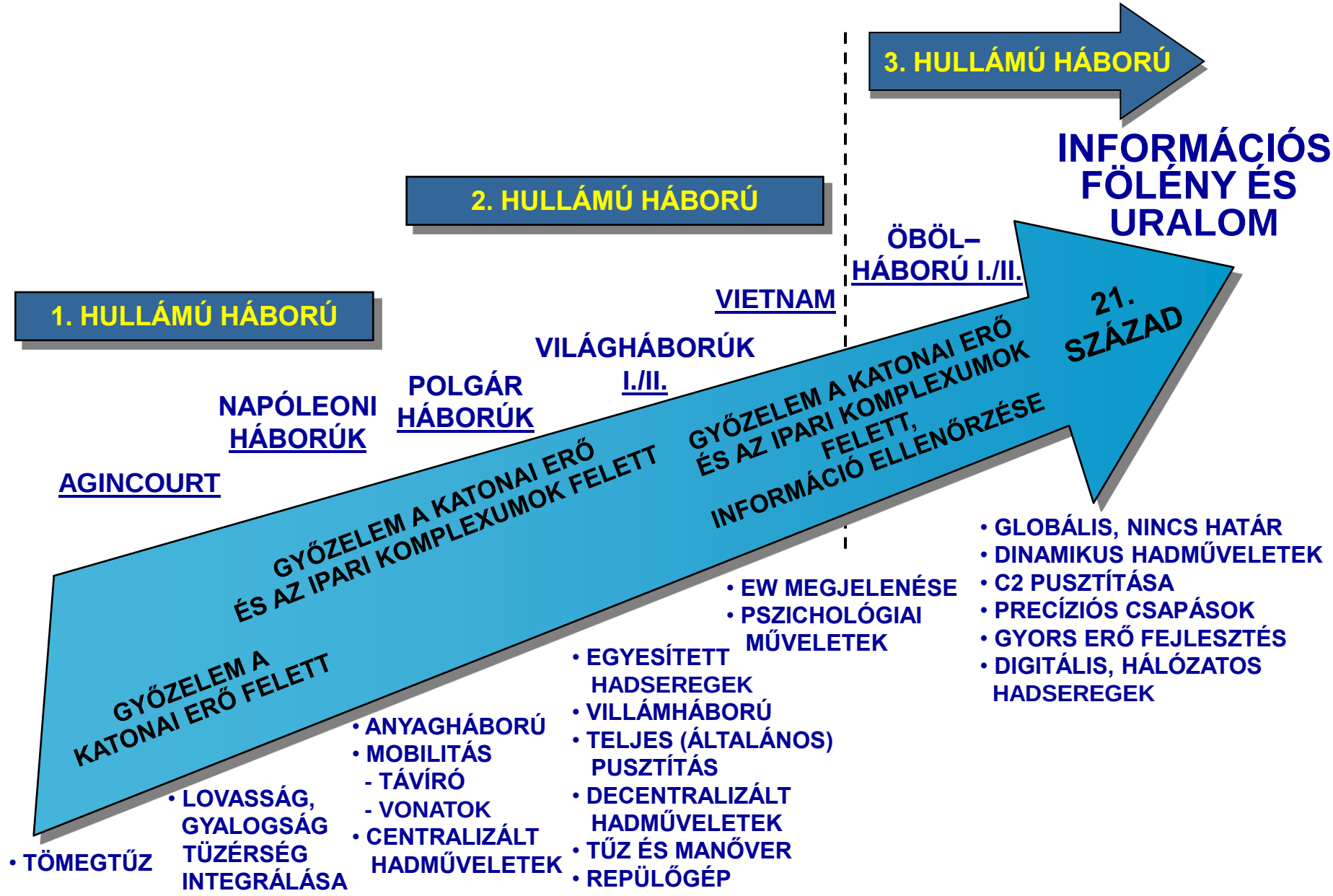
NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
Informatikai és Elektronikai Hadviselés Tanszék

INFORMÁCIÓS MŰVELETEK

Prof. dr. Haig Zsolt mk. ezredes, egyetemi tanár
HM 29-343 haig.zsolt@uni-nke.hu

HADVISELÉSI MÓDOK VÁLTOZÁSA



HADVISELÉSI MÓDOK VÁLTOZÁSA

TEGNAP (MA)	HOLNAP (MA)
Pusztítás	Hatékonyság
Élőerő pusztítása	Élőerő megóvása
Célpontalapú támadás	Hatékonyság alapú támadás
Célpont-, platform-alapú műveletek	Hatásalapú műveletek (EBO)

Hatásalapú megközelítésnek megfelelően az információs tevékenységek szerepe felértékelődik, az információalapú hadviselési módok előtérbe kerülnek

A JÖVŐ HADSZÍNTERE ÉS HADVISELÉSÉNEK JELLEMZŐI

A SIKER ELÉRÉSÉT BIZTOSÍTÓ TÉNYEZŐK:

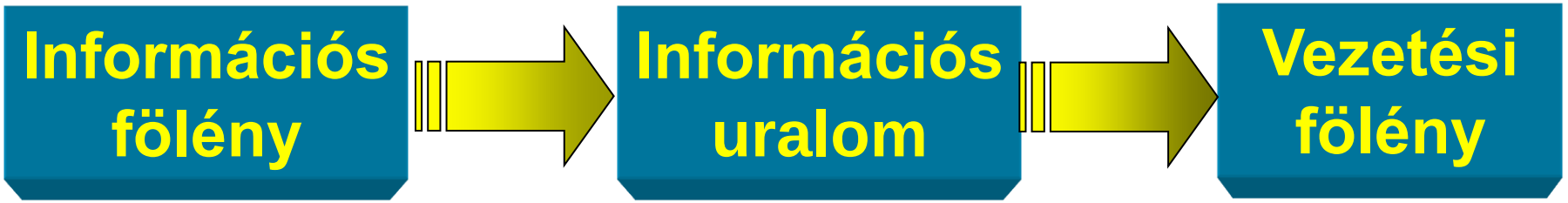
- ✓ Távoli felderítés
- ✓ Pontos cél azonosítás és követés
- ✓ Kapcsolat az együttműködőkkel
- ✓ Mindenre kiterjedő helyzetértékelés
- ✓ Erők megóvása
- ✓ A harc folyamatos vezetése, erők követése
- ✓ INFORMÁCIÓS FÖLÉNY

JELLEMZŐK:

- ✓ Több dimenziós
- ✓ Digitalizált
- ✓ Nem vonalas
- ✓ Erőviszony 1:1 v. <
- ✓ Minden idős tevékenység
- ✓ Erők alkalmazási sorrendje
- ✓ Elektronikus céltervezés

INFORMÁCIÓS FÖLÉNY

Az információs fölény birtokosának lehetővé teszi, hogy információs rendszereit és azok képességeit kihasználva a társadalmi élet különböző területein előnyre tegyen szert, vagy a kialakult helyzetet folyamatosan úgy irányítsa, hogy emellett a másik felet megfossza e képességeitől.

