sor. A Digitális Katona Program keretein belül beszerzésre kerültek a katonák egyéni felszerelését képező új sisakok. Az eszközök beszerzését követően a cél, hogy egységes rendszert képezzenek és digitális technológiával lássák el őket. A már beszerzett eszközök: az egyenruha; a fegyverzet; a vegyivédelmi felszerelés és az egészségügyi felszerelés rendszerbe integrálása már folyamatban van. A rendszert a tesztelések során digitális platformra állítják. Többek között a szárazföldi haderőnem fejlesztése során beszerzett Lynx harcjárművek is segítik a Digitális Katona Program tesztelését. A Digitális Katona Programot nemzetközi tapasztalatok alapján – amerikai, francia, olasz és német mintára – egy magyar kutatócsoport dolgozta ki, a szárazföldi haderőnemi szemlélő és a felderítő csoportfőnök irányításával, akik együttesen felelnek a szárazföldi haderőnem digitális platformra állításáért. A program sikeressége az eszközök és a technológia naprakészségében rejlik. Ennek érdekében az MH MI feladata monitorozni az új trendeket és javaslatot tenni az

elavult eszközök cseréjére. A jövőbeli cél a digitális eszközrendszer teljes körű felmérése, kiszolgálása, beszerzése és rendszerbe állítása. A katonák digitalizációja azonban az új felszerelésen és kiképzésen túl a katonák és vezetőik gondolkodásmódját is megváltoztatja, ez azt jelenti, hogy a centralizált vezetési rend és ezzel együtt az MH is egyre inkább decentralizálttá válik.

A beszerzett felszereléseket a szentendrei Altiszti Akadémia Acélkocka programjában résztvevő katonák kapták meg, azonban a honvédség tervei között szerepel, hogy a közeljövőben már egy teljes zászlóaljat felszerelnek az új eszközökkel, hosszú távon pedig minden katonának, köztük a tartalékosoknak is biztosítanak digitális eszközöket. A külföldi missziókban szolgáló katonák felszerelésének digitalizációja még folyamatban van. A NATO követelmények szerint 2028-ra kell a honvédség egy nehézdandárját az új felszerelésekkel ellátni és az eszközök használatára kiképezni. A hosszú távú cél az, hogy 2030-2032-re az egész honvédség rendelkezzen digitális felszereléssel és a használatukhoz szükséges tudással. [168 pp. 56-70]

4.5 Az MI alkalmazása a harctéren

A technológiai előrehaladás következtében megváltoztak az emberek és gépek közti szerepek. A disszertációban már bemutatásra került a hadsereg átalakulása, modernizációja. Amíg a hagyományos hadviselés korában emberek harcoltak egymással, addig az ipari forradalom hatására egyre inkább előtérbe került a gépek, harci eszközök használata. A technológiai forradalom és digitális robbanás következtében felgyorsult a digitalizáció és az analóg alapú rendszereket felváltották a hálózatalapú rendszerek.

Az 1950-60-as években számítógépek segítségével egyes, időigényes munkafolyamatok automatizálásra kerültek. Az emberi intelligencia szimulálásának lehetőségével jött létre az MI kutatási területe. Az MI egy gép, program vagy mesterségesen létrehozott tudat által megnyilvánuló intelligencia. Az MI kutatás első fázisának alapjául szolgált az az igazolt feltételezés, hogy az MI képes olyan problémamegoldásra, amely alapvetően emberi intelligenciához kötött. A második fázisban a gépi tanulás került előtérbe. A harmadik fázis célja pedig, hogy az MI K+F tevékenységek túlmutassanak az emberi parancsok gépek általi végrehajtásán. A DOD kutatásokért felelős részlege, a Defense Advanced Research Projects Agency (a továbbiakban: DARPA) célja, hogy az MI által vezérelt robotok, gépek, eszközök kollégaként, az emberi intelligencia kiegészítéseként működjenek. A fenti cél érdekében üzemeltetett informatikai rendszerek engedélyeztetése kritikus fontosságú tekintettel

arra, hogy az érzékelő, a kommunikációs rendszerek és az információk halmazával, olyan sebességgel generálódhatnak adatok, amelyek gyorsabbak az emberi intelligenciánál. Ez azt jelenti, hogy az emberek lemaradhatnak a gépekhez képest. Ezen technológia hadviselésben működő katonai rendszerekbe való beépítésével elérhető, hogy jobb, gyorsabb és komplexebb döntések következtében – akár a pilóta nélküli rendszerek autonómiájával – katonai hadászati feladatok kerüljenek végrehajtásra. [169 pp. 71-79]

Az MI tudományterülete nemcsak a műszaki tudományterület, hanem a haderő számára is kihívást jelent. Az MI szempontjából a civil piaci szereplőkön túl nagy szerepet játszanak a katonai alkalmazási területek is. A NATO tagországok közül az USA képviseli az MI kutatások vezérfonalát, azonban Oroszország és Kína is nagy hangsúlyt fektet az MI hadviselésben történő alkalmazására. Az USA célja, hogy az MI beépítésre kerüljön az autonóm járművekbe.

Ez azt jelenti, hogy az MI-t az alábbi területeken alkalmazzák:

(1) a környezet észlelése;
(2) az akadályok feltérképezése;
(3) a navigáció tervezése;
(4) más járművekkel való kommunikáció során.

Az új generációs harci robotok fejlesztése is megkezdődött, így lánctalpas, gumikerekes egyre nagyobb hatótávolságú, okosabb rendszerek is hadrendbe állhatnak.

Kína kutatási területe a gyors és tájékozott döntéshozatal megkönnyítésére és az autonóm katonai járművek fejlesztésére fókuszál, míg az oroszok a robotika fejlesztését tűzték ki célul. [170]

Az MI kutatási területén a NATO és az EU célja is azonos, miszerint a kormányzati, ipari szereplők és további kapcsolódó testületetek együttes részvételével akarnak kialakítani egy koalíciót az MI fejlesztések érdekében. NATO tagországként Magyarországon is fejlődik az MI kutatási területe, amelynek keretein belül együttműködések alakultak ki a kormányzat, egyetemek, KKV-k és egyéb piaci szereplők, tudósok részvételével. Az ITM (jogutódja: TIM) gondozásában 2018 októberében jött létre az MI Koalíció (a továbbiakban: MIK), [171] amelynek célja az MI területén résztvevő magyarországi szereplők közti koordináció az MI széles körű felhasználása érdekében. 2020-ban került elfogadásra a MIS, [172] amely végrehajtása érdekében 2019 őszén Nemzeti MI Akcióterv indult.

Az Akcióterv kapcsán megalakult munkacsoportok hat terület mentén kerültek kialakításra:

(1) alkalmazások és piacfejlesztés;
(2) technológia és biztonság;
(3) adatipar és adatvagyon;
(4) nemzetközi kapcsolatok;
(5) oktatás és tudatosítás;
(6) szabályozási és etikai keretek.

A Stratégia kidolgozása érdekében az Akcióterv keretein belül a HM is képviseltette magát a kibervédelem és felhőalapú technológiák MI fejlesztési területen belül, a Technológia és Biztonság Munkacsoport tagjaként. 2019 januárjában került létrehozásra az MH MI a védelmi célú K+F tevékenységek támogatása érdekében.

Az MI katonai érdekeltségű kutatási területei az alábbiak mentén határozhatók meg:

- autonóm irányítású szárazföldi járművek vezérlése, útvonal-megválasztás optimalizálása, autonóm szárazföldi jármű képességfejlesztések;
- radartelepítési helymeghatározás a felderítési képességek optimalizálása érdekében, radarcéltárgy észlelésének optimalizálása, automatizált céltárgy osztályozás;
- vezetési rendszer szoftveres döntéstámogatása és helyzetértékelés;
- kamerákból származó képek feldolgozásán alapuló anomália észlelés, automatizált riasztás, digitális katonai, felderítési képességek fejlesztése. [173 pp. 3-12]

A nemzetközi és hazai minták alapján megállapítom, hogy az MI katonai hasznosítása földön, vízen és levegőben egyaránt kiemelkedő szerepet játszik a harctéren.

A 2022. február 24-én kezdődött orosz-ukrán háború kapcsán is alkalmazzák az MI-t. Az ukránok az elesett orosz katonák azonosítására használják a Clearview AI-t, amely egy USA-beli arcfelismerő cég által elérhető szoftver. Az ukránok ingyenes hozzáférést kaptak a vállalat adatbázisához az azonosítás érdekében. A fenti példa a bizonyíték arra, hogy a 21. századi harctéren eredményesen alkalmazható az MI, ugyanakkor fontos kiemelni, hogy az adatok sértetlenségéről, azok megfelelő kezeléséről is gondoskodni kell, még egy fennálló háborús helyzet során is. [175]

A Zrínyi 2026 kapcsán az előzőekben bemutatott új beszerzések és a már meglévő eszközök modernizálása és hadrendbe való állítása az első lépés ahhoz, hogy az MH is kiépítse az MI hadszíntéren történő eredményes használatát.

4.6 Digitális képességek fejlesztése

A honvédség jelentős átalakulásokon megy keresztül, melynek keretében a legkorszerűbb eszközök kerülnek beszerzésre, mindez megteremti a K+F+I alapjait. Információs hadviselés megy végbe a kibertérben, és valamennyi hadszíntéren egyaránt bekövetkeznek a változások. A terrorszervezetekkel szemben a hagyományos haderő már nem képes hatékonyan fellépni, ezáltal megkezdődött a negyedik generációs hadviselés kora. Ennek tükrében a honvédség legfontosabb feladata a reagálóképesség növelése és a megoldások keresése a digitális transzformáció haderőben történő sikeres végrehajtásához.

A 21. századi siker kulcsa a központi vezetői szándék decentralizálása mellett a kor aktuális kihívásainak felismerése és kezelése. Mindezek érdekében szükséges a problémamegoldás, a kritikus gondolkodás, kreativitás, a hálózatépítés és a változó körülményekhez történő gyors alkalmazkodás, mint emberi képességek fejlesztése. A hadviselés innovációját nemcsak az új technológia jelenti, hanem e technológiák készségszintű alkalmazása, gyors elsajátítása, újszerű hasznosítása a legújabb fegyverek és gépek terén. Mindezek hozzájárulnak ahhoz, hogy az ország egy rugalmasabb haderővel rendelkezzen és az új technológiák alkalmazásához egy megfelelő szervezeti struktúra kerüljön kiépítésre.

Az új technológiák, a modern fegyverek és a védelmi képességek fejlesztése nemcsak fizikai többletterhet jelentenek a katonák számára, hanem megkövetelik a kognitív képességek fejlesztését is. Az agyi képességek fejlesztése ugyanúgy kivitelezhető, mint a fizikai állóképesség kiépítése. A haderőfejlesztés és modernizáció kapcsán digitalizált eszközök, fegyverek, ruházat és felszerelés ugyanúgy algoritmusokon alapszanak, mint a civil életben használatos applikációk. Ezek alapja a *deep learning*, amely neuronhálózatok alkalmazását jelenti. [176]

A DARPA és a Platypus Institute a katonai teljesítmény neurotechnológiai fejlesztésével foglalkozik. Az intézetek a kognitív képességek fejlesztésének lehetőségeit veszik számba az agy alkalmazkodóképességének a dinamikusan fejlődő technológiai környezetben történő vizsgálatával. [177] A kutatás tárgya a katona egyéni kognitív képességeinek és a katonai csoportok együttes műveleti tevékenységének vizsgálata.

Ezenfelül a vizsgálatok tárgyát képezi az ember és a robot együttműködése is. A kutatásokra azért van szükség, mert a digitális technológia rohamosabb mértékben fejlődik, mint ahogy azzal az emberi agy képes lenne lépést tartani, ezért szükséges az egyéni képességek kognitív fejlesztése. Az USA hadseregének különleges műveleti erő felkészítő programjában alkalmaznak egy szimulációs programot is. Az *online* szimulációs rendszert a parancsnoki képzési programon belül a vezetői magatartás és módszerek oktatására használják. [178]

Magyarországon a Digitális Katona Program keretein belül az eszközpark kialakításának biztosítása mellett a kutatók az eszközök kezeléséhez és a napi munkához szükséges fizikai, kognitív (VR alapú szimulációs rendszer) és mentális képességeket fejlesztő programok kialakításával foglalkoznak. A katonák teljesítménye függ a megfelelő szituációs, döntési- és stresszkezelő technikák alkalmazásától is. Ennek érdekében alkalmazzák a komplex humán fejlesztési programot. A humán fejlesztés célja, hogy a katonák egészségi, fizikai, pszichés és mentális felkészültsége, továbbá egyes területeket érintő specifikus képessége maximális szinten tudjon kibontakozni. A komplex humán képességfejlesztés a maximális katonai teljesítmény kiaknázására és az újonnan beszerzett eszközök szakszerű használatának összhangjára fókuszál. A katonák humán teljesítőképességének fokozása érdekében a tudományos eredményeket hasznosítva, a megfelelő jogi, etikai és morális keretek alkalmazásával biztosítják a hatékonyságot fokozó harctéri fölény megteremtését és a túlélőképesség fokozását. [179 pp. 56-70]

A HM-ben és az MH-ban 2019-ben kezdődtek meg az intézményi átalakulások és ezzel együtt a szervezetfejlesztés is. Létrejött az MH MI és a Védelmi Kutatóintézet. A HM magyar felsőoktatási intézményekkel működik együtt számos kutatási projekt beindítása kapcsán. Az NKE képzései és továbbképzései biztosítják az új technológiák szakszerű használatának elsajátítását, és az új biztonsági kihívásokkal való eredményes szembeszállást úgy a mérnökképzések, mint a hibrid hadviselés kialakítása szempontjából jelentős kiberbiztonsági képzések tekintetében. [180]

4.7 A katonai kiképzési és oktatási rendszer

A Zrínyi 2026 kapcsán modernizálásra, digitalizálásra kerül az MH technológiája, a fegyverek és az eszközpark is. Mindez azt eredményezi, hogy nemcsak az eszközöket fogadó és működtető infrastruktúrát, hanem a katonák képzési, kiképzési rendszerét is modernizálni kell. Az analóg technológiai alapú rendszereket felváltják a digitalizált,

modern eszközök, a rohamos technológiai fejlődés és a megnövekedett internethasználat következtében a katonáknak is alkalmazkodniuk kell az információs túlterheltség kihívásaihoz.

