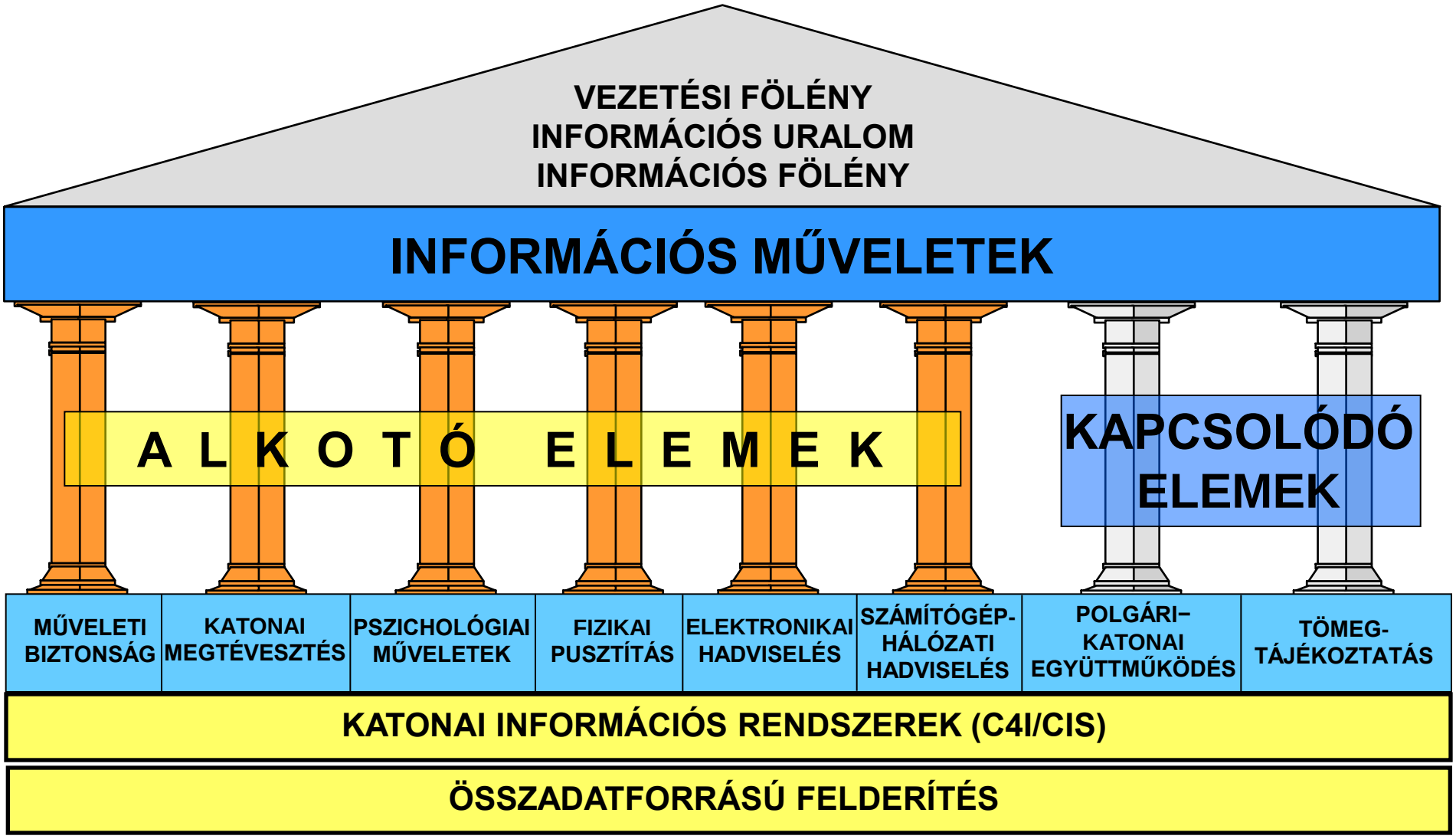
NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
Informatikai és Elektronikai Hadviselés Tanszék

INFORMÁCIÓS MŰVELETEK

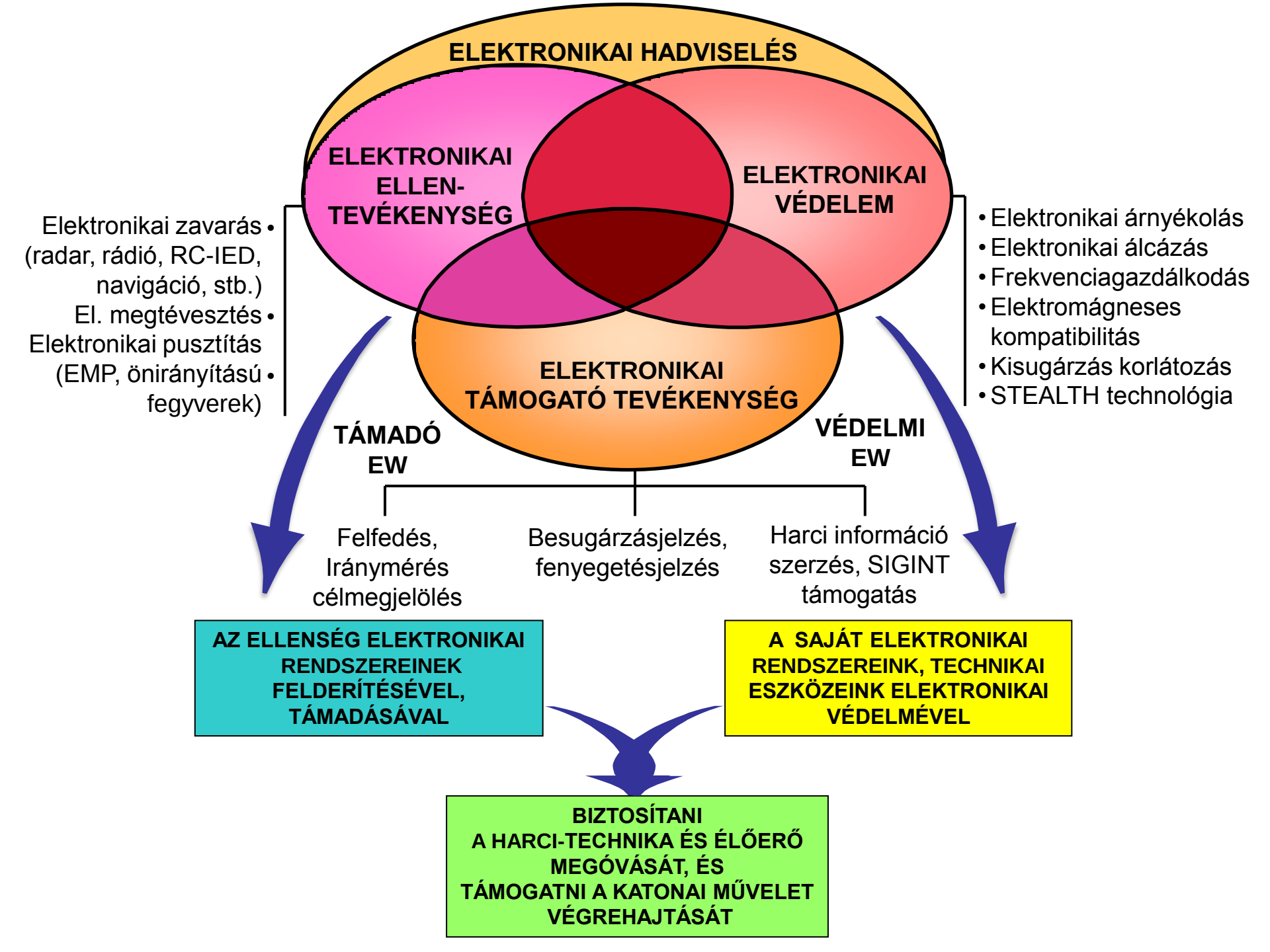
Prof. dr. Haig Zsolt mk. ezredes, egyetemi tanár
HM 29-343 haig.zsolt@uni-nke.hu

INFORMÁCIÓS MŰVELETEK ELEMEI



ELECTRONIC WARFARE - EW

Az elektronikai hadviselés azon katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti, vagy megakadályozza az elektromágneses spektrum ellenség részéről történő használatát és biztosítja annak a saját csapatok általi hatékony alkalmazást.


ELEKTRONIKAI HADVISELÉS
ELEKTRONIKAI ELLEN-TEVÉKENYSÉG
ELEKTRONIKAI VÉDELEM
ELEKTRONIKAI TÁMOGATÓ TEVÉKENYSÉG
Elektronikai zavarás (radar, rádió, RC-IED, navigáció, stb.)
El. megtévesztés
Elektronikai pusztítás (EMP, önirányítású fegyverek)
Elektronikai árnyékolás
Elektronikai álcázás
Frekvenciagazdálkodás
Elektromágneses kompatibilitás
Kisugárzás korlátozás
STEALTH technológia
TÁMADÓ EW
VÉDELMI EW
Felfedés, Iránymérés célmegjelölés
Besugárzásjelzés, fenyegetésjelzés
Harci információ szerzés, SIGINT támogatás
AZ ELLENSÉG ELEKTRONIKAI RENDSZEREINEK FELDERÍTÉSÉVEL, TÁMADÁSÁVAL
A SAJÁT ELEKTRONIKAI RENDSZEREINK, TECHNIKAI ESZKÖZEINK ELEKTRONIKAI VÉDELMÉVEL
BIZTOSÍTANI A HARCI-TECHNIKA ÉS ÉLŐERŐ MEGÓVÁSÁT, ÉS TÁMOGATNI A KATONAI MŰVELET VÉGREHAJTÁSÁT

ELECTRONIC SUPPORT MEASURES - ESM

Az elektronikai támogató tevékenység az elektronikai hadviselés azon része, amely magába foglalja - a fenyegetés azonnali jelzése érdekében - az elektromágneses kisugárzások felkutatására, elfogására, és azonosítására, valamint a források helyének meghatározására irányuló tevékenységeket.

