KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ A KOGNITÍVNA BEZPEČNOSŤ – HROZBY, AKTÉRI, OPATRENIA

KYBERNETICKÁ BEZPEČNOSŤ

- **Definícia:** ochrana systémov, sietí, dát a digitálnych infraštruktúr pred neoprávneným prístupom, útokmi a zneužitím (Craigen et al., 2014).
- **Zastrešuje:**
  - prevenciu (ochrana pred útokmi),
  - detekciu (odhalenie narušenia),
  - reakciu (riešenie incidentov),
  - obnovu (návrat k funkčnosti po útoku).
- **Vzťah k informáciám:** ide o ochranu **dátovej integrity, dôvernosti a dostupnosti** – tzv. **CIA triáda** (Confidentiality, Integrity, Availability).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOGNITÍVNA BEZPEČNOSŤ

- **Definícia:** ochrana myslenia jednotlivcov a spoločnosti pred manipuláciou, dezinformáciami a psychologickými operáciami (Paul & Matthews, 2016, RAND).
- **Zastrešuje:**
  - mediálnu a informačnú gramotnosť,
  - odolnosť voči dezinformáciám,
  - schopnosť kriticky hodnotiť zdroje,
  - strategickú komunikáciu štátu a inštitúcií.
- **Vzťah k informáciám:** ide o ochranu **vnímanej reality a interpretácie faktov**, teda toho, ako informácie pôsobia na myslenie a rozhodovanie ľudí.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AKO SPOLU SÚVISIA?

- **Kybernetická bezpečnosť** chráni **technické kanály**, cez ktoré sa informácie prenášajú.
- **Kognitívna bezpečnosť** chráni **mentálne kanály**, cez ktoré ľudia spracovávajú a prijímajú informácie.
- V praxi sú tieto dve dimenzie prepojené:
  - kyberútok → získanie alebo zverejnenie citlivých dát → využitie v informačnej kampani (kognitívna rovina).
  - manipulatívny obsah → mobilizácia útokov hackerov proti inštitúciám.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

INFORMAČNÁ BEZPEČNOSŤ

- **Informačná bezpečnosť** je širší pojem, ktorý zahŕňa:
  - ochranu dát (kybernetická dimenzia),
  - ochranu interpretácie a vnímania (kognitívna dimenzia).
- Oba koncepty sú teda **podmnožinami informačnej bezpečnosti**, ktorá chráni dáta aj ich pôsobenie na ľudí.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

HROZBY V KYBERNETICKOM PRIESTORE

Typológia útokov:

- **Malware a ransomware** – škodlivý softvér, ktorý poškodzuje alebo šifruje dáta, útočníci následne žiadajú výkupné.
- **Phishing a spear-phishing** – podvodné správy na získanie prístupových údajov.
- **DDoS útoky (Distributed Denial of Service)** – zahltenie serverov masívnym prenosom dát, čím sa stávajú nedostupné.
- **APT (Advanced Persistent Threats)** – sofistikované, dlhodobé kybernetické operácie podporované štátmi.
- **Útoky na kritickú infraštruktúru** – energetika, doprava, zdravotníctvo.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CIELE KYBERNETICKÝCH ÚTOKOV

- **Ekonomické zisky** – krádež údajov, finančný podvod, ransomvér.
- **Politické ovplyvňovanie** – kompromitácia aktérov, únik dokumentov, narušenie dôvery vo vládu.
- **Spravodajské účely** – krádež citlivých dát (štátne tajomstvá, obchodné know-how).
- **Destabilizácia spoločnosti** – útoky na nemocnice, dopravné systémy alebo médiá.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KĽÚČOVÉ TRENDY

- **Štátom sponzorované útoky:** rastúci počet operácií vedených Ruskom, Čínou, Iránom.
- **Kyberkriminalita ako služba (CaaS):** prenájom hackerských nástrojov na darknete.
- **Prepojenie s informačnými operáciami:** kyberútok → únik dát → využitie v propagande (tzv. hack-and-leak operations).
- **Zameranie na „soft targets“:** univerzity, médiá, NGO (ľahšie ciele ako armáda).