Az új képzési- és kiképzési rendszer alapja az új eszközök és a kiképzett katona összekapcsolása. A korábbi kiképzési rendszert az új helyzet kihívásaihoz mérten szükséges átalakítani. Ez azt jelenti, hogy a katonáknak a hagyományos kiképzés mellett rendelkezniük kell a modern, digitális alapú eszközök ismeretével is. A kiképzési rendszer átalakítása az új haditechnikai eszközök rendszerbe állításával párhuzamosan jelenik meg. A jelenlegi kiképzési rendszer alapját 80%-ban a hagyományos és 20%-ban a szimulációs kiképzés alkotja. Az új rendszer viszont megköveteli az arányok megfordítását, amely azt jelenti, hogy a szimulációs eszközök teljes körű ismerete után tudnak majd a katonák a gyakorlótereken kiképzést végrehajtani. A rendszer működése a technikai eszközök, a szervezeti felépítés, az eljárásrendek és a vezetési elv szinkronjában rejlik. A szimulációs gyakorlatokhoz segítséget nyújtanak a lőkiképzést támogató virtuális és valós gyakorló eszközök, berendezések, a kétoldali gyakorlásra (force on force tactical training) használható lézeres szimulációs rendszerek (MILES, iMILES). A szimulációs gyakorlatok előnye, hogy költséghatékonyak és a szimulátorok segítségével az új eszközök képességeit jóval gyorsabban elsajátíthatják a kezelők. [181 pp. 223-234]

A régebbi és az új szimulációs eszközök rendszerbe illesztése során azonban fontos alapelv a hagyományos és a szimulációs kiképzés összhangja, mert a terepen történő kiképzés nem helyettesíthető teljes mértékben a szimulátorokkal. A digitális katona alapképességeit is a fizikai állóképesség, a tájékozódó képesség, a lőkészség és a hagyományos eszközökkel való kommunikációs képesség adják. A négy alapképesség meglétét követően tudják elsajátítani a katonák azokat a digitális készségeket és képességeket, amelyek a modernizált eszközök kezeléséhez és működtetéséhez szükségesek. [54 pp. 141-157]

A NATO 2014-ben kiadott ajánlásának megfelelően, valamint a megváltozott biztonsági környezet és az MH feladatainak bővülése eredményeként a Zrínyi 2026-tal összhangban 2019 őszétől alakította át a honvédség az altisztképzési rendszerét is, amely az Acélkocka nevet kapta. [182]

Az Acélkocka altisztképzési rendszeren belül tanfolyamrendszerű felkészítés során elméleti és gyakorlati ismereteket sajátíthatnak el az MH altisztjelöltjei. A képzés kereteit (1) a megváltozott biztonsági környezet; (2) a terrorizmus elleni küzdelem kihívásai; (3) a harceljárások; (4) és a technikai eszközök korszerűsítési folyamatai adják. Az

altisztekkel szemben támasztott követelmények között szerepel – a feladat végrehajtáson túl – a vezetői képességek kialakítása, fejlesztése is. A honvédség technikai korszerűsítése a Zrínyi 2026 keretein belül zajlik, az újonnan beszerzett, modern eszközök kezelésére és üzemeltetésére készítik fel a katonákat a szentendrei központú Altiszti Akadémián. Az altisztek képzésének átalakítása mellet a legénységi állomány felvételi és képzési követelményeit is a haderőfejlesztés folyamatához és a technikai eszközök korszerűsítéséhez igazítják. Az altisztek képzése – összhangban a NATO ajánlásaival – öt alegységben történik. Az első három szakaszban az altiszti pályára hivatottak, a negyedikben a haladó altiszti pályára készülők és az ötödikben a zászlósi tanfolyamokban tanulók vesznek részt. [183 pp. 93-115]

4.8 A nyilvántartási rendszerek digitalizálása

A közigazgatásbeli rendszerek digitalizálásának egyik fontos lépcsőfoka az Integrált Jogalkotási Rendszer (a továbbiakban: IJR) fejlesztése, amely 2016-ban kezdődött meg a közigazgatás adminisztratív terheinek csökkentése, valamint a szolgáltató képességének növelése érdekében. [184]

Az IJR célja a színvonalasabb jogalkotás, ennek érdekében a rendszeren belül minden jogszabállyal kapcsolatos tevékenység informatikailag támogatott, az első tervezet megszületésétől a Magyar Közlönyben történő kihirdetésig.

Az IJR több modulból áll, ilyen az Elektronikus Jogszabály-előkészítő Rendszer (EJR), amely a jogszabály-tervezet szerkesztést és szövegezést, azaz a kodifikációt támogatja. Az IJR alrendszerei közé tartozik a GovLex a ParLex és a LocLex. A GovLex a kormányzati jogszabályok előkészítéséért felelős. Olyan informatikai háttérrel rendelkezik, amely *interface* biztosítja a jogszabályok, előterjesztések, és jelentések véleményezését, megosztását, továbbá szervező, lekérdező, nyilvántartó és végrehajtó, ellenőrző szolgáltatások is elérhetőek. A törvényalkotás parlamenti informatikai rendszere a ParLex, amely egy parlamenti dokumentum- és irományszerkesztő, folyamatkezelő rendszer. A ParLex a megfelelő felhasználói- és adatbiztonság mellett biztosítja az egyes irományok szerkesztését és elektronikus benyújtását. [185] A LocLex rendszer az önkormányzatok jogszabály előkészítési-, szerkesztési- és feltöltési folyamatait támogatja.

A HM az elektronikus ügyintézés jegyében 2015 februárjától alkalmazza sikeresen a HM Költségvetés Gazdálkodási Információ Rendszer, Ügyfélszolgálati Rendszert (HM KGIR ÜSZR), amely univerzális portálként alkalmas a pénzügyi nyilvántartások és

személyi ügyintézés mellett, a teljes állomány számára elérhető gyors és személyes megjelenést mellőző elektronikus ügyintézésre is. A Nemzeti Infokommunikációs Stratégiában (NIS) foglaltak szerint a digitális állam koncepciójának megfelelően 2017. május 1-jétől lehetőség nyílt a kormánytisztviselők személyügyi okmányainak elektronikus aláírására, és 2018. január 1-jétől bevezetésre került az elektronikus ügyvitel és ügyintézés az MH-nál és a HM-ben egyaránt. [186][1]

A HM is csatlakozott az IJR projekthez, így a tesztüzemet követően az éles rendszer a tárcán belül is bevezetésre került. Az IJR éles üzemének bevezetésére a tesztüzemet követően, 2020. augusztus 1. napjától került sor. [187]

4.9 A magyar űrprogram

Az NKS szerint a világűr, mint műveleti tér lehetőséget ad a nagyhatalmaknak, hogy a szárazföldi és vizek felett telepített rendszerek által békeidőben katonai előnyre tehessenek szert, háború esetén pedig biztosított legyen hadászati fegyverrendszereik működtetése, a hadszíntér felderítés, ellenőrzése és csapásmérése. [39]

Az NBS-ben meghatározottak alapján az űrtechnológia területét érintő gyors fejlődés a területet érintő nagy technológiai minőségi ugrás várható. Az űrtechnológia ezért meghatározó jelentőségű lesz az országok fejlettsége, gazdasági, társadalmi viszonyai és politikai érdekérvényesítő képessége tekintetében. A magas technológiájú know-how kereteit biztosító és innováció alapú űrszektorban elfoglalt helyünk kiemelt fontosságú, mert ez adja az alapját világűr gazdasági, nemzetbiztonsági és védelmi területeihez való hozzáférésnek. Magyarország célja egy olyan 21. századi rendszer felállítása, amely jelentős magyar ipari hozzájárulással történik és a NATO által, vagy akár világviszonylatban is elismert.

A külgazdasági és külügyminiszter 2019-ben, az ESA konferenciáján jelentette be, hogy Magyarország fokozza a világűrbeli jelenlétét. A magyar űrprogram fellendítése érdekében 2019 novemberében a magyar külgazdasági és külügyminiszter az Orosz Szövetségi Űrügynökség (Roszkoszmosz) igazgatójával folytatott tárgyalásokat. A magyar-orosz koalíció célja, hogy a jelenleg Oroszországban futó magyar technikai és technológiai értéket képviselő űrprogramok hivatalosan is magyar-orosz űrkutatási projektekként folytatódjanak. Az együttműködés hosszú távú célja egy magyar űrhajós kutató munkájának a Nemzetközi Űrállomáson, International Space Station (a

[1] A NIS-t az NDS váltotta fel [3]

továbbiakban: ISS) történő biztosítása, továbbá, hogy a kutatóűrhajós magyar fejlesztésű és szellemi értékű űripari eszközöket telepíthessen az ISS-en. [188]

A magyar-orosz koalíció új lehetőséget ad a magyar űripar fejlődéséhez, fejlesztéséhez és a már meglévő magyar technológiák elterjedéséhez. [2]

2021 novemberében a Magyar Kormány űrkutatási együttműködésről szóló stratégiai megállapodást kötött a francia-olasz Thales Alenia Space-szel, amely a világ egyik vezető űripari vállalata. Az együttműködés célja közös K+F projektek indítása, ezentúl a cég biztosítja a magyar űripari szakemberek képzését, továbbá segítséget nyújt a magyar vállalatoknak az európai és világszintű műholdprogramokban való részvételben. Jelenleg a Thales Alenia Space biztosítja az ISS-en található eszközök felét. Magyarország érdekelt az űripar fejlesztésében, ezért kiemelten fontos a szektor további fejlesztése.[189]

A magyar űrprogram a hazai űripari vállalatok és egyetemek űriparral és űrtechnológiával foglalkozó kutatóinak segítségével jöhet létre. A sikeres koalíció és a magyar űripar fejlesztése érdekében az űrkutatás területével, a nemzeti űrkutatási alap létrehozásával bővült ki a Külgazdasági és Külügyminisztérium (a továbbiakban: KKM) portfóliója. [190] A magyar űripar fejlesztése érdekében 2022-ban újra kinevezték a KKM-ben az űrkutatásért felelős miniszteri biztost, akinek feladata többek között az űrkutatási tárgyú szerződések és szabályzók kidolgozása; az űrkutatás fejlesztésére vonatkozó stratégiák tudományos-szakmai felügyelete; a Kormány álláspontjának kialakításában való közreműködés az űrkutatással kapcsolatos tudományos témákhoz kapcsolódó, hazai és nemzetközi űrkutatási szervezetekben és fórumokon. [191]

A magyar űrképesség kialakításában a KKM mellett az MH is részt vesz. Az űrkutatás kapcsán a civil tudósok és a katonák együttműködése elengedhetetlen ahhoz, hogy kialakíthassuk az űrképességeket és alkalmazkodjunk az űrhöz, mint új műveleti területhez. Hazánkban jelenleg is jelentős az űripari tevékenység, mert számos vállalkozás vesz részt műholdak alkatrészeinek és részegységeinek a gyártásában. A távlati cél viszont, hogy magyar űreszközök – távérzékelési szolgáltatásokat nyújtó, vagy távközlési műholdak – kerüljenek a világűrbe. A KKM koordinálásával és az MH közreműködésével 2021 augusztusában elkészült a magyar Űrstratégia. [192 pp. 18-24],[193]

[2] A 2022 február 24-én kirobbanó orosz-ukrán háború hatással lehet a nemzetközi űrkoalícióra és az együttműködésekre, azonban jelenleg ennek következményeit egyelőre nem látjuk.

Az MH a felderítés és távközlés tekintetében jelenleg is alkalmazza az űrszolgáltatásokat. További cél a napjainkban használt műholdas távközlési szolgáltatások integrálása a Zrínyi 2026 által beszerzett haditechnikai eszközökbe és az adatszolgáltatás fejlesztése. Az űrhadsereg létrehozásában az USA űrhadereje, a United Space Force (USSF) áll az élen. Európában Franciaország és Nagy-Britannia vizsgálja az űrhaderőnem kiépítését. Ez a folyamat nem feltétlen jelenti új képességek elsajátítását, hanem elsősorban a meglévő képességek köré kerülnek kialakításra olyan szervezetek, amelyek szervezeti kultúrájukban, működési rendjükben és feladataikban a világűr felé összpontosítanak. Az űrbéli műveletek jellemzően elektronikai- és kiberműveletek. Az űrhaderő feladata, hogy támogassa az összhaderőnemi erőt és az államvédelmi, biztonsági feladatait végrehajtó szerveket. A katonai űrműveletek jellemzően támogató jellegűek, de vannak az elektronika- és kibervédelem területéhez tartozó saját űreszközök és képességek megvédése érdekében tett támadó műveletek is. A világűrben használt valamennyi űrfegyver tömegpusztító fegyvernek minősül, tekintettel arra, hogy a világűrt érintő pusztító hatások térben és időben is egyetemlegesek. [194]

Az MH a Zrínyi 2026 elindításakor felmérte a világban jelentkező kihívásokat. A szárazföldi- és légierő képességeinek növelése és a logisztikai rendszer átalakítása egyértelmű a honvédség számára, azonban az új műveleti területeken érkező kihívások az ún. *domainek*, mint a kibertér és a világűr szakmai kihívást és jelentős képességfejlesztési feladatot jelentenek.

A kibertéri képességek kiépítése az MHP-n jelenleg is működő kibervédelmi szemlélőség, és az MH KKK kialakításával kezdődött meg. A honvédség biztonságos kommunikációjának érdekében a légi távérzékelés és a műholdas távközlés képességének kialakítása is szükséges. [195 pp. 60-62]

Annak ellenére, hogy a nemzetközi jog egyelőre nem engedi a világűr militarizálását, előreláthatólag az USA, Oroszország és Kína is vezetési pontok telepítése céljából fogják használni az űrt. Mindez magában hordozza olyan autonóm rendszerek megalkotását és űrbéli pályára állítását, amelyek képesek a Földön telepített rakéták és pilóta nélküli eszközök működtetésére. Ahhoz, hogy ebben a folyamatban részt vehessünk, szükséges a honvédség képességfejlesztése is. Ennek érdekében jelentkezett az első tíz katona a Debreceni Egyetem, az Eötvös Loránd Tudományegyetem, a Budapesti Műszaki Egyetem és számos ipari cég közreműködésével indult közel fél éves űrképzésre. A honvédség rövid távú célja egy magyar, nemzeti műholdképesség kialakítása, ezért jelenleg a civilek bevonásával folyik az elméleti képzés és a szabályzók kialakítása. A

hosszú távú cél pedig egy nemzeti műholdflotta kialakítása. A célok elérésében fontos szerepet játszik az önerőn túl a nemzetközi együttműködés is, valamint a NATO-tagságunk. [196]

4.10 Katonai hírközlő és kommunikációs rendszer digitalizációja

Napjainkban a honvédség híradó, informatikai, valamint információvédelmi szolgáltatási tevékenysége új generációt képvisel, mert a rohamos technológiai fejlődés következtében az MH vezetéstámogató rendszere is változik, és az új biztonsági kihívások kezeléséhez mérten fejlődik. A Zrínyi 2026 keretein belül beszerzett új haditechnikai eszközök és képességfejlesztések megkövetelik a híradó informatikai rendszerek fejlesztését.

Az NKS a következőképpen határozza meg a honvédség vezetés-irányítási képességeinek fejlesztését:

- kialakításra kerül a küldetésorientált vezetés-irányítási struktúra és eljárásrend;
- kiépítésre kerülnek a fejlett, autonóm, hálózatalapú vezetéstámogató képességek, amelyek alkalmazása a technológiailag elmaradottabb, nem támogató környezetben is biztosításra kerül;
- biztosítva lesz a nagy sávszélességű, zavarvédett nyílt és minősített adatkapcsolat;
- biztosításra kerül a távközlési hálózatok kiber-és elektronikai hadviselés elleni védelme;
- nagy hangsúlyt fektetnek a kormányzati együttműködési készség javítására;
- nagy sávszélesség hiányának esetére kidolgozásra kerül egy eljárásrend;
- kiemelt szerepet kap az MI alapú döntéstámogató rendszerek, a szenzoros adatgyűjtő, -tároló, - és továbbító eszközök fejlesztése;
- kiépítésre kerül egy országhatáron kívüli támogató infokommunikációs hálózati rendszer;

A fejlesztések eredményeképp a honvédség vezetés-irányítási eljárásai, képességei rendszerei és szervezetei képesek lesznek a békeidőszakon túl a válság és konfliktushelyzetben is részlegesen vagy teljesen helyt állni. Az MH a vezetési elemeit úgy alakítja ki, hogy korlátozó, nukleáris, biológiai és vegyi szennyezés esetén is el tudják látni a haderő műveleti vezetés-irányítását. [39]

Az elmúlt évek során az alábbi fejlesztések történtek a honvédelmi tárcánál és a honvédségnél:

- bevezetésre került a kormányzati rádiótelefon rendszer,
- nőtt a missziók híradó-informatikai támogatottsága;
- fokozódott a harcjárművek híradó-informatikai eszközcseréje;
- megkezdődött az MH nagytávolságú adatátviteli hálózat kapacitás növelése;
- elkezdődött a tábori C2 szoftverfejlesztés;
- kibővültek a központi informatikai szolgáltatások;
- korszerűsödtek az ágazati informatikai rendszerek;
- a hagyományos, papír alapú iratkezelést felváltotta a digitális ügyintézés;
- bevezetésre került az Elektronikus dokumentum- és iratkezelő rendszer (EIR). [197 pp. 96-105]

A hatékony kormányzás, az ütőképes és korszerű haderő és a modern társadalom alapja az infokommunikációs rendszerek széles körű alkalmazása. A fejlett országok hadereje az elmúlt évek során nagymértékben függött az informatikai rendszerek hatékonyságának alkalmazásától és sérülékenységétől. A kormányzati, banki, piaci, katonai szektorban elkövetett kibertérbeli támadások káros hatása ugyanolyan mértéket ölthet, mint egy esetleges hagyományos fegyveres konfliktus következménye. Éppen ezért az ország védelemnek a kibertérben is helyt kell állnia. A honvédségnek és a HM-nek kötelessége és feladata az infokommunikációs rendszerek védelmének garantálása. A honvédelmen belüli kibervédelemért, az elektronikus információvédelmi felügyeletért és a hatósági feladatok ellátásért a KNBSZ felelős. Az MH Kormányzati Célú Elkülönült Hírközlő Hálózatának (a továbbiakban: MH KCEHH) kibervédelmi tevékenységét pedig a Honvéd Vezérkar Híradó, Informatikai és Információ védelmi Csoportfőnökség (IICSF) felügyeli és irányítja. [198 pp. 5-16]

Az MH átfogó digitalizációjának eléréséhez elengedhetetlen az MH KCEHH fejlesztése. Az MH KCEHH egy speciális, zártcélú infokommunikációs hálózat, amelynek képesnek kell lennie akár békeidőben, akár minősített időszakban az MH vezetés- és irányítási rendszereinek a támogatására a technológiai, technikai és szolgáltatási háttér, valamint a működési környezet biztosításával. A rendszer egy olyan hálózati alapú kritikus infrastruktúra, amely híradó és informatikai rendszerek és eszközök alapjain nyugszik. A hálózat feladata, hogy kiszolgálja a katonai felsővezetés híradó és informatikai igényeit, biztosítsa a vezetési-irányítási rendszerek technológiai és

technikai alapjait, valamint lehetővé tegye béke- és minősített időszakban is a híradó és informatikai szolgáltatások elérését. További feladata más infokommunikációs hálózatokhoz való csatlakozás és az arról való leoldás, azaz önálló működés biztosítása is. [199]

Az MH KCEHH rendelkezésre állása honvédelmi érdek. A digitális kornak megfelelő alapú technikák és szolgáltatások mentén működő hálózat fejlesztése azonban nem odázható tovább. Egyrészt meg kell felelnie a digitális robbanás következtében fejlődő nemzetközi elvárásoknak azért, hogy más nemzetek hálózataival és rendszereivel tudjon együttműködni, másrészt ehhez összhangban kell állnia a szövetségi tagságunkból adódó követelményrendszerrel.