SIGINT – ESM kapcsolat:

- azonos eszközök, módszerek
- különböző célok (felderítési információ vs. harci információ)

A RÁDIÓELEKTRONIKAI FELDERÍTÉS FOLYAMATA

1.adatszerzés

ESM

- felfedés
- iránymérés

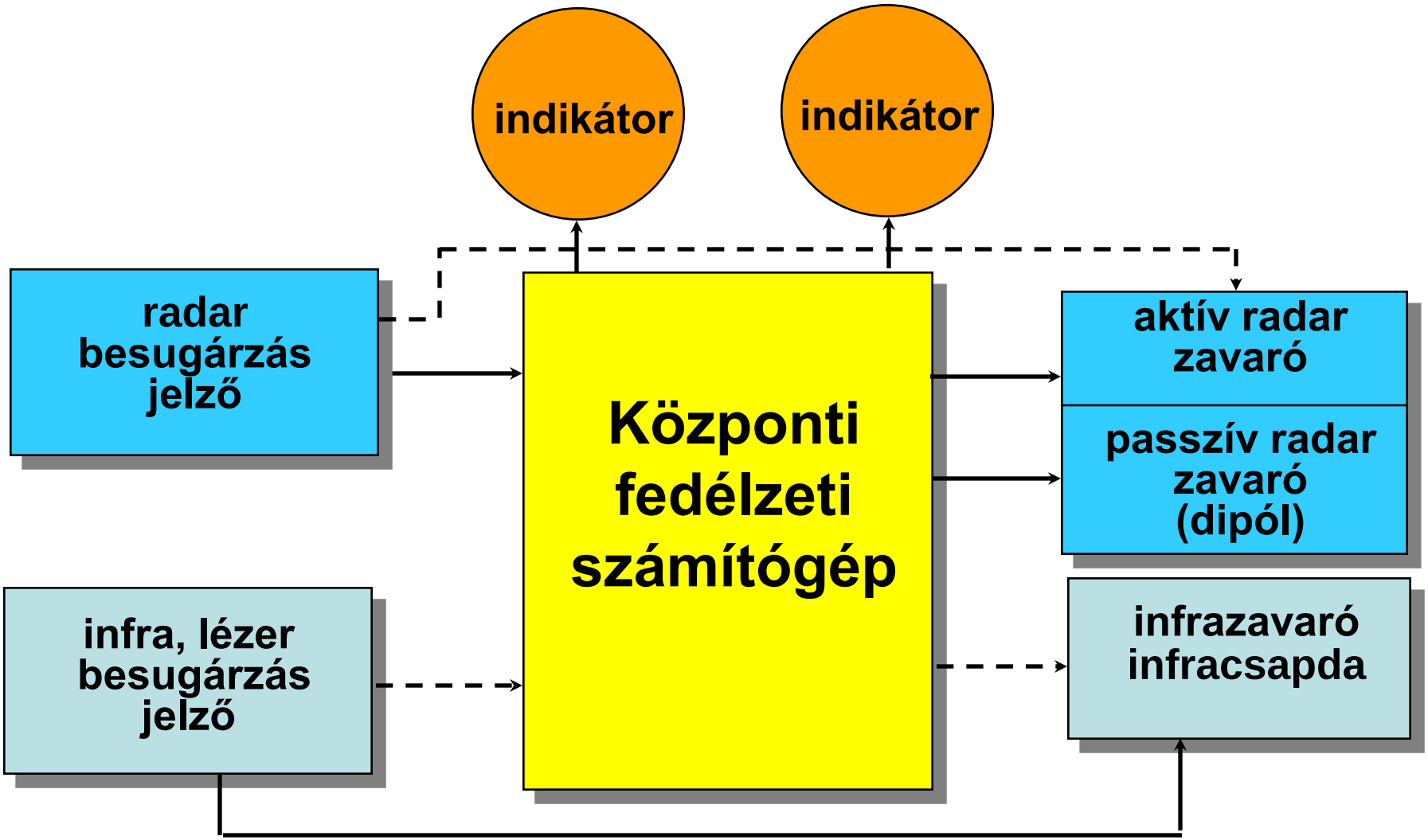
- lehallgatás, figyelés

SIGINT

ELEKTRONIKAI TÁMOGATÁSI RENDSZER

A védendő objektumon, vagy annak közelében elhelyezett speciális vevőberendezésekkel érzékeli a fenyegetéseket, annak irányát, figyelmeztető jelzést állít elő és - ha lehetőség van rá - automatikusan megindítja az ellentevékenységi rendszer működését.

FEDÉLZETI INTEGRÁLT EW RENDSZER



ELEKTRONIKAI ELLENTEVÉKENYSÉG

Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát.

ELEKTRONIKAI ELLENTEVÉKENYSÉG

TERÜLETEI

ELEKTRONIKAI ZAVARÁS

SUGÁRZOTT
- célzott,
- elnyomó,
- csúszó

VISSZA-SUGÁRZOTT

VISSZAVERT
- dipólok
- szögvisszaverők
- lencsék

ELEKTRONIKAI MEGTÉVESZTÉS

- MANIPULÁCIÓS
- IMITÁCIÓS
  - kommunikációs
  - nem kommuni-kációs
- SZIMULÁCIÓS

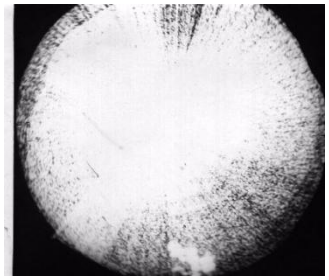
ELEKTRONIKAI PUSZTÍTÁS

- ELEKTRO-MÁGNESES ENERGIÁK
- IRÁNYÍTOTT ENERGIÁK,
- ÖNRÁVEZETÉSŰ FEGYVEREK

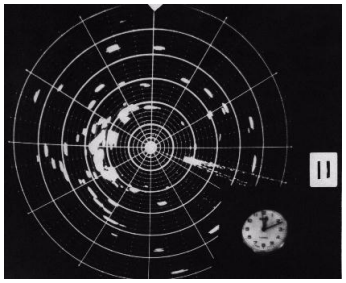
ELEKTRONIKAI ZAVARÁS

Az elektromágneses energia szándékos kisugárzása, visszasugárzása, vagy visszaverése, abból a célból, hogy megakadályozzuk, vagy csökkentsük az ellenség számára az elektromágneses spektrum hatékony felhasználását.

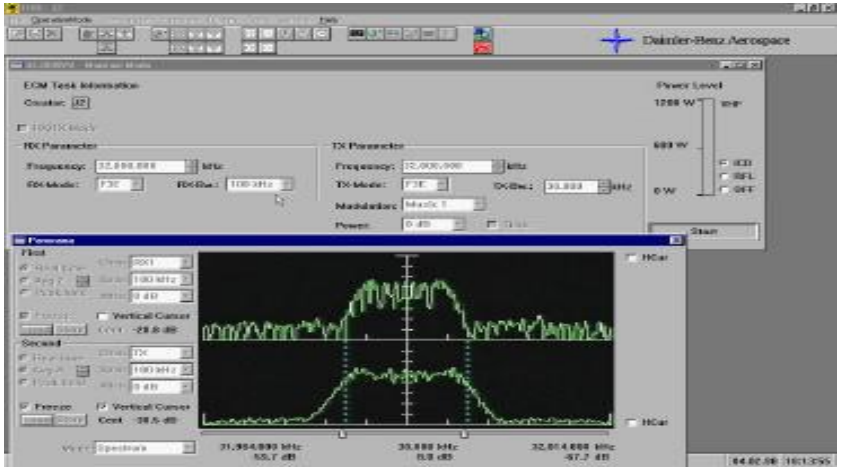
Az ellenséges elektronikai eszközök vevőinek bemenetén létrehozott szükséges zavarójel teljesítmény sűrűség információ veszteséget okoz és lehetetlenné teszi, vagy megnehezíti az információ feldolgozását (felhasználását).



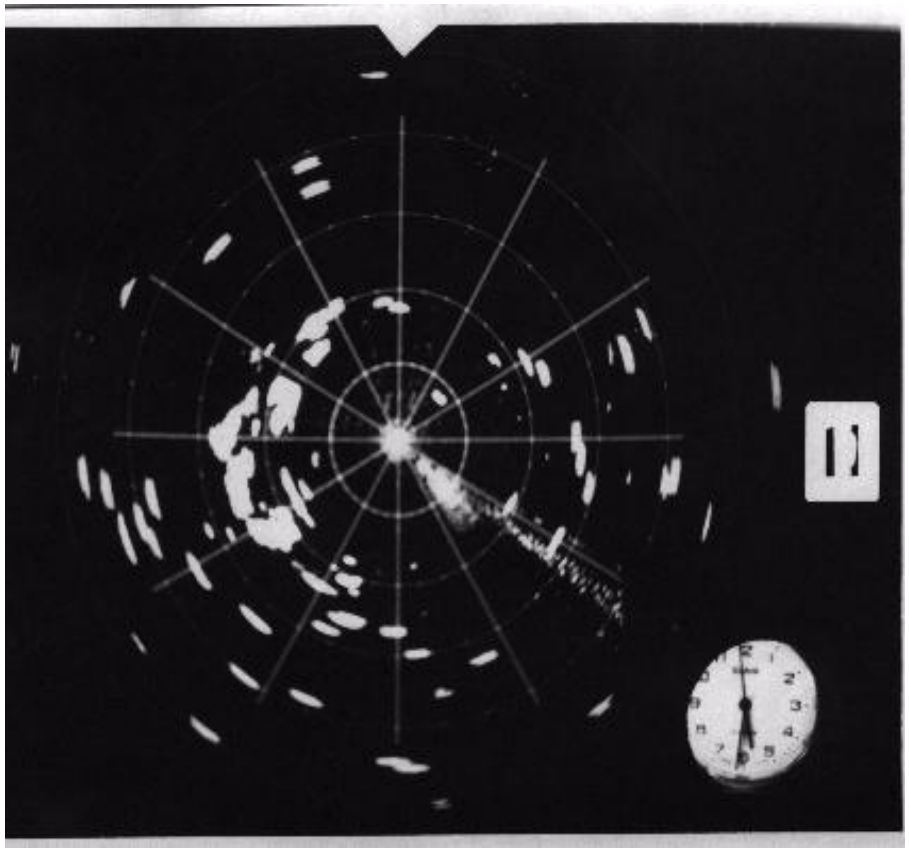
Zajzavar



Válaszzavar



VISSZASUGÁRZOTT (VÁLASZ) ZAVARÁS



A válasz zavarásnál egy vevő veszi az ellenséges kisugárzásokat (impulzusokat), azokat bizonyos szempontok szerint átalakítják, majd visszasugározzák az ellenséges elektronikai eszköz vevőjébe.