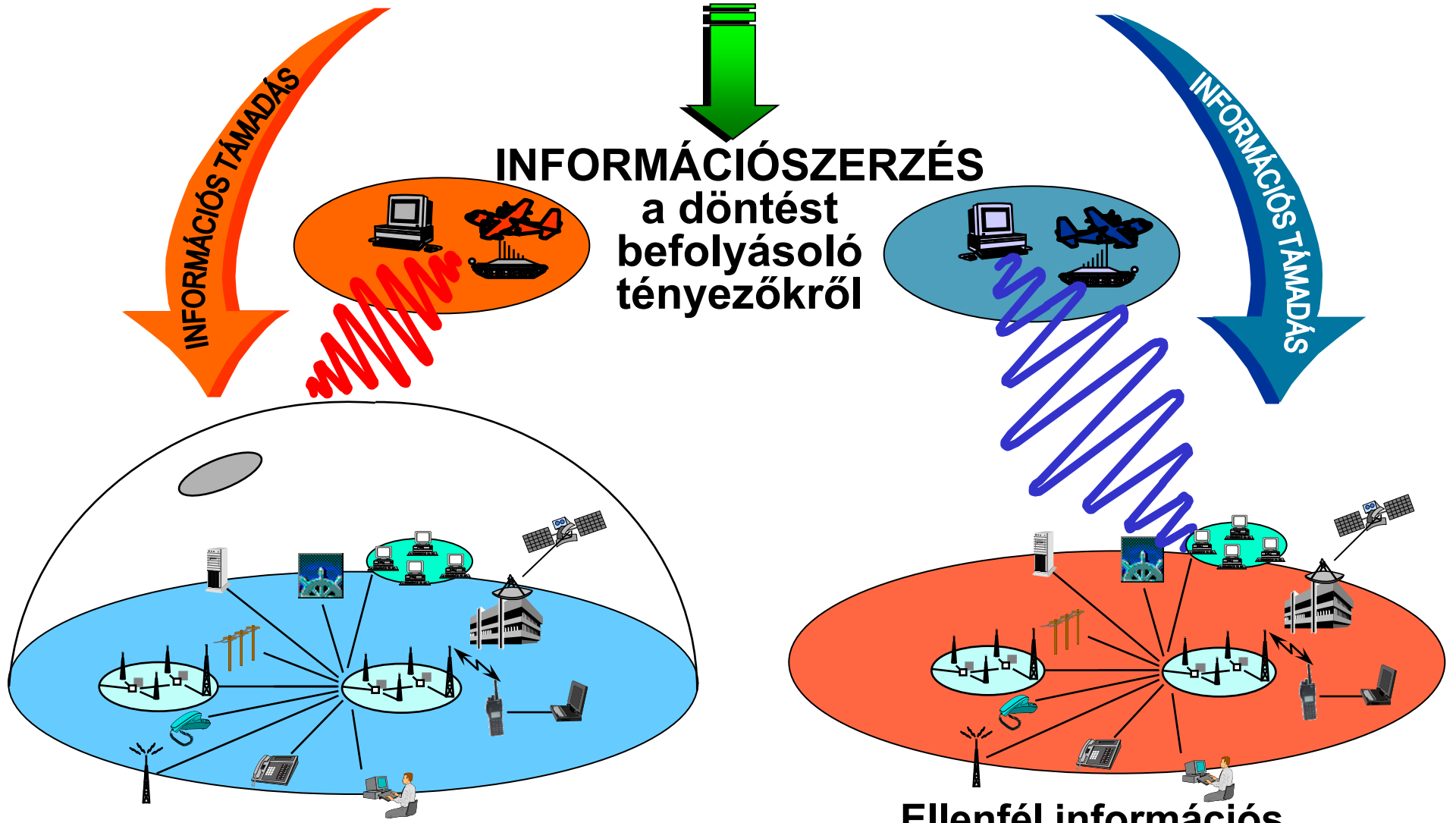


Az információs fölény megléte a birtoklója számára az alábbiakat jelenti

- többet tud a másik félről, mint amit ő tud a saját erőkről;
- eredményesen tudja korlátozni a másik fél vezetési és információs rendszereit, valamint döntési folyamatait, miközben ilyen behatásoktól képesek megóvni a saját rendszereiket;
- a sajátoldali döntési folyamat tudományra támaszkodó, alaposabb, gyorsabb és ennek következményeként hatékonyabb, mint az ellenfél hasonló vezetési folyamata;
- az információ-technológia terén egy lépéssel a másik fél előtt jár, és ezt a fölényt állandóan növeli.

