



# HIBRID, FENYEGETÉSEK



# HIBRID

## FENYEGETÉSEK

INFORMATION

CYBER

POLITICS

ECONOMY

DIPLOMACY

CULTURE

### AKTOROK

állami és nem-állami szereplők

### KOORDINÁCIÓ

műveletek stratégiai szintű összehangolása

### AMBIGUITÁS

anonimitás, proxy szereplők alkalmazása, tagadhatóság, attribúció nehézsége

### SZÁNDÉKOSSÁG

destabilizációs és nyomásgyakorlási céllal végrehajtott műveletek

### SZÜRKE ZÓNA

deklarált hadviselés szintje alatti műveletek, a katonai és politikai megtorlás kerülése

# FOGALMI KERET

„Hibrid fenyegetések alatt állami vagy nem állami szereplők összehangolt tevékenységét értjük, amelyek a fegyveres konfliktus küszöbszintje alatt maradva, jogi vagy etikai szempontból nem egyértelműen szabályozott vagy meghatározott szürke zónában kerülnek végrehajtásra, céljuk pedig a sérülékenységek kihasználásán keresztül megvalósuló nyomásgyakorlás annak érdekében, hogy a célállam viselkedését, percepcióját vagy döntéshozatalát az ellenérdekelt fél stratégiai érdekei mentén befolyásolják.”\*

\*Egységesen elfogadott meghatározás nem áll rendelkezésre, a fenti definíciót saját használatra a NIK dolgozta ki.

# FOGALMI ELTÉRÉSEK

## HIBRID FENYEGETÉS

A célállam gyenge pontjait kihasználó, nyílt és fedett, konvencionális és nem-konvencionális, bomlasztó és kényszerítő eszközöket vegyítő, háborús küszöb alatti műveletek.

A NIK elsősorban hibrid fenyegetésekkel foglalkozik.

## HIBRID HADVISELÉS

A hibrid eszközök tudatos, összehangolt alkalmazása fegyveres konfliktus részeként. Célja a katonai műveletek támogatása.

A hibrid fenyegetéseknél szűkebb kategória, azzal nem összetévesztendő. A "hibrid háború" kifejezés kerülendő!



politika



hírszerzés



diplomácia



gazdaság



világűr



közigazgatás



információs tér



társadalom



katonai tér



kulturális tér



kibertér



jogi tér



infrastruktúra

# HIBRID FENYVEGETÉSEK *számokban*

A Marylandi Egyetem becslése szerint minden 39 másodpercben végrehajtanak egy kibertámadást. Az állami intézmények a leggyakoribb célpontok között vannak.

A Stratégiai és Nemzetközi Tanulmányok Központjának (CSIS) adatai alapján az Oroszországhoz köthető szabotázs-műveletek száma 2022 (3 támadás) és 2024 (34 támadás) között tizenegyszeresére növekedett.

Az ID Crypt Global által készített 2024-es elemzés szerint naponta összesen min. 1,5 milliárd álhírt és dezinformációs tartalmat terjesztenek különböző közösségimédia-platformokon.

Közel 700 diplomáciai fedésben tevékenykedő orosz hírszerző EU-ból való kiutasítását követően Moszkva európai civil állampolgárokat ("eldobható ügynököket") használ kémkedési célokra. Jelenleg összesen 12 európai országban 130 személyt gyanúsítanak azzal, hogy Oroszországnak dolgozik.

A Reuters értesülései szerint az amerikai energiaügyi hatóságok a rendszer távoli manipulálására, a tűzfalak megkerülésére alkalmas, oda nem illő kommunikációs eszközöket találtak egyes kínai gyártmányú napelemek invertereiben.

A The Cube 12 országra és 24 reptérre kiterjedő jelentése szerint az európai légiközlekedést veszélyeztető vagy zavaró drónincidensek száma 2024 januárja és 2025 novembere között megnégyszereződött.