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

POLITICKÉ A SPOLOČENSKÉ DÔSLEDKY

- Strata dôvery občanov v štátne inštitúcie (ak sú paralyzované).
- Politická diskreditácia (únik emailov alebo dokumentov).
- Zhoršenie medzinárodných vzťahov (kybernetické útoky ako akt nepriateľstva).
- Potreba medzinárodnej regulácie kyberpriestoru (Tallinn Manual).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

HROZBY V KOGNITÍVNEJ DIMENZII

- **Dezinformácie (disinformation):** zámerne vytvorené a šírené nepravdivé informácie s cieľom manipulovať.
- **Misinformácie (misinformation):** neúmyselné šírenie nepravdivých informácií.
- **Malinformácie (malinformation):** pravdivé informácie použité v škodlivom kontexte (napr. selektívne úniky).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PROPAGANDA A PSYCHOLOGICKÉ OPERÁCIE (PSYOPS)

- **Propaganda:** systematické formovanie postojov a správania (Jowett & O'Donnell, 2019).
- **PSYOPS:** vojenské a politické operácie zamerané na ovplyvnenie správania protivníka a verejnosti.
- **Príklad:** ruské naratívy o „denacifikácii Ukrajiny" – legitimizácia invázie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

NARATÍVY A FRAMING AKO NÁSTROJE MANIPULÁCIE

- **Naratívy:** príbehy, ktoré vysvetľujú realitu jednoduchým spôsobom a apelujú na emócie.
- **Framing:** spôsob, akým sa téma prezentuje (bezpečnostný vs. humanitárny rámec migrácie).
- **Príklad:** „NATO obkľučuje Rusko“ vs. „NATO chráni svojich členov“.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOGNITÍVNE SKRESLENIA A HEURISTIKY

- Útočníci využívajú **psychologické slabiny človeka**:
  - **Konfirmačné skreslenie** – prijímame len informácie, ktoré potvrdzujú naše názory.
  - **Efekt opakovania** – čím častejšie informácia zaznie, tým je dôveryhodnejšia.
  - **Strach a hnev** – emócie znižujú schopnosť kritického myslenia.
- **Príklad:** antivax kampane využívali obrazy detí a strachu z neznámeho.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SOCIÁLNE MÉDIA A ALGORITMY

- Algoritmy sociálnych sietí zvýhodňujú **emocionálne a polarizujúce obsahy** (Vosoughi et al., 2018, *Science*).
- „Filter bubbles“ a „echo chambers“ posilňujú uzavreté svetonázorové komunity (Pariser, 2011).
- **Príklad:** Facebook skupiny zdieľajúce proruský obsah počas volieb v EÚ.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

HYBRIDNÉ KAMPANE

- Kombinácia kybernetických a kognitívnych útokov.
- **Príklad:** „hack-and-leak“ operácie – získanie emailov (kyber) a ich využitie na diskreditáciu v médiách (kognitívne).
- Ukazuje, že hranica medzi kyber a kognitívnou bezpečnosťou je tenká.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

POLITICKÉ A SPOLOČENSKÉ DÔSLEDKY

- **Erozia dôvery** – ľudia strácajú dôveru v médiá, inštitúcie, štát.
- **Polarizácia spoločnosti** – „my vs. oni“ naratívy.
- **Podkopanie demokratických procesov** – ovplyvňovanie volieb, protestov, verejnej mienky.
- **Zraniteľnosť menších štátov** – obmedzená kapacita čeliť veľkým informačným operáciám.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AKTÉRI V KYBER- A KOGNITÍVNEJ DIMENZII

ŠTÁTNI AKTÉRI

- **Charakteristika:** disponujú najväčšími kapacitami (technickými, finančnými, spravodajskými).
- **Ciele:** geopolitické záujmy, ovplyvňovanie verejnej mienky, destabilizácia oponentov.
- **Príklady:**
  - Rusko – kombinované kybernetické a informačné operácie (Ukrajina, voľby v USA 2016).
  - Čína – kyberšpionáž + globálne mediálne projekty (CGTN, Xinhua).
  - Západné demokracie – využívanie kyber operácií v obrannom i ofenzívnom zmysle, strategická komunikácia NATO/EÚ.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AKTÉRI V KYBER- A KOGNITÍVNEJ DIMENZII

