Kiberhadviselés: kiberháborúk kora a 21. század?

Kiberhadviselés rövid bemutatása

Tamás J. Varga
MSEE, MBA, CEH/CPTE, CVA
https://www.linkedin.com/in/tamas-j-varga-msee-mba/

Tartalomjegyzék

Tartalomjegyzék

Kiberhadviselés | Bemutatkozás

Személyes és szakmai háttér

Varga J. Tamás

MSEE, MBA, CEH/CPTE, CVA

https://www.linkedin.com/in/tamas-j-varga-msee-mba/

Budapest University of Technology and Economics

Information Technology of Robot, Mobile Communication

Master of Business Administration - MBA, Infocommunication & Economics and Finance

PROJECT

P27 - Threat Analysis and Risk Assessment of Azure based Build Infrastructure as a Service
P28 - Microsoft Defender for Endpoint migration in enterprise scale
P29 - Establishing, implementing and improving L2 support for Fishing Email and Malware Attack Simulations
P30.1 - Establish and improve L2 support for VM and Penetration Testing services
P31 - Establish, handover and improve specific shared SecOps IT services
P32 - Global IT Infrastructure Operations Team establishment
P33.1 - Relocation and transferring centrally shared ICT services among corporate data centers
P33.2 - Participating in the Lean Six Sigma company transformation, leading ICT service transformatio
P34.2 - Establishing backup and geographical redundant services in Backup & Recovery Data Center

thyssenkrupp Presta AG
Full-time · 6 yrs 7 mos

Global IT Security Operations Department Leader
Dec 2021 - Present · 3 yrs 4 mos

As Head of Global IT Security Operations Department is responsible to lead, operate, and maintain specific Global IT Infrastructure services at thyssenkrupp Automotive Technologies, Steering Business Unit. The main r ...see more

Global IT Infrastructure Operations Team Leader
Sep 2018 - Nov 2021 · 3 yrs 3 mos

As Head of Global IT Infrastructure Operations Team is responsible to lead, operate, and maintain specific Global IT Infrastructure services at thyssenkrupp Automotive Technologies, Steering Business Unit. The main resp ...see more

BUNDY REFRIGERATION
Full-time · 19 yrs 1 mo

Global ICT Manager
2017 - 2018 · 1 yr
Hungary

Defining and executing strategic as well as tactical ICT plans to improve the international corporate ICT organization and related services at Bundy Refrigeration (Europe and Americas regions in 9 countries, 1 ...see more

Global ICT Infrastructure Manager
2007 - 2017 · 10 yrs
Hungary

Planning, organizing, controlling and leading global ICT Infrastructure services at Bundy Refrigeration Group. Standardizing shared services, managing local and global ICT providers/vendors. Establish and continuc ...see more