A fejlesztéseket az alábbiak mentén szükséges eszközölni:

(1) sávszélesség, adatátviteli sebesség növelése;
(2) hardveres és szoftveres átviteli utak kapacitásbővítése;
(3) hardver, szoftverplatform, szerverfarmok cseréje, korszerűsítése;
(4) tartalékképzés, tartalékeszközök biztosítása;
(5) kibervédelmi képesség kialakítása, növelése;
(6) hálózati, felhasználói, hardveres, szoftveres biztonság kiépítése;
(7) rendelkezésre állás, megbízhatóság, rugalmasság biztosítása;
(8) a szolgáltatás minőségének növelése. [200 pp. 223-236]

Az alapvető cél tehát a híradó és informatikai rendszer, szolgáltatás- és információcentrikussá tétele, a felhasználóbarát többfunkciós, konvergált és korszerű digitális hálózat kiépítése és az általános fejlődés mellett a védelmi szféra fejlődése. További cél, hogy a szolgáltatások eljuthassanak a harctéren küzdő katonákhoz, valós idejű kép közvetítésével. A hálózatnak egyrészt biztosítania kell a polgári és rendvédelmi szervek hálózataival való együttműködést, másrészt kibertámadás, illetve különleges jogrend esetén az önálló zavartalan működést is. Az MH KCEHH fejlesztésének hosszú távú célja tehát, hogy a digitális- és hálózatalapú rendszerek képesek legyenek önállóan működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő jogrendben is. [201 pp. 94-105]

A katonai- és csapatvezetés működésének feltétele a híradó és informatikai támogatás. A katonai műveletek eredményességének feltétele a vezetési fölény, amelynek feltétele az információs fölény és a közös helyzetismeret megléte és fenntartása. Mindez

megkívánja a korszerű, modern távközlési- és információtechnológiát, a híradó-és informatikai eszközrendszer megfelelő alkalmazását. Valamennyi vezetési és szervezeti szinthez tartozó katonai információs és kommunikációs rendszer összekapcsolásával lehetővé tehető az információk valós idejű közvetítése és elérése a munkaállomásokon és mobil kommunikációs eszközökön. Ezzel a technológiai és szemléleti fejlődéssel jöhetett létre a hálózatalapú hadviselés a fejlett, korszerű haderővel rendelkező államokban.

A Hálózatalapú Műveleti Képesség rendszerbe szervezi az alábbiakat:

(1) csapatinformációk;
(2) műveleti környezeti térkép, - és terepinformációk és időjárás adatok;
(3) valós idejű felderítési adatok;
(4) műveleti környezeti és civil környezeti információk;
(5) a navigációs -és GPS adatokat;
(6) a saját csapat nyomkövető rendszerének adatait;
(7) a fegyverirányítási rendszerek digitális adatait;
(8) egyéb automatizált rendszerből származó adatokat és információkat, amelyek mind a Közös Műveleti Képen tudnak megjelenni.

Mindezek mentén zajlik a tábori híradó- informatikai rendszer digitális alapokra történő helyezése, modernizálása és fejlesztése, az infokommunikációs képességek hálózatba szervezése és a modern, korszerű híradó-informatikai rendszer kialakítása.[202]

Az elkövetkező évek fejlesztésének iránya a sokfunkciós, hordozható, komplex infokommunikációs szolgáltatások felé halad, amely lehetőséget ad (1) a mozgókép, hang, írásos és egy egyéb információk, adatok integrált kezelésére; (2) a többrésztvevős kommunikáció azonos idejű kivitelezésére; (3) és az automatikus információ keresésre, valamint adattársításra egyaránt. Ezáltal lehetőség nyílik az egymástól távol levő azonban együttműködő hírrendszerek, adatközpontok és szolgáltatások alkalmazására. Mindezek mellett a lokális hálózat által kiépített asztali munkaállomások, az irodai szolgáltatások elérhetősége az internet adta szolgáltatásokkal megteremti az otthoni, távoli munkavégzés feltételeit. A katonai információs rendszerek fejlődési és fejlesztési irányait a kormányzati és civil, piaci szereplőkkel történő átfogó kommunikációs képességre való törekvés határozza meg, az információbiztonság követelményeinek és a szolgáltatások folyamatos rendelkezésre állásának jegyében.

A fejlesztések tehát:

(1) az elavult számítógépek cseréjére;
(2) a szerverpark megújítására;
(3) a nagytávolságú adatátvitel sebességének növelésére;
(4) az adatátviteli kapcsoló berendezések, routerek fejlesztésére;
(5) a video-telekonferencia rendszer újítására;
(6) a védett és minősített informatikai hálózat megfelelő kiépítésére;
(7) az elektronikus iratkezelés szervezetszintű alkalmazására;
(8) az elektronikus aláírás és digitális időbélyeg szolgáltatás szervezetszintű kiterjesztésére;
(9) a szoftverek megújítására;
(10) és az üzemeltetés-támogatás újraszervezésére fókuszálnak.

A fejlesztések megvalósulásaként növelhető a rendszer biztonsága, a szolgáltatások színvonala és rendelkezésre állása, az üzemeltetés hatékonyabbá tehető és lehetőség nyílik modern és korszerű programrendszerek és alkalmazások használatára. A digitális platformra való átálláshoz azonban a katonai hírközlő és kommunikációs rendszer modernizációja mellett szükséges a megfelelő képzettségű és szaktudással rendelkező állomány biztosítása is. [197 pp. 96-105]

Összegzésképp megállapítom, hogy az MH digitalizációja érdekében ajánlásokként megfogalmazott tíz platform különböző intenzitással bír. Ez azt jelenti, hogy nem azonos súllyal jelennek meg a digitalizációs célok eléréséhez tett lépésekben. Ahhoz azonban, hogy az MH áttérjen és felzárkózzon a fejlett katonai, informatikai, digitális- és hálózatalapú rendszerekhez, ezzel biztosítva e rendszerek önálló és független működését, szükséges az ajánlások szerinti platformok azonos súllyal és intenzitással való kezelése.

4.11 Részösszefoglalás

A Zrínyi 2026 célkitűzési között szerepel a honvédség áttérése és felzárkózása az informatikai, digitális- és hálózatalapú katonai rendszerekhez. Annak érdekében, hogy valamennyi műveleti területen országunk a digitalizáció következtében kialakult új biztonsági kihívások ismeretével és ezek leküzdéséhez szükséges képességekkel rendelkezzen, a honvédségnek új szemléletű, digitális platformra szükséges átállnia.

A negyedik fejezet hipotézise az volt, hogy az MH széles körű digitalizációja akkor érhető el, ha a Zrínyi 2026 keretein belül megvalósuló/megvalósult fejlesztéseken és beszerzéseken túl a tíz platform azonos súllyal és intenzitással jelenik meg a honvédelem rendszerében.

A Zrínyi 2026 kapcsán már elért eredmények és a további célok ismeretének hatására fogalmazódott meg a tíz ajánlásba rendezett platform, amelyek megismerése, alkalmazása és fejlesztése által a honvédelem egésze digitális alapokra helyeződne. Ahhoz azonban, hogy az MH áttérjen és felzárkózzon az informatikai, digitális- és hálózatalapú katonai rendszerekhez, szükséges az ajánlások szerinti platformok azonos súllyal és intenzitással való kezelése.

Összességében tehát a Zrínyi 2026 célkitűzéseinek megvalósulása, valamint a digitális platformok azonos súllyal és intenzitással való kezelése esetén a honvédelem egésze digitális platformra állítható, amely azt eredményezné, hogy a piaci *high-tech* rendszerek és a közigazgatás által használt infrastruktúrákhoz igénybe vett védelmi, katonai, nemzeti biztonsági rendszerek önállóan, leválasztva is működhetnek a Kormány infokommunikációs támogatása érdekében.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A doktori értekezés az alábbi kérdéseket kutatta:

- Milyen módon igazolható, hogy a 21. századi kihívások hatékony kezelése komplex nemzetközi együttműködéssel, ugyanakkor a védelmi szektor adaptív képességfejlesztésével, a honvédség modernizációjával, strukturális és eljárásrendbeli átalakításával érhető el?
- Milyen módon állapítható meg, hogy a digitalizáció az egyik leghangsúlyosabb biztonsági kihívás?
- Milyen módon igazolható, hogy a honvédelmi, katonai és nemzeti biztonsági rendszerek hazai digitális hálózatba való beágyazódása a Zrínyi keretein belül a légierő- és a szárazföldi erők modernizálásával érhető el?
- Milyen súllyal és intenzitással jelenik meg az MH digitalizációja érdekében ajánlott tíz digitális platform?

A szakirodalom széles körű felhasználása, és a digitalizációnak mint a 21. század új biztonsági kihívásának különös tekintettel a kiberbiztonság és kibervédelem releváns összetevőinek elemzése, értékelése alapján a kutatómunkám célja az volt, hogy megvizsgáljam azokat a folyamatokat, amelyek által levezethető, rendszerezhető, bizonyítható, hogy a mai európai biztonsági környezet részeként – az európai országok mintáját követve – Magyarország tekintetében is elengedhetetlen a honvédelem területét érintő digitalizáció.

A kutatási cél érdekében megfogalmazott hipotézis az volt, hogy a digitalizációt irányító kormányzati szerveknek jobban, vagy tevékenyebben kellene befogadniuk a katonai tényezőket és a katonai kiberbiztonság szakterületeit és fordítva, a katonai kiberrendszereknek jobban kellene kapcsolódniuk a kormányzati hálózatokhoz. Jóllehet a katonai rendszereknek külön, a többi kormányzati biztonsági rendszertől leválasztva is működniük kell, azonban békeidőben összekapcsolódhatnak azért, hogy a rendszerek kölcsönösen fejlődhessenek. A kormányzati rendszer platformja jóval nagyobb, mint a katonai azonban utóbbi specifikusságában eltér az általánosabb kormányzatiétól. Ezért fontos, hogy a két rendszer már békeidőben jó gyakorlatot szerezzen egymásról azért, hogy különleges jogrendben hatékonyabban működhessenek. A rész és egész elve alapján célszerű lenne, ha a katonai rendszerek a kormányzati biztonsági rendszer részeként, ugyanakkor különleges jogrend esetén pedig külön, leválasztva is működnének a Kormány infokommunikációs támogatása érdekében azért, mert:

(1) Feltételeztem, hogy a 21. századi biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel, vagyis multilateralizmussal, ugyanakkor a védelmi szektor adaptív képességfejlesztésével érhető el;
(2) Feltételeztem, hogy a digitalizáció a biztonságpolitikai trendek közül, mint technológiai faktor, az egyik leghangsúlyosabb biztonsági kihívás.
(3) Feltételeztem, hogy a Zrínyi 2026 mind a légierő mind a szárazföldi erők modernizálásával hozzájárul ahhoz, hogy a honvédelmi, katonai és nemzeti biztonsági rendszerek beágyazódjanak a hazai digitális hálózatba.
(4) Feltételeztem, hogy az MH széles körű digitalizációja akkor érhető el, ha a Zrínyi 2026 keretein belül megvalósuló/megvalósult fejlesztéseken és beszerzéseken túl a tíz platform azonos súllyal és intenzitással jelenik meg.

Annak érdekében, hogy valamennyi műveleti területen országunk a digitalizáció következtében kialakult új biztonsági kihívások ismeretével és ezek leküzdéséhez szükséges képességekkel rendelkezzen, a honvédségnek új szemléletű, digitális platformra szükséges átállnia.

A hipotézisek igazolása érdekében a disszertáció négy fejezetből áll. A fejezetek logikai felépítése során elsősorban a technológiai és információs hadviselés 21. századi biztonsági és műveleti környezetét vizsgáltam, majd a kibertér jellemzőit fejtettem ki a kiberbiztonság és kibervédelem tekintetében, részletesen elemeztem az MH digitalizációját a Zrínyi 2026 tükrében különös figyelmet fordítva a légi- és szárazföldi haderőnem digitalizációjára, végül tíz digitális platformot fogalmaztam meg a honvédség digitalizációja érdekében.

Az első fejezet hipotézise az volt, hogy ha a hagyományos és az új biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel, vagyis multilateralizmussal, ugyanakkor a védelmi szektor adaptív képességfejlesztésével érhető el, akkor a védelmi szektornak, ideértve a honvédségnek az országvédelmi, katonai feladatok ellátása mellett szükséges az új biztonsági kihívásokhoz alkalmazkodni. Ahhoz, hogy a hagyományos katonai feladatok ellátása mellett az információs hadviselés korában jelentkező új biztonsági kihívásokat a honvédség felismerje és megfelelően kezelje, szükséges a hadviselés átalakítása, modernizációja.

A hipotézis igazolása érdekében e fejezetben elemeztem a 21. századi európai biztonsági környezetet; a digitalizációt, mint globális biztonsági kihívást; az

információtechnológia jellemzőit a biztonságpolitikában és a hadügyben. Elemeztem és értékeltem a haditechnikai forradalom egyes szakaszait, átfogó és általános képet adtam a haderőreform történelmileg jelentős pontjairól. Vizsgáltam a hadviselés generációit, különös tekintettel a negyedik generációs, vagy hibrid hadviselésre. Kifejtettem a 21. század műveleti környezeti és az információs hadviselés jellemzőit különös tekintettel az információs infrastruktúrák tulajdonságaira. A hadügyi forradalom hullámait négy fejlődési szakaszban tekintettem át a haditechnikai-katonatechnikai képességek mentén.

Az első fejezet összegzett következtetéseképp megállapítottam, hogy az új típusú biztonsági kihívások, amelyek a poszthidegháború korában jelentkeztek, a korábban hangsúlyos egyirányú, katonai dimenzió kibővülésével jöttek létre. Ez azt jelenti, hogy a biztonságot meghatározó tényezők a katonai dimenzió mellett kibővültek, átalakultak és újak jöttek létre. A hagyományos és új biztonsági kihívások gyakran összekapcsolódnak, ezáltal a fenyegetések egyértelműen összefüggenek egymással, hatnak egymásra, folyamatosan befolyásolva a stabilitás adott szintjét.