NEŠTÁTNI AKTÉRI

- **Hacktivisti:** (Anonymous) – útočia na štátne alebo korporátne ciele v mene ideológie.
- **Teroristické organizácie:** (ISIS) – sofistikovaná online propaganda, nábor bojovníkov.
- **Kriminálne skupiny:** kybernetická kriminalita, ransomware, phishing → ekonomické ciele, ale s politickými dopadmi.
- **Think-tanky a občianske združenia:** niektoré slúžia ako proxy pre mocenské záujmy, iné ako „watchdogy“.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AKTÉRI V KYBER- A KOGNITÍVNEJ DIMENZII

TECHNOLOGICKÉ PLATFORMY

- **Sprostredkovatelia aj aktéri:** určujú, čo vidíme, a teda aj aký obraz sveta vnímame.
- **Algoritmy** → posilňujú polarizáciu a virálnosť dezinformácií.
- **Príklady:**
  - Facebook (kritika po roku 2016 za nedostatočnú moderáciu obsahu).
  - TikTok (obavy z čínskeho vplyvu a zbierania dát).
  - Twitter/X (od kúpy Muskom oslabené kontrolné mechanizmy).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AKTÉRI V KYBER- A KOGNITÍVNEJ DIMENZII

MÉDIÁ A ALTERNATÍVNE ZDROJE

- **Tradičné médiá:** často pod tlakom → môžu byť cieľom kyberútokov aj dezinformačných kampaní.
- **Alternatívne médiá:** poskytujú platformu pre dezinformačné a konšpiračné naratívy.
- **Príklad:** Sputnik a RT – zahraničné mediálne projekty s cieľom ovplyvniť verejnú mienku v Európe.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AKTÉRI V KYBER- A KOGNITÍVNEJ DIMENZII

OBČIANSKA SPOLOČNOSŤ A AKADEMICKÁ SFÉRA

- **Fact-checking iniciatívy:** (Demagog.sk, AFP Fact Check, EUvsDisinfo).
- **Mediálna výchova a gramotnosť:** školské a univerzitné programy.
- **Výskumné inštitúcie:** poskytujú analytické výstupy (Oxford Internet Institute, NATO StratCom COE).
- **Slabiny:** obmedzené zdroje, nižšia viditeľnosť oproti masovým médiám a štátom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AKTÉRI V KYBER- A KOGNITÍVNEJ DIMENZII

SÚHRA A KONFLIKT MEDZI AKTÉRMI

- **Štát vs. platformy:** štátne regulácie (EÚ – DSA, USA – debaty o Section 230) vs. komerčné záujmy platforiem.
- **Štát vs. neštátni aktéri:** vlády vs. hacktivisti či teroristi.
- **Občianska spoločnosť vs. dezinformačné weby:** zápas o dôveru verejnosti.
- **Západ vs. autoritárske režimy:** informačná vojna, odlišné normy (sloboda prejavu vs. cenzúra).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TECHNICKÉ OPATRENIA (KYBER)

- **Prevencia:** firewally, antivírusy, šifrovanie, segmentácia sietí.
- **Detekcia:** systémy včasného varovania, monitoring anomálií, threat intelligence.
- **Reakcia:** incident response teams (CERT, CSIRT), krízové plány.
- **Obnova:** zálohovanie, redundancia systémov.
- **Príklad:** Estónsko – vybudovanie silnej kybernetickej infraštruktúry po útokoch 2007.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

POLITICKÉ A LEGISLATÍVNE OPATRENIA

- **Národné stratégie kybernetickej bezpečnosti** – integrované prístupy štátov.
- **Medzinárodné rámce:**
  - EÚ: NIS2 (kybernetická bezpečnosť), Digital Services Act (obsah na platformách).
  - NATO: kybernetický priestor ako piata doména vojenských operácií.
  - Tallinn Manual – pravidlá medzinárodného práva v kyberkonfliktoch.
- **Príklad:** EÚ po roku 2016 zaviedla prísnejšie pravidlá pre platformy v súvislosti s dezinformáciami.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SPOLOČENSKÉ A VZDELÁVACIE OPATRENIA