IT Manager
2001 - 2007 · 6 yrs
Jászárokszállás, Jász-Nagykun-Szolnok, Hungary

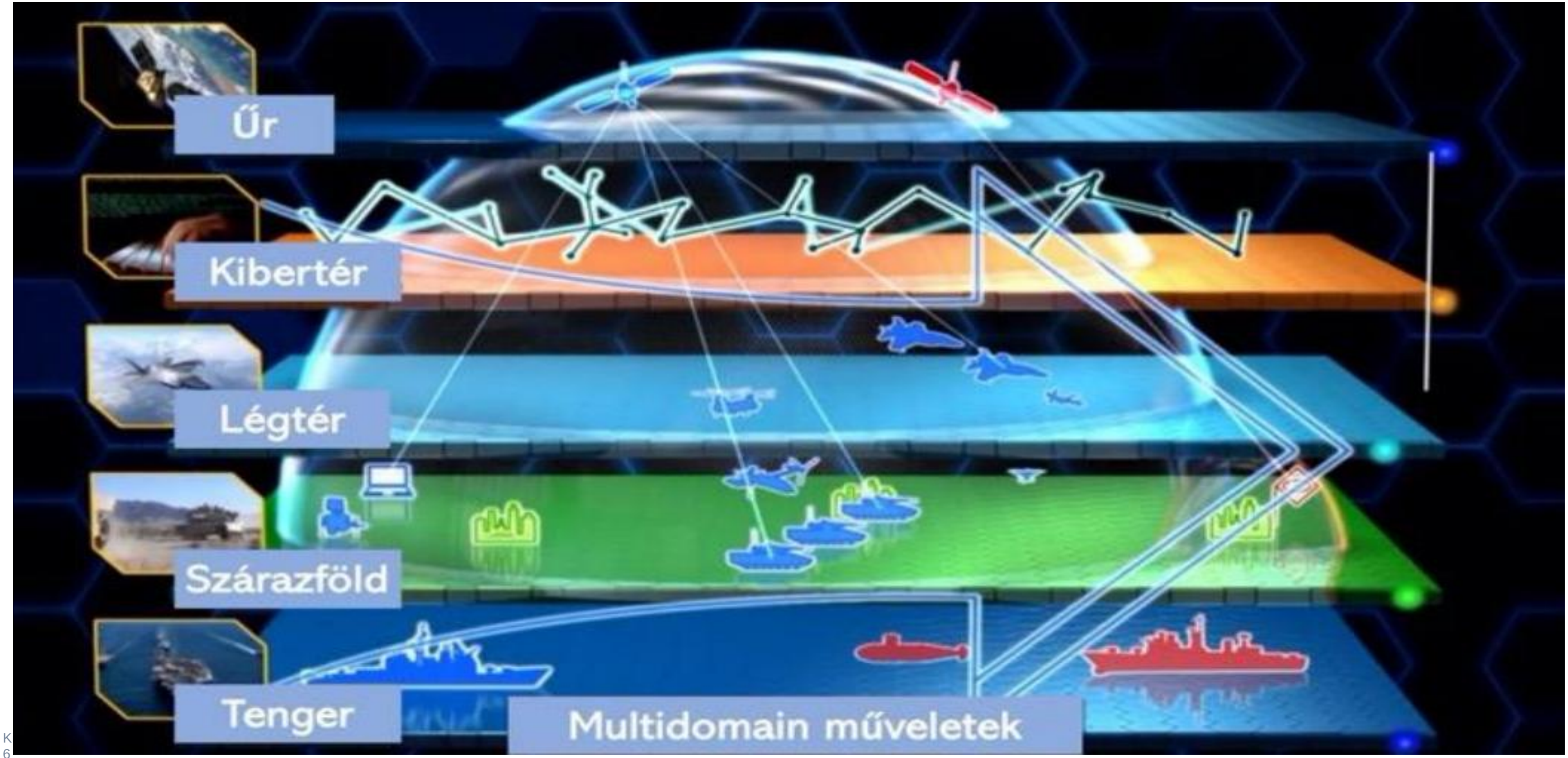
Planning, organizing, leading and controlling of the infocommunication requirements and resources at Hungarian site. Determine current and future local ICT needs by consulting with management and employees at a ...see more

Személyes, nem szakértői előadás…

Tartalomjegyzék

Kiberhadviselés | Bevezetés

Információs és digitális társadalom, geopolitika, hadszínterek bővülése

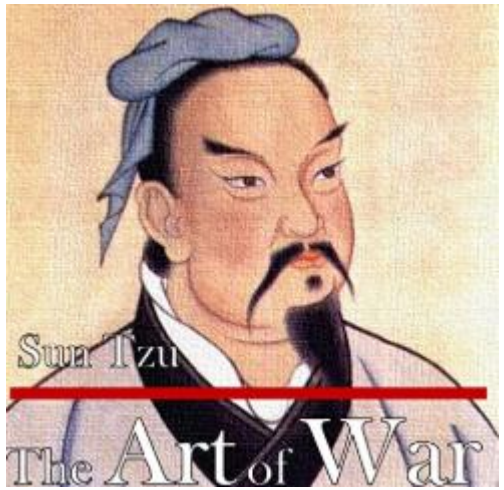


Kiberhadviselés | Bevezetés

A háború művészete

Szun-Ce – A háború művészete (*The Art of War*)

- A hadviselés egészében a megtévesztésre épül.
- Ismerd meg az ellenséged és önmagad, és száz csatát vívhatsz meg vereség nélkül.
- A legnagyobb győzelem az, amely harc nélkül győz.