A válaszimpulzus zavarás lehet egyszeres vagy többszörös attól függően, hogy a zavaró állomás egy impulzust vagy több zavaró impulzust bocsát ki a vett jel hatására.

VISSZAVERT (PASSZÍV) ZAVARÁS

Passzív zavarást olyan speciális eszközökkel valósítják meg, melyek a reájuk eső elektromágneses hullámokat a kisugárzó eszköz irányába nagy intenzitással visszaverik.

A passzív zavarok létrehozásával létre lehet hozni hamis célokat, vagy a harci technikai eszközöket el lehet rejteni a felderítő eszköz elől.

ESZKÖZEI:

- dipól visszaverők;
- szögvisszaverők (sarok reflektorok);
- Lüneberg lencsék;
- ionizált atmoszféra (atomrobbantás);
- radar hullámokat elnyelő bevonatok

COMPASS CALL

AN/ALQ-131 ÖNVÉDELMI ZAVARÓ KONTÉNER

EA-18G ELEKTRONIKAI HADVISELÉSI REPÜLŐGÉP

EGYSZERI ALKALMAZÁSÚ ZAVARÓ ESZKÖZÖK

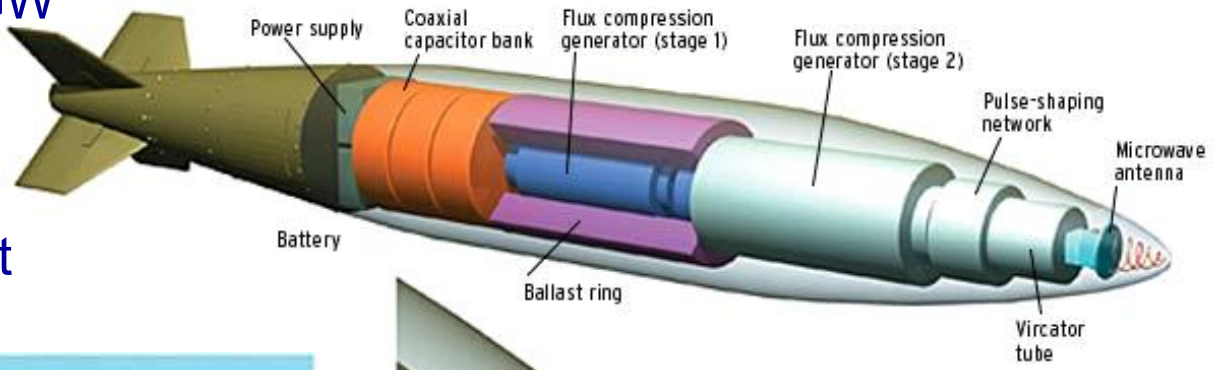
Azon objektumok ellen, amelyek ellen földi, vagy légi zavaró eszközök hatékonyan nem alkalmazhatók (terep, távolsági viszonyok, mobil zavaró eszközök hiánya) egyszeri alkalmazású zavaró eszközöket alkalmaznak.

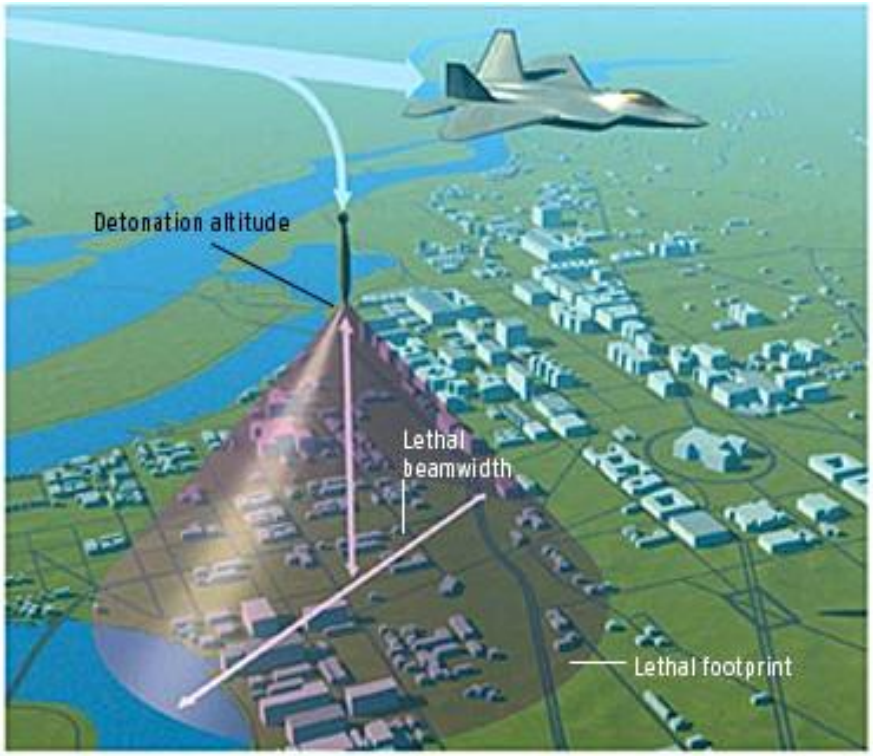
Kijuttatása:

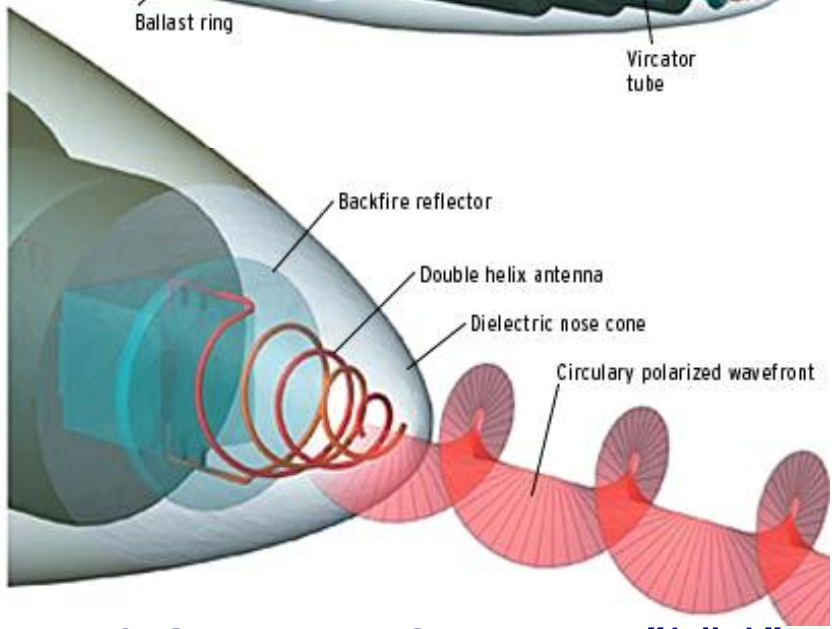
- **kézi úton;**
- **légi eszközből kidobással;**
- **tüzérségi löveggel.**

E-BOMBA

Az E-bomba két fluxus kompressziós generátora GW nagyságú teljesítményt biztosít a virtuális katód oszcillátor (VIRCATOR) számára, amely nagy teljesítményű mikrohullámot sugároz ki.







Egy 10 GW-os, 5-GHz-en működő E-bomba néhány kV/m térerősséggel 400-500 méter átmérőjű területen fejti ki hatását.

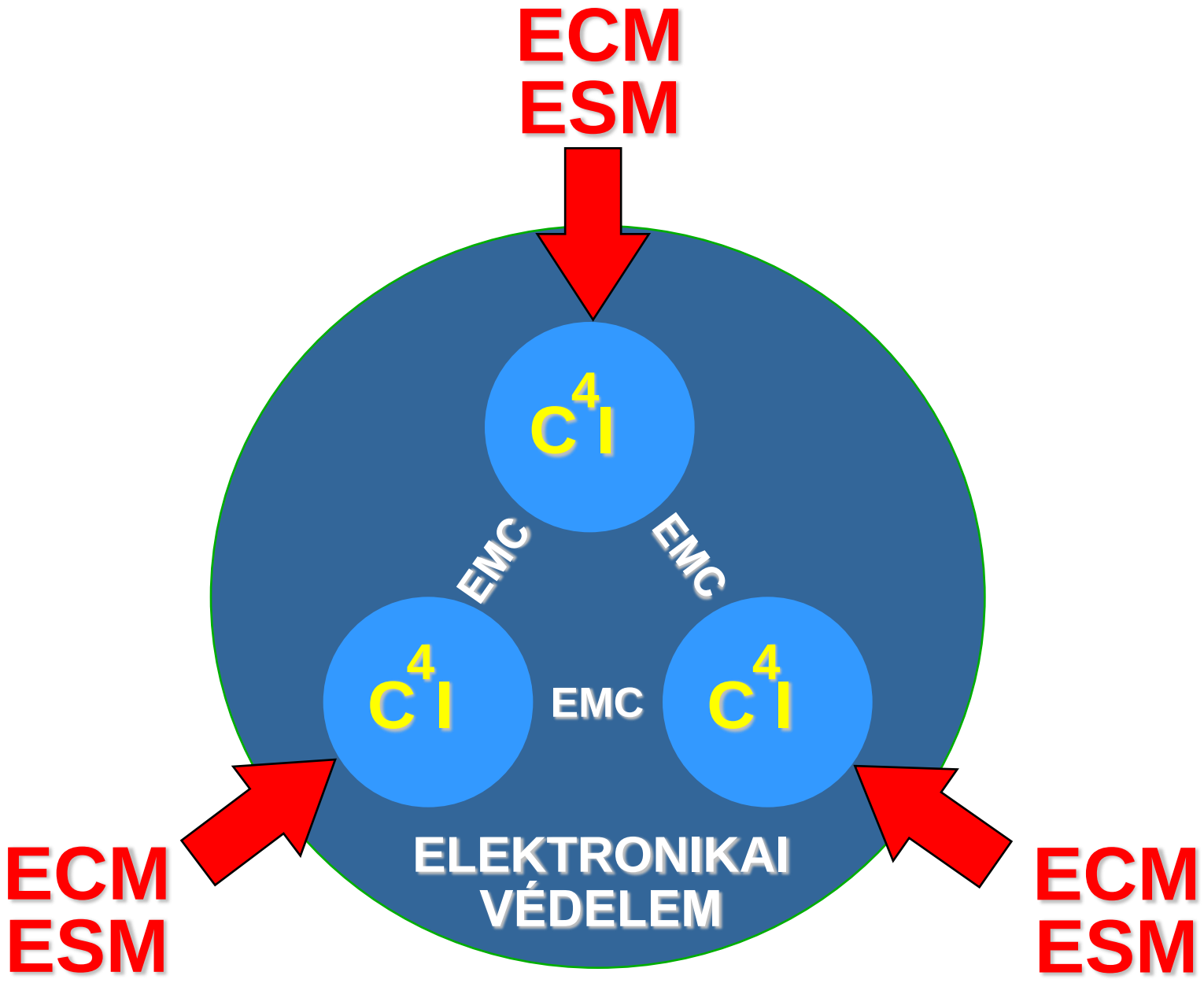
ELEKTRONIKAI MEGTÉVESZTÉS

Olyan tervezett tevékenység, melynek célja, az ellenség - elektromágneses eszközei által szerzett információk alapján való - félrevezetése. Rendszerint részét képezi az átfogó hadműveleti megtévesztésnek és szinte sosem alkalmazzák önállóan.