- **Mediálna a digitálna gramotnosť:** rozvoj kritického myslenia, schopnosť identifikovať dezinformácie.
- **Fact-checking iniciatívy:** Demagog.sk, EUvsDisinfo, AFP Fact Check.
- **Strategická komunikácia štátu:** proaktívne informovanie verejnosti, rýchle reakcie na hoaxy.
- **Príklad:** Litva – úspešné využívanie stratkomu proti ruským naratívom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SPOLOČENSKÉ A VZDELÁVACIE OPATRENIA

- **Mediálna a digitálna gramotnosť:** rozvoj kritického myslenia, schopnosť identifikovať dezinformácie.
- **Fact-checking iniciatívy:** Demagog.sk, EUvsDisinfo, AFP Fact Check.
- **Strategická komunikácia štátu:** proaktívne informovanie verejnosti, rýchle reakcie na hoaxy.
- **Príklad:** Litva – úspešné využívanie stratkomu proti ruským naratívom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOOPERAČNÉ PRÍSTUPY

- **Partnerstvá štát – súkromný sektor – akademická sféra.**
- **Platformy:** zavádzanie pravidiel proti botom a deepfake videám.
- **Občianska spoločnosť:** watchdog aktivity, investigatívne médiá.
- **Medzinárodná spolupráca:** zdieľanie dát o hrozbách medzi štátmi (NATO StratCom COE v Rige).

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍPADOVÉ ŠTÚDIE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

RUSKO – INFORMAČNÉ OPERÁCIE A HYBRIDNÁ STRATÉGIA

- **Charakteristika:**
  - Rusko využíva kombináciu kybernetických útokov a informačných operácií → tzv. *hybridná vojna*.
  - Cieľom je destabilizovať oponentov, oslabiť dôveru v inštitúcie a polarizovať spoločnosť.
- **Metódy:**
  - Trollie farmy (Internet Research Agency, Petrohrad).
  - Štátom podporované médiá (RT, Sputnik).
  - Kybernetické útoky typu *hack-and-leak*.
- **Príklady:**
  - Voľby v USA 2016 → šírenie polarizujúcich naratívov na Facebooku a Twitteri.
  - Inváziа na Ukrajinu 2022 → naratívy o „denacifikácii“, „oslobodzovaní Donbasu“.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ESTÓNSKO – MODEL ODOLNOSTI

- **Charakteristika:**
  - Po kybernetických útokoch v roku 2007 (proti štátnym inštitúciám a bankám) Estónsko vybudovalo jeden z najpokročilejších systémov kybernetickej bezpečnosti.
- **Opatrenia:**
  - Založenie **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)** v Tallinne.
  - Kybernetická gramotnosť a vzdelávanie → už od základných škôl.
  - Silné partnerstvo medzi štátom, občianskou spoločnosťou a súkromným sektorom.
- **Príklady:**
  - Integrovaný systém elektronickej identity (eID).
  - Pravidelné cvičenia (Locked Shields – najväčšie kybernetické cvičenie na svete).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

USA – OTVORENÝ SYSTÉM S DÔRAZOM NA REGULÁCIU PLATFORIEM

- **Charakteristika:**
  - USA sú technologickým centrom (Google, Meta, Twitter/X).
  - Otvorený informačný priestor = vysoká dynamika, ale aj zraniteľnosť.
- **Problémy:**
  - Zásahy do volieb 2016 a 2020 → ukázali slabiny v regulácii sociálnych médií.
  - Polarizácia a „echo chambers“.
- **Opatrenia:**
  - Posilnenie spolupráce medzi FBI a platformami.
  - Debata o legislatívnych rámcoch (Section 230 – zodpovednosť platforiem za obsah).
  - Investície do výskumu dezinformácií (Harvard Kennedy School, Stanford Internet Observatory).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY