SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

A kiberbiztonság szabályozásának aktuális kérdései - A 21. század IKT közegének fő kockázatai, működésének immanens gyengeségei és a jog (fél)megoldásai

2025.06.12.

dr. Vikman László alezredes,
egyetemi tanársegéd
SZE DF ÁJK, Modern Technológiai és Kiberbiztonsági Jogi Tanszék

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

KUTATÁSI CÉL

- A korszerű digitális technológiák alkalmazásából származó kockázatok és fenyegetések elemzésére használt általános megközelítések többsége technikai, listaszerű, aktualitásokra koncentrál

- A cél a legfontosabb tényezőket a katonai műveletervezésből ismert PMESII-modell keretei között feldolgozva értékelni alternatív analitikai eszközök hasznosságát a stratégiai megközelítésben

A SZABÁLYOZÁS SZEREPE A KIBERBIZTONSÁGBAN

A hatékony kiberbiztonság kereteinek megteremtése nem működhet tisztán jogi eszközökkel, mint alapvetően műszaki terület, elsősorban technológiai oldalról determinált, de többek közt társadalmi, üzleti, politikai aspektusok is erősen hatnak rá

A szabályozás szintjeit leírhatjuk katonai fogalmakkal

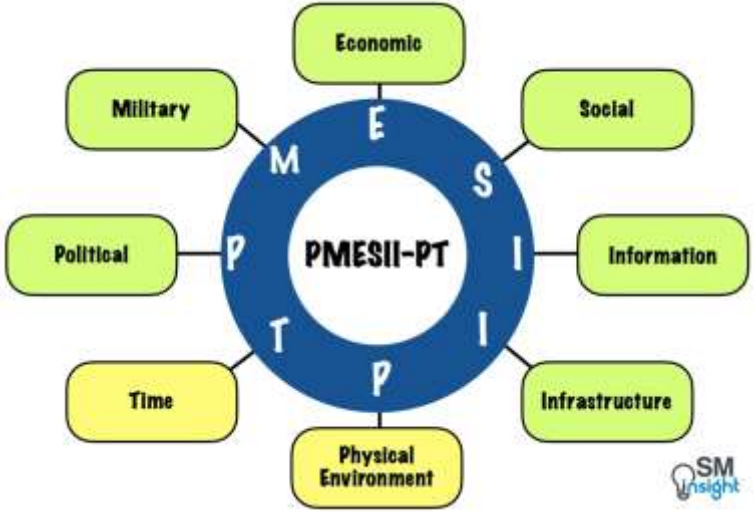
- stratégia (jogalkotás)
- hadműveleti (szervezeti felépítés, erőforrás-menedzsment)
- harcászati (szervezeti kiberbiztonsági eljárások és folyamatok)