ELECTRONIC COUNTER - COUNTERMEASURES – ECCM ELECTRONIC PROTECTIVE MEASURES - EPM

Az elektronikai védelem az elektronikai hadviselés azon része, amely biztosítja az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére.

ELEKTRONIKAI VÉDELEM



ELEKTRONIKAI VÉDELEM

FELDERÍTÉS ellen

Ellenség Felderítő eszközei, Irányított fegyverei

Technikai felderítés, Fegyver-irányítás.

- Megsemmisítés
- Zavarás
- Megtévesztés
  - álcázás
  - imitálás
- Felderítés hatékonyságának csökkentése
  - titkosítás
  - kitérés:
    - teljesítmény
    - frekvencia
    - tér
    - idő

ZAVARÁS ellen

Ellenség Elektronikai hadviselési erői

Szándékos zavarás

Zavarforrás megszüntetése:
- megsemmisítés
- kikapcsolás

Zavarás hatékonyság csökkentése (kitérés):
- teljesítmény
- frekvencia
- tér
- idő

Saját elektronikai eszközök

Nem szándékos zavarás

COMPUTER NETWORK OPERATIONS - CNO

A számítógép-hálózati hadviselés egyrészt a szembenálló fél hálózatba kötött informatikai rendszerei működésének befolyásolására, lerontására, lehetetlenné tételére irányul, másrészt viszont a saját hasonló rendszerek működésének fenntartására törekszik.

SZÁMÍTÓGÉP-HÁLÓZATI HADVISELÉS

FAJTÁI

SZÁMÍTÓGÉP-HÁLÓZATI HADVISELÉS (CNO)

ELLENTEVÉKENYSÉG

SZÁMÍTÓGÉP-HÁLÓZATI FELDERÍTÉS (CNE)

Szoftveres, vagy hardveres úton való behatolást jelent a szembenálló fél számítógépes rendszereibe, illetve hálózataiba, azzal a céllal, hogy hozzáférjünk az adatbázisaiban tárolt adatokhoz, információkhoz, és azokat felderítési céllal hasznosítsuk.

SZÁMÍTÓGÉP-HÁLÓZATI TÁMADÁS (CNA)

Szoftveres, vagy hardveres úton való behatolást jelent a szembenálló fél számítógépes rendszereibe, illetve hálózataiba, azzal a céllal, hogy tönkretegyük, módosítsuk, manipuláljuk vagy hozzáférhetetlenné tegyük az adatbázisaiban tárolt adatokat, információkat, illetve magát a rendszert vagy hálózatot.

VÉDELEM

SZÁMÍTÓGÉP-HÁLÓZATI VÉDELEM (CND)

A saját számítógép-hálózat védelmét jelenti a jogosulatlan hozzáféréssel és behatolással szemben, amelyet abból a célból hajtanak végre, hogy megszerezzék az adatbázisokban tárolt adatokat és információkat, illetve, hogy szándékosan lerontsák, működésképtelenné tegyék e rendszerre alapozott információs rendszerünket.

SZÁMÍTÓGÉP-HÁLÓZATI ELLENTEVÉKENYSÉG
(felderítés és támadás)

ROSSZINDULATÚ SZOFTVEREK (MALWARE)

Fő változatai egyfajta felosztás szerint:

- Levélbombák
- Lánclevelek
- Hoax-ok
- Időzített bombák
- Kémprogramok, fülelők
- Interloper programok
- Adat-túszejtők
- Tűzfal-támadók
- Jelszólopók
- Programférgek
- Trójai programok
- Dropperek
- Vírusok
- Vírusgyártó automaták.

DENIAL OF SERVICE
DoS

- A kiszemelt célpontot a támadó elárasztja olyan adatcsomagokkal, amelyek a célpont informatikai rendszerét túlterheli, így a normál működés lehetetlenné válik.
- Például: egy http kérés néhány 100 byte méretű. Mai átlagos ADSL kapcsolaton másodpercenként 50 elküldhető belőle. Ha a kiszolgáló egy másodperc alatt ennél kevesebb választ tud előállítani, akkor túlterhelődik.

DISTRIBUTED DENIAL OF SERVICE
DDoS

- Manapság a legveszélyesebb támadási forma.
- A támadó nem egyetlen végpontról indítja a túlterheléses támadást, hanem egyszerre sok helyről.
- Ezek térben és hálózati topológiában is elosztva helyezkednek el.
- Általában vírussal fertőzött gépekről (bot-ok, „zombie-k”).
- A támadók ezekből hálózatot szerveznek (botnet), és egy adott cél érdekében felhasználják.
- Detektálni nagyon nehéz, mivel a nagyszámú támadó végpont a „normál” végpontok közé rejtőzik.
- A hálózati forgalom célzatos blokkolása nem lehetséges, a nagyszámú támadó miatt.
- A támadás időben elnyújtott lehet, így az okozott kiesés is sokkal nagyobb károkat képes okozni.

SZÁMÍTÓGÉP-HÁLÓZATI VÉDELEM

A védelem megvalósítása lehet *passzív és aktív*.

Passzív védelmi módszerek és eszközök:

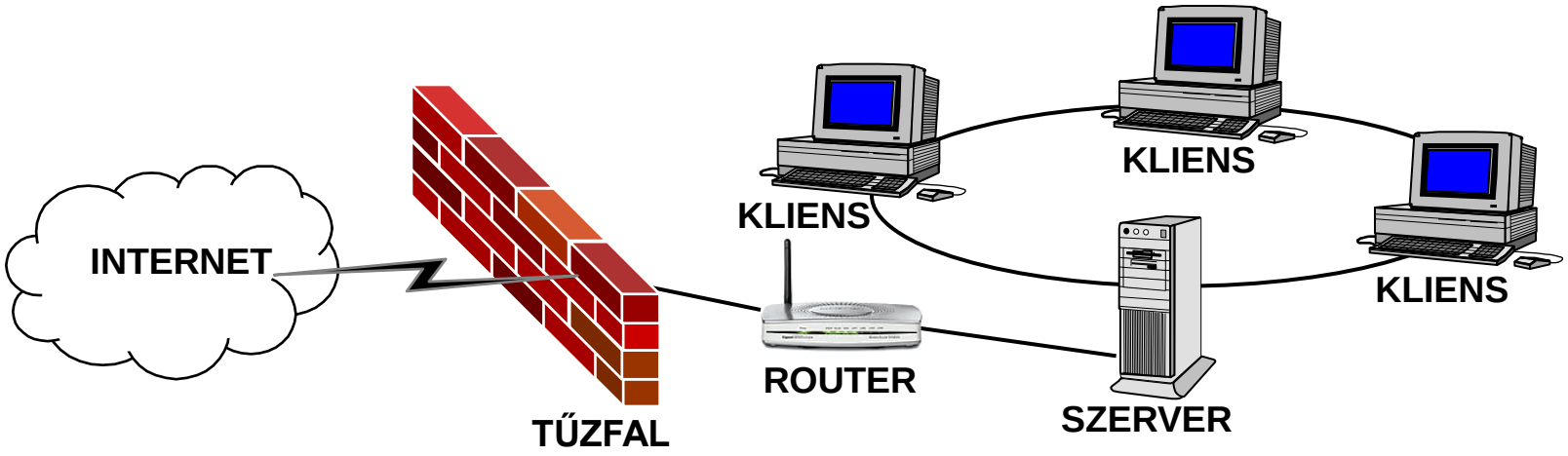
- tűzfalak (Firewall);
- vírusirtók (Antivirus Softwares);
- hozzáférés szabályozás (Access Control);
- behatolás detektálás és adaptív válaszlépések (Intrusion Detection and Adaptive Response Tools)

Aktív védelem módszerei:

- megelőző támadások (Pre-emptive Attacks);
- ellentámadások (Counterattacks);
- aktív megtévesztés (Active Deception).

PASSZÍV SZÁMÍTÓGÉP-HÁLÓZATI VÉDELEM
TŰZFAL

- a saját hálózat és az Internet közé beépítve szűrik az adatforgalmat.
- nem csökkentik a támadás lehetőségét, hanem akadályt állítanak a támadó elé és ezáltal csökkentik a behatolás valószínűségét.

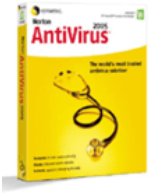


A TŰZFAL LEHET:

- Külső tűzfal – a teljes helyi hálózatot elszigeteli az Internettől
- Belső tűzfal - a helyi hálózat egy különösen védendő részét zárja el annak többi részétől

- Hardver alapú – nagyobb biztonság, drágább, bonyolultabb konfigurálhatóság
- Szoftver alapú – kisebb biztonság, általában személyes célúak

PASSZÍV SZÁMÍTÓGÉP-HÁLÓZATI VÉDELEM
VÍRUSIRTÓK



Vírusazonosító adatbázis alapján működő vírusirtók

Háttérben állandóan futó (On Access) keresők

A számítógép indításával egyidőben elindulnak, és a beállított paraméterek alapján, folyamatosan ellenőrzik az operációs rendszert, a használatba vett lemezek boot szektorát, az összes megnyitott fájlt, keresik azokat a rosszindulatú programokat, melyek megegyeznek az adatbázisukban tárolt vírus-adatállományokkal. Jelentős az erőforrás igényük.