Az **ellenség megtévesztése**, a **stratégiai fölény**, és a **gyengeségek kihasználása** – a **kiberhadviselés** világában is rendkívül aktuálisak.

Lehet-e egy háborút megvívni úgy, hogy egyetlen lövés sem dördül el?

Tartalomjegyzék

Kiberhadviselés | Alapfogalmak tisztázása

A kibertér, digitális tér építőkockái: jel, adat és információ

A kibertérben megtalálható számítógépek adatokkal dolgoznak, és feladatuk az adatok feldolgozása, továbbítása, tárolása és visszanyerése.

Jel – A jel valamely fizikai mennyiség értéke vagy értékváltozása. A folytonos, az ún. **analóg** jel, a másik a diszkrét, úgynevezett **digitális** jel. A digitális jel értékei diszkrétek, csak meghatározott értékeket vehet fel.

Kód – a kód jelek (szimbólumok) sorozata, mellyel valamely információ egyértelműen megadható.

Adat – Minden adat kódolt formában van jelen. Az adat valamilyen jelrendszerben ábrázolt jelek vagy elemi jelek sorozata.

Információ – Az információ értelmezett adat. Az információ új ismeret, új tudás. Az információ olyan új ismeret, amely megszerzője számára szükséges.

Tudás – feldolgozott és tapasztalatba ágyazott információ, amely alapján döntés születhet.

Kommunikáció – két felet feltételez, amelyek közösen kialakított csatornán kommunikálnak egymással.

Mi az elküldött adatok jelentése, milyen információt közöltem?

Kiberhadviselés | Alapfogalmak tisztázása

Kiberbiztonság, információbiztonság

Kiberbiztonság (Cybersecurity) – Az információs, digitális rendszerek és adatok védelme a jogosulatlan hozzáférés, módosítás, károkozás vagy megzavarás ellen.

Sérülékenység (Vulnerability) – A rendszer olyan gyengesége, amelyet kihasználva a támadó kárt okozhat vagy hozzáférhet az erőforrásokhoz.

Kitettség (Exposure) – Az a mérték, amennyire a rendszer vagy az eszköz ki van téve fenyegetéseknek.

Kihasználás (Exploitation) – amikor a támadás, támadó ténylegesen kihasználja a sérülékenységet.

Fenyegetés (Threat) – Olyan potenciális esemény vagy szándékos cselekedet, amely károsíthatja az informatikai rendszert vagy az adatok bizalmasságát, sértetlenségét, rendelkezésre (CIA triad) állását. Például: egy ismert hacker csoport, aki bizonyos típusú rendszereket céloz.

Támadás (Attack) – az a konkrét cselekmény, amikor ez a csoport megpróbál betörni.

Incidens (Incident) – az a helyzet, amikor a támadás elindul, sikerrel jár és káros (adverse) esemény keletkezik.

Támadó (Threat Actor) – Egyén, csoport vagy szervezet, amely képes és hajlandó végrehajtani a támadást.

Kiberhadviselés | Alapfogalmak tisztázása

A kiber- és kognitív tér kapcsolata

Kibertér – számítógép-rendszerek és -hálózatok által alkotott metaforikus tér, amelyben elektronikus adatok tárolódnak és online adatforgalom, valamint kommunikáció zajlik.

Kognitív tér – az emberi elme által létrehozott mentális reprezentációk összessége (emlékképek, vélemények, meggyőződések), amelyben az információk értelmezése, összekapcsolása és új ismeretek létrehozása zajlik.

Kiber hadszíntér – a kibertér azon része, ahol technikai eszközökkel (pl. vírusok, hackertámadások, hálózati műveletek) hajtanak végre katonai operatív, taktikai és/vagy stratégiai célú beavatkozásokat. Ez lehet például infrastruktúrák megbénítása vagy információs rendszerek manipulálása.

Kognitív hadszíntér – A kiberhadviselés azon dimenziója, amely az emberek gondolkodásának, észlelésének, véleményének és döntéseinek befolyásolását célozza, például manipulált információval, pszichológiai műveletekkel, vagy dezinformációval a közösségi médiákon keresztül.