INFORMÁCIÓS FÖLÉNY

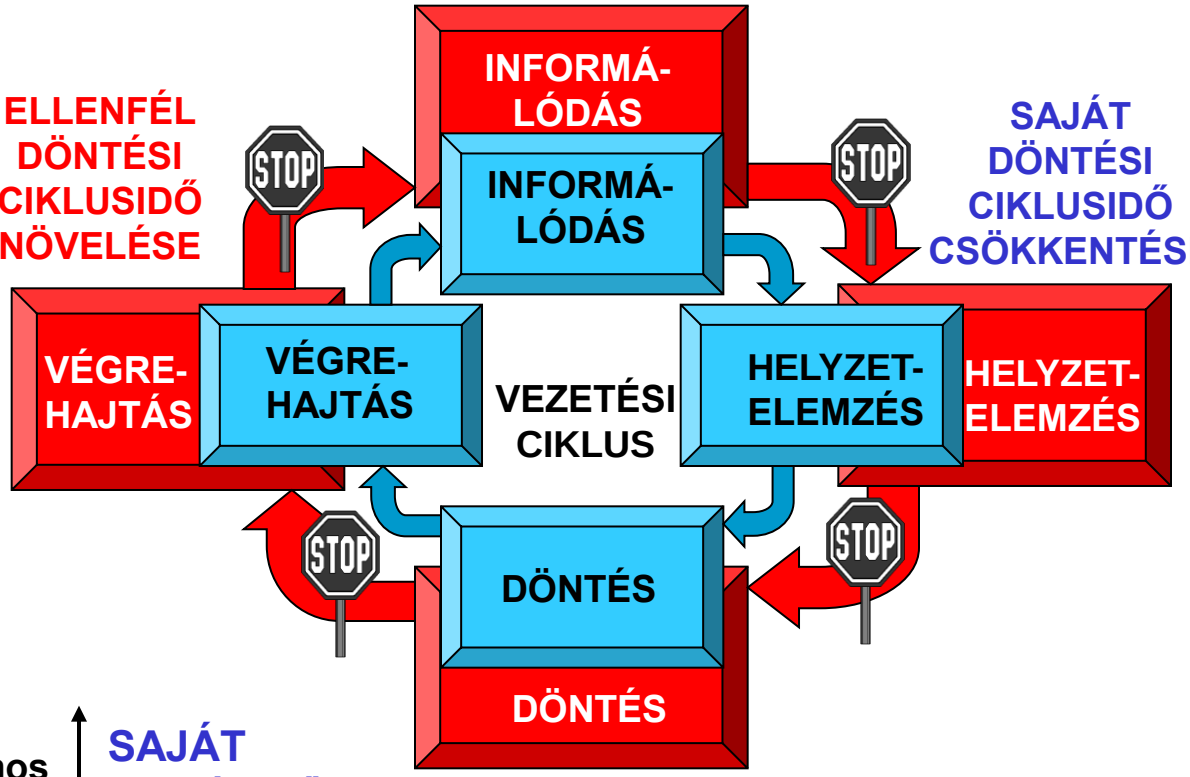
INFORMÁCIÓS FÖLÉNY KIALAKÍTÁSA

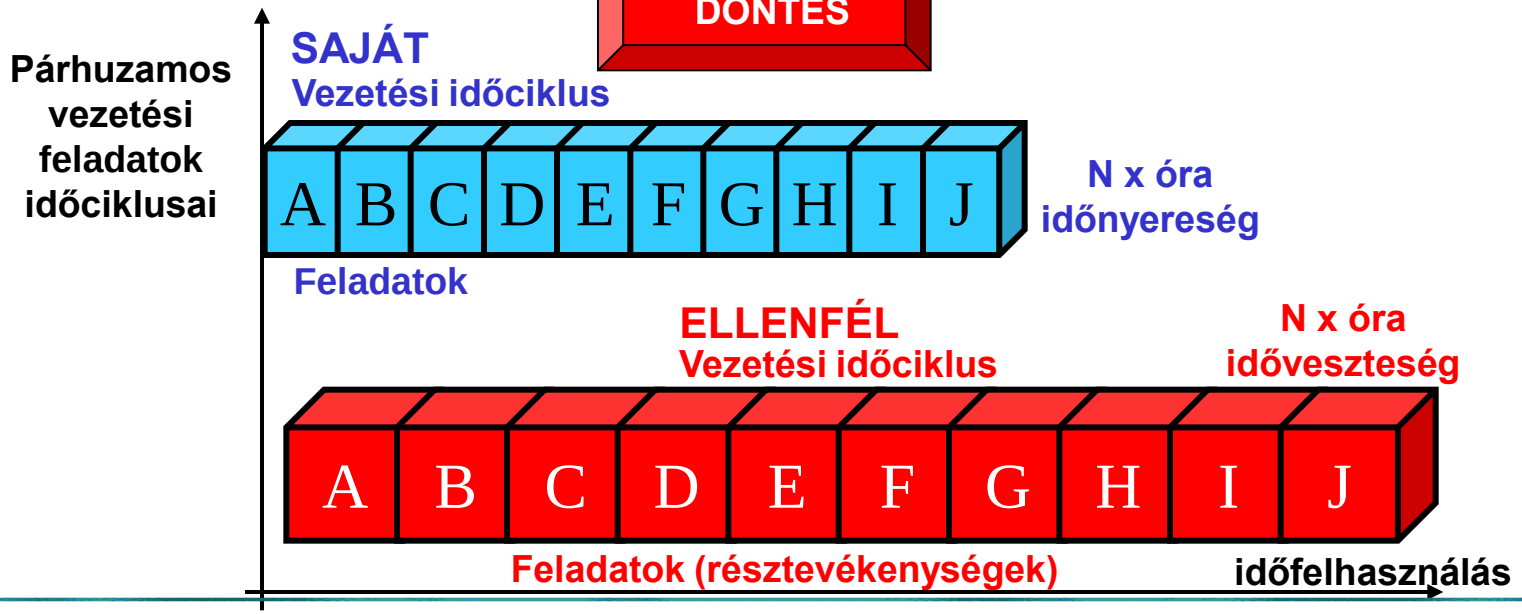


Saját információs képességek
KIHASZNÁLÁSA, VÉDELME

Ellenfél információs
lehetőségeinek
GYENGÍTÉSE, LERONTÁSA

VEZETÉSI FÖLÉNY ÉRTELMEZÉSE





HATÁSALAPÚ MEGKÖZELÍTÉS

A katonai műveletekben alkalmazott hatásalapú megközelítés elve szerint a hadszíntéren **egymással hálózatba kapcsolt** objektumok vannak. Egy kiválasztott központ és a benne található nagyfontosságú célpontok elleni támadás különböző **hatásokat eredményezhet a többi, hozzájuk kapcsolódó** objektum működésében is.

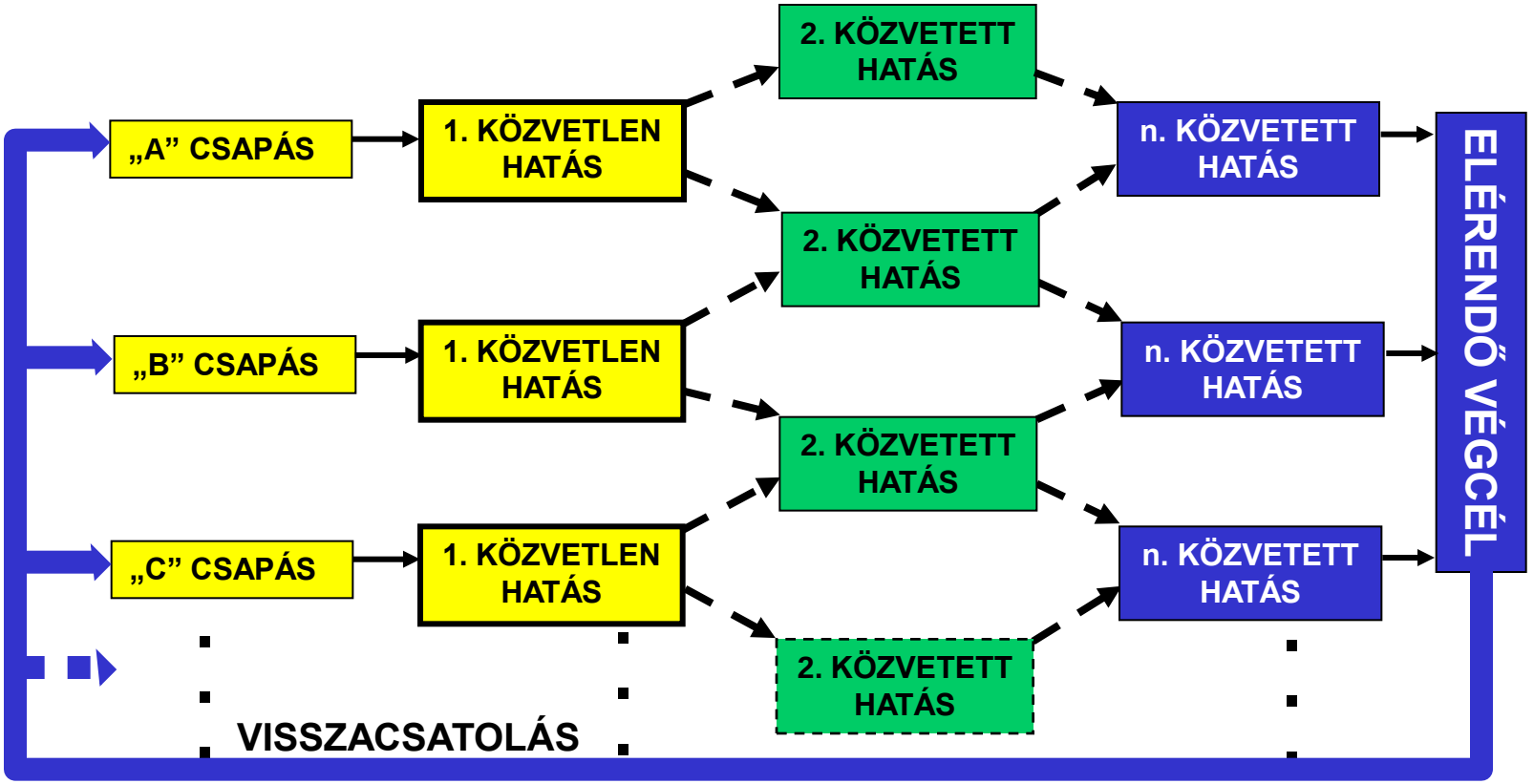
Mindez igaz a polgári létesítményekre, infrastruktúrákra is, amelyek – az információs társadalom alapelvéből fakadóan – az **infokommunikációs hálózatokon keresztül szintén szoros kapcsolatban állnak** egymással. Tehát bármely fontos, kritikus információs infrastruktúra illetve annak eleme elleni információs vagy fizikai támadás **további működésbeli korlátokat idézhet elő** a többi, hozzá kapcsolódó infrastruktúrában, rendszerben is.

HATÁSALAPÚ MŰVELETEK

A hatásalapú műveletekben a korábbi felfogáshoz képest komolyan figyelembe veszik azt a láncreakcióhoz hasonlító elvet, miszerint a **kezdeti közvetlen hatással** – első csapással – törvényszerűen **további közvetett károsító, korlátozó hatásokat** lehet elérni, amely a teljes rendszerre különböző mértékű negatív hatást fejt ki. Az előidézett hatások eredőjének, vagyis az **összhatás eredményének elemzése és értékelése** képezi a hatásalapú műveletek lényegét. Ez az új műveleti felfogás a **holisztikus** elvű **szemlélet** alkalmazását igényli.

A HATÁSALAPÚ MŰVELETEK HATÁSLÁNCOLATA

A közvetlen és közvetett hatások elve szerint egy rendszer belső - kulcsszerepet játszó - elemeire mért pusztító, vagy korlátozó jellegű csapás mind a rendszeren belül, mind pedig a rendszerek közötti kapcsolatokban másod, harmad és n–edik típusú és erősségű hatásokat vált ki.

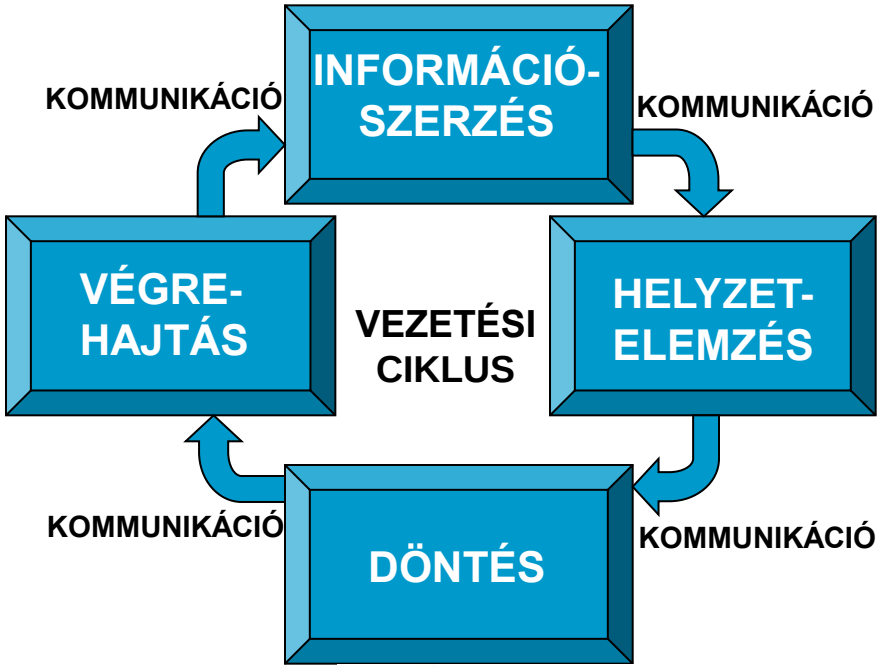


Az elérendő végállapotból kiindulva tervezik a különböző kinetikus és nem kinetikus energia elven működő csapásokat, vagy ráhatásokat.