A globalizáció és a technológiai forradalom hatásai előbb-utóbb minden nemzethez elérnek. Az információs társadalmak fejlődésének hatására az új fenyegetések nem ismernek országhatárokat, ezért a hagyományos és az új biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel és a védelmi szektor adaptív képességfejlesztésével érhető el. Egyre nő az esélye a kiberbűnözésnek, a terrorizmusnak, a migrációnak, a katasztrófahelyzeteknek. Nagy veszélyt hordoz magában az aszimmetrikus hadviselés és a tömegpusztító fegyverek proliferációja. Az új biztonsági kihívások kezelésére minden országnak fel kell készülnie, ezért szükséges a védelmi szektornak az országvédelmi, katonai feladatok ellátása mellett az új kockázati tényezők mentén kialakult/kialakuló biztonsági fenyegetésekhez a honvédség digitális képességfejlesztésével, a hadviselés átalakításával, modernizációjával alkalmazkodni.

A háborúk elsődleges célpontjait napjainkban az információs rendszerek és az információs infrastruktúrák adják. Az információs támadások és agressziók ugyanolyan veszélyforrások, mint a nemzetközi, globális, regionális, vagy nemzeti érdekeket ért kihívások, kockázatok és veszélytényezők. Éppen ezért fontos a honvédség átalakítása, képesség alapú fejlesztése, digitális platformra állítása.

A fejezet arra hívja fel a figyelmet, hogy a digitalizáció, a haditechnikai-katonatechnikai fejlődés, az összhaderőnemi képességfejlesztés, a humán erőforrás szakszerű képzése már elkezdődött. A kérdés csak az, hogy mely ország, hogyan, milyen módon és mennyire zárkózott fel az információs társadalom kihívásaihoz? Vagy a

felzárkózás helyett inkább elzárkózott előlük? Ez utóbbi esetben ugyanis biztosra vehető, hogy a felzárkózott és elzárkózott országok között komoly töréspontok keletkeznek, amelyek konfliktusforrást indukálnak.

A problémafelvetés tükrében az értekezés második fejezetének hipotézise az volt, hogy ha a digitalizációt, mint technológiai faktort vizsgálom, akkor ez az egyik leghangsúlyosabb biztonsági kihívás azért, mert leginkább ez kapcsolódik az emberhez és ez van hatással leginkább a mai modern világ fejlődésére, Európa, és benne Magyarország biztonságára, hiszen a gazdasági, technológiai fejlődés mellett erre épülnek a haditechnikai, katonai fejlesztések is. Ennek következtében nőnek a technikai, informatikai rendszerek és kibertérbeli kockázatok is. Ezért Magyarországnak képesnek kell lennie a kibertérbeli fenyegetések felismerésére és kezelésére, a kiberbiztonság kiépítésére, a kritikus információs infrastruktúra zavartalan működésének biztosítására, a támadások elhárítására és a kibervédelmi feladatok ellátására. Az infokommunikációs rendszerek elleni támadások száma folyamatosan nő, így szükséges azok védelmének erősítése, valamint a felhasználók információbiztonsági szintjének növelése. [62]

A hipotézis igazolása érdekében a második fejezetben megvizsgáltam a kibertér és kiberbiztonság alapvetéseit; elemeztem és értékeltem a kibertér vonatkozó hazai és nemzetközi doktrínáit különösképpen a NATO megközelítéséből; ismertettem a kiberbiztonság, a kiberműveletek és a kibertérbeli fenyegetések általános jellemzőit, különös tekintettel a kiberbűnözésre, a hacktivizmusra, a kiberkémkedésre, a kiberhadviselésre és a kiberterrorizmusra; végül feltártam a kiberbiztonság és kibervédelem magyarországi helyzetének katonai, honvédelmi vetületeit.

A második fejezet összegzett következtetéseként megállapítottam, hogy a jelenlegi, instabil biztonsági környezetben a biztonságra ható tényezők és kockázatok, veszélyforrások változnak. Ez azt jelenti, hogy a gazdasági, pénzügyi, társadalmi, kulturális, vallási, környezeti, közbiztonsági, migrációs gondokon túl a digitalizáció következtében szembe kell néznünk a technikai, informatikai rendszerek és ezzel együtt a kibertérbeli kockázatok növekedésével. A digitalizáció hatására a társadalmi folyamatok jelentős részéhez használjuk a kiberteret, ennek következtében a kiberbiztonsági kihívások dinamikus és folyamatos növekedése tapasztalható, ezért a kiberbiztonsággal foglalkozó szervezetek tevékenysége is fokozódik, ezzel hozzájárulva a kihívások mielőbbi felismeréséhez és az ellenük történő eredményes fellépéshez.

A NATO a *Global Common* projekt keretében közel 20 éve felismerte azt, hogy a hadsereg digitalizációja és fejlesztése elengedhetetlen az új biztonsági kihívásokkal való

szembenézés sikeressége érdekében. Az állami, katonai, nemzeti biztonsági rendszereknek ezért szükséges digitálisan felzárkózniuk, a nemzetállamoknak pedig a stratégiai dokumentumaikat szükséges az új biztonsági kockázatokhoz mérten felülvizsgálniuk.

A kiberbűnözés, a hacktivizmus, a kiberkémkedés, a kiberhadviselés és a kiberterrorizmus valós fenyegetésként van jelen, és a rohamos technológiai fejlődés következtében egyre szélesebb körben terjed a kibertérbeli támadásokhoz szükséges tudás, és az eszközök elkészítéséhez szükséges forrás az infokommunikációs eszközök használatával.

Ahhoz, hogy hazánk képes legyen felvenni az új biztonsági kihívásokkal a küzdelmet különös tekintettel a kibertérre szükséges a honvédségnek jól felszerelt és megfelelően kiképzett erőkkel, hatékony, telepíthető és fenntartható képességekkel rendelkeznie. A fegyveres erők szempontjából fontos a haderő műveleteinek kibertérbeli támogatása, ezért szükséges a honvédség kibervédelmi és kiberműveleti erőinek tervszerű fejlesztése. A kiberbiztonság kiépítése céljából Magyarország szempontjából ugyanolyan súllyal jelenik meg a hazai szabályozás, mint a nemzetközi szerepvállalás. A digitalizáció és a digitális átalakulás a globalizáció hatására jelen van az egész világban, ezért Magyarországnak és az MH-nak is rendelkeznie kell azzal a képességgel, hogy a kibertérbeli fenyegetéseket felismerje és kezelje, a kiberbiztonságot kiépítse, a kritikus információs infrastruktúra zavartalan működését biztosítsa, a támadásokat elhárítsa és a kibervédelmi feladatokat – alaptörvényi kötelezettségének megfelelően – maradéktalanul elvégezze.

A problémafelvetés tükrében az értekezés harmadik fejezetének hipotézise az volt, hogy ha a honvédelmi, katonai és nemzeti biztonsági rendszerek hazai digitális hálózatba beágyazódnak, akkor a békeidőben megfelelően működő katonai informatikai, digitális- és hálózatalapú rendszerek képesek lesznek önállóan működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő különleges jogrendben is. [1 pp. 122-145]

A hipotézis igazolása érdekében a fejezetben kutattam az MH feladatait az új biztonsági kihívások tekintetében, a Zrínyi 2026 cél- és eszközrendszerét. Elemeztem és értékeltem a légierő és a szárazföldi erők modernizálása érdekében már beszerzett és a még beszerzés alatt álló eszközöket, képességeket és digitális fejlesztéseket.

A harmadik fejezet összegzett következtetéseként megállapítottam, hogy az új biztonsági kihívások megfelelő kezeléséhez szükséges az MH strukturális, eljárásrendbeli, hadviselési és modernizációs átalakítása, amely a Zrínyi 2026 indulásával

vette kezdetét. Az MH képességfejlesztési irányait tekintve a 21. századbéli magyar haderő a haderőfejlesztés tekintetében képessé válik a szimmetrikus és az aszimmetrikus hadviselés folytatására. Az MH-nak megújult, szervezett, önállóan működő és szövetségi szinten alkalmazható – önkéntes tartalékos rendszerrel szervezett – haderőként kell működnie. Ehhez szükséges egy megfelelően képzett és kiképzett, korszerű, modern és digitális eszközökkel felszerelt, nemzetközi tapasztalatokkal rendelkező állomány, amely képes az ország szuverenitásának védelmére, így lehetővé téve a szövetségesi műveletben történő érdemi segítségnyújtást. Ezáltal érvényesítve mind a nemzeti önerő fejlesztését, mind a szövetségesi szerepvállalást az ország biztonságának kialakításáért és fenntartásáért.

Az új Airbus H145M és H225M típusú helikopterek, a sugárhajtású kiképző repülőgépek beszerzésével, továbbá a Gripenek modernizálásával, az A319-es MEDEVAC képességfejlesztésével és a Dassault Falcon 7x és a KC 390-esek beszerzésével, a MISTRAL légvédelmi rakétarendszer korszerűsítésével, valamint a SAMOC légvédelmi rakéta vezetési rendszer és a NASAMS földi telepítésű légvédelmi rakétarendszer, az IRIS-T rakéták és az ELM- 2084 radar beszerzésekkel új dimenzióba került a honvédség légierő képességének modernizálása és ezen keresztül megnyílt az út a légierő-képességek digitalizációja előtt. A fentiekben rögzített eredmények és megfogalmazott célok mind egy-egy lépéssel közelebb hozzák a honvédség digitális platformra történő átállítását.

A katonák egyéni harcászati felszerelésének modernizálásával, a 2015M mintájú gyakorlóruha rendszeresítésével, az MH MI létrehozásával, a kiberképességek fejlesztésével, az MH KKK és az MH KIMK megalakulásával, továbbá az olyan új eszközök honvédségnél történő rendszeresítésével, mint a Polaris MRZR-4-es „homokfutók”; a Leopard 2A4 és Leopard 2A7+ harckocsik; PzH 2000 önjáró lövegek, Carl Gustaf M4 gránátvetők; hazai gyártású lőfegyverek; Gidránok és Lynxek a szárazföldi haderőnem digitalizációja és modernizációja is kezdetét vette, ezzel biztosítva a honvédség digitális platformra történő átállását.

A Zrínyi 2026 tehát mind a légierő mind a szárazföldi erők modernizálása által hozzájárul ahhoz, hogy a honvédség áttérjen az informatikai, digitális- és hálózatalapú katonai rendszerek széles körű alkalmazására. Mindez alátámasztja a tézist, amely alapján a fejlesztések megvalósulásának következtében a honvédelem egésze digitális platformra állítható át, ezzel biztosítva azt, hogy a védelmi, katonai, nemzeti biztonsági rendszerek

önállóan, más rendszerektől leválasztva is képesek legyenek működtetni a közigazgatást, fenntartani az ország vezetését békeidőben és a békétől eltérő különleges jogrendben is.

A Zrínyi 2026 célkitűzési között szerepel a honvédség áttérése és felzárkózása az informatikai, digitális- és hálózatalapú katonai rendszerekhez. Annak érdekében, hogy valamennyi műveleti területen országunk a digitalizáció következtében kialakult új biztonsági kihívások ismeretével és ezek leküzdéséhez szükséges képességekkel rendelkezzen, a honvédségnek új szemléletű, digitális platformra szükséges átállnia.

A negyedik fejezet hipotézise az volt, hogy az MH széles körű digitalizációja akkor érhető el, ha a Zrínyi 2026 keretein belül megvalósuló/megvalósult fejlesztéseken és beszerzéseken túl a tíz platform azonos súllyal és intenzitással jelenik meg a honvédelem rendszerében.

A Zrínyi 2026 kapcsán már elért eredmények és a további célok ismeretének hatására fogalmazódott meg a tíz ajánlásba rendezett platform, amelyek megismerése, alkalmazása és fejlesztése által a honvédelem egésze digitális alapokra helyeződne. Ahhoz azonban, hogy az MH áttérjen és felzárkózzon az informatikai, digitális- és hálózatalapú katonai rendszerekhez, szükséges az ajánlások szerinti platformok azonos súllyal és intenzitással való kezelése.

A negyedik fejezet összegzett következtetése, hogy a Zrínyi 2026 célkitűzéseinek megvalósulása, valamint a digitális platformok azonos súllyal és intenzitással való kezelése esetén a honvédelem egésze digitális platformra állítható, amely azt eredményezné, hogy a piaci *high-tech* rendszerek és a közigazgatás által használt infrastruktúrákhoz igénybe vett védelmi, katonai, nemzeti biztonsági rendszerek önállóan, leválasztva is működhetnek a Kormány infokommunikációs támogatása érdekében.

Új tudományos eredmények

A konkrét tudományos eredmények az alábbiak:

(1) Igazoltam, hogy a 21. század biztonsági kihívásainak kezeléséhez és leküzdéséhez - a multilateralizmus tükrében - szükséges az MH strukturális, eljárásrendbeli, hadviselési és modernizációs átalakítása.

(2) Bizonyítottam, hogy a digitalizáció következtében szembe kell néznünk a technikai, informatikai rendszerek és ezzel együtt a kibertérbeli kockázatok növekedésével.

(3) Bizonyítottam, hogy a Zrínyi 2026 néven indított haderőfejlesztési program mind a légierő mind a szárazföldi erők modernizálása által hozzájárul ahhoz, hogy a honvédség áttérjen az informatikai, digitális- és hálózatalapú katonai rendszerek alkalmazására.

(4) Igazoltam azt, hogy az MH széles körű digitalizációját a tíz platform teszi lehetővé, amely különböző súllyal és intenzitással bír.

Ajánlások

A digitalizáció, mint a 21. század új biztonsági kihívása, különös tekintettel Magyarország kibervédelmére című doktori értekezésemet ajánlom azoknak a doktoranduszoknak, doktorjelölteknek, kutatóknak, kormánytisztviselőknek és katonáknak, akik a digitalizációra, mint egy új biztonsági kihívásra tekintenek, akik hozzám hasonlóan érzékelik a mindennapjaikban a globalizáció hatására feltörekvő digitalizációt, technológiai fejlődést. Azoknak, akik átfogó képet szeretnének kapni a technológiai és információs hadviselésről, akik érdeklődést mutatnak a hadsereg digitalizációjának történeti és történelmi előzményeiről és folyamatairól, azon kollégáknak, akik elfogadják azt, hogy a 21. században már a kibertér is egy önálló műveleti tér, ezért az információs hadszíntér és az információs hadviselés kihívásaihoz a honvédelem egészének fel kell zárkóznia. Végül, de nem utolsó sorban ajánlom azoknak, akik átfogó képet akarnak kapni a Zrínyi 2026-ról, a beszerzett és beszerzésre kerülő eszközökről, a képességfejlesztésekről és alapvetően a honvédség digitalizációjáról.

IRODALOMJEGYZÉK

Saját publikációs jegyzék

[T1] BEREGI, A.L.: The digitalisation of the Hungarian Defence Forces in the light of the Zrínyi 2026 Defence and Armed Forces Development Programme, In: BABOS, T. /ed./: Digital security policy in the cyber space. Hungarian University of Agriculture and Life Sciences Gödöllő, 2021., pp. 39-59. ISBN 978-963-269-974-5 (Printed) ISBN 978-963-269-975-2(PDF) https://hunexpert.hu/wp-content/uploads/2022/05/DIGITAL-SECURITY-POLICY-IN-THE-CYBER-SPACE.pdf (letöltve: 2022.09.16.)

[T2] BEREGI Alexandra Lilla: A Magyar Honvédség digitalizációja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program tükrében, In: BABOS, T. /szerk./: Digitális biztonságpolitika a kibertérben. Magyar Agrár- és Élettudományi Egyetem Gödöllő, 2021., pp. 39-58. ISBN 978-963-269-974-5 (nyomtatott) ISBN 978-963-269-975-2 (PDF) https://hunexpert.hu/wp-content/uploads/2022/05/DIGIT%C3%81LIS-BIZTONS%C3%81GPOLITIKA-A-KIBERT%C3%89RBEN.pdf (letöltve: 2022.09.16)

[T3] BEREGI Alexandra Lilla-BABOS Tibor: Technological and information warfare in the XXI. century, In: Biztonságtudományi Szemle, III. évfolyam 1. különszám 2021., ISSN 2676-9042., pp. 123-135. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/127/156 (letöltve: 2022.09.16.)