Kiberhadviselés | Alapfogalmak tisztázása

Műveleti szintek és célok, Kiberfegyver

Kiberhadművelet (Cyber Operations) – minden olyan tevékenység, amely a kibertérben zajlik katonai, hírszerzési vagy stratégiai céllal. A művelet lehet: Kiberfelderítés, Kibertámadás, Kiberzavaraás, Információs befolyásolás, Védelmi műveletek.

Típus	Leírás	Módszerek	Példák
Kiberfelderítés Cyber Reconnaissance	Titkos adatok vagy rendszerek feltérképezése és megszerzése.	Spear phishing, hátsó ajtók, jogosultságszint-emelés OSINT (Open Source Intelligence) – nyílt forrásból származó adatok gyűjtése SIGINT (Signals Intelligence) – elektronikus kommunikáció lehallgatása HUMINT (Human Intelligence) – emberi forrásokon keresztüli gyűjtés Malware alapú felderítés – APT csoportok által használt eszközök (pl. Turla, APT29)	APT10, APT29 – kormányzati és vállalati célpontok ellen
Kibertámadás Cyber Attack	Információs rendszerek szándékos megrongálása vagy zavarása.	Malware, DDoS, ransomware, zsarolóvírus	Stuxnet (2010), BlackEnergy (2015), NotPetya (2017)
Kiberzavarás Cyber Denial	Digitális szolgáltatások működésének megzavarása.	DDoS támadások, spam, szoftverhibák kihasználása	Észtország (2007), Anonymous támadások
Kiberbefolyásolás Cyber Influence	Felhasználók véleményének vagy viselkedésének manipulálása digitális térben.	Social media kampányok, deepfake, dezinformáció PSYOPS / PhyOps (Psychological Operations) – félelemkeltés, zavarás Dezinformáció – hamis hírek, deepfake-ek terjesztése Social Engineering – célzott manipuláció emberi szereplőkön keresztül	USA választások 2016 (APT28), deepfake kampányok
Kiberkémkedés Cyber Surveillance	Folyamatos megfigyelés és adatgyűjtés, gyakran jogosulatlanul.	Keylogger, spyware, hálózati sniffing	Pegasus kémszoftver használata
Kiberelhárítás Cyber Defense	Ellenséges kiberműveletek visszaverése vagy megelőzése.	Threat hunting, attribution, exploit blokkolás Incident Response Active Defense (csapdák, honeypotok, deception technikák) Attribution (támadók azonosítása) Hack-back / Counterstrike (megtorlás, jogi vagy technikai úton)	USA vs. APT33 (iráni szerverek lekapcsolása)

Tartalomjegyzék

Kiberhadviselés | Információs hadviselés történeti áttekintése

Ókor

Szun-ce (Sun Tzu) – A háború művészete (~Kr. e. 5. század): az első rendszeresített hadtudományi mű, amely kiemeli a megtévesztés, kémkedés és pszichológiai hadviselés szerepét.

Kémkedés és **megtévesztés módszereinek alkalmazása már** Mezopotámiában, Egyiptomban és Görögországban is ismert volt. **Trójai faló** – dezinformációs hadviselés mitológiai példája. Egy Malware típus napjainkban.

Zhuge Liang (Három Királyság kora):

- Meghamisított hadijelentések, tábortüzek: az ellenség félrevezetése célzott dezinformációval.
- Üres erőd stratégiája: pszichológiai manipuláció – erődemonstráció látszata valójában gyengeség elfedésére.

Kiberhadviselés | Információs hadviselés történeti áttekintése

Középkor

Hírvivők elfogása, **félrevezető üzenetek** küldése.

Hamis zászlók alatt indított támadások, megtévesztő katonai jelzések alkalmazása.

Kémkedés – Anonymus: Gesta Hungarorum

- A **honfoglalás során** a magyarok gyakran **küldtek** előőrsöket és **felderítőket** a Kárpát-medencébe, hogy **pontos információkat szerezzenek** a helyi népek elhelyezkedéséről és védelméről (HUMINT).
- Álmos és Árpád népei már a Duna-Tisza közére történő bevonulás előtt kémeket (HUMINT) küldtek, hogy felmérjék a morva és bolgár ellenállást.