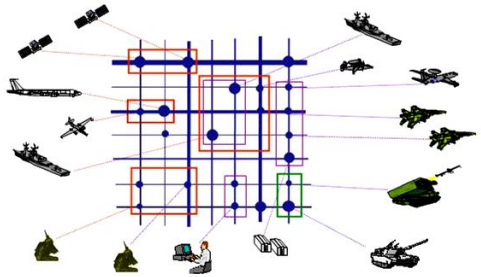
INFORMÁCIÓ FELHASZNÁLÁSA A HADVISELÉSBEN

INFORMÁCIÓFELHASZNÁLÁS

Információ a vezetésben, fegyverirányításban



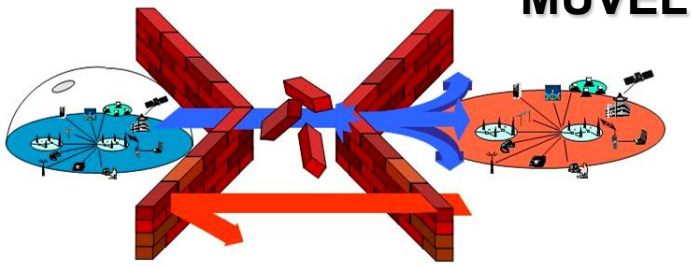
HÁLÓZAT-KÖZPONTÚ HADVISELÉS



Információ, mint támadó és védő fegyver

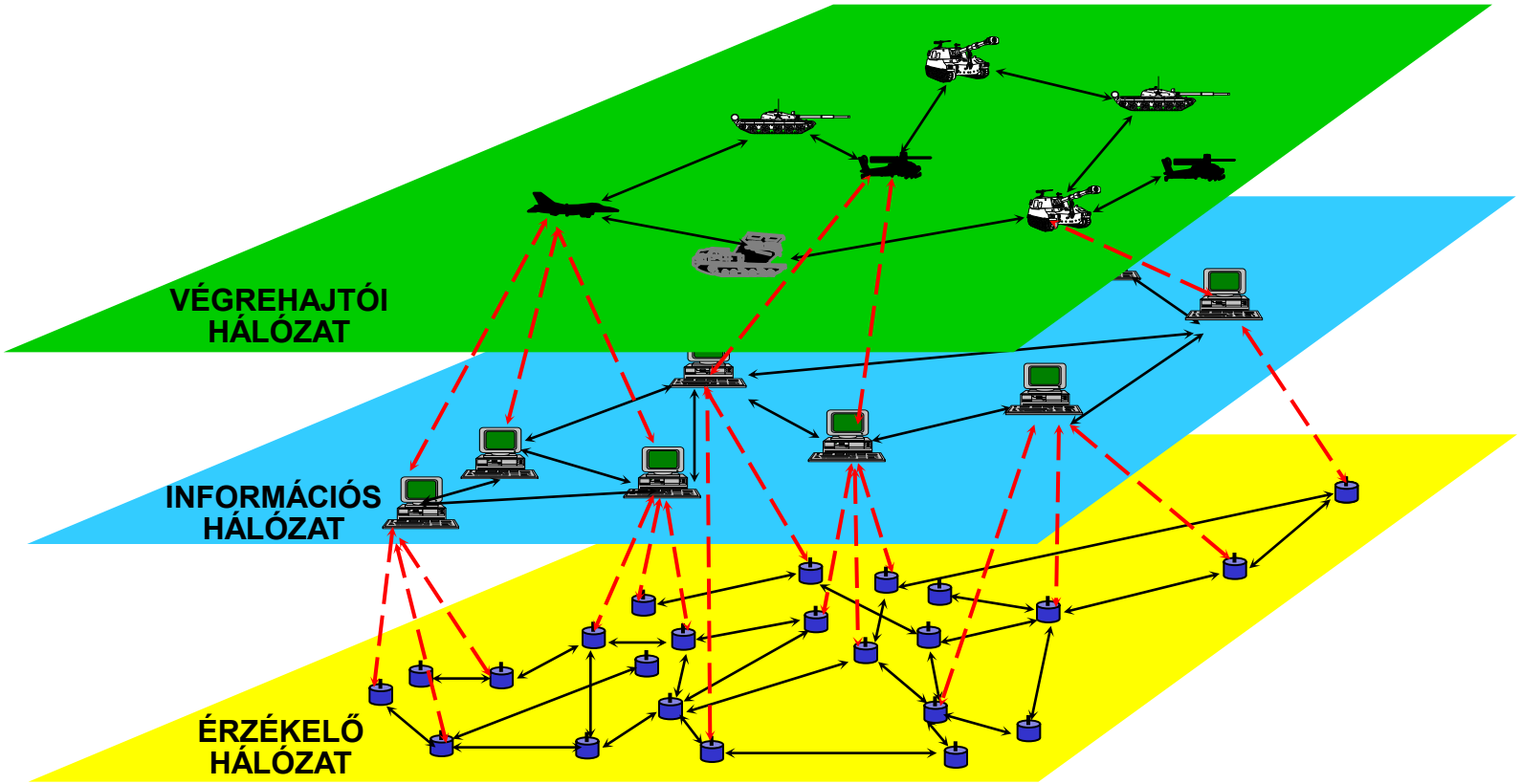
VÉDŐ INFORMÁCIÓS TEVÉKENYSÉGEK		TÁMADÓ INFORMÁCIÓS TEVÉKENYSÉGEK	
MŰVELETI BIZTONSÁG	ELHÁRÍTÁS	ELEKTRONIKAI TÁMADÁS	PSYOPS
ELEKTRONIKAI VÉDELEM	ELLEN-PROPAGANDA	MEGTÉVESZTÉS	FIZIKAI PUSZTÍTÁS
ELLEN-MEGTÉVESZTÉS			

INFORMÁCIÓS MŰVELETEK



A HÁLÓZATOK ÖSSZEKAPCSOLÁSA

A szenzortól kezdve a döntéshozón át a végrehajtóig egységes hálózatba rendezett elemek közötti információk egyik pontból a másik pontig történő eljutása jóval kevesebb időt igényel, mint korábban.



A végrehajtók– jogosultság alapján – olyan információkhoz is hozzájuthatnak, amelyek más felderítési forrásból származnak, és amelyek világosabbá teszik a helyzetet, ezáltal megalapozottabb döntéseket tudnak hozni.

INFORMÁCIÓS HADVISELÉS KIALAKULÁSA

- Első definíció: Thomas Rona (1976)
- Egyes összetevői - mint elkülönült információs tevékenységek - már a korábbi háborúkban is jelen voltak (pl. felderítés, megtévesztés, pszichológiai műveletek, műveleti biztonság, EW)
- Hidegháborús médiatevékenység (SZER, propaganda - zavarás)
- Információ fontossága és az IT fejlettsége ➡ összehangolt információs tevékenységek szükségességének felismerése
- Az összehangolt információs hadviselés kezdeti jegyei először az 1991-es Öbölháborúban figyelhetők meg. (+ CNN jelenség)

INFORMÁCIÓS HADVISELÉS KIALAKULÁSA

AZ IW „POLGÁRI” ÉRTELMEZÉSE

Martin C. Libicki (1995) – Az információs hadviselés (IW) egymással összefüggő részterületei civil és katonai értelmezésben:

- Vezetési hadviselés - Command and Control Warfare (C2W)
- Hírszerzés alapú hadviselés - Intelligence Based Warfare (IBW),
- Elektronikai hadviselés - Electronic Warfare (EW),
- Pszichológiai hadviselés - Psychological Warfare (PSYOP),
- Hacker hadviselés - Hacker Warfare (HW)
- Gazdasági információs hadviselés - Economic Information Warfare (EIW)
- Cyberhadviselés – Cyberwarfare (CW)

Nem egzakt kategorizálás, egymást átfedő területek!