[T4] BABOS Tibor-BEREGI Alexandra Lilla: Security and Military Relevancies of Digitisation, Globalisation and Cyberspace, AARMS XX. évfolyam 1. szám 2021., ISSN 2498-5392 pp. 81-93. http://doi.org/10.32565/aarms.2021.1.6 (letöltve: 2022.09.12.)

[T5] BEREGI Alexandra Lilla-BABOS Tibor: Az európai terrorizmus aktuális trendjei az új biztonságpolitikai kihívások tükrében, In: Rendőrségi tanulmányok, IV. évfolyam 2. szám 2021., ISSN 2630-8002., pp. 4-25., https://archive.bm-tt.hu/rtt/assets/letolt/rt/202102/rt202102.pdf (letöltve: 2022.09.12.)

[T6] BEREGI Alexandra Lilla-BABOS Tibor: Magyarország biztonsága az európai folyamatok viszonyrendszerében, In: Hadmérnök, XIV. évfolyam 4. szám 2020., pp. ISSN 1788-1919., pp. 223-239. http://doi.org/10.32567/hm.2019.4.15 (letöltve: 2022.09.12.)

[T7] BEREGI Alexandra Lilla: Magyarország Nemzeti Biztonsági Stratégiája (2012) a mai biztonságpolitikai kihívások tükrében, In: Hadmérnök, XV. évfolyam 2. szám 2020., ISSN 1788-1919., pp. 205-217.https://doi.org/10.32567/hm.2020.2.14 (letöltve: 2022.09.12.)

[T8] BEREGI Alexandra Lilla: A Magyar Honvédség 2018/19. évi balkáni katonai szerepvállalása, In: Biztonságtudományi Szemle, II. évfolyam 1. szám 2020., ISSN 2676-9042., pp. 11-20., https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/31/38 (letöltve: 2022.09.12.)

[T9] BEREGI Alexandra Lilla-BABOS Tibor: A védelemgazdaság biztonságpolitikai összefüggései napjainkban, In: Hadmérnök, XIII. évfolyam 3. szám 2018., ISSN 1788-1919., pp. 339–352 http://hadmernok.hu/183_25_babos.pdf (letöltve: 2022.09.12.)

[1] BABOS T.: A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái, In: Hadtudomány, XXVIII. évfolyam, Elektronikus lapszám 2018., pp. ISSN 1588-0605., 122-145. https://doi.org/10.17047/HADTUD.2018.28.E.122 (letöltve: 2022.09.12.)

[2] SZENES Z.: A katonai biztonság reneszánsza, In: Honvédségi Szemle: A Magyar Honvédség központi folyóirata, CXLV. évfolyam, 2. szám 2017., ISSN 2732-3226., pp.3-24. http://real.mtak.hu/124538/1/HSZ_2017_145_2_Szenes_Zoltan.pdf (letöltve: 2022.09.12.)

[3] Innovációs és Technológiai Minisztérium: Nemzeti Digitalizációs Stratégia 2021-2030; Budapest, 2020 június. https://2015-2019.kormany.hu/download/f/58/d1000/NDS.pdf (letöltve: 2022.09.12.)

[4] REMEK Éva: Az európai biztonságfelfogás változása. In: KARLOVITZ János Tibor /szerk./: Tanulmányok a kompetenciákra épülő, fenntartható kulturális és technológiai fejlődés köréből. Komárno, Szlovákia: International Research Institute s.r.o., 2019., pp. 147-155.

[5] PETERSEN, T-STEINER, F.: The Bigger Picture, How globalization, digitalization and demographic change challenge the world. https://rsm-bst-live.bertelsmann-stiftung.de/fileadmin/files/user_upload/MegatrendBrief_MT_The_Bigger_Picture_How_globalization_digitalization_and_demographic_Change_challenge_the_world_2019.pdf (letöltve: 2022.09.12.)

[6] RESPERGER I.: A biztonsági környezet, az aszimmetrikus hadviselés és a terrorizmus jellemzői, In: Hadtudományi Szemle, IX. évfolyam 3. szám, 2016., ISSN 2060-0437., pp. 115-181. http://epa.oszk.hu/02400/02463/00032/pdf/EPA02463_hadtudomanyi_szemle_2016_03_115-181.pdf (letöltve: 2022.09.12.)

[7] RESPERGER I.: A válságkezelés elméleti kérdései. In: SZENES Zoltán /szerk./: Biztonságpolitika és válságkezelés. Budapest, Magyarország: NKE Szolgáltató Nonprofit Kft., 2016., ISBN: 9786155527708., pp. 5-17. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10138/Biztonsagpolitika_valsagkezeles.pdf?sequence=1&isAllowed=y (letöltve: 2022.09.12.)

[8] GAZDAG Ferenc-REMEK Éva: A biztonsági tanulmányok alapjai; Dialóg Campus Kiadó, Budapest, 2018. ISBN 9786155845888 https://nkerepo.uni-

nke.hu/xmlui/bitstream/handle/123456789/12604/web_PDF_EKM_Biztonsagi_tanulmanyok_alapjai.pdf?sequence=1 (letöltve: 2022.09.12.)

[9] SZARKA Gábor: Biztonsági kihívások és konfliktusok a XXI. században Európa és Magyarország szemszögéből; Nemzeti Közszolgálati Egyetem; Közigazgatási Továbbképzési Intézet, Budapest, 2020. ISBN 978-963-498-349-1 https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/6847/Biztons%E1gi%20kih%EDv%E1sok%20%E9s%20konfliktusok%20a%20XXI.%20sz%E1zadban%20Eur%F3pa%20%E9s%20Magyarorsz%E1g%20szemsz%F6g%E9b%20l.pdf;jsessionid=8E214A8938321CFF5B0BFE35A0D6CEBF?sequence=1(letöltve: 2022.09.12.)

[10] BARRY Buzan: New Patterns of Global Security in the Twenty-First Century, In: International Affairs, Volume 67 Issue 3 1991., pp. 431-451. https://doi.org/10.2307/2621945 (letöltve: 2022.09.29.)

[11] REMEK É.: Az EBESZ válságkezelő tevékenysége (intézmények, működési elv, eredmények) – különös tekintettel a válságkezelés elméleti és fogalmi hátterére, In: Hadtudományi Szemle, X. évfolyam 4. szám 2017., ISSN 2060-0437., pp. 214-234. http://real.mtak.hu/85314/1/17_4_bp_remek.pdf (letöltve: 2022.09.12.)

[12] TÁLAS Péter-GAZDAG Ferenc: A biztonság fogalmának változása; In: TÁLAS Péter /szerk./: Az integrált biztonsági szféra magyarországi megteremtése felé, Budapest, MTA Szociológiai Kutatóintézet (SZKI), 2008., pp. 9-18.

[13] SZENES Zoltán /szerk./: Biztonságpolitika és válságkezelés. Budapest, Magyarország: NKE Szolgáltató Nonprofit Kft., 2016., ISBN: 9786155527708 http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10138/Biztonsagpolitika_valsagkezeles.pdf?sequence=1&isAllowed=y (letöltve: 2022.09.12.)

[14] BABOS T.: Az európai biztonság öt központi pillére; Zrínyi, Budapest, 2007. ISBN 978-963-327-425-5.

[15] BABOS T.: A biztonság globális és európai összefüggései, In: Hadtudomány, XXIX. évfolyam 4. szám 2019., ISSN 1215-4121., pp. 16–29. https://doi.org/10.17047/HADTUD.2019.29.4.16 (letöltve: 2022.09.12.)

[16] ROPOLYI L.: Digitális írásbeliségek; In: Korunk, XXV. évfolyam 10. szám 2014., pp. 8-14.

https://www.academia.edu/22995836/Digit%C3%A1lis_%C3%ADr%C3%A1sbelis%C3%A9gek (letöltve: 2022.09.12.)

[17] CSIKI VARGA Tamás-TÁLAS Péter: Magyarország Új Nemzeti Biztonsági Stratégiájáról, In: Nemzet és Biztonság XIII. évfolyam 3.szám ISSN 2559-8651., 2020., pp. 89-112. http://doi.org/10.32576/nb.2020.3.7 (letöltve: 2022.09.12.)

[18] Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence. Cc. europa.eu. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 (letöltve: 2022.09.12.)

[19] European Commission: Shaping Europe's digital future. European Union, 2020, ISBN 978-92-76-16362-6. https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf (letöltve: 2022.09.12.)

[20] Szakmai bizottság alakult a kvantuminformatika, mesterségesintelligencia-fejlesztés és más digitális innovációk ösztönzésére, Digitalisjoletprogram.hu, 2021.07.01. https://digitalisjoletprogram.hu/hu/hirek/szakmai-bizottsag-alakult-a-kvantuminformatika-mestersegesintelligencia-fejlesztes-es-mas-digitalis-innovaciok-osztonzesere (letöltve: 2022.09.16.)

[21] RAJNAI Z.: Információbiztonság tudatosság, In: Műszaki Tudományos Közlemények 7., 2017. pp. 37-42. https://www.eme.ro/publication-hu/mtk/mtk7/MTK7_02_Rajnai-plen.pdf (letöltve: 2022.09.12.)

[22] KOVÁCS L.: Biztonságpolitika: a kibertérben; Nemzeti Közszolgálati Egyetem, Budapest, 2019. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12821/Biztonsagpolitika%20a%20kiberterben.pdf?sequence=1 (letöltve: 2022.09.12.)

[23] SZENES Z.: Akadémiai viták a hadtudomány struktúrájáról, In: Hadtudomány, XXIII. évfolyam 3-4. szám 2013., ISSN 1588-0605., pp. 59-66. https://www.mhtt.eu/hadtudomany/2013/3_4/Hadtudomany_2013_3-4_6.pdf (letöltve: 2022.09.12.)

[24] J. ROGERS, C.: „Military Revolutions" and „Revolutions in Military Affairs": A Historian's Perspective; https://books.google.hu/books?hl=hu&lr=&id=lxP0qyBw2cYC&oi=fnd&pg=PA21&dq=military+revolutions&ots=mPuzh3V74d&sig=-

TJvPrICjqKOI8LdybdIOpdNvlM&redir_esc=y#v=onepage&q=military%20revolutions&f=false (letöltve: 2022.09.12.)

[25] COHEN E.: Technológia és hadviselés. In: TÁLAS P. /szerk./: A stratégia a modern korban. Budapest: Zrínyi Kiadó, 2005., pp. 295-316.

[26] SZÜCS L.: Tíz kevésbé közismert tény az Öbölháborúról. Honvedelem.hu, Budapest, 2014.09.13. https://honvedelem.hu/hatter/multidezo/tiz-kevesbe-kozismert-teny-az-obolhaborurol.html (letöltve: 2022.09.12.)

[27] B-2 Spirit. https://www.military.com/equipment/b-2-spirit (letöltve: 2022.09.12.)

[28] A Magyar Űripari Klaszter. http://hunspace.org/ (letöltve: 2022.09.12.)

[29] RUSSELL D., et al.: Service-oriented integration of systems for military capability, In: 2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC), 2008. pp. 33-41. https://doi.org/10.1109/ISORC.2008.45 (letöltve: 2022.09.12.)

[30] HAUBEN M.: History of ARPANET, Behind the Net - The untold history of the ARPANET Or - The "Open" History of the ARPANET/Internet; https://www.jbcoco.com/Arpa-Arpanet-Internet.pdf (letöltve: 2022.09.12.)

[31] J. WILSON III. E..: The information Revolution and developing countries. The MIT press, Cambridge, Massachussets, London, England, 2004. https://books.google.hu/books?hl=hu&lr=&id=TlD8gVgYndoC&oi=fnd&pg=PR7&dq=information+revolution&ots=n3aXSb4KDg&sig=zRh1SsrO2ta2Il0V5a5C6KAcP7Y&redir_esc=y#v=onepage&q=information%20revolution&f=false (letöltve: 2022.09.12.)

[32] A hadviselés generációi – Generációváltás a hadviselésben és ezek kihívásai, hatásai a Magyar Honvédségre, az MHTT Konferenciája, In: Hadtudomány, XXVII. évfolyam 3-4. szám 2017., ISSN 1588-0605., pp.75-76. https://www.mhtt.eu/hadtudomany/2017/2017_3-4/Ht_201734_77-78.pdf (letöltve: 2022.09.12.)

[33] JACOB, F.-VISONI-ALONZO, G.: Global Military Revolutions? In: The Military Revolution in Early Modern Europe. Palgrave Pivot, London, 2016., pp. 15-51. https://doi.org/10.1057/978-1-137-53918-2_2 (letöltve: 2022.09.12.)

[34] SZENDY I.: Korunk és hadviselése, In: Hadtudomány, XXVIII. évfolyam 2. szám, 2018., ISSN 1215-4121., pp. 3-17. https://doi.org/10.17047/HADTUD.2018.28.2.3 (letöltve: 2022.09.12.)

[35] HOFFMAN, Frank G.: Hybrid warfare and challenges; National Defense Univ. Washington DC Inst. for National Strategic Studies, 2009. https://apps.dtic.mil/sti/pdfs/ADA516871.pdf (letöltve: 2022.09.12.)

[36] RESPERGER István-KISS Álmos Péter-SOMKUTI Bálint: Negyedik generációs hadviselés: néhány alapfogalom, In: Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata, CXLII. évfolyam 1. szám, 2014., ISSN 2732-3226., pp. 4-12. https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/issue/view/61/62 (letöltve: 2022.09.12.)

[37] KISS Á.P.: Generációk a hadviselésben – a negyedik generáció, In.: Hadtudományi Szemle, II. évfolyam 2. szám 2009., ISSN 2060-0437., pp.10-18. https://epa.oszk.hu/02400/02463/00005/pdf/EPA02463_hadtudomanyi_szemle_2009_2_010-018.pdf (letöltve: 2022.09.12.)

[38] KOVÁCS L.: Offenzív kiberműveletek II.: Kibererők és képességeik, In.: Hadmérnök, XVI. évfolyam 3. szám, 2021., ISSN 1788-1929., pp.119-137. https://doi.org/10.32567/hm.2021.3.7 (letöltve: 2022.09.12.)

[39] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

[40] KOMJÁTHY Lajos József: A műveleti környezet és körülményei változásainak hatása napjaink katonai tevékenységére, In: Hadtudományi Szemle, X. évfolyam 3.szám, 2017., ISSN 2060-0437., pp.63-77. https://epa.oszk.hu/02400/02463/00036/pdf/EPA02463_hadtudomanyi_szemle_2017_3_063-077.pdf (letöltve: 2022.09.12.)

[41] SOMODI Zoltán-KISS Álmos Péter: A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban, In: Honvédségi Szemle–Hungarian Defence Review, CXLVII. évfolyam 6. szám 2019., ISSN 2732-3226., pp. 22-28. https://doi.org/10.35926/HSZ.2019.6.2 (letöltve: 2022.09.12.)

[42] LIBICKI M. C.: Conquest in Cybersapce, National Security and Information Warfare. Cambridge University Press, 2007.

[43] HAIG Zsolt-HAJNAL Béla-KOVÁCS László-MUHA Lajos-SIK Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana; ENO Advisory Kft., 2009.https://nki.gov.hu/wp-content/uploads/2010/01/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf (letöltve: 2022.09.12.)

[44] HAIG Zsolt-VÁRHEGYI István: Hadviselés az információs hadszíntéren. Budapest, Zrínyi Kiadó, 2005.

[45] HAIG Zsolt-KOVÁCS László-VÁNYA László-VASS Sándor.: Elektronikai hadviselés; Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Budapest, 2014. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10964/webview.pdf?sequence=1&isAllowed=y (letöltve: 2022.09.12.)

[46] HAIG Zsolt-KOVÁCS László.: New way of terrorism: Internet- and cyber-terrorism, In.: AARMS, Vol. 6. No. 4., 2007., ISSN 2786-0744., pp. 659-671. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1884/10haig.pdf?sequence=1&isAllowed=y (letöltve: 2022.09.12.)