Alkalmilag futtatandó (Ad Hoc) keresők

Csak akkor lépnek működésbe, ha a felhasználó elindítja, és meghatározza az ellenőrizendő lemezeket, objektumokat, fájlokat. Ezeknek a víruskeresőknek a folyamatosan futókkal szemben jóval kisebb az erőforrásigényük. Ezért ezeknek elsősorban ott van létjogosultságuk, ahol kicsi a számítógép teljesítménye.

Heurisztikus keresők

Nem a vírusadatbázisok alapján kutatnak vírusok után, hanem a vizsgált program viselkedése, működése, utasításai alapján döntik el, hogy vírussal állnak–e szemben. A heurisztikus keresés általános formája, amikor a program olyan műveleteket figyel, amelyek általában vírusokban fordulnak elő. Gyanús művelet lehet például, a végrehajtható állományokba való írás.

PASSZÍV SZÁMÍTÓGÉP-HÁLÓZATI VÉDELEM
HOZZÁFÉRÉS SZABÁLYOZÁS

JELSZAVAK

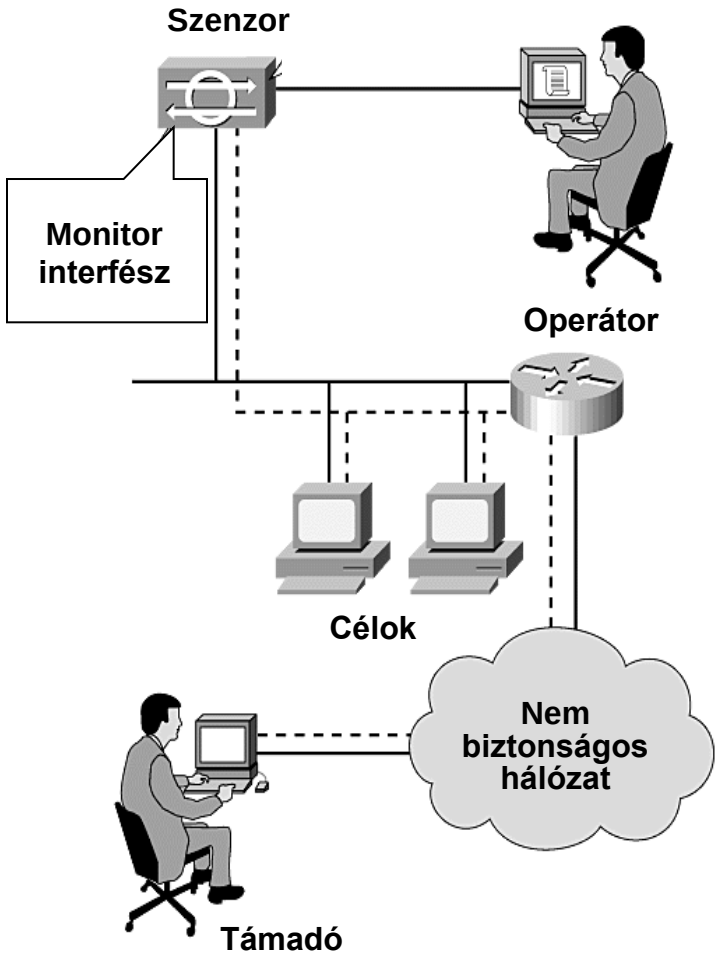
- Lehetnek többször felhasználható, vagy egyszer használatos jelszavak.
- Többszintű jelszavas védelem (kiemelten biztonságos hálózatokban).
- Többfaktoros védelem – jelszó kombinálása PIN kártyával, ujjlenyomat ellenőrzéssel, írisz letapogatással stb.
- Jelszó megválasztása döntő fontosságú (több karakteres, betű, szám és írásjel váltakozása).

HITELESÍTÉS

- Illetéktelen hozzáférés kizárása.
- Az illetékes személy jogosult az adott művelet végrehajtására, pl. csak neki van hozzáférési joga (Account).
- Kriptográfiai módszerek alkalmazása (küldő rejtjelzi, fogadó visszafejti): szimmetrikus és aszimmetrikus (nyilvános) kulcsú titkosítás (privát és publikus kulcspár).
- Digitális aláírás – titkosított karaktersorozat, melyet csak a küldő kódolhatott.

PASSZÍV SZÁMÍTÓGÉP-HÁLÓZATI VÉDELEM
BEHATOLÁS DETEKTÁLÁS ÉS ADAPTÍV VÁLASZOK

- Képesek a hálózatot fenyegető **külső és belső** betörési kísérleteket észlelni, azonosítani és a támadót elszigetelni.
- Működési alapelv: a betörők a hálózati forgalom elemzésével és a rendszerben észlelt abnormális események alapján azonosíthatók.
- A hálózatban lévő szenzorok és monitor-programok a behatolási eseményeket észlelik, időrendben rögzítik, majd ezeket a védelmi rendszer elemzi.
- A támadások detektálásának eredménye: e-mail riasztás, kapcsolat bontása, vagy tűzfal konfiguráció megváltoztatása.



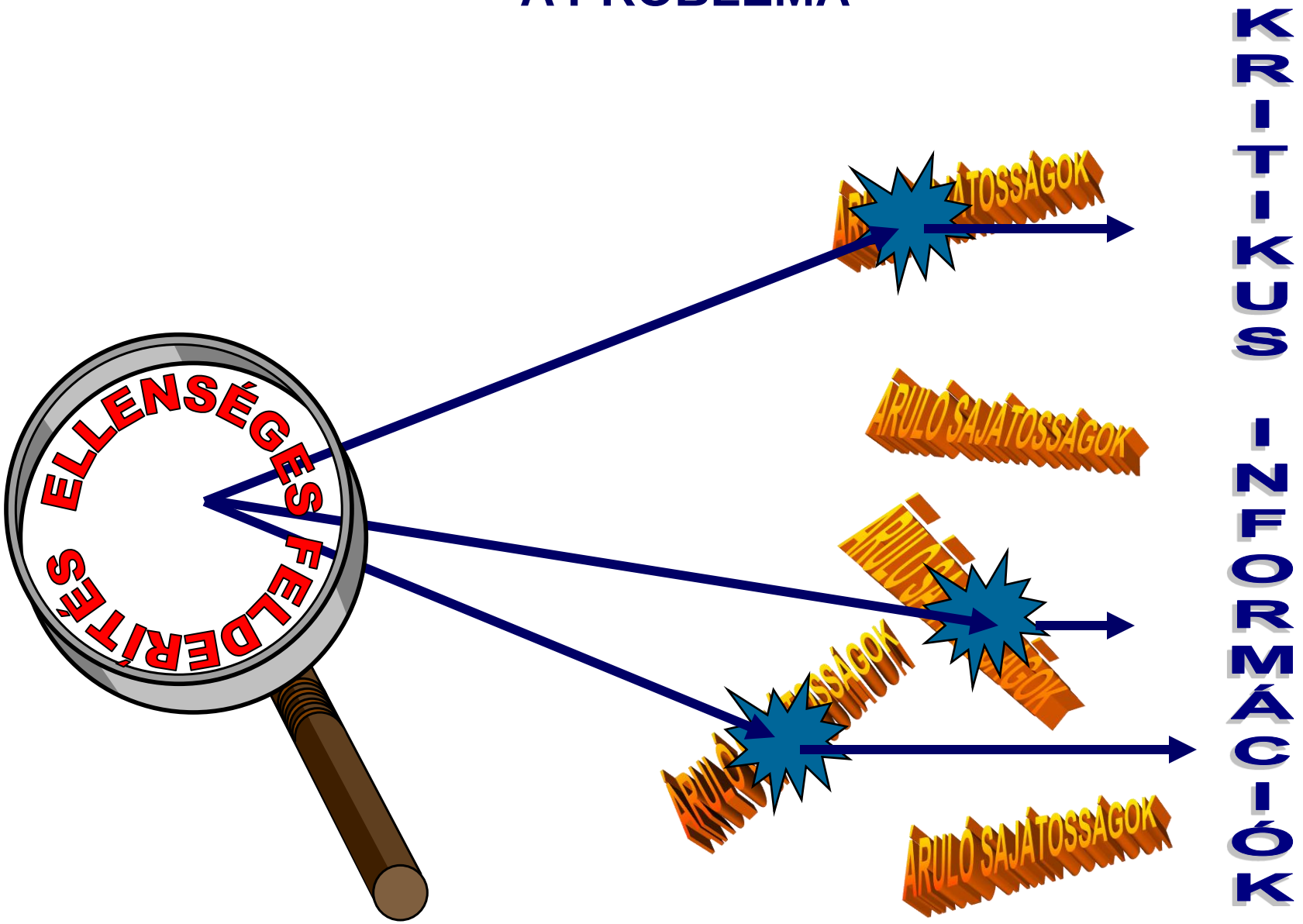
Minta alapú IDS: Hálózati-, hosztalapú (gépalapú) ill. hibrid
Viselkedés alapú IDS

MŰVELETI BIZTONSÁG

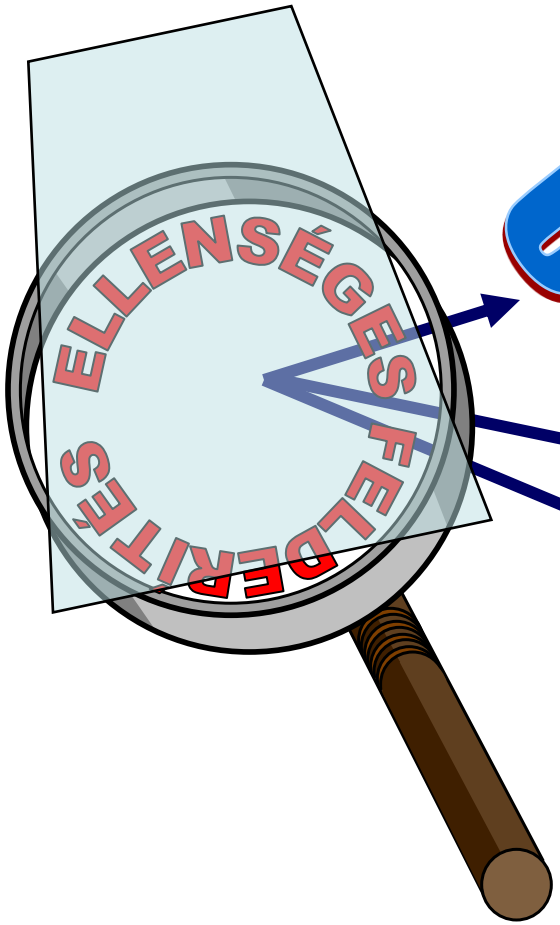
OPERATION SECURITY - OPSEC

A műveleti biztonság olyan folyamatok, tevékenységek és rendszabályok összessége, amelyek aktív és passzív eszközök felhasználásával megfelelő biztonságot nyújtanak a katonai művelet, vagy gyakorlat számára azáltal, hogy megfosztja az ellenséget a saját csapatok elhelyezkedésének, képességeinek és szándékainak ismeretétől.

A PROBLÉMA


ELLENSÉGES FELDERÍTÉS
ÁRULÓ SAJÁTOSSÁGOK
ÁRULÓ SAJÁTOSSÁGOK
ÁRULÓ SAJÁTOSSÁGOK
ÁRULÓ SAJÁTOSSÁGOK
KRITIKUS INFORMÁCIÓK

A MEGOLDÁS



OPSEC

ÁRULÓ SAJÁTOSSÁGOK

ÁRULÓ SAJÁTOSSÁGOK

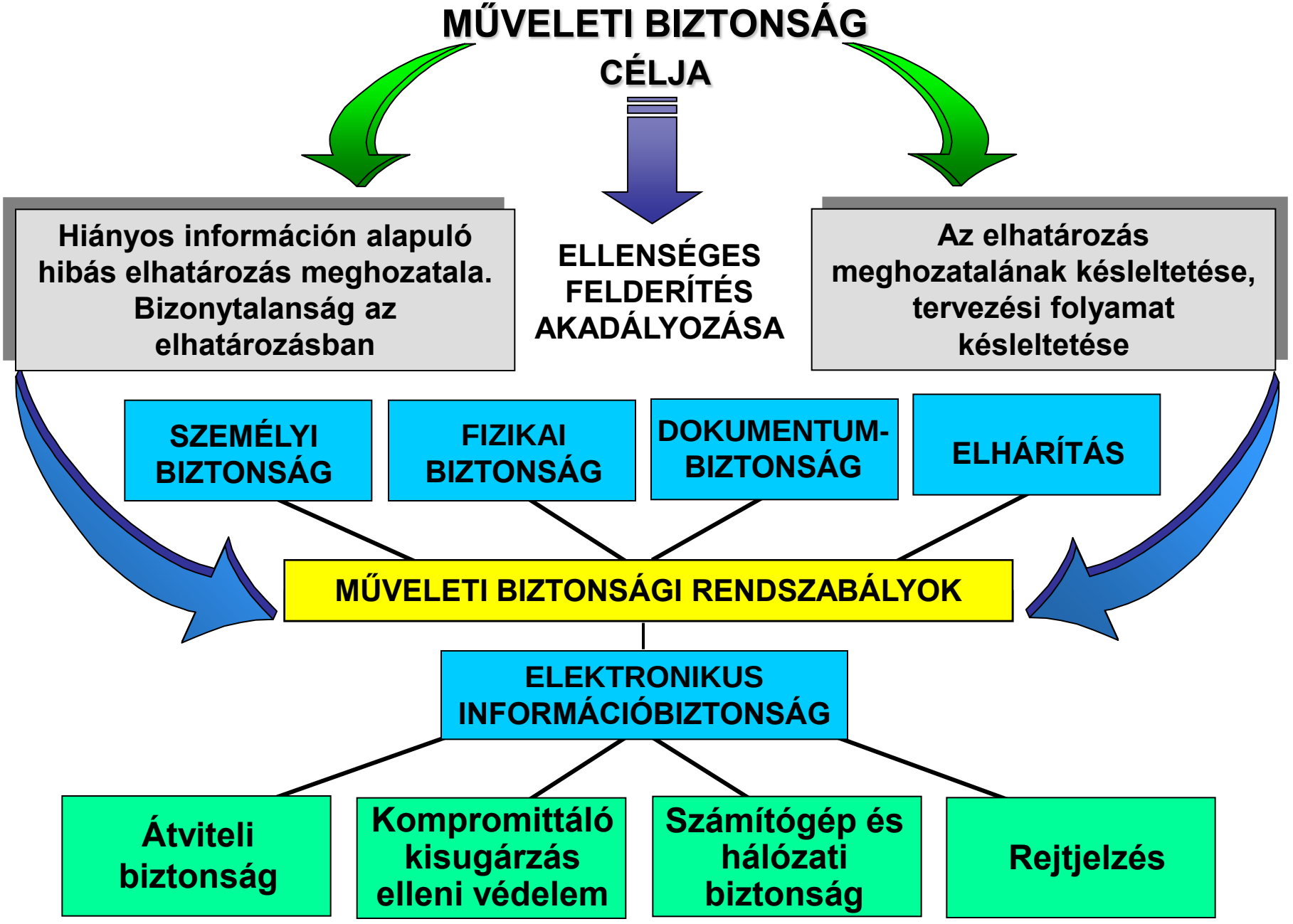
ÁRULÓ SAJÁTOSSÁGOK

ÁRULÓ SAJÁTOSSÁGOK

ÁRULÓ SAJÁTOSSÁGOK

KRITIKUS INFORMÁCIÓK

MŰVELETI BIZTONSÁG




KATONAI
MEGTÉVESZTÉS

MILITARY DECEPTION - MILDEC FOGALMA

A katonai megtévesztés mindazon tevékenységek összessége, melyekkel az ellenséges parancsnok szándékosan félrevezethető saját erőink képességeit, erejét, szándékát, elhelyezkedését és műveleteit illetően. Ezáltal az ellenséget olyan helyzetbe hozzuk, hogy tevékenységeivel (vagy tétlenségével) hozzájárul a saját feladatunk sikeres végrehajtásához.

FŐERŐKIFEJTÉSE

Az ellenséges parancsnokok a hadműveleti területen kialakult helyzetet, saját erőink elhelyezkedését, képességeit, sebezhetőségét és szándékát helytelenül értékeljék.

KATONAI MEGTÉVESZTÉS

KATONAI MEGTÉVESZTÉS

AKTÍV (TÁMADÓ) MEGTÉVESZTÉS

MÓDSZER: Hamis, félrevezető információk (áruló jellemzők) továbbítása az ellenség felé

EREDMÉNY: Meglepés elérése, a kezdeményezés megragadása, megtartása

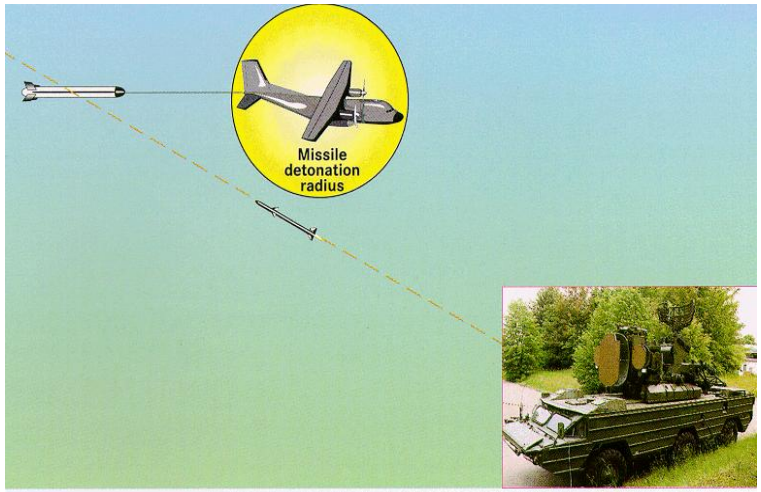
PASSZÍV (VÉDELMI) MEGTÉVESZTÉS

MÓDSZER: Hamis, félrevezető információk (áruló jellemzők) hozzáférhetővé tétele a kezdeményezés birtokában lévő ellenség számára

EREDMÉNY: Műveleti biztonság növelése

MÓDSZEREI

- különböző felderítési fajtákkal szembeni álcázási tevékenységek (elektronikai álcázás, optikai álcázás, stb);
- eltérítő csapdák *(decoy)*, makettek alkalmazása;
- félrevezető manőverek, műveletek végrehajtása (félrevezető- csapatmozgások, állásváltások, átcsoportosítások, stb.)
- hamis információk továbbítása (dezinformáció) stb.



ELTÉRÍTŐ CSAPDÁK, MAKETTEK

TÜZÉRSÉGI MAKETT

SA-9 MAKETT

ELTÉRÍTŐ CSAPDÁK, MAKETTEK

ELTÉRÍTŐ CSAPDÁK, MAKETTEK

PSZICHOLÓGIAI MŰVELETEK

PSYCHOLOGICAL OPERATIONS - PSYOPS

FOGALMA

A pszichológiai műveletek azon tervezett pszichológiai tevékenységeket jelentik, melyek békében, válságban és háborúban egyaránt alkalmazhatók az ellenség- és a saját erők, valamint a semleges érintettek magatartásának és viselkedésének befolyásolására, a politikai és katonai célok elérése érdekében.

PSZICHOLÓGIAI MŰVELETEK

TÁMADÓ CÉLÚ PSYOPS

- az erőviszonyok számunkra kedvező módon való hangsúlyozása;
- a saját csapatok technikai fölényének felnagyítása;
- a katonai megtévesztés hatásainak növelése;
- bizonytalanság előidézése.

VÉDELMI CÉLÚ PSYOPS

- az ellenséges propaganda elleni tevékenység;
- az ellenséges erők meggyőzése, hogy képesek vagyunk
  - semlegesíteni erőfeszítéseiket;
  - megvédeni az országot;
  - jelentős veszteséget okozni.

CÉL

Az ellenség és a saját erők, valamint a semleges érintettek magatartásának és viselkedésének befolyásolása a politikai és katonai célkitűzések elérése érdekében.