Forrás: Martin Libicki: What is Information Warfare? (1995)

INFORMÁCIÓS HADVISELÉS KIALAKULÁSA

AZ IW „POLGÁRI” ÉRTELMEZÉSE

Winn Schwartau féle osztályozás:

- **Class 1: Személyes (Personal) IW** – az egyén a célpont, személyiséglopás: az áldozat nem csak pénzét, de hitelképességét, sőt barátait is elveszítheti
- **Clas 2: Vállalati (Corporate) IW** – pl:. ipari kémkedés,
- **Class 3: Kormányzati (Government) IW** – pl.: grúz v. észt cybertámadás

Alapvetően a számítógép-hálózati környezetben zajló információs támadások és védelem.

Forrás: Winn Schawartau: Information Warfare. (1996)

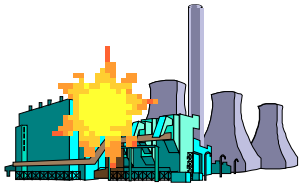
AZ INFORMÁCIÓS MŰVELETEK FOGALMA

Az információs műveletek azon **koordinált** tevékenységeket jelentik, melyek a szembenálló fél információira, információalapú folyamataira és infokommunikációs rendszereire gyakorolt **ráhatásokkal** képesek **támogatni** a döntéshozókat a politikai és katonai célkitűzéseik elérésében úgy, hogy e mellet a saját hasonló folyamatokat és rendszereket hatékonyan **kihasználják és megóvják**.

Az információs műveletek - az információs fölény, -uralom és végül a vezetési fölény elérése és megtartása érdekében - **minden szinten** (politikai, gazdasági, kulturális, hadászati, hadműveleti, harcászati) és **minden időben** (béke, válság, háború) alkalmazott információs tevékenységek közötti **integráló és koordináló tevékenység**.

INFORMÁCIÓS MŰVELETEK DIMENZIÓI

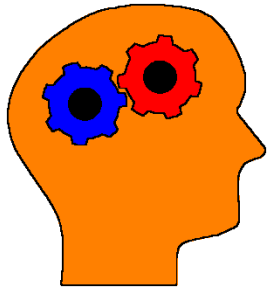
A fizikai dimenzióban zajlanak a katonai műveletek (földi, légi, tengeri stb.). Itt működnek a különböző információs infrastruktúrák, rendszerek. A különböző információs infrastruktúrák, információs rendszerek elemei elleni támadásokat („Hard Kill”), illetve ezek védelmét jelenti.



Az információs dimenzióban a különböző információs folyamatok (adatszerzés, adatfeldolgozás, kommunikáció, stb.) zajlanak, és többnyire azok elektronikus úton való támadását („Soft Kill”) és a saját információs folyamatainkra irányuló támadások megakadályozását jelenti.

A kognitív dimenzióban megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást (véleményt, vélekedést) veszik célba (pl. elektronikus és nyomtatott médiával vagy közvetlen beszéd formájában).

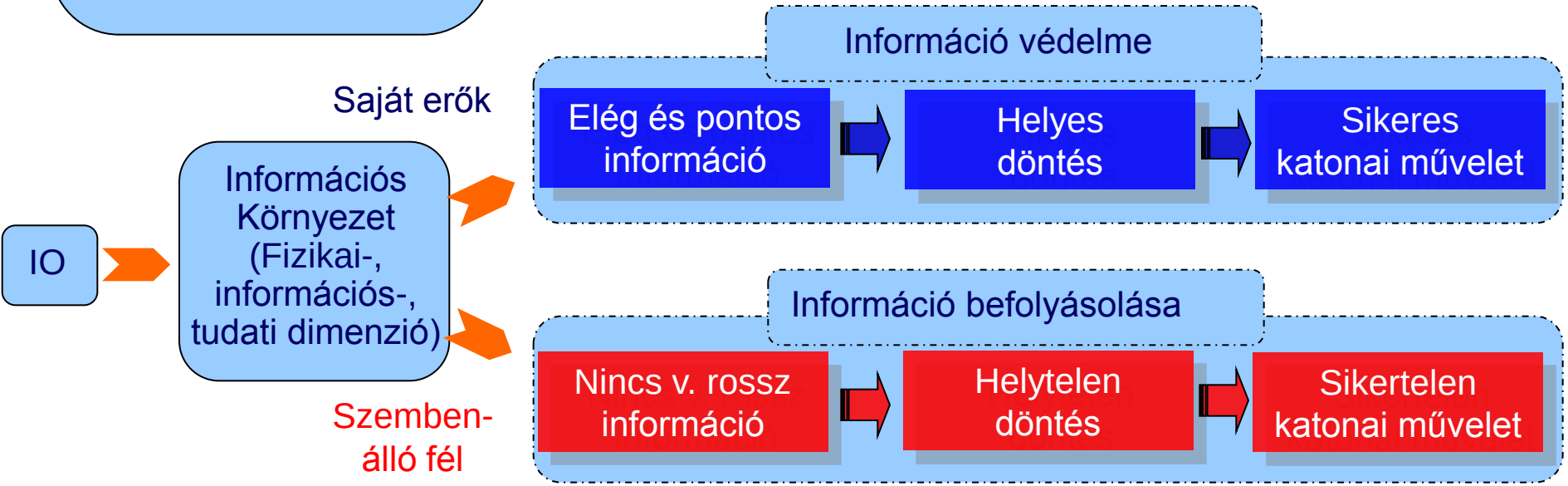
Végső cél: A döntéshozók befolyásolása



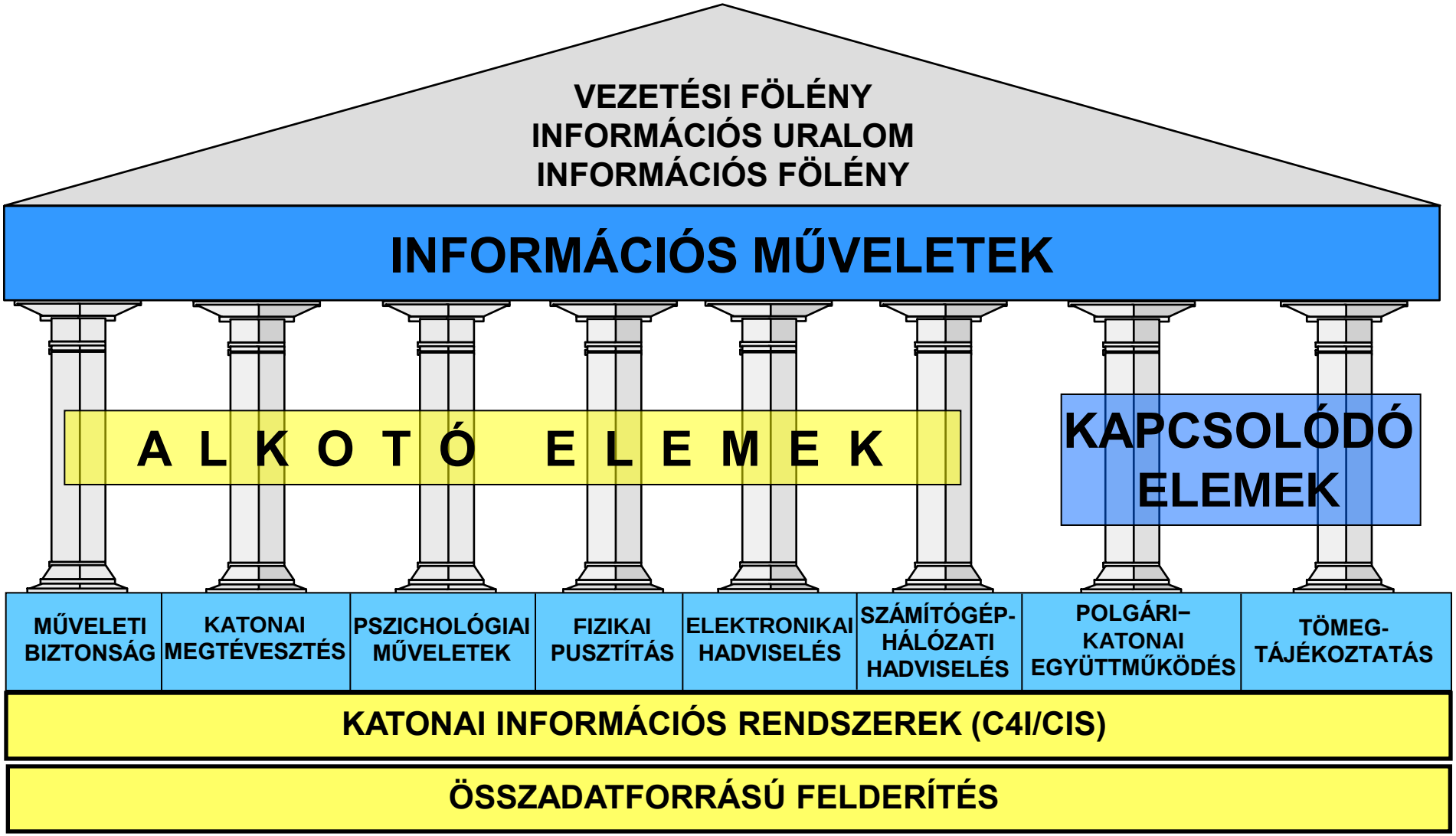
INFORMÁCIÓS MŰVELETEK

Információs műveletek:
- Negatív hatások a szembenálló fél **döntési folyamataira**
- saját **döntési folyamatok** védelme