[47] COOPER J. R.: Another View of the Revolution in Military Affairs; U.S. Army War College, Strategic Studies Institute, 1994. https://books.google.hu/books?hl=hu&lr=&id=R5kHT-FaIGQC&oi=fnd&pg=PA1&dq=revolution+is+military+affairs&ots=SerxuWqiPM&sig=tR05rrkZ68srx3EhWSGNBqVu6l4&redir_esc=y#v=onepage&q=revolution%20is%20military%20affairs&f=false (letöltve: 2022.09.12.)

[48] United States. Department of the Army-United States. Department of Defense: United States Army: 2004 Army Transformation Roadmap; 2004. https://www.hsdl.org/?abstract&did=464516 (letöltve: 2022.09.12.)

[49] 1298/2017. (VI.2.) Korm. határozat a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról

[50] HAIG Zs.: Az információs hadviselés kialakulása, katonai értelmezése, In: Hadtudomány, XXI. évfolyam 1-2 szám., 2011., pp.12-28. https://www.mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf (letöltve: 2022.09.12)

[51] KNOX, MacGregor, et al. /ed./: The dynamics of military revolution, 1300-2050; Cambridge University Press, 2001. https://books.google.hu/books?hl=hu&lr=&id=zIIbUmwXitAC&oi=fnd&pg=PP17&dq=military+revolution+first+wave&ots=puaWJmBkwt&sig=dsLuyeWl6p7V3NH8dmhchBOL1YI&redir_esc=y#v=onepage&q=military%20revolution%20first%20wave&f=false (letöltve: 2022.09.12.)

[52] C4ISR. https://www.c4isrnet.com (letöltve: 2022.09.12.)

[53] SZENES Z.: Tudomány és a korszerű haderő, In: Magyar Tudomány, CLXXVI. évfolyam 2. szám 2015., ISSN 0025 0325., pp. 194-201. http://www.matud.iif.hu/2015/02/10.htm (letöltve: 2022.09.12.)

[54] PORKOLÁB Imre: Küldetés alapú vezetés a digitális transzformáció korában; In: LÓDERER Balázs-STOHL Róbert /szerk./: Fegyver nélküli műveletek és háttértényezőik: tanulmánykötet, Budapest, Magyarország: Honvéd Tudományos Kutatóhely, 2019., pp. 141-157., ISBN 978-615-5585-12-8 http://real.mtak.hu/id/eprint/105357 (letöltve: 2022.09.12.)

[55] ROBERTSON A.: America's Digital Army: Games at Work and War, London, University of Nebraska Press, 2017.

[56] NASA Armstrong Fact Sheet: Hyper-X Program. Nasa.gov. https://www.nasa.gov/centers/armstrong/news/FactSheets/FS-040-DFRC.html (letöltve: 2022.09.12.)

[57] VÁRHEGYI I.: Az információs hadviselés második hulláma, In: Hadtudomány, XXI. évfolyam 1-2. szám 2011., ISSN 1588-0605., pp.49-64. https://www.mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_7.pdf (letöltve: 2022.09.12.)

[58] PORKOLÁB I.: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? In: Hadtudomány, XXV. évfolyam 3-4. szám 2015., ISSN 1215-4121., pp. 36-48. https://www.mhtt.eu/hadtudomany/2015/3_4/2015_3_4_5.pdf (letöltve: 2022.09.12.)

[59] KOVÁCS L.: Kiberbiztonság és -stratégia; Dialóg Campus Kiadó 2018. http://kovacsx.hu/download/books/KovacsLaszlo_A_kiberbiztonsag_es_strategia.pdf (letöltve: 2022.09.12.)

[60] BABOS Tibor: A Biztonság Globális és Európai Összefüggései előadás és tanulmány, Kutatás és Innováció a Hazáért c. Tudományos Konferencia. Budapest, 2019. 11.05.

[61] BABOS Tibor-BEREGI Alexandra Lilla: Security and Military Relevancies of Digitisation, Globalisation and Cyberspace, In: AARMS, XX. évfolyam 1. szám 2021., ISSN 2786-0744., pp. 81-93. http://doi.org/10.32565/aarms.2021.1.6 (letöltve: 2022.09.12.)

[62] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[63] Department of Defense Dictionary of Military and Associated Terms. https://irp.fas.org/doddir/dod/dictionary.pdf (letöltve: 2022.09.12.)

[64] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[65] BERZSENYI Dániel: Kiberbiztonság. In: TÁLAS Péter-CSIKI VARGA Tamás-ETL Alex- BERZSENYI Dániel /szerk./: A Globalizált Világ Kihívásai. Budapest, Ludovika Egyetemi Kiadó, 2021., pp.341-356. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16247/A_globalizalt_vilag_kihivasai_elektronikus.pdf?sequence=1#page=12 (letöltve: 2022.09.12.)

[66] BERZSENYI Dániel: Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép Európában, In: Nemzet és Biztonság, X. évfolyam 3. szám 2017., ISSN 1789-5286., pp. 69-79. http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_3_07_berzsenyi_daniel_-_globalis_kihivas_regionalis_valaszok_-_kiberbiztonsag_kele-kozep-europaban.pdf (letöltve: 2022.09.12.)

[67] Európai Uniós Kiberbiztonsági Ügynökség (ENISA). https://europa.eu/european-union/about-eu/agencies/enisa_hu#milyen-feladatokat-l%C3%A1t-el (letöltve: 2022.09.12.)

[68] BEDERNA Zsolt-RAJNAI Zoltán-SZÁDECZKY Tamás: Further Strategy Analysis of Cybersecurity Incidents, In: Revista Academiei Fortelor Terestre = Land Forces Academy Review, 2021., Vol. 26 No.3. ISSN 2247-840X., pp. 251-260. https://doi.org/10.2478/raft-2021-0032 (letöltve: 2022.09.12.)

[69] NATHALIE C.: Cyber War: the Challenge to National Security, In: Global Security Studies, 4, No. 1. 2013., pp. 93-116.

[70] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[71] RAJNAI Z.- FREGAN B.: Új alapokon a magyarországi kibervédelmi stratégia, In: Műszaki Tudományos Közlemények, 7. kiadás, 2017., pp. 351-354. https://www.eme.ro/publication-hu/mtk/mtk7/MTK7_80_Rajnai.pdf (letöltve: 2022.09.12.)

[72] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról

[73] A hálózati és információs rendszerek biztonságára vonatkozó Stratégia (Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján). https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf (letöltve: 2022.09.12.)

[74] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

[75] SZENTGÁLI G.: A NATO kibervédelmi politikájának fejlődése, In: Nemzet és Biztonság, VI. évfolyam 3-4. szám 2013., ISSN 1789-5286., pp. 76-83. http://www.nemzetesbiztonsag.hu/cikkek/nb_2013_3-4_07_szentgali_gergely_-_a_nato_kibervedelmi_politikajanak_fejlodese.pdf (letöltve: 2022.09.12.)

[76] VARGA G.: A NATO Új, Lisszaboni Stratégiai Koncepciója, In: Nemzet és Biztonság: Biztonságpolitikai Szemle, 3. évfolyam 10. szám 2010., ISSN 1789-5286., pp.79-86. http://nemzetesbiztonsag.hu/cikkek/varga_gergely-a_nato_uj__lisszaboni__strategiai_koncepcioja.pdf (letöltve: 2022.09.12.)

[77] NATO Communications and Information Agency. https://www.ncia.nato.int/index.html (letöltve: 2022.09.12.)

[78] TÁLAS P.: A varsói NATO-csúcs legfontosabb döntéseiről, In: Nemzet és Biztonság: Biztonságpolitikai Szemle, IX. évfolyam 2. szám 2016., ISSN 1789-5286., pp.

97-101. http://www.nemzetesbiztonsag.hu/cikkek/nb_2016_2_09_talas_peter_-_a_varsoi_nato-csucs_legfontosabb_donteseirol.pdf (letöltve: 2022.09.12.)

[79] BABOS T.: ”Globális Közös Terek” a NATO-ban, In: Nemzet és Biztonság: Biztonságpolitikai Szemle 4. évfolyam 3. szám 2011., ISSN 1789-5286., pp. 34-46. http://nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf (letöltve: 2022.09.12.)

[80] KOVÁCS Zoltán: Kibervédelem és biztonság, In: KISS Tibor /szerk./: Kibervédelem a bűnügyi tudományokban. Budapest: Dialóg Campus, 2020., pp. 65-90. http://real.mtak.hu/108475/1/web_PDF_Kibervedelem_bunugyi_tudomanyokban.pdfjsessionidC9DCEB40521EE6AF752818ADF7964DBEsequence1 (letöltve: 2022.09.12.)

[81] KOVÁCS L.: Offenzív kiberműveletek 1.: Az offenzív kiberműveletek természete, In: Hadmérnök, XVI. évfolyam 2. szám, 2021., ISSN 1788-1929., pp. 187–204. https://doi.org/10.32567/hm.2021.2.13 (letöltve: 2022.09.12.)

[82] KRASZNAY Cs.: Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése, In: Külügyi Szemle, XX. évfolyam 2021-es különszám, ISSN 2060-4904., 2021., pp. 191-214. https://doi.org/10.47707/Kulugyi_Szemle.2021.2.09 (letöltve: 2022.09.12.)

[83] KOVÁCS László-KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, In.: Nemzet és Biztonság: Biztonságpolitikai Szemle, X. évfolyam 1. szám 2017., ISSN 1789-5286., pp. 3-16. https://folyoirat.ludovika.hu/index.php/neb/article/view/3780/3050 (letöltve: 2022.09.12.)

[84] KRASZNAY CS.: A polgárok védelme egy kiberkonfliktusban, In.: Hadmérnök, VII. évfolyam 4. szám, 2012., ISSN 1788-1929., pp.142-151. http://hadmernok.hu/2012_4_krasznay.pdf (letöltve: 2022.09.12.)

[85] KRASZNAY Csaba-VARGA-PERKE Bálint: Ifjúságvédelem a hacker szubkultúrában, In: BÍRÓ A. Zoltán-GERGELY Orsolya /szerk.: Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra. Csíkszereda, Románia: Státus Kiadó, 2013., pp. 179-202. https://www.researchgate.net/profile/Csaba-Krasznay/publication/281712522_Ifjusagvedelem_a_hacker_szubkulturaban/links/60e30d84458515d6fbfd771b/Ifjusagvedelem-a-hacker-szubkulturaban.pdf (letöltve: 2022.09.12.)

[86] MUNK S.: Interoperability Services Supporting Information Exchange Between Cybersecurity Organizations, In: AARMS, Vol. 17. No. 3. 2018., ISSN 2786-0744., pp. 131-148. https://folyoirat.ludovika.hu/index.php/aarms/article/view/1072 (letöltve: 2022.09.12.)

[87] HELYES M.: Cyberterrorism and the protection of critical information infrastructures: A snapshot of the current state of certain regulatory issues, In: Lélektan és hadviselés, III. évfolyam 1. szám 2021., ISSN 2676-9964., pp. 51-68. https://doi.org/10.35404/LH.2021.1.51 (letöltve: 2022.09.12.)

[88] PAPP Z.I.: A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái, Nemzeti Közszolgálati Egyetem, NKE HHK Katonai Műszaki Doktori Iskola, Disszertáció benyújtásának éve: 2018, Védés éve: 2019 Megjelenés/Fokozatszerzés éve: 2019. https://nkerepo.uninke.hu/xmlui/bitstream/handle/123456789/13335/papp_zoltan_doktori_ertekezes_2018.pdf?sequence=1 (letöltve: 2022.09.12.)

[89] A Digitális Jólét Program 2.0; Budapest, 2017. https://digitalisjoletprogram.hu/files/30/49/304943b37e297ac422f43c46ee5834a1.pdf (letöltve: 2022.09.12.)

[90] MUNK S.: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interoperabilitással, In: Hadmérnök, XIII. évfolyam „KÖFOP" szám 2018., ISSN 1788-1929., pp. 205-217. http://hadmernok.hu/180kofop_12_munk.pdf (letöltve: 2022.09.12.)

[91] KOVÁCS L.: Európai Országok Kiberbiztonsági Politikáinak és Stratégiáinak Összehasonlító Elemzése I., In: Hadmérnök, VII. évfolyam 2. szám 2012., ISSN 1788-1929., pp. 302-311. Online: http://hadmernok.hu/2012_2_kovacsl.pdf (letöltve: 2022.09.12.)

[92] RAJNAI Z.: A kritikus információs infrastruktúrák összetétele, biztonsági kérdése, In: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar /szerk./ Nemzetközi Gépész és Biztonságtechnikai Szimpózium: a Magyar Tudomány Ünnepe tiszteletére: Budapest, 2012. november 20., 21., 26.: Bánki Donát Emlékülés, 2012. november 22. Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar (2012) pp. 15-22.

[93] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[94] KOVÁCS Z.: Az infokommunikációs rendszerek nemzeti biztonsági kihívásai; Dissertationes Doctorale, Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó Iroda, Budapest. 2021. ISBN 978-963-531-065-4(PDF). http://real.mtak.hu/128878/1/722_az_infokommunkicios_rendszerek.pdfjsessionid513BA7B61ED404292AF714063F446241sequence1 (letöltve: 2022.09.12.)

[95] ORBÓK Á.: A kibertér, mint hadszíntér, In: Biztonságpolitika: Biztonságpolitikai Szakportál, 2013., pp. 101-108. https://biztonsagpolitika.hu/wp-content/uploads/2015/04/Orbok-Akos-A-kiberter-mint-hadszinter.pdf (letöltve: 2022.09.12.)

[96] BHARDWAJ, A.: 5G for Military Communications, In: Procedia Computer Science, Volume 171, 2020. ISSN 1877-0509., pp. 2665-2674 https://doi.org/10.1016/j.procs.2020.04.289. (letöltve: 2022.09.12.)

[97] TÓTH Dávid-GÁSPÁR Zsolt: Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén, In: Büntetőjogi Szemle, IX. évfolyam 2. szám 2020., ISSN 2063-8183., pp. 140-150.

[98] BABOS Tibor-ZÁHONYI Lajos: Az információbiztonság fejlődéstörténeti vizsgálata – az ERP rendszerek fejlődése, In: Biztonságtudományi Szemle, II. évfolyam 3. szám 2020., ISSN 2676-9042., pp.55-66. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/63/64 (letöltve: 2022.09.12.)

[99] ESTÓK Sándor: Az űrhaderő és az űrstratégia a többpólusú világban, In: Repüléstudományi Közlemények, XXXIII. évfolyam 2. szám, 2021., ISSN 1417-0604., pp. 153-165. http://doi.org/10.32560/rk.2021.2.11 (letöltve: 2022.09.12.)

[100] RAJNAI Z. /szerk./: Kiberbiztonság-Cybersecurity 2.; Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2019., ISBN 978-963-449-185-9. https://bdi.uni-obuda.hu/sites/default/files/oldal/csatolmany/kiadvany-2019.pdf (letöltve: 2022.09.12.)

[101] PESCO: a hatékonyabb védelmi együttműködésért az EU-ban. https://www.europarl.europa.eu/news/hu/headlines/security/20171208STO89939/pesco-a-hatekonyabb-vedelmi-egyuttmukodesert-az-eu-ban (letöltve: 2022.09.12.)

[102] PESCO Projects Cyber and Information Domain Coordination Center (CIDCC). https://pesco.europa.eu/project/cyber-and-information-domain-coordination-center-cidcc/ (letöltve: 2022.09.12.)

[103] KOMJÁTHY L. J.: A Hatékony Haderő Felkészítésének Néhány Területe a Várható Alkalmazás Szempontjából, In: Hadtudományi Szemle, XI. évfolyam 1. szám 2018., ISSN 2060-0437., pp.71-84. https://epa.oszk.hu/02400/02463/00038/pdf/EPA02463_hadtudomanyi_szemle_2018_01_071-084.pdf (letöltve: 2022.09.12.)

[104] RESPERGER I.: Új magyar Katonai Nemzeti Stratégia - beszélgetés Dr. Resperger István ezredessel 2021. https://soundcloud.com/spiritfmbp/leirasuj-magyar-katonai-nemzeti-strategia-beszelgetes-dr-resperger-istvan-ezredessel/s-WvVPO7OkQJi (letöltve: 2022.09.12.)

[105] SZENES Z.: Katonai kihívások a 21. század elején, In: Hadtudomány XIV. évfolyam 4. szám 2005. https://www.mhtt.eu/hadtudomany/2005/4/2005_4_5.html (letöltve: 2022.09.12.)

[106] Megjelent az új Nemzeti Katonai Stratégia, Honvedelem.hu, Budapest, 2021. 06. 25. https://honvedelem.hu/hirek/megjelent-az-uj-nemzeti-katonai-strategia.html (letöltve: 2022.09.12.)

[107] RESPERGER I.: A hibrid hadviselési mód jellemzői korunk konfliktusaiban, In: Rendőrségi tanulmányok III. évfolyam 2. szám 2020., ISSN 2630-8002., pp. 104-118. https://www.bm-tt.hu/rtt/assets/letolt/rt/202002a/resperger.pdf (letöltve: 2022.09.12.)

[108] STICZ László-SEPRŐDI-KISS Árpád: A Magyar Honvédség képességfejlesztése, egy korszerű haderő megteremtése, In: Hadtudomány: A Magyar Hadtudományi Társaság folyóirata, XXX. évfolyam 4. szám, 2020., ISSN 1215-4121., pp. 3-21.http://doi.org/10.17047/HADTUD.2020.30.4.3 (letöltve: 2022.09.12.)

[109] Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében. Budapest. https://jogalappal.hu/letoltheto-zrinyi-2026-program/ (letöltve: 2022.09.12.)

[110] A haza védelme, a nemzet szolgálata. Honvedelem.hu, Budapest, 2019. https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf (letöltve: 2022.09.12.)

[111] Hamarabb teljesíthetjük a NATO-célt. Vg.hu, 2022.03.18. https://www.vg.hu/vilaggazdasag-magyar-gazdasag/2022/03/hamarabb-teljesithetjuk-a-nato-celt (letöltve: 2022.09.12.)

[112] MTI: Palkovics: Nagyon jól halad az együttműködés a Rheinmetall és Magyarország között. Hirado.hu, Budapest, 2022.06.13. https://hirado.hu/belfold/gazdasag/cikk/2022/06/13/palkovics-nagyon-jol-halad-az-egyuttmukodes-a-rheinmetall-es-magyarorszag-kozott (letöltve: 2022.09.12.)

[113] Térképre tettük a haderőfejlesztési programot: hol épülnek most hadiüzemek Magyarországon? Novekedes.hu, 2021.03. 26. https://novekedes.hu/elemzesek/terkepre-tettuk-a-haderofejlesztesi-programot-hol-epulnek-most-hadiuzemek-magyarorszagon (letöltve: 2022.09.12.)

[114] DRAVECZKY-URY Ádám: Zrínyi 2026. Honvedelem.hu, Budapest, 2017.01.16. https://honvedelem.hu/cikk/zrinyi-2026/ (letöltve: 2022.09.12.)

[115] A járványról és a haderőfejlesztésről is beszélt a honvédelmi miniszter. Honvedelem.hu, Budapest, 2020. 12.05. https://honvedelem.hu/hirek/a-jarvanyrol-es-a-haderofejlesztesrol-is-beszelt-a-honvedelmi-miniszter.html (letöltve: 2022.09.12.)

[116] „Innentől már nem a régi vasakból kell kifacsarni az utolsó lehetőségeket” Interjú dr. Sticz László dandártábornokkal (1. rész). Honvedelem.hu, Budapest, 2021. 01. 20. https://honvedelem.hu/hirek/innentol-mar-nem-a-regi-vasakbol-kell-kifacsarni-az-utolso-lehetosegeket.html (letöltve: 2022.09.12.)

[117] Már a szolnoki bázison vannak a honvédség első új helikopterei. Honvedelem.hu, Budapest, 2019.11.19. https://honvedelem.hu/cikk/mar-a-szolnoki-bazison-vannak-a-honvedseg-elso-uj-helikopterei/ (letöltve: 2022.09.12.)

[118] Tovább gyarapodó légi képesség. Honvedelem.hu, Budapest, 2020. 06. 22. https://honvedelem.hu/media/aktualis-videok/tovabb-gyarapodo-legi-kepesseg.html (letöltve: 2022.09.12.)

[119] Újabb helikopterek érkeztek. Honvedelem.hu, Budapest, 2020.12.10. https://honvedelem.hu/hirek/ujabb-helikopterek-erkeztek.html (letöltve: 2022.09.12.)

[120] Magyarországon az utolsó előtti Airbus. Honvedelem.hu, Budapest, 2021.11.23. https://honvedelem.hu/hirek/magyarorszagon-az-utolso-elotti-airbus.html (letöltve: 2022.09.12.)

[121] RÉVÉSZ Béla: Csúcstechnika a levegőben. Honvedelem.hu, Budapest, 2019.11.18. https://honvedelem.hu/galeriak/csucstechnika-a-levegoben/ (letöltve: 2022.09.12.)

[122] BARANYAI Gábor: Megérkeztek a honvédség új helikopterei a német gyárból. Magyarnemzet.hu, 2019.11.19. https://magyarnemzet.hu/belfold/megerkeztek-a-honvedseg-uj-helikopterei-a-nemet-gyarbol-7505657/ (letöltve: 2022.09.12.)

[123] Minőségi csere, In: Magyar Honvéd, XXX. évfolyam 1. szám., pp. 40-45. https://honvedelem.hu/images/media/5f58bed3c3005218226075.pdf (letöltve: 2022.09.12.)

[124] Irán támadást intézett két amerikai bázis ellen Irakban. Hirtv.hu, Budapest, 2020.01.08. https://hirtv.hu/hirtvkulfold/iran-ballisztikus-raketakkal-tamadott-meg-amerikai-celpontokat-irakban-2492968 (letöltve: 2022.09.12.)

[125] KC-390-es hadszíntéri szállító repülőgépeket vásárol a Magyar Honvédség Honvedelem.hu, Budapest, 2020. 11.1.7. https://honvedelem.hu/hirek/kc-390-es-hadszinteri-szallito-repulogepeket-vasarol-a-magyar-honvedseg.html (letöltve: 2022.09.12.)

[126] Haderőfejlesztés: Légvédelmi Rakéta Műveleti Központ Győrben. Honvedelem.hu, Budapest, 2021.08. 13. https://honvedelem.hu/hirek/haderofejlesztes-legvedelmi-raketa-muveleti-kozpont-gyorben.html (letöltve: 2022.09.12.)

[127] Csúcstechnológia a légvédelem szolgálatában. Honvedelem.hu, Budapest, 2020.11.30. https://honvedelem.hu/hirek/csucstechnologia-a-legvedelem-szolgalataban.html (letöltve: 2022.09.12.)

[128] Múlt, jelen, jövő- egy radarképen. Honvedelem.hu, Budapest. 2021. 03.31.https://honvedelem.hu/hirek/mult-jelen-jovo-egy-radarkepen.html (letöltve: 2022.09.12.)

[129] A legkorszerűbb légiharc-rakétákkal bővül a Magyar Honvédség Gripen harci gépeinek fegyverzete. Honvedelem.hu, Budapest, 2021.12.20. https://honvedelem.hu/hirek/a-legkorszerubb-legiharc-raketakkal-bovul-a-magyar-honvedseg-gripen-harci-gepeinek-fegyverzete.html (letöltve: 2022.09.12.)

[130] Hamarosan eljön a „szuperkatonák” kora? Honvedelem.hu, Budapest, 2021.02. 23. https://honvedelem.hu/hirek/hamarosan-eljon-a-szuperkatonak-kora.html (letöltve: 2022.09.12.)

[131] Átadták a Magyar Honvédség Kiber Képzési Központját. Kormany.hu, Budapest, 2019.06.13. https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat (letöltve: 2022.09.12.)

[132] Katonáink a kibertér biztonságáért. Honvedelem.hu, Budapest, 2022.03.18. https://honvedelem.hu/hirek/katonaink-a-kiberter-biztonsagaert.html (letöltve: 2022.09.12.)

[133] Polaris MRZR 4: nincs akadály! Honvedelem.hu, Budapest, 2018.04.20. https://honvedelem.hu/media/aktualis-videok/polaris-mrzr-4-nincs-akadaly.html (letöltve: 2022.09.12.)

[134] Megérkezett Tatára mind a 12 Leopard 2A4 harckocsi. Portfolio.hu, Budapest, 2020.12.03. https://www.portfolio.hu/global/20201203/megerkezett-tatara-mind-a-12-leopard-2a4-harckocsi-460280# (letöltve: 2022.09.12.)

[135] Lánctalpasok a startvonalnál (1. rész.), Honvedelem.hu, Budapest, 2021.05.20. https://honvedelem.hu/hirek/lanctalpasok-a-startvonalnal.html (letöltve: 2022.09.12.)

[136] Dr. Maróth Gáspár: elkezdődhet az önjáró lövegek gyártása a honvédség számára, Honvedelem.hu, Budapest, 2022.01.26. https://honvedelem.hu/hirek/dr-maroth-gaspar-elkezdodhet-az-onjaro-lovegek-gyartasa-a-honvedseg-szamara.html (letöltve: 2022.09.12.)

[137] KURCZ Kristóf-VÉG Róbert-HEGEDŰS Ernő: A Leopard 2 harckocsi család és a Magyar Honvédség 2A4 és 2A7+ típusváltozatai, In: Haditechnika, LIV. évfolyam 5. szám, 2020. https://doi.org/10.23713/HT.54.5.01 (letöltve: 2022.09.12.)

[138] Páncéltörő-rendszerváltás. Honvedelem.hu, Budapest, 2019.09.12. https://honvedelem.hu/hirek/a-magyar-honvedseg-parancsnokanak-helyettese/panceltoro-rendszervaltas.html (letöltve: 2022.09.12.)

[139] Nemzetközi színvonalú magyar fegyvergyár. Honvedelem.hu, Budapest, 2020.12.03.https://honvedelem.hu/hirek/nemzetkozi-szinvonalu-magyar-fegyvergyar.html (letöltve: 2022.09.12.)

[140] Harci paripa, kerekeken. Honvedelem.hu, Budapest, 2021.02.13. https://honvedelem.hu/hirek/harci-paripa-kerekeken.html (letöltve: 2022.09.12.)

[141] Hadiipari üzem épül Zalaegerszegen. Honvedelem.hu, Budapest, 2020.12.17. https://honvedelem.hu/hirek/lynx-megkezdodott-az-epitkezes.html (letöltve: 2022.09.12.)

[142] A legmodernebb védelmi rendszerekkel szerelik fel a magyar páncélosokat. Portfolio.hu, Budapest, 2021.05.13. https://www.portfolio.hu/global/20210513/a-legmodernebb-vedelmi-rendszerekkel-szerelik-fel-a-magyar-pancelosokat-483040 (letöltve: 2022.09.12.)

[143] Szemlélet- és típusváltás a szárazföldi haderőnemnél. Beszélgetés Takács Attila vezérőrnaggyal. Honvedelem.hu, Budapest, 2021.03.10. https://honvedelem.hu/hirek/szemlelet-es-tipusvaltas-a-szarazfoldi-haderonemnel.html (letöltve: 2022.09.12.)

[144] Védelmi ipar ágazati koncepciója. Hmarzenal.hu, Budapest, 2018. http://www.hmarzenal.hu/vedelmi-ipar/vedelmi-ipar-agazati-koncepcioja.pdf (letöltve: 2022.09.12.)

[145] Szerződéskötés a repülőtéren. Honvedelem.hu, Budapest, 2020.09.24. https://honvedelem.hu/hirek/szerzodeskotes-a-repuloteren.html (letöltve: 2022.09.12.)

[146] Ősszel kezdődik a hadiipari üzem építése Kaposváron. Portfolio.hu, Budapest, 2021.04.15. https://www.portfolio.hu/global/20210415/osszel-kezdodik-a-hadiipari-uzem-epitese-kaposvaron-478812 (letöltve: 2022.09.12.)

[147] Napokon belül kész a magyar védelmi ipari stratégia. Origo.hu, Budapest, 2021.01.21. https://www.origo.hu/itthon/20210121-napokon-belul-kesz-a-magyar-vedelmi-ipari-strategia.html (letöltve: 2022.09.12.)

[148] 2021-ben is dübörög a magyar hadiipar fejlesztése. Portfolio.hu, Budapest, 2021.02.10. https://www.portfolio.hu/global/20210210/2021-ben-is-duborog-a-magyar-hadiipar-fejlesztese-megtudtuk-mit-tervez-a-kormany-465188 (letöltve: 2022.09.12.)

[149] 5GK-Magyarországi 5G Koalíció. Digitalisjoletprogram.hu, Budapest. https://digitalisjoletprogram.hu/hu/tartalom/5gk-magyarorszagi-5g-koalicio (letöltve: 2022.09.12.)

[150] BLACKMAN-COLIN-FORGE, Simon: 5GDeployment. Europarl.europa.eu, Brussels, 2019. https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf (letöltve: 2022.09.12.)

[151] Zalazone.hu. https://zalazone.hu/ (letöltve: 2022.09.12.)

[152] Autonóm on- és offroad járművek katonai alkalmazhatóságának lehetőségei, Tudományos konferencia Zalaegerszegen, a ZalaZone járműipari tesztpályán. Haditechnika LIII. évfolyam, 1. szám 2019. http://real.mtak.hu/98531/1/HT_2019-1_cikk-11.pdf (letöltve: 2022.09.12.)

[153] KISS Adorján: Okosfegyverekkel látnák el a hadsereget. Vg.hu. 2019.10.21. https://www.vg.hu/gazdasag/gazdasagi-hirek/okosfegyverekkel-latnak-el-a-hadsereget-2-1821681/ (letöltve: 2022.09.12.)

[154] Orosz okos-sörétes: Kalasnyikov MR-155 Ultima “Smartgun”. Kaliberinfo.hu, 202.08.22.http://www.kaliberinfo.hu/hirek/orosz-okos-soretes-kalasnyikov-mr-155-ultima-smartgun/ (letöltve: 2022.09.12.)

[155] Lockheed Martin - F-35 Lightning II. Aerotech.hu. http://www.aerotech.hu/f-35.php (letöltve: 2022.09.12.)

[156] Rakétatámadások Irakban: Irán gyorsan megtorolta Szulejmáni likvidálását. Hvg.hu, Budapest, 2020.01.08. https://hvg.hu/vilag/20200108_Iran_raketacsapast_mert_az_amerikaiak_egy_iraki_tamaszpontjara (letöltve: 2022.09.12.)

[157] Tényleg olyan veszélyes az oroszok által Ukrajnában bevetett hiperszonikus fegyver? Raketa.hu, 2022.03.19. https://raketa.hu/tenyleg-olyan-veszelyes-az-oroszok-altal-ukrajnaban-bevetett-hiperszonikus-fegyver (letöltve: 2022.09.12.)

[158] PORKLOÁB Imre-NÉGYESI Imre: A mesterséges intelligencia alkalmazási lehetőségeinek kutatása a haderőben, In: Honvédségi Szemle: A Magyar Honvédség központi folyóirata, CXLVII. évfolyam 5. szám, 2019., ISSN 2732-3226., pp. 3-21. http://real.mtak.hu/125496/1/HSZ_2019_147_5_Porkolab_Imre_Negyesi_Imre.pdf (letöltve: 2022.09.12.)

[159] TRAUTMANN Balázs: Fémharcosok. Honvedelem.hu, Budapest, 2016.07.24. https://honvedelem.hu/hatter/haditechnika/femharcosok.html (letöltve: 2022.09.12.)

[160] GÁCSER Zoltán: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben c. PhD értekezés. Budapest, 2008. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12102/ertekezes.pdf;jsessionid=E53B0E3B1B43A817529E3C72C25CEF01?sequence=1 (letöltve: 2022.09.12.)

[161] Torchbearer National Security Report: Key Issues Relevant to The U.S. Army's Transformation to the Objective Force, An AUSA Torchbearer Issue, Vol. II. USA, 2002. https://www.ausa.org/sites/default/files/TBNSR-2002-The-US-Armys-Transformation-to-the-Objective-Force-Vol2.pdf (letöltve: 2022.09.12.)

[162] Land Warrior Integrated Soldier System. Army-technology.com, USA. https://www.army-technology.com/projects/land_warrior/ (letöltve: 2022.09.12.)

[163] Future Force Warrior. Military-history.fandom.com. https://military-history.fandom.com/wiki/Future_Force_Warrior (letöltve: 2022.09.12.)

[164] A jövő hadserege: láthatatlan katonák és robotok szolgálnak majd? Honvedelem.hu, Budapest. 2021.04.10. https://honvedelem.hu/hirek/a-jovo-hadserege-lathatatlan-katonak-es-robotok-szolgalnak-majd.html (letöltve: 2022.09.12.)

[165] A jövő már a jelen? Sci-fibe illő hadiipari technikák. Honvedelem.hu, Budapest, 2021.02.07. https://honvedelem.hu/hirek/a-jovo-mar-a-jelen-sci-fibe-illo-hadiipari-technikak-1.html (letöltve: 2022.09.12.)

[166] Elérhető közelségbe kerültek a szuperkatonák? Honvedelem.hu, Budapest, 2021.02.14. https://honvedelem.hu/hirek/elerheto-kozelsegbe-kerultek-a-szuperkatonak.html (letöltve: 2022.09.12.)

[167] Katonás Info tér. Honvedelem.hu, Budapest, 2019.10.16. https://honvedelem.hu/hirek/hazai-hirek/katonas-infoter.html (letöltve: 2022.09.12.)

[168] TÖRÖK P.: A Brief Overview of Digital Military Systems Used in the Armies of NATO Member Countries, In: Nemzetbiztonsági Szemle, IX. évfolyam 1. szám, 2021., ISSN 2064-3756., pp. 56-70. https://doi.org/10.32561/nsz.2021.1.4 (letöltve: 2022.09.12.)

[169] NÉGYESI Imre: A mesterséges intelligencia és a hadsereg, Hadtudomány, XXVIIII. évfolyam 3. szám, 2019., ISSN 1215-4121., pp. 71-79. http://doi.org/10.17047/HADTUD.2019.29.3.71 (letöltve: 2022.09.12.)

[170] Robotok uralják a jövő harctereit? Honvedelem.hu, Budapest, 2010.08.05. https://honvedelem.hu/hirek/robotok-uraljak-a-jovo-harctereit.html (letöltve: 2022.09.12.)

[171] Mesterséges Intelligencia Koalíció. Digitalisjoletprogram.hu. https://digitalisjoletprogram.hu/hu/tartalom/mesterseges-intelligencia-koalicio (letöltve: 2022.09.12.)

[172] Magyarország Mesterséges Intelligencia Stratégiája 2020-2030. Budapest, 2020. https://ai-hungary.com/api/v1/companies/15/files/137203/view (letöltve: 2022.09.12.)

[173] PORKOLÁB I.: Szervezeti adaptáció a Magyar Honvédségben: küldetésalapú vezetés 2.0 a digitális transzformáció korában, In: Honvédségi Szemle: A Magyar Honvédség központi folyóirata, CXLVII. évfolyam 1. szám, 2019. ISSN 2732-3226., pp. 3-12. http://real-j.mtak.hu/13949/13/Honvedsegi_Szemle_2019_1_teljes_szam.pdf#page=4 (letöltve: 2022.09.12.)

[174] Ukrajnában az MI segítségével azonosítják a halott orosz katonákat. Computerworld.hu, 2022.03.25. https://computerworld.hu/biztonsag/ukrajnaban-ai-segitsegevel-azonositjak-a-halott-orosz-katonakat-308358.html (letöltve: 2022.09.12.)

[175] Ukrajnában az MI segítségével azonosítják a halott orosz katonákat. Computerworld.hu, https://computerworld.hu/biztonsag/ukrajnaban-ai-segitsegevel-azonositjak-a-halott-orosz-katonakat-308358.html (letöltve: 2022.09.12.)

[176] Digitális megoldások a jövő hadseregében. Uni-nke.hu, Budapest, 2019. https://www.uni-nke.hu/hirek/2019/08/07/digitalis-megoldasok-a-jovo-hadseregeben (letöltve: 2022.09.12.)

[177] DARPA, Army & Team Platypus: Big Boosts For Artificial Intelligence. Breakingdefense.com, 2018. https://breakingdefense.com/2018/09/darpa-the-army-team-platypus-artificial-intelligence-for-future-war/ (letöltve: 2022.09.12.)

[178] Darpa.mil. https://www.darpa.mil/ (letöltve: 2022.09.12.)

[179] TÖRÖK P.: A NATO-tagországok által alkalmazott digitális katonai rendszerek rövid áttekintése, In: Nemzetbiztonsági Szemle 9. évfolyam 1. szám 2021., ISSN 2064-3756., pp.56-70. https://doi.org/10.32561/nsz.2021.1.4 (letöltve: 2022.09.12.)

[180] Középpontban a katona. Kormany.hu, Budapest, 2019.05.01. https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/kozeppontban-a-katona (letöltve: 2022.09.12.)

[181] POHL Á.: A magyar tisztképzés előtt álló kihívások, In: Hadtudományi Szemle, XII. évfolyam Különszám 2019., ISSN 2060-0437., pp.223-234. http://doi.org/10.32563/hsz.2019.1.ksz.16 (letöltve: 2022.09.12.)

[182] Acélkocka. Honvedelem.hu, Budapest, 2019.03.23. https://honvedelem.hu/hirek/hazai-hirek/acelkocka.html (letöltve: 2022.09.12.)

[183] VARTMANN György: Altisztszakképzés a Magyar Honvédség Altiszti Akadémián (2012–2020), In: Honvédségi Szemle: A Magyar Honvédség központi folyóirata, CXLIX. évfolyam 2. szám 2021., ISSN 2732-3226., pp. 93-115. https://doi.org/10.35926/HSZ.2021.2.8 (letöltve: 2022.09.12.)

[184] 1004/2016. (I. 18.) Korm. határozat a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról

[185] Elektronikus irományszerkesztés és benyújtás (ParLex rendszer) Parlament.hu, Budapest, https://www.parlament.hu/elektronikus-iromanyszerkesztes-es-benyujtas-a-parlex-rendszer- (letöltve: 2022.09.12.)

[186] Nemzeti Infokommunikációs Stratégia 2014-2020. https://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (letöltve: 2022.09.12.)

[187] 1612/2019. (X. 24.) Korm. határozat az Integrált Jogalkotási Rendszer bevezetéséről és az ahhoz kapcsolódó feladatokról

[188] „Oroszországgal közös cél, hogy magyar űrhajós kezdhessen el dolgozni 2025-re” Magyarhirlap.hu, Budapest, 2019.12.13. https://www.magyarhirlap.hu/kulfold/20191213-magyar-orosz-urkutatasi-projektek-indulnak (letöltve: 2022.09.12.)

[189] Stratégiai megállapodás űrkutatási együttműködésről a Thales Alenia Space űripari vállalattal. Space.kormany.hu, 2021.11.16. https://space.kormany.hu/strategiai-megallapodas-urkutatasi-egyuttmukodesrol-a-thales-alenia-space-uripari-vallalattal (letöltve: 2022.09.12.)

[190] Urvilag.hu. http://www.urvilag.hu/ (letöltve: 2022.09.12.)

[191] 7/2022. (VI. 24.) KKM utasításminiszteri biztos kinevezéséről

[192] FERENCZ Orsolya-BONYHÁDY Elek-HORVÁTH Anna-TRAUTMANN Gábor-TRAUTMANN László: Az űrkutatás és az űripar globális perspektívái: Interjú dr. Ferencz Orsolyával (PhD), az űrkutatásért felelős miniszteri biztossal, In: Köz-gazdaság, 15. évfolyam 3. szám, 2020. ISSN: 1788-0696., pp. 18-24. https://doi.org/10.14267/RETP2020.03.02 (letöltve: 2022.09.12.)

[193] 1606/2021. (VIII. 18.) Korm. határozat Magyarország Űrstratégiája elfogadásáról

[194] „A világűr az egész emberiség közös öröksége". Beszélgetés Horváth Attila alezredessel, az MH Modernizációs Intézet megbízott osztályvezetőjével. Honvedelem.hu, Budapest, 2021.03.18. https://honvedelem.hu/hirek/a-vilagur-az-egesz-emberiseg-kozos-oroksege.html (letöltve: 2022.09.12.)

[195] HEGEDŰS Ernő-SIMON Csilla: Interjú prof. Dr. Kovács László dandártábornokkal, a Magyar Honvédség Parancsnokságának kibervédelmi szemlélőjével, In: Haditechnika, LIV. évfolyam 3. szám 2020, ISSN 0230-6891., pp. 60-62. https://doi.org/10.23713/HT.54.3.11 (letöltve: 2022.09.12.)

[196] „Elsőnek lenni dicsőség, elsőnek lenni felelősség". Honvedelm.hu, Budapest, 2021.05.06. https://honvedelem.hu/hirek/elsonek-lenni-dicsoseg-elsonek-lenni-felelosseg.html (letöltve: 2022.09.12.)

[197] GERŐFI Szilárd: A Magyar Honvédség vezetéstámogató rendszere alkalmazásának lehetőségei a XXI. századi kihívások tükrében, In: Hadtudomány, XXVII. évfolyam 3-4. szám, 2017., ISSN 1215-4121., pp. 96-105. https://doi.org/10.17047/HADTUD.2017.27.3-4.96 (letöltve: 2022.09.12.)

[198] FARKAS T.: A védelmi tevékenységeket támogató MH Kormányzati Célú Elkülönült Hírközlő Hálózat fejlesztési lehetőségeinek vizsgálata a honvédelmi és haderőfejlesztési program (Zrínyi 2026) tükrében – Hazai/nemzetközi szakirodalmi összefoglaló, Hadtudományi Szemle, XII. évfolyam 4. szám, 2019., ISSN 2060-0437., pp. 5-16. http://doi.org/10.32563/hsz.2019.4.1 (letöltve: 2022.09.12.)

[199] 55/2013. (IX. 13.) HM utasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint a központilag biztosított szolgáltatások igénybevételének szabályairól

[200] JOBBÁGY Szabolcs: A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata, In: Hadmérnök, XII. évfolyam 3. szám, 2017., ISSN 1788-1929., pp. 223-236. http://hadmernok.hu/173_20_jobbagy.pdf (letöltve: 2022.09.12.)

[201] MUNK S.: A híradó-informatikai terminológia kérdései a Magyar Honvédségben I. rész: A terminológia alapjai és környezete, In: Hadtudomány, XXIV. évfolyam 3-4. szám, 2014., ISSN 1215-4121., pp. 94-105.http://mhtt.eu/hadtudomany/2014/3_4/2014_3_4_7.pdf (letöltve: 2022.09.12.)

[202] MUNK Sándor-NÉGYESI Imre: Informatikai eszközök a 172 éves Magyar Honvédségben: Jövőbeli célok és feladatok; Budapest, Magyarország: Zrínyi Kiadó,2020. ISBN: 9789633277751

RÖVIDÍTÉSJEGYZÉK

Advanced Research Projects Agency Network: ARPANET

Amerikai Egyesült Államok: USA

Canadian Disruptive Pattern: CADPAT

Defense Advanced Research Projects Agency: DARPA

Digitális Jólét Program: DJP

Egyesült Államok Védelmi Minisztériuma, Department of Defense: DOD

Egyesült Nemzetek Szervezete: ENSZ

Elektronikus dokumentum- és iratkezelő rendszer: EIR

Észak-atlanti Szerződés Szervezete: NATO

Európa Tanács: ET

Európai Bizottság: EB

Európai Biztonsági és Együttműködési Szervezet: EBESZ

Európai Unió Kiberbiztonsági Ügynökség, European Union Agency for Cybersecurity: ENISA

Európai Unió: EU

Európai Űrügynökség, European Space Agency: ESA

Európai Védelmi Ügynökség, European Defence Agency: EDA

Honvéd Vezérkar Híradó, Informatikai és Infromációvédelmi Csoportfőnökség: IICSF

Honvédelmi Minisztérium Költségvetés Gazdálkodási Információ Rendszer, Ügyfélszolgálati Rendszer: HM KGIR ÜSZR

Honvédelmi Minisztérium: HM

Innovációs és Technológiai Minisztérium: ITM

Integrált Jogalkotási Rendszer: IJR

Interdiszciplináris Technológiai Alkalmazások Bizottság: ITAB

Katonai Nemzetbiztonsági Szolgálat: KNBSZ

Kiber és Információs Domain Koordinációs Központ, Cyber and Information Domain Coordination Center: CIDCC

Kiberincidens-kezelési képesség (NATO), NATO Computer Incident Response Capability: NCIRC

Kis- és középvállalkozás: KKV

Kooperatív Kibervédelmi Kiválósági Központ (NATO), NATO Cooperative Cyber Defence Centre of Excellence: CCDCOE

Közepes hatótávolságú hálózatalapú légvédelmi rakétarendszer, National Advanced Surface to Air Missile System: NASAMS

Kutatás, fejlesztés, innováció: K+F+I

Kutatás, fejlesztés: K+F

Külgazdasági és Külügyminisztérium: KKM

Légi egészségügyi kiürítési képesség, Medical Evacuation: MEDEVAC képesség

Magyar Honvédség Kiber- és Információs Műveleti Központ: MH KIMK

Magyar Honvédség Kiber Képzési Központja: MH KKK

Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata: MH KCEHH

Magyar Honvédség Modernizációs Intézet: MH MI

Magyar Honvédség Parancsnoksága: MHP

Magyar Honvédség: MH

Marine Pattern: MARPAT

Mesterséges Intelligencia Koalíció: MIK

Mesterséges intelligencia: MI

Nemzeti Biztonsági Stratégia: NBS

Nemzeti Digitális Stratégia: NDS

Nemzeti Hírközlési és Informatikai Tanács: NHIT

Nemzeti Infokommunikációs Stratégia: NIS

Nemzeti Katonai Stratégia: NKS

Nemzeti Kiberbiztonsági Stratégia: NKBS

Nemzetközi Távközlési Egyesület, International Telecommunication Union: ITU

Nemzetközi Űrállomás, International Space Station: ISS

Orosz Szövetségi Űrügynökség: Roszkoszmosz

Permanent Structured Cooperation: PESCO

Technológiai és Ipari Minisztérium: TIM

United Space Force: USSF

Universal Camouflage Pattern: UCP

Védelmi Beszerzési Ügynökség Zrt.: VBÜ

Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program: Zrínyi 2026

KÖSZÖNETNYILVÁNÍTÁS

2017-ben lettem az Óbudai Egyetem doktorandusza. Közel 5 és fél éven keresztül végeztem elméleti és gyakorlati kutatómunkát a doktori témám kapcsán érintett területeken. A kutatásaim során abban a szerencsés helyzetben voltam, hogy a közigazgatásban olyan területeken dolgozhattam, ahol valóban testközeli információkkal gazdagodhattam a témámat illetően.

Köszönettel tartozom minden kollégámnak és vezetőmnek, akik végig segítettek az úton. Külön köszönettel tartozom a témavezetőmnek, Dr. Babos Tibornak, aki miatt bátran vágtam bele ebbe a folyamatba, aki minden nehézségben támogatott és kiváló munkájának köszönhetően végig hitt és bízott bennem. Köszönöm, hogy közös munkánk során törekedett a szakmabeli kapcsolatrendszerem kiépítésére, hogy a Biztonságtudományi Szakkollégium alelnökeként tapasztalatot szerezhettem és közösen dolgozhattam vele számos projekten.

Köszönöm Prof. Dr. Rajnai Zoltánnak és a Doktori Iskola titkárságának, hogy mindig rendelkezésre álltak, támogattak és segítették a munkámat. Szeretném megköszönni volt doktorandusztársaimnak és tanáraimnak, hogy bíztatásukkal, ötleteikkel és tapasztalataikkal időt és fáradtságot nem kímélve segítettek nekem végig menni ezen az általuk már megjárt úton. Nem utolsó sorban szeretném megköszönni a családomnak és a barátaimnak mindazt a támaszt, ami nélkül ez a disszertáció nem készülhetett volna el.