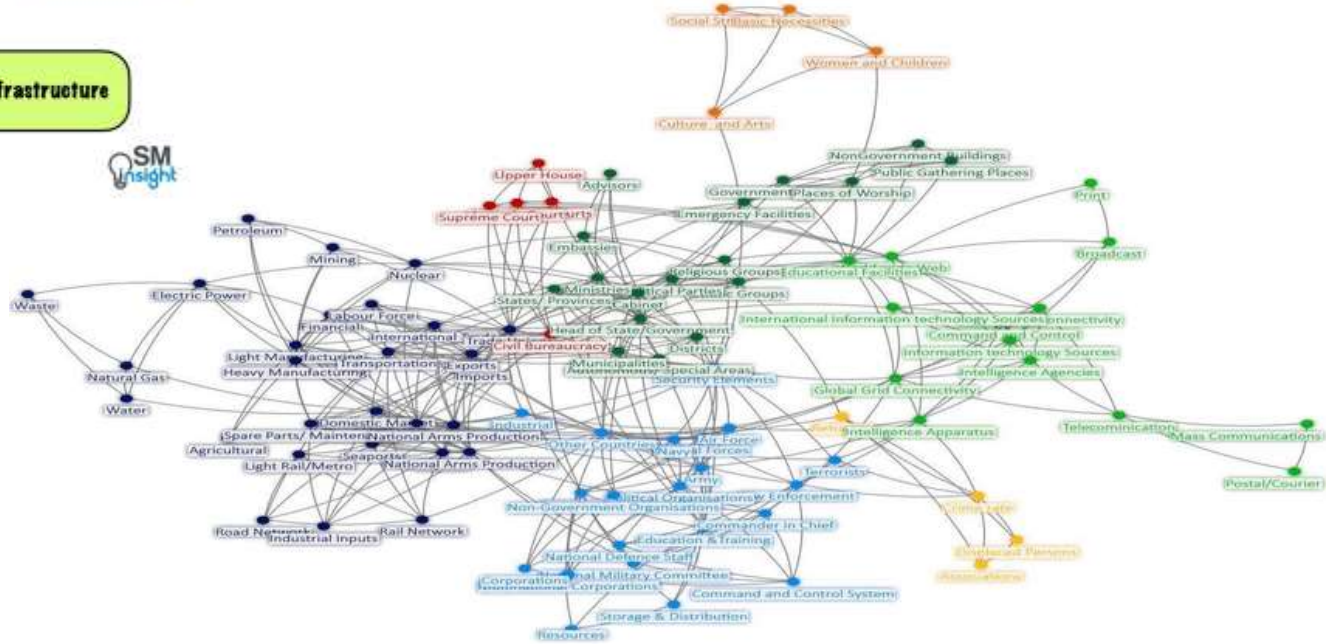
szinten egyaránt.

A PMESII-PT MODELL

- Stratégiai helyzetértékelésben alkalmazott, komprehenzív elemző megközelítés
- Betűszó a módszerben vizsgált tényezők kezdőbetűiből megalkotva: Political, Military, Economic, Social, Information, Infrastructure és a kiegészítő további két elem Physical, Time.
- Jelentőségét katonai közegben annak köszönheti, hogy a NATO átfogó összhaderőnemi műveletttervezési módszertana, a COPD (Comprehensive Operations Planning Directive), és az USA műveletttervezési doktrínája is alkalmazza

Cím


Economic
Military
Social
Political
Information
Time
Infrastructure
Physical Environment
PMESII-PT
P
M
E
S
I
I
P
T
SM Insight


Social Stratasic Necessities
Women and Children
Culture and Arts
Upper House
Advisors
Supreme Court/Courts
Government
Non-Government Buildings
Public Gathering Places
Places of Worship
Emergency Facilities
Print
Broadcast
Petroleum
Mining
Nuclear
Electric Power
Waste
Embassies
Religious Groups
Educational Facilities
Web
Ministries
Political Parties
Basic Groups
States/ Provinces
Cabinet
Labour Force
Financials
International Trade
Head of State/Government
Civil Bureaucracy
Districts
Municipalities
Special Areas
Security Elements
International information technology Sources
Connectivity
Command and Control
Information technology Sources
Intelligence Agencies
Global Grid Connectivity
Natural Gas
Water
Light Manufacturing
Heavy Manufacturing
Transportation
Exports
Imports
Domestic Markets
Industrial
Spare Parts/ Maintenance
National Arms Productions
Agricultural
Seaports
Light Rail/Metro
National Arms Production
Other Countries
Air Force
Navy/ Naval Forces
Army
Terrorists
Intelligence Apparatus
Telecommunications
Mass Communications
Postal/Courier
Non-Government Organisations
Political Organisations
Law Enforcement
Commander In Chief
Education & Training
National Defence Staff
Corporations
National Military Committee
Command and Control System
Storage & Distribution
Resources
Road Networks
Industrial Inputs
Rail Network

	Political, P	Military, M	Economic, E	Social, S	Infrastructure, I	Information, I
Areas, A	District boundary, Party affiliation areas	Area of interest, Influence and operations, Safe havens	Sectors, Formal/informal economies, Natural resources, Trade routes, Movement of goods and services	Diaspora, Camps, Enclaves, Migration pattern, Neighborhood, Boundaries of influence	Commercial, Industrial, Residential, Rural, Urban	Coverage of different media types
Structures, S	Government centers	Bases, Headquarters	Banking, Fuel, Manufacturing, Warehousing, Markets, Stockyards	Penal facilities, Historical structures and facilities, Libraries, Schools and universities, Stadiums	Emergency shelters, Energy (distribution, natural gas, power plants), Medical (hospitals), Public buildings, Transportation (airfields, bridges, ports and harbors, railroads, roadways and subways), Waste treatment and storage, Water treatment and storage	Communication (lines, towers), Command and control systems, Internet services, Cellular and mobile services, Postal service, Print shops, Telephone
Capabilities, C	Administration, Framework (legislative, judicial, etc.)	Doctrine, Training, Materials, Manpower, Facilities, Equipment, etc.	Fiscal (currency, monetary policy)	Medical, Language and dialects, Social networks, Property records and control	Clean water, Clothing, Communication system, Law enforcement, Firefighting, Medical capacity, Sanitation	Indigenous communications networks, communication links to other areas, Internet access, Printed materials, Propaganda mechanisms, Radio, Television, Messaging, etc.
Organization, O	International partners, Political parties, etc.	Border guards, Corrections, Insurgents, Terrorists, Tribal militias, etc.	Business organizations, Guilds, Labor unions, Volunteer groups	Clan, Community, Criminal, Familial, Patriotic and service organizations, Religions, Tribes, etc.	Government ministries, Business communities	Media groups, Influential groups, Foreign governments, International organization groups, etc.
People, P	Leaders, Partnerships	Key leaders	Labor occupations, Business leaders, Consumption patterns, Avg. daily wage, Income distribution	Education, Ethnicity, Key figures, Racial structure, Vulnerable populations, Gender roles, etc.	Officials, Local people, Business communities, Facility managers, Workers, etc.	Decision makers, Leaders, Newspaper publishers, Journalists, Media
Event, E	Elections, Meetings, Speeches,	Historical, Non-combat	Agricultural and market schedules, Harvesting periods, Market days, Paydays, Planting schedule	Celebrations, Census, Civil disturbance, Criminal, National holidays, Religious holidays	Maintenance activities, Construction of projects	News cycles, Press conferences, Group meetings

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

ENISA THREAT LANDSCAPE 2024

7 fő fenyegetési forma: ransomware, malware, social engineering, adatok elleni fenyegetések, DOS-támadások, információ manipulációk, ellátási láncok elleneni támadások

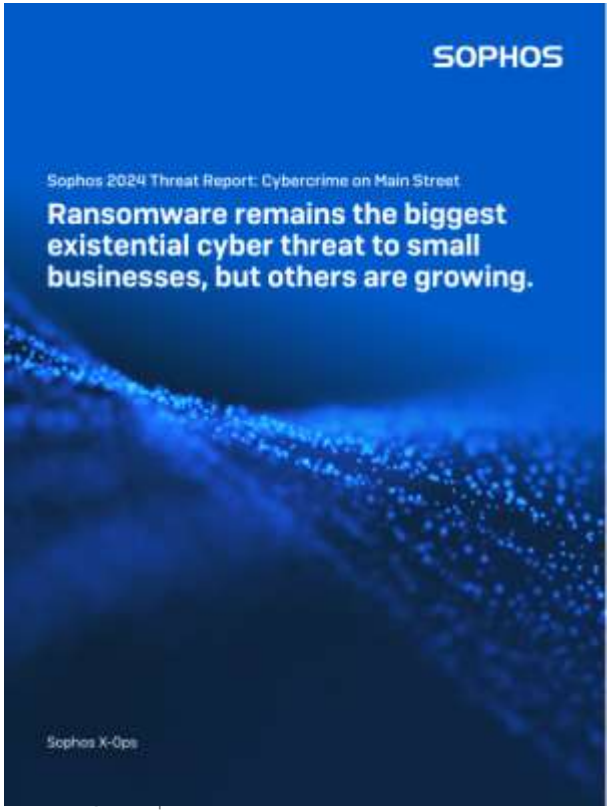
4 fő fenyegetési vektor kategória: állami szereplők, szervezett bűnözők és hackerek, üzleti/magánszektorbeli támadók, hacktivisták

EUROPOL, INTERNETES BŰNÖZÉS ÉRTÉKELÉSE 2024

Öt fő jelenségcsoportot emel ki:
- a kriptovaluták és dark web növekvő jelentősége a kiberbűnözésben,
- a ransomware és malware támadások,
- kiskorúak szexuális kizsákmányolása (MI növekvő szerepe),
- az online és fizetési rendszerekkel elkövetett visszaélések (idértve a phishing-et, az account-lopást, a befektetési és romantikus csalásokat, az ATM-ek támadását, az online visszaéléseket és a pénzmosást),
- végül a jövőben várható trendeket, mint pl. diszruptív technológiák felhasználásával összefüggő bűncselekményeket, de ideértve az MI rossz szándékú alkalmazását, a szervezett bűnözés szolgáltatási szintek szerinti tagolódását (ransomware-as-a-service), a pénzügyi rendszerek fokozott védelmét, a tiltott tartalmak szűrését, stb.

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

SOPHOS FENYEGETETTSÉG JELENTÉS 2024



A vezetői összefoglalójában
- a zsarolóvírusok,
- az adatlopás,
- a malware-ek,
- a védtelen, nem megfelelően menedzselt, vagy már nem támogatott technikai eszközökből származó sérülékenységek szervezett bűnözők által kihasználása,
- a visszaélések az egyes hardvereszközöket meghajtó ún. driver-programok rosszindulatú módosításával,
- az egyre szofisztikáltabb e-mail-támadások,
- végül a kifejezetten mobil-felhasználókat célzó közösségi médiát és social engineering-et kombináló, egyes esetekben kriptovaluta-pénztárcákat célzó támadások szerepelnek.

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

LEVONHATÓ KÖVETKEZTETÉSEK, KÖZÖS JELLEMZŐK

- Természetes, hogy minden elemzést végző szervezet saját perspektívából, küldetéséhez, feladatrendszeréhez illeszkedően határozza meg a vizsgálat fókuszát, témáit, ezeket gyakran dominálják az éppen aktuális, divatos trendek és témák, ezekhez igazítva prezentálják aztán az eredményeiket is, időnként toplistás megközelítésben, a figyelem megragadására koncentrálva

- A kiberbiztonsági szféra természetéből fakadóan műszaki-technikai szemlélet, nyelvezet és kultúra által dominált, az azonosított jelenségek, ezek leírása is gyakran a technológiai részletekre koncentrál, politikai vagy stratégiai szintű döntéshozatalt kevésbé képes közvetlenül informálni további interpretáció nélkül

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

A 21. század IKT közegének fő kockázatai, a digitális technológiák működésének immanens gyengeségei és a jog (fél)megoldásai - PMESII-PT elemzési szempontok mentén

POLITIKA

- Nemzetközi jogi háttér hiányosságai
- Nemzetközi büntetőjog hiányosságai
- A diszruptív technológiák szabályozásban nincs konszenzus csak verseny
- Kognitív és információs műveleteknek sincsenek jogi korlátai

ERŐK, KÉPESSÉGEK

- Kiberbiztonságért felelős állami intézményrendszerek (EU NIS2)
- Nemzeti megoldásokban a fő szereplő általában egy nb. szolgálat, vagy egy szakosított szerv, több kiegészítő szereplővel
- A kormányzati koordináció kulcskérdés
- A szervezeti képességek nem tartanak lépést a szabályozás elvárásaival
- A felhasználói képességek nem tartanak lépést a fenyegetésekkel (jótékony hatások a fizikai bűnözésre, megdöbbentő hatékonyság a kiberbűnözésben)

GAZDASÁG

- Nyomasztó techszektor-fölény, az állam követő szerepe inkább lemaradást jelent
- EU szabályozási generációváltás
- „Move fast and break things”, patch-kultúra, gyors termékciklusok
- Kontrollvesztést eredményező technológiák (kripto, titkosított kommunikáció, MI-használat…)
- Exportkorlátozások (NVIDIA és más chipgyártók)

TÁRSADALMI

- A társadalmi szerveződés és diskurzus új formái
- Az ajánló algoritmusok nem kívánt mellékhatásai
- Egyéni és csoportszintű mentálhigiénés következmények
- Személyes adatok feletti kontrollvesztés – adatbrókerek
- Hagyományos jogi területek lehetséges lépései:
  - Kellékszavatosság magasabb szintje a szoftvereknél
  - Szerzői jogban kód-visszafejtés biztonsági céllal

INFORMÁCIÓS

- Hagyományos média fokozatos visszaszorulása
- A közösségi oldalak tartalomfelelőssége más követelmények mentén működik – CDA Section 230
- Információs szuverenitás elvesztése – adattárházak, felhő
- EU Platformszabályozás gyakorlati eredményei még kétségesek (a gyakorlatban gyakran csak néhány globális-USA szereplőre hatályosak)
- A működtető algoritmusok etikája komolyan megkérdőjelezhető

INFRASTRUKTÚRA

- Tervezési hibák, gyors fejlesztési ciklusok, komplexitás
- A biztonság a DARPANET-től kezdve nem az első számú szempont
- Az egymásra épülő szintek bármelyikének gyengesége borítja a rendszert, a legacy-rendszerek mindenhol felbukkannak
- A létező biztonságos fejlesztési módszertanok alkalmazása költség-haszon elven gyakran háttérbe szorul – mit változtat ezen majd a tanúsítás és kiberreziliencia
- A domináns szereplők útmutatása, felelősségvállalása nélkül nem lesz drasztikus változás – a szűkös erőforrásokkal tevékenykedők nem tudnak lépést tartani

FIZIKAI KÖRNYEZET

- Alapkövetelmény az elektromos-energia és a klimatizálás folyamatos, redundáns és az amortizációval lépést tartó biztosítása
- BCP és katasztrófa-helyreállítási tervezés kulcsfontosságú
- Klímaváltozás jelentősége
- Elektromágneses spektrum zavarai - napkitörések

IDŐTÉNYEZŐ

- A kibertérre az emberi érzékelés feletti, nagy részben automatizált folyamatok a jellemzők, ezek korrekciója viszont emberi léptékben történik
- A sérülékenységi információknak is van lejárati idejük: zero-day
- Lehetnek egyes szolgáltatások esetében kiemelt időszakok (választás, sportesemények)

NÉHÁNY SZÓ AZ ÚJ KIBERSTRATÉGIÁRÓL

- 1089/2025. (III. 31.) Korm.határozat, Magyarország Kiberbiztonsági Stratégiájáról, 3. pont
  - a válságok megjelenése (máshogy romló biztonsági környezet),
  - az egyén és társadalom összhangjának megzavarása (káros hatások szociális kohézióra),
  - függőség kialakulása (ami szintén szociális elem),
  - ellátási láncok megzavarása (ami értékelhető gazdasági és infrastrukturális problémaként is),
  - valamint az adatbiztonság sérülékenysége (ami képességbeli, gazdasági, szociális kérdés is lehet).

- Más csoportosításokban, és mélységben de megjelenik a fenti elemekből néhány, de átfogó stratégiai módszertan, logikus egymásra építkezés a tartalomban nem azonosítható

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

Összegzés

- A PMESII-PT vagy más összetett stratégia-alkotási modellek hasznosak lehetnének a katonai kereteken kívül is, különösen az interdependenciák, a legfontosabb „csomópontok” azonosítására
- További eszközök lehetnének: súlypontelemzés, ends-ways-means

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI KAR

Köszönöm a figyelmet!