Információs művelete célja:
- információs fölény elérése
- befolyásoló képesség fenntartása



INFORMÁCIÓS MŰVELETEK ELEMEI

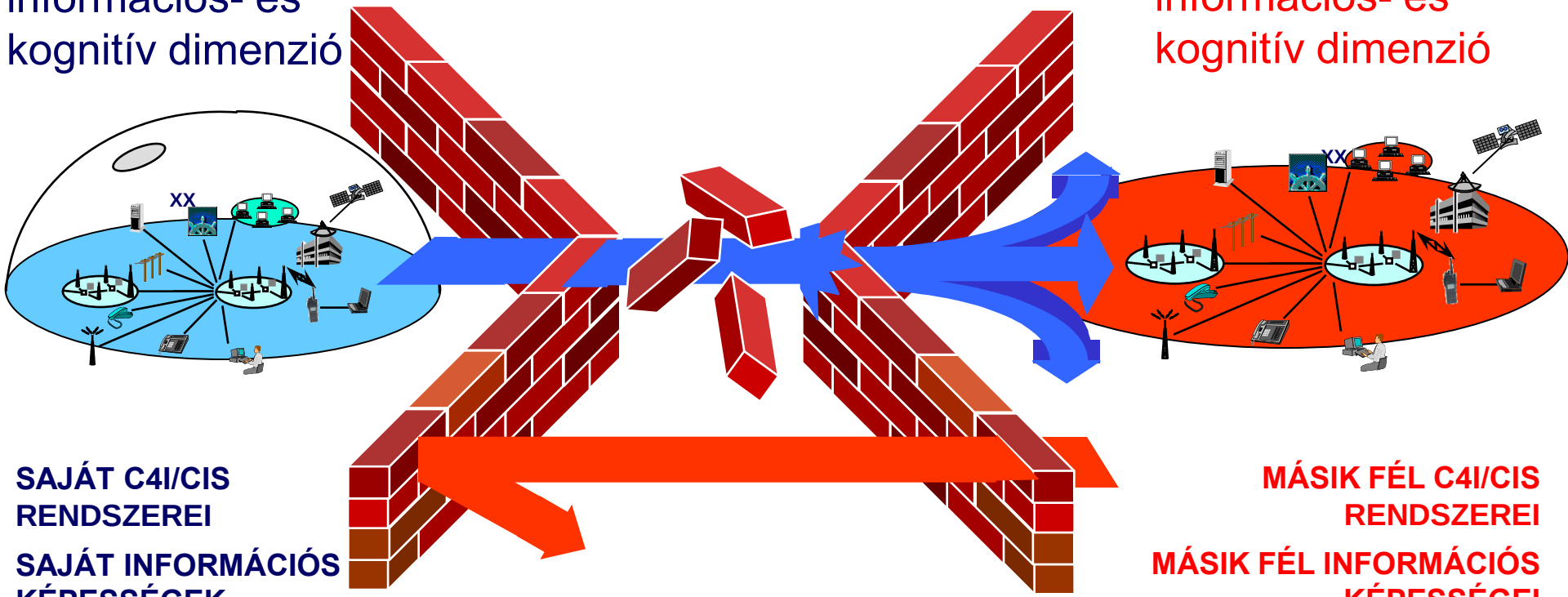


INFORMÁCIÓS MŰVELETEK

VÉDELMI TEVÉKENYSÉGEK ⟵ **BEFOLYÁSOLÓ TEVÉKENYSÉGEK** ⟶ **ELLENTEVÉKENYSÉGEK**

Fizikai-, információs- és kognitív dimenzió

Fizikai-, információs- és kognitív dimenzió



SAJÁT C4I/CIS RENDSZEREI

SAJÁT INFORMÁCIÓS KÉPESSÉGEK

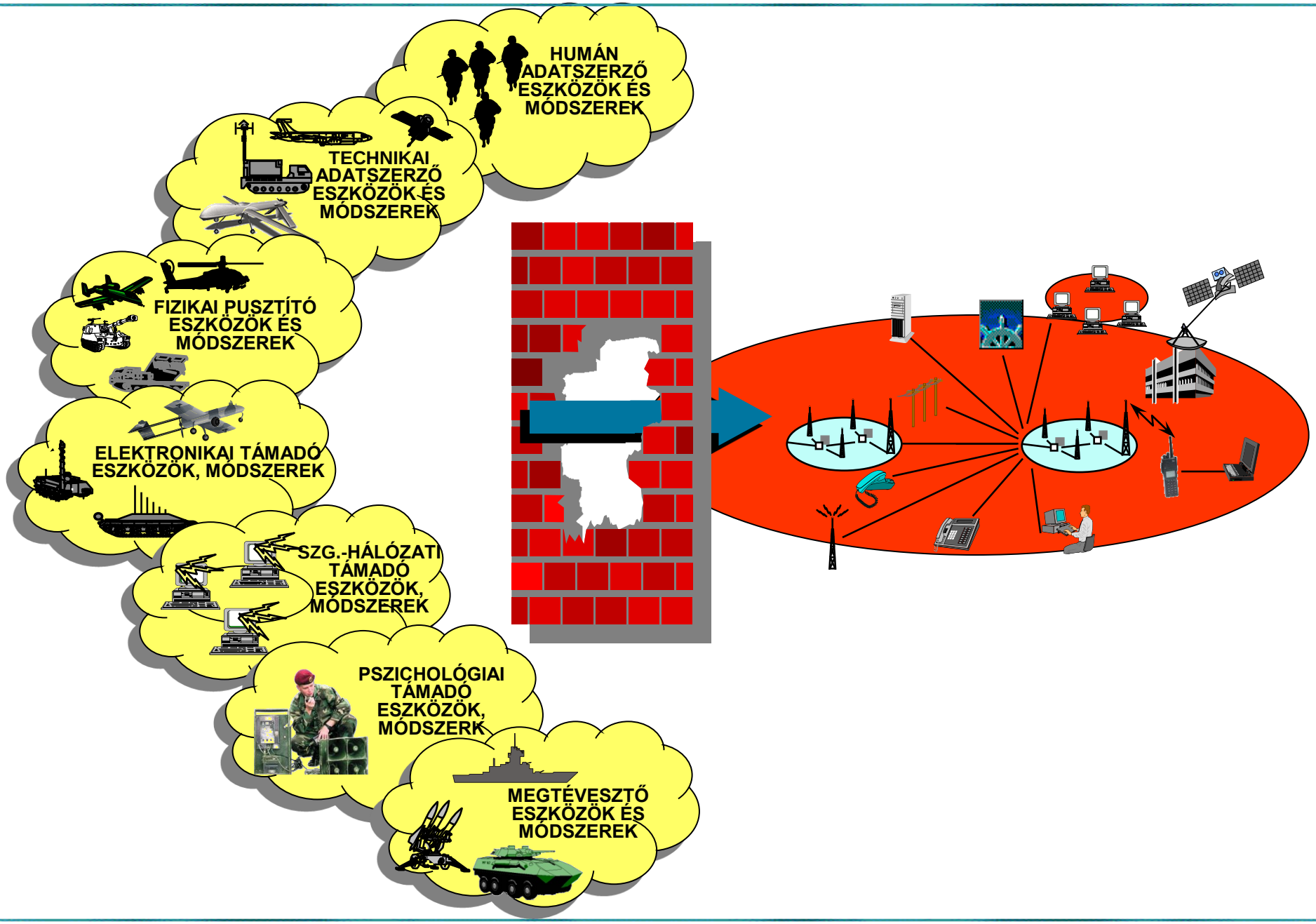
KRITIKUS INFORMÁCIÓK

MÁSIK FÉL C4I/CIS RENDSZEREI

MÁSIK FÉL INFORMÁCIÓS KÉPESSÉGEI

KRITIKUS INFORMÁCIÓK

TÁMADÓ INFORMÁCIÓS MŰVELETEK ESZKÖZEI ÉS ELJÁRÁSAI



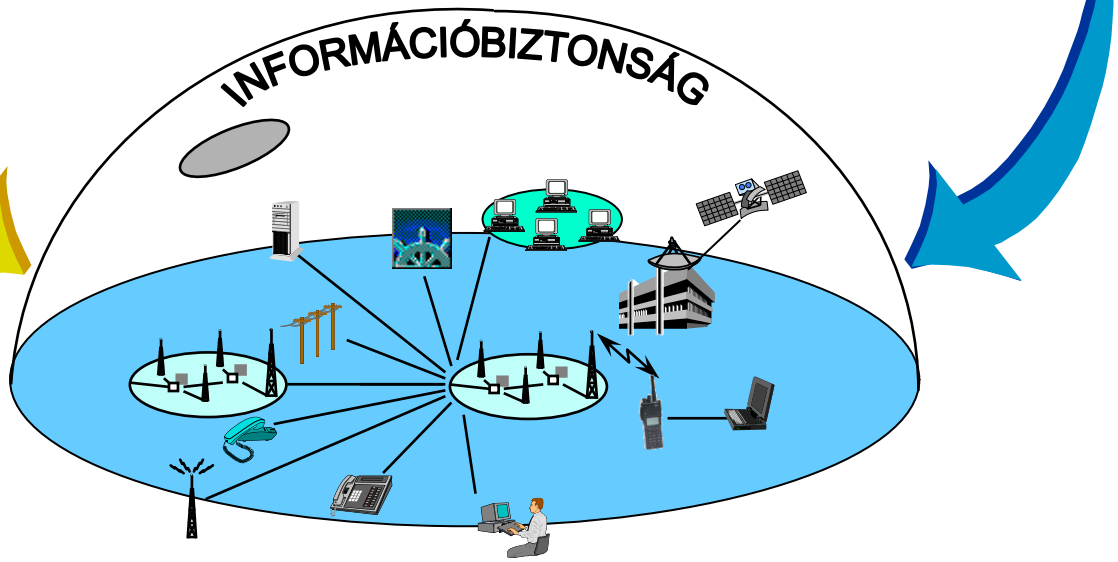
INFORMÁCIÓS TÁMADÁS HATÁSA ÉS TÁMADÁSI DIMENZIÓI

Funkció:	ELFOGÁS, FELFEDÉS		BEFOLYÁSOLÁS, TÖNKRETÉTEL					
Biztonsági jellemző:	Bizalmasság sérül		Adatok sérülékenysége nő Szolgáltatások elérhetősége csökken					
Forma:	Közvetett	Közvetlen	Közvetett			Közvetlen		
Szint:	Információ források felderítése		Megtévesztés	Zavarás	Pusztítás	Megtévesztés	Zavarás	Pusztítás
Tudati dimenzió	Viselkedési formák, megfigyelése, következtetés döntési folyamatokra	Döntési folyamatok figyelése HUMINT módszerekkel	Döntéshozatal, megértési folyamat befolyásolása PSYOPS tevékenységekkel (szórólapok, média, Internet alkalmazása)			Titkos műveletekkel beszivárgás a célközönség közé és ott a megértési folyamatot befolyásoló témák terjesztése		
Információs dimenzió	Üzenetek, passzív módszerekkel való lehallgatása. Hálózati topológia feltárása, rejtjel dekódolás	Szenzorok alkalmazása Számítógép hálózatok felderítése trójai programokkal, jelszólopókkal Van Eck sugárzás felfedése.	Megtévesztő e–mail-ek továbbítása. Megtévesztő hálózati tevékenység folytatása.	Hálózatok mesterséges túlterhelése (*Flood Attack*), így a hálózati hozzáférés akadályozása (DDoS). Nyílt forrású információkkal a figyelem elterelése		Trójai programok bejuttatása. Működő programokkal adatok módosítása	Rosszindulatú szoftverekkel hálózati szolgáltatásokhoz való hozzáférés megakadályozása, adatok, adatbázisok tönkretétele	