ESZKÖZÖK ÉS MÓDSZEREK

- Személyes kommunikáció, meggyőzés
- TV műsorszórás
- Rádió adások és műsorszórás
- Hangosbeszélő
- Szórólapok (meggyőző, felvilágosító, utasító)
- Videó és hangkazetták terítése
- SMS, MMS üzenetek
- E-mail levelek

ESZKÖZÖK ÉS MÓDSZEREK
AFGANISZTÁN

RÖPLAP

یك افغانستان متحد صلح و شگوفانی بار میآورد.

یو متحد افغانستان سوله او نیکمرغی په برخه موکوی.

AF G105

آینده افغانستان متکی بر حمایت شما از حکومت جدید میباشد. حکومت جدید آزادی های جدیدی را برای شما میسر میسازد.

د افغانستان د راتلونکی د تاسو ملا تړ د نوی حکومت سره اړه لری. نوی حکومت تاسی ته نوی آزادی په برخه کوی.

EGY EGYESÜLT AFGANISZTÁN

AFGANISZTÁN

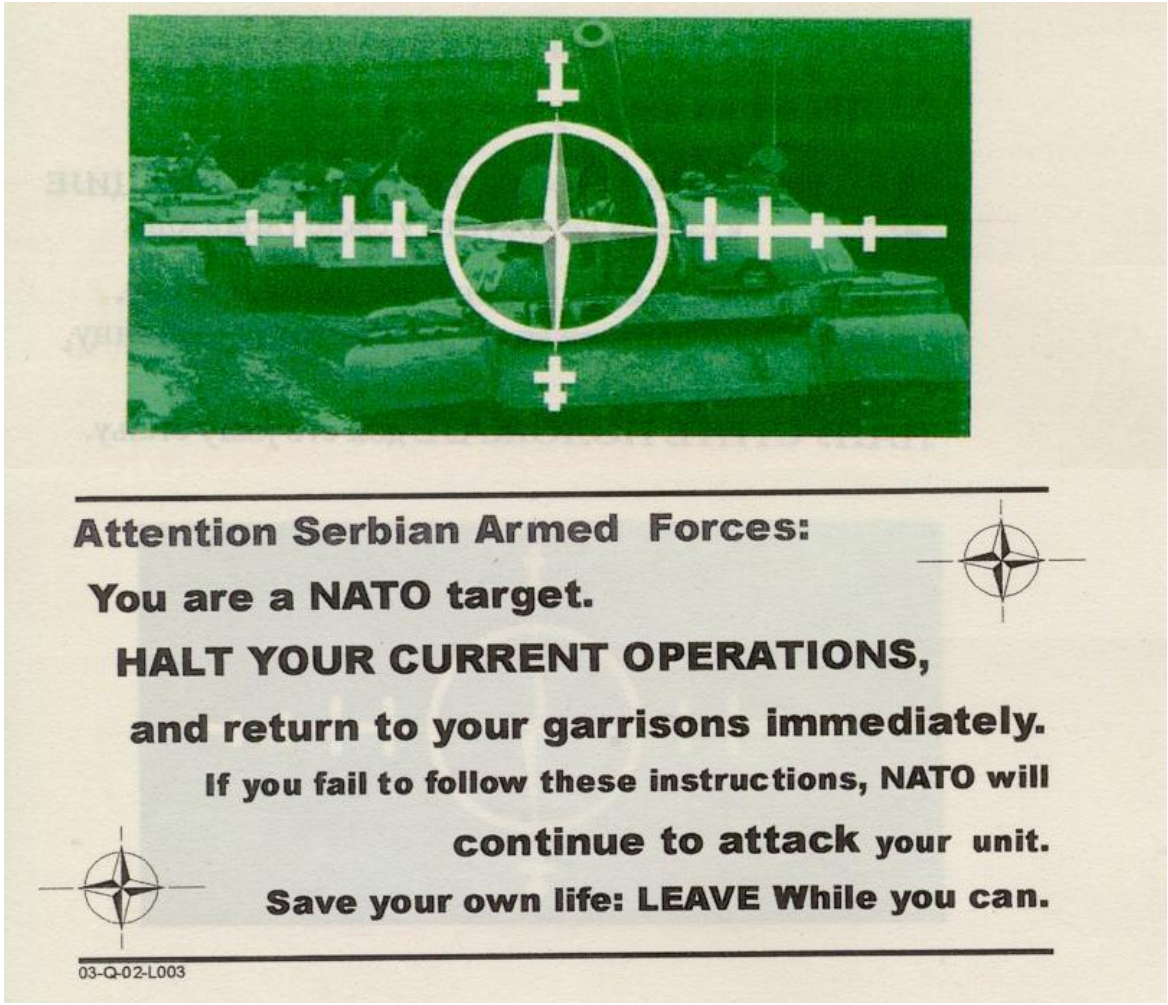
BÉKÉT ÉS FEJLŐDÉST AJÁNL

AZ ÚJ KORMÁNY EGY ÚJ SZABADSÁGOT IGÉR

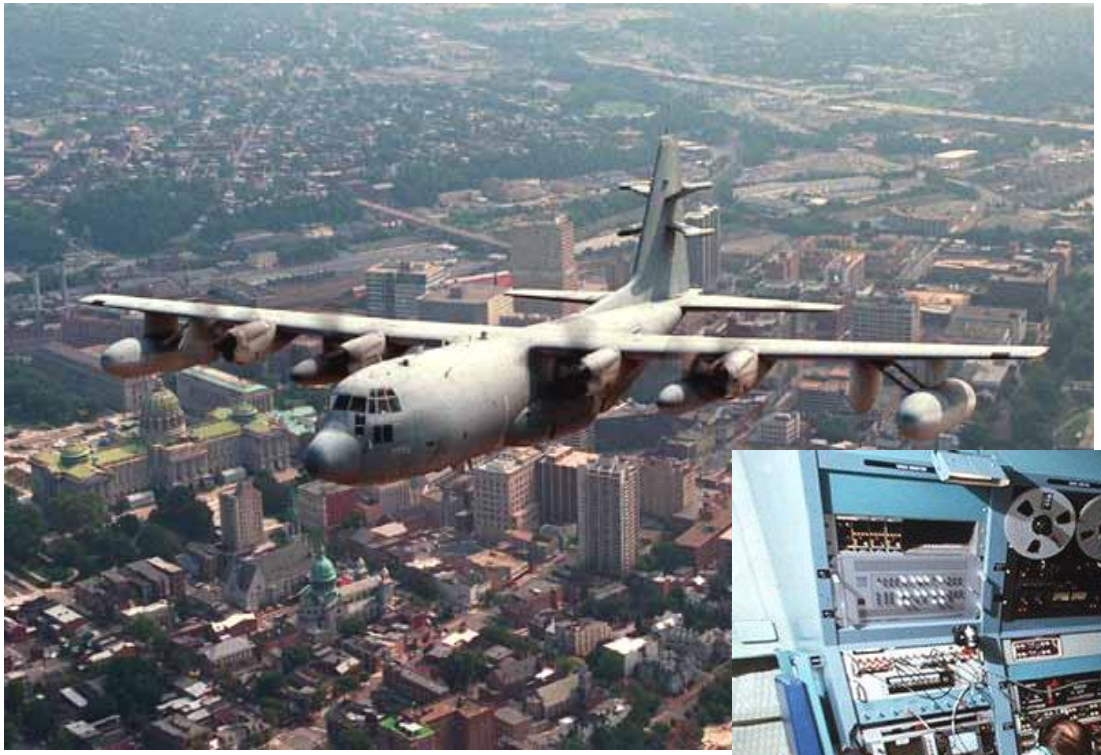
TÁMOGASD AZ ÚJ KORMÁNYT, ETTŐL FÜGG AFGANISZTÁN JÖVŐJE

ESZKÖZÖK ÉS MÓDSZEREK
KOSZOVÓ

RÖPLAP

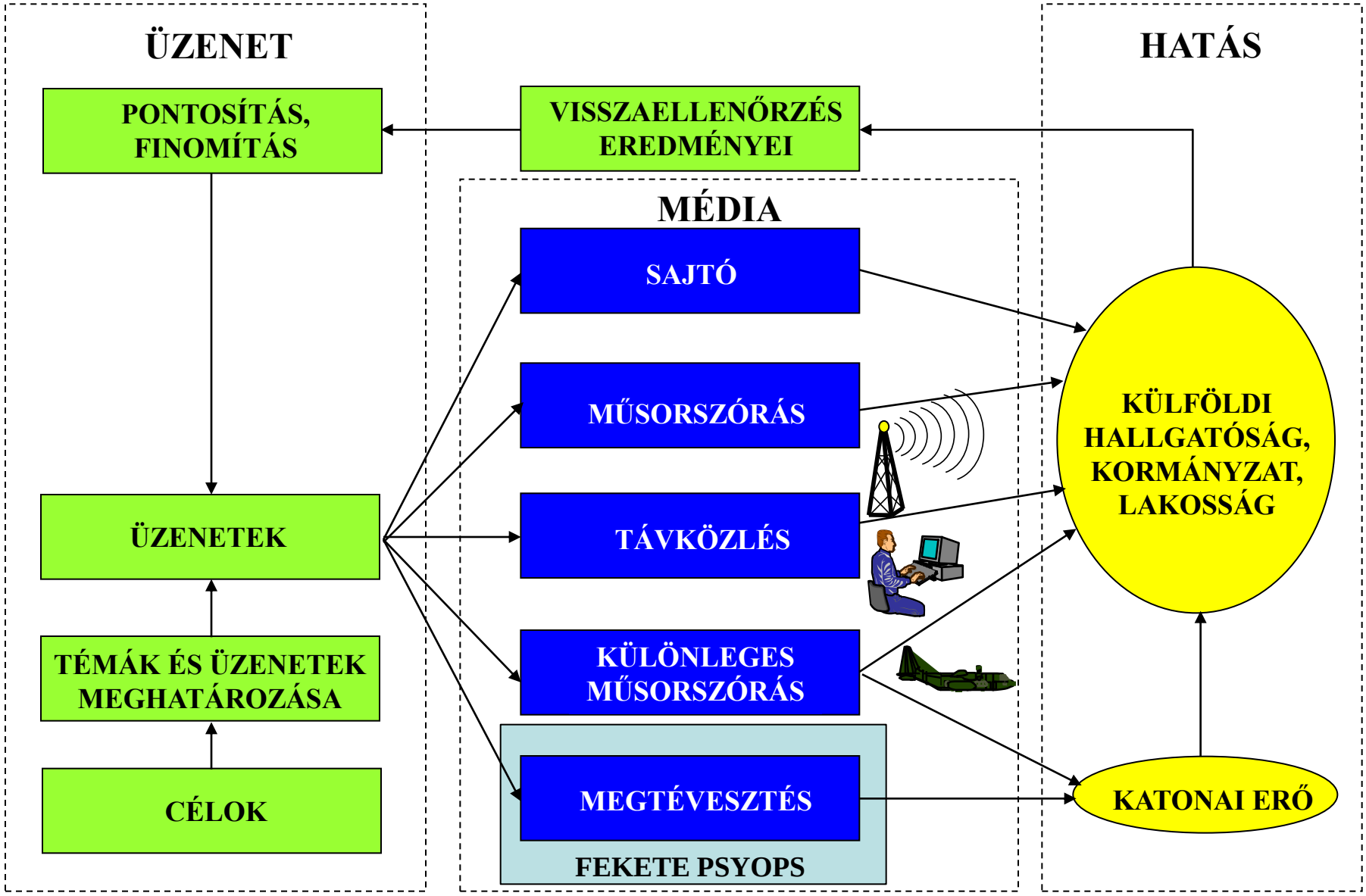


ESZKÖZÖK ÉS MÓDSZEREK



COMMANDO SOLO

A VÉGREHAJTÁS FOLYAMATA



FIZIKAI PUSZTÍTÁS

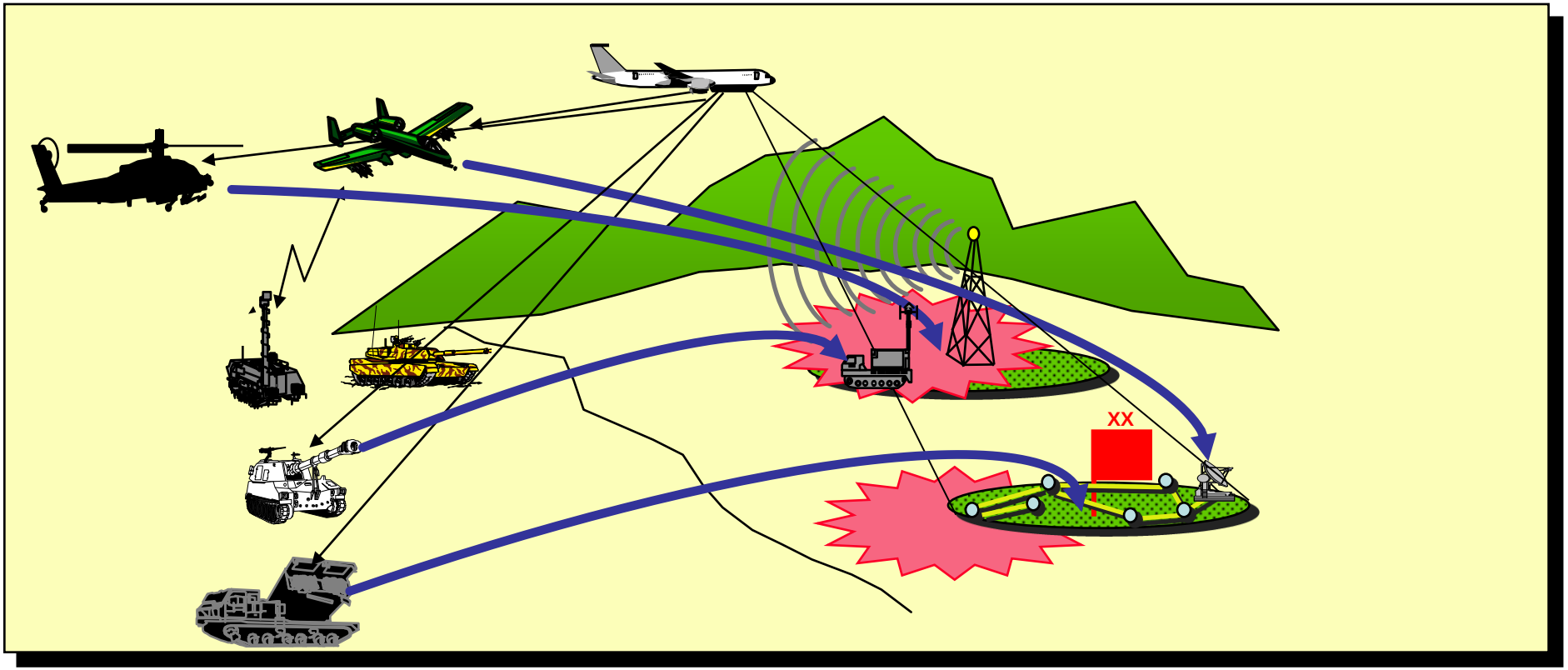
PHYSICAL DESTRUCTION - PD

FOGALMA

A fizikai pusztítás, mint az összehangolt információs műveletek egyik eleme, a pusztító-, romboló hatású *(un. "Hard Kill")* fegyverek, fegyverrendszerek alkalmazását jelenti az ellenség kijelölt információs célobjektumaira.

FIZIKAI PUSZTÍTÁS

CÉLOBJEKTUMAI ÉS VÉGREHAJTÓI



VÉGREHAJTÓK:

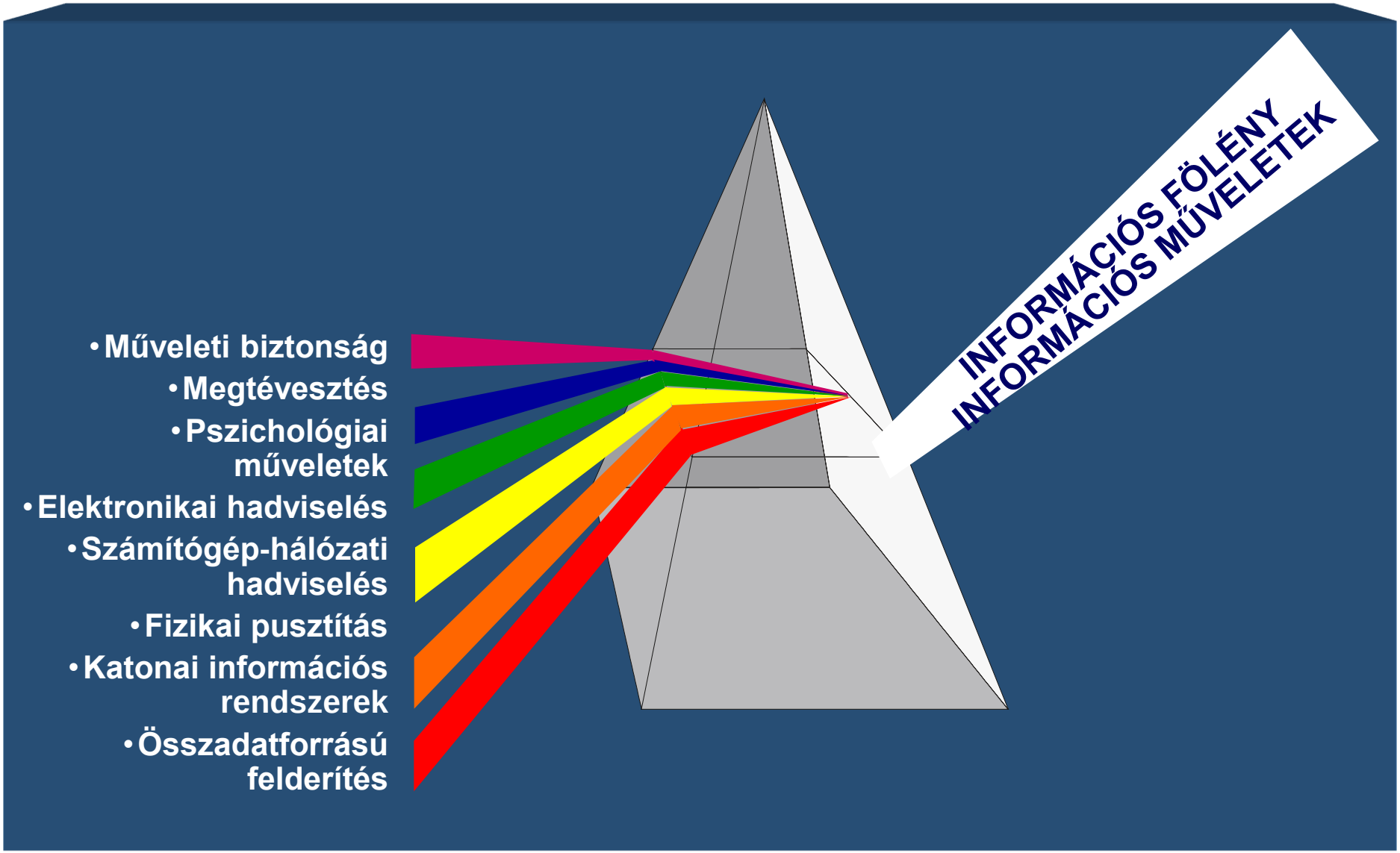
TÜZÉRSÉGI ESZKÖZÖK;
REPÜLŐGÉP ÉS HELIKOPTER FEDÉLZETI IRÁNYÍTOTT FEGYVEREK;
LÉGVÉDELMI TÜZÉR- ÉS RAKÉTAESZKÖZÖK;
GÉPESÍTETT LÖVÉSZ ÉS HARCKOCSI ALEGYSÉGEK;
SPECIÁLIS ERŐK (KOMMANDÓK).

CÉLOBJEKTUMOK:

INFORMÁCIÓS INFRASTRUKTÚRÁK

VEZETÉSI PONTOK;
HÍRADÓKÖZPONTOK;
ADATSZERZŐ ÉS ADATFELDOGOZÓ KÖZPONTOK;
VILLAMOS ENERGIAELOSZTÓ–PONTOK
EGYÉB ELEKTRONIKAI OBJEKTUMOK.

ÖSSZEGZÉS


• Műveleti biztonság
• Megtévesztés
• Pszichológiai műveletek
• Elektronikai hadviselés
• Számítógép-hálózati hadviselés
• Fizikai pusztítás
• Katonai információs rendszerek
• Összadatforrású felderítés
INFORMÁCIÓS FÖLÉNY
INFORMÁCIÓS MŰVELETEK