Fizikai dimenzió	Vezetékek lehallgatása. Papírhulladék	Információs eszközök, fizikai és titkosító kulcsok, adathordozók ellopása.	Titkos információhoz való hozzáférés a felhasználó félrevezetésével (*Social Engineering*)	Bomlasztó tevékenységek előidézése a felhasználók félrevezetésével		Fizikai biztonságot feltörve, titkos adatokhoz való hozzáférés	Információs infrastruktúrák fizikai rombolása.	

VÉDELMI INFORMÁCIÓS MŰVELETEK FAJTÁI

TÁMADÓ JELLEGŰ
CÉLJA: CSÖKKENTENI AZ ELLENFÉL LEHETŐSÉGEIT INFORMÁCIÓS RENDSZEREINK TÁMADÁSÁRA, AZ INFORMÁCIÓS MŰVELETEK MINDEN ELEMÉVEL

VÉDELMI JELLEGŰ
CÉLJA: SAJÁT INFORMÁCIÓS RENDSZEREINK SEBEZHETŐSÉGÉNEK CSÖKKENTÉSE AZ INFORMÁCIÓS MŰVELETEK PASSZÍV ELEMEIVEL



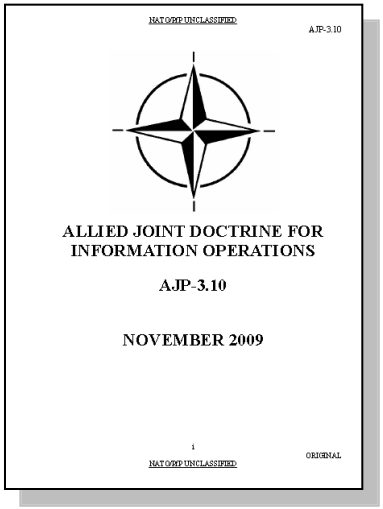
NATO INFORMÁCIÓS MŰVELETEK

NATO Információs műveletek definíció:

„a. „Info Ops is a military function to provide advice and **coordination** of **military information activities** in order to create desired effects on the **will**, **understanding** and **capability** of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives.

b. Information activities are actions designed to affect information and or information systems. They can be performed by any actor and **include protective measures**.”

Forrás: AJP-3.10 Allied Joint Doctrine for Information Operations. November, 2010 1-3p.


NATO/PfP UNCLASSIFIED

AJP-3.10

ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS

AJP-3.10

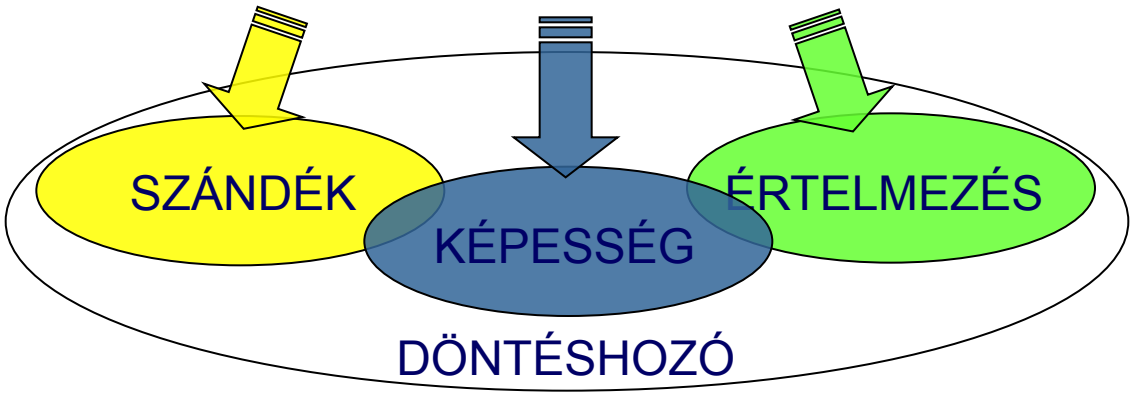
NOVEMBER 2009

i

NATO/PfP UNCLASSIFIED

ORIGINAL

Katonai információs tevékenységek
Tudatos ráhatás



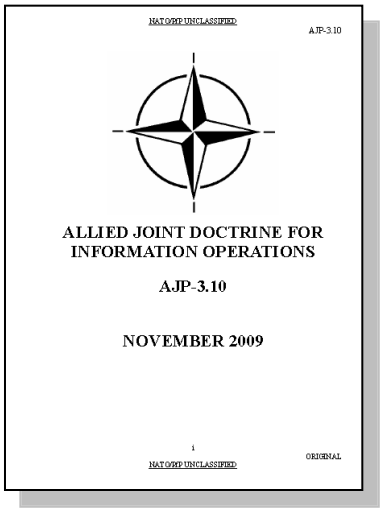
NATO INFORMÁCIÓS MŰVELETEK

Információs műveletek tevékenységi területei:

a. **Befolyásoló tevékenységek:** („Information activities that focus on **changing, influencing, or reinforcing** perceptions and attitudes of adversaries and other NAC approved parties.”)

b. **Védelmi tevékenységek:** („Information activities that focus on **preserving** and **protecting** Alliance freedom of manoeuvre in the information environment by **defending the data and information** that supports Alliance decision-makers and decision-making processes.”)

c. **Ellentevékenységek:** („Information activities that focus on **countering** command functions and capabilities, by **affecting the data and information** that support adversaries and other NAC approved parties, and are used in command and control, intelligence, surveillance and target acquisition, and weapon systems.”)


NATO/PfP UNCLASSIFIED

AJP-3.10

ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS

AJP-3.10

NOVEMBER 2009

i

ORIGINAL

NATO/PfP UNCLASSIFIED

Korábban csak támadó és védelmi típusú INFOOPS

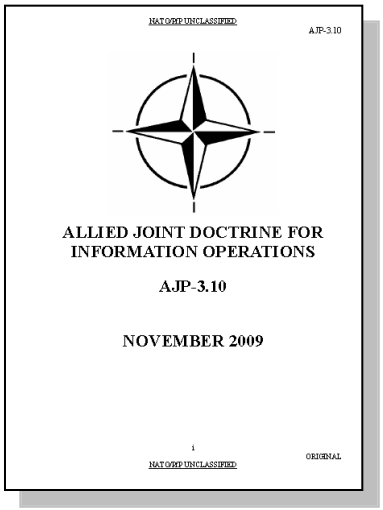
Forrás: AJP-3.10 Allied Joint Doctrine for Information Operations. November, 2010

NATO INFORMÁCIÓS MŰVELETEK

Képességek, eszközök és eljárások:

- Psychological Operations
- Presence, Posture and Profile
- Operations Security
- Information Security
- Deception
- Electronic Warfare
- Physical Destruction
- Key Leader Engagement
- Computer Network Operations
- Civil-Military Cooperation

Kapcsolódó tevékenység:
Public Affairs


NATO/PfP UNCLASSIFIED

AJP-3.10

ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS

AJP-3.10

NOVEMBER 2009

i

ORIGINAL

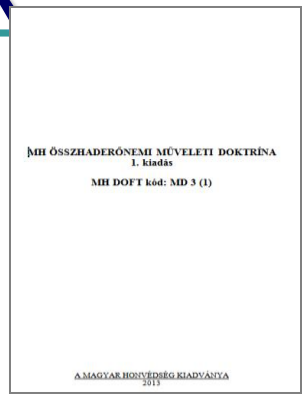
NATO/PfP UNCLASSIFIED

Pl.: Information Security része az OPSEC-nek és a CNO-nak

„As part of OPSEC the goal of Information Security (INFOSEC)…
INFOSEC is an integral element of all military operations and encompasses… Computer Network Defence (CND), an integral part of Computer Network Operations (CNO), … [AJP-3.10; p.:1-9]

Forrás: AJP-3.10 Allied Joint Doctrine for Information Operations. November, 2010

MH INFORMÁCIÓS MŰVELETEK


MH ÖSSZHADERŐNEMI MŰVELETI DOKTRÍNA
1. kiadás
MH DOFT kód: MD 3 (1)
A MAGYAR HONVÉDSÉG KIADVÁNYA
2013

Az információs műveletek területei:

a) Lélektani műveletek (Psychological Operations, PSYOPS):

b) Megjelenés, viselkedés és arculat (Presence, Posture, Profile, PPP):

c) Műveleti biztonság (Operational Security, OPSEC):

d) Információs (sic) biztonság (Information Security, INFOSEC):

e) Megtévesztés (Deception)

f) Elektronikai hadviselés (Electronic Warfare, EW)

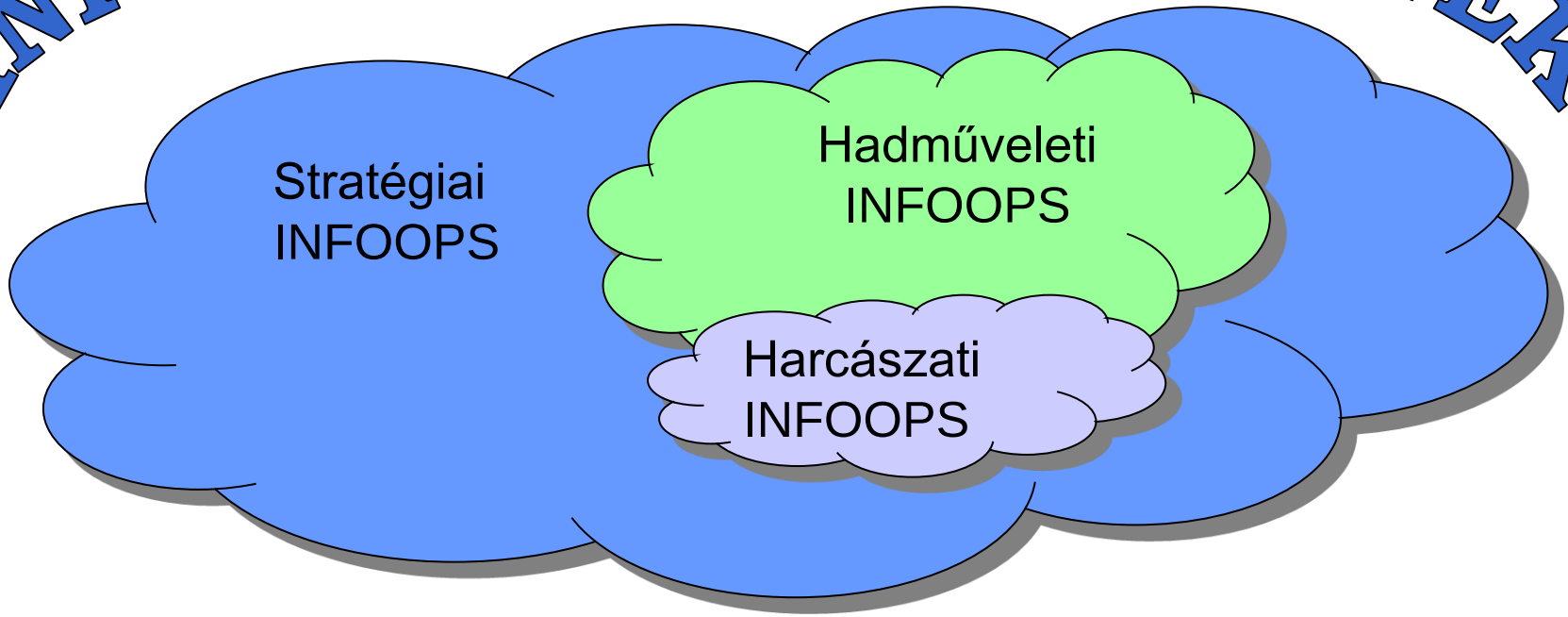
g) Fizikai megsemmisítés

h) Kulcsbeosztású személyekkel kapcsolatos tevékenységek (Key Leader Engagement, KLE)

i) Számítógépes hálózati műveletek (Computer Network Operations, CNO)

Forrás: Magyar Honvédség Összhaderőnemi Műveleti Doktrína 1. kiadás 2013, p. 1 - 19-21 (draft)

INFORMÁCIÓS MŰVELETEK



NEM KATONAI TEVÉKENYSÉGEK

KATONAI TEVÉKENYSÉGEK

NEM KATONAI TEVÉKENYSÉGEK

Béke I. **Válság** **Háború** **Béketeremtés** **Béke II.**