Megtévesztés és Pszichológiai hadviselés – Hunyadi János, nándorfehérvári diadal

- Hunyadi János alkalmazott olyan megtévesztő taktikákat, amelyekkel azt a látszatot keltette, hogy serege sokkal nagyobb és jobban felszerelt, mint valójában volt.
- Emellett Kapisztrán János vezette a paraszthadak morális buzdítását – amely pszichológiai hatást gyakorolt a török seregre (PHYOPS), mint propagandaelem.

Kiberhadviselés | Információs hadviselés történeti áttekintése

Modern kor

Krími háború (1853–56) – az első háború, ahol távírót használtak stratégiai katonai kommunikációra a brit haderők. A londoni The Times olyan pontos katonai információkat közölt az eseményekről, hogy ezáltal az orosz hadvezetés lényeges előnyökhöz (OSINT) jutott.

Titkosított Zimmermann-távirat (1917) – egy német diplomáciai üzenet volt. A brit hírszerzés legnagyobb első világháborús sikerének tartják a kódolt üzenet feltörését, és az egyik első olyan esetnek, amikor egy jelhírszerzési információ (SIGINT) világtörténelmi eseményre volt hatással.

Enigma feltörése (1942) – a brit Bletchley Parkban Alan Turing vezetésével sikerült feltörni a német haditengerészet Enigma-kódját (SIGINT), mely kulcsfontosságú volt az Atlanti-csata megfordításához.

Röplapot ledobása (1943-1945) - Németország felett, amelyekben a Wehrmacht katonáit a megadásra (PSYOPS) bíztatták.

Kubai rakétaválság (1962): Az amerikai U-2 felderítő gépek által készített képeken észlelték a Szovjetunió rakétaállásait Kubában. (IMINT)

Kiberhadviselés | Információs hadviselés történeti áttekintése

Jelen kor

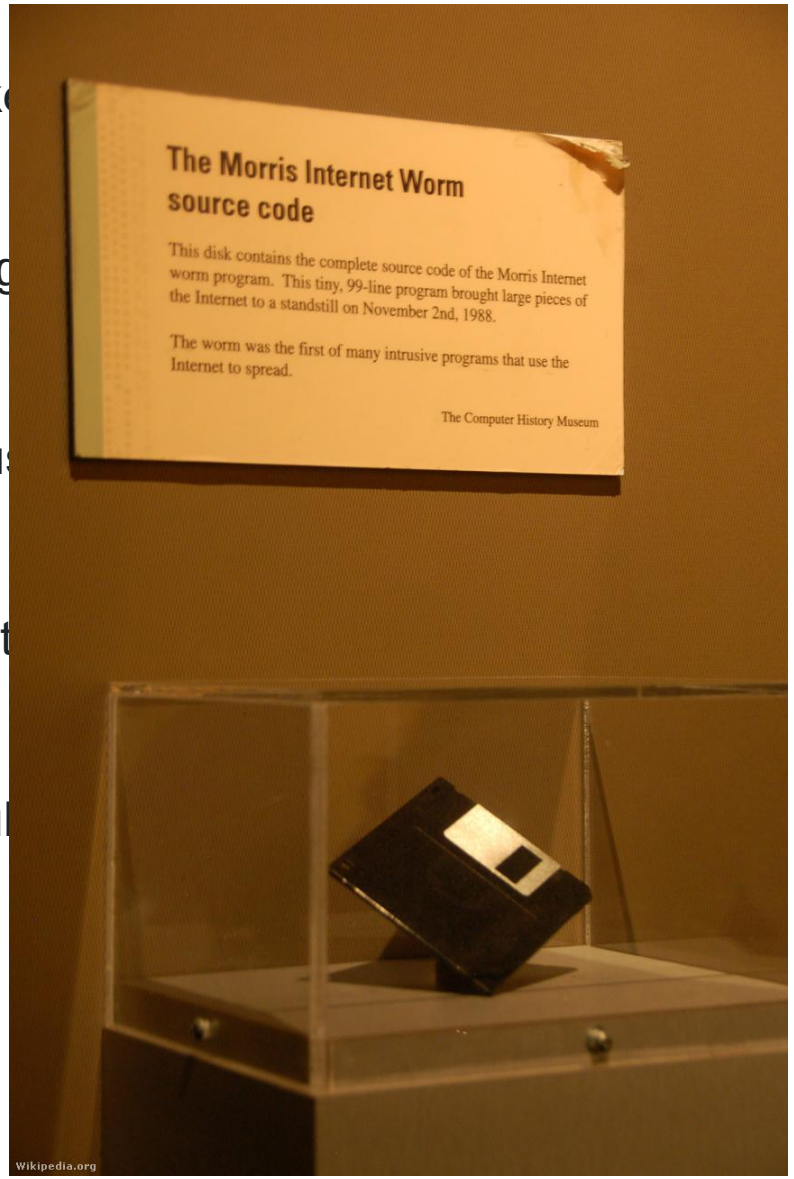
Öbölháború (1991) – műholdképeket használtak az iraki csapatok és bunk
precíziós bombázásokhoz (IMINT).

Elk Cloner (1982), **Morris Worm** (1988), első vírusok, férgek (worm) – még

Stuxnet (2010) – Az USA és Izrael által fejlesztett féreg, amely iráni urándú
szabotáolta. Az első ismert kiberfegyver.

SolarWinds (2020): Az orosz APT29-hez (Cozy Bear) köthető ellátási lánc t
kormányzati és vállalati rendszerekbe hatoltak be.

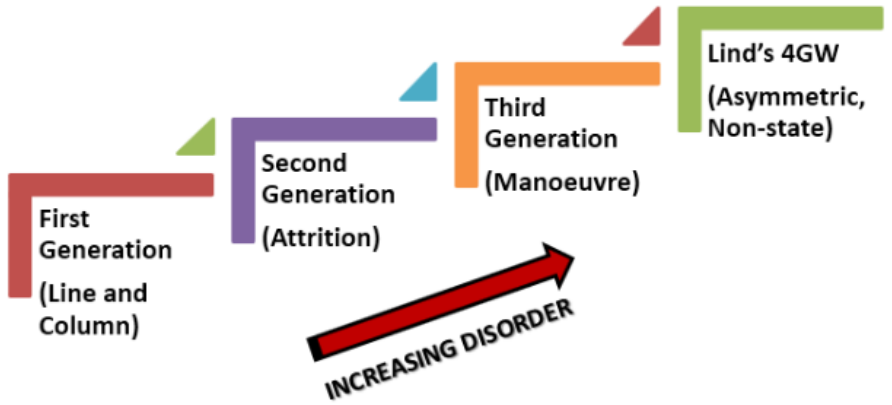
Microsoft Exchange támadás (2023): Storm-0558 APT-csoport titkosítóku
kompromittálta kormányzati emailfiókokat.



Kiberhadviselés | Információs hadviselés történeti áttekintése

Hadviselés generációs elmélete

Generáció	Időszak	Kulcsjellemzők	Megjegyzés	Példa
1. generáció	17–19. század	Vonalas hadviselés, sorkatonaság, puska, ágyú	Állandó hadseregek megjelenése, vesztfáliai rendszer után	Napóleoni háborúk (1803–1815)
2. generáció	19. sz. vége – I. vh	Tüzérség, géppuska, árkok, tűzerődominancia	Modern ipari háború kezdete	I. világháború
3. generáció	I. vh vége – II. vh	Harckocsik, repülők, rádió és gyors manőverek. A cél a meglepetés és áttörés a mélyben.	A német Blitzkrieg volt a modell. Az ellenség döntéshozatalának megbénítása vált fő céllá.	II. világháború – német villámháború (Blitzkrieg)
4. generáció	1970-es évektől	Aszimmetrikus, gerilla, médiahadviselés. Társadalmi támogatottság kulcsfontosságú.	A háború nem kizárólag államok hadseregei között zajlik, hanem államok és nem állami szereplők – például gerillacsoportok, terrorhálózatok – között is. A hadszíntér kiterjed a civil társadalomra, a médiára és a lakosságra is.	2001. szeptember 11. – besorolás és jelentőség Elkövető: Al-Káida – nem állami szereplő Cél: Pszichológiai és politikai hatás, félelemkeltés, amerikai stratégiai jelenlét visszaszorítása
5. generáció	2010-től (vitatott)	Multidomain hadviselés: föld, víz, levegő: + űr, kibertér, információs tér, kognitív tér Klasszikus kinetikus haderő + drónok, különleges erők, műholdas fegyverek	Nincs még egységes katonai konszenzus Minden korábbi hadszíntér megmaradt, csak kiegészült és összeolvadt velük	Orosz–ukrán háború (2014-től, főként 2022 után) Nincs még egységes katonai konszenzus



Tartalomjegyzék

Kiberhadviselés | Kiberháborús incidensek – esettanulmányok

Legjelentősebb globális kibertámadások 1999–2025 között

Év	Esemény	Leírás	Elkövető	Katonai / Hibrid jelleg
1999	Moonlight Maze	Amerikai kormányzati rendszereket ért kiberbeszivárgás, mely hónapokon át tartott. A támadás célja érzékeny katonai és tudományos adatok megszerzése volt.	Orosz Állami Hírszerzés, SVR háttér gyanú	Katonai hírszerzés
2007	Észtország elleni DDoS	Tömeges DDoS támadások bénították meg Észtország kormányzati, médiabeli és banki online rendszereit. A támadások egy szovjet emlékmű eltávolítását követően történtek, politikai feszültséget tükrözve.	Orosz nacionalista hackerek, GRU háttér gyanú	Hibrid hadviselés
2008	Grúzia elleni kibertámadás	Az orosz hadsereg grúziai katonai műveleteit kísérő kibertámadások célpontjai állami és média weboldalak voltak. A cél a kommunikáció megzavarása és a pánikkeltés volt.	Orosz GRU és szövetséges hackerek	Katonai művelet része
2010	**Stuxnet**	**A Stuxnet nevű kártevő célzottan az iráni Natanz urándúsító létesítmény ellen irányult. Fizikai károkat okozott az ipari vezérlőrendszerek manipulálásával, megelőzve katonai beavatkozást.**	**USA (NSA) és Izrael (Unit 8200)**	**Katonai kiberfegyver**
2014	Sony Pictures hack	A támadás során az Észak-Koreához köthető Lazarus Group érzékeny adatokat szivárogtatott ki a Sony Pictures rendszeréből. A támadás válasz volt a rezsimellenes filmre.	Észak-Korea (Lazarus Group)	Állami kibertámadás
2015	BlackEnergy – Ukrajnai áramszünet	Az orosz Sandworm csoport malware-t használt az ukrán áramszolgáltatók rendszereinek megbénítására. Ez volt az első sikeres, fizikai következményekkel járó kibertámadás energiahálózat ellen.	Orosz GRU (Sandworm csoport)	Hibrid hadviselés, katonai fegyver
2016	DNC Hack – Guccifer 2.0	Az amerikai Demokrata Párt szervereit feltörték, és belső email-kommunikációt szivárogtattak ki. A támadás célja a 2016-os választások befolyásolása volt, politikai zavart keltve.	Orosz GRU (Fancy Bear/APT28)	Hibrid információs hadviselés
2017	**NotPetya**	**A NotPetya nevű malware Ukrajna ellen indult, de globálisan okozott milliárdos károkat. A kártevő wiper funkcióval rendelkezett, célja az infrastruktúra megsemmisítése volt.**	**Orosz GRU (Sandworm)**	**Hibrid hadviselés, Katonai kiberfegyver**
2019	USA vs APT33	Irán APT33 csoportja amerikai katonai és ipari célpontokat támadott, amire válaszul az USA kiberellentámadást indított. Ez kétoldalú kiberműveleti spirál része volt.	APT33 (Irán) / USCYBERCOM (USA)	Kétoldalú katonai kiberműveletek
2020	**SolarWinds / Sunburst**	**Az orosz SVR által végrehajtott támadás során a SolarWinds szoftverfrissítési rendszerét használták ki, így kormányzati és céges hálózatokba jutottak be hónapokra titokban.**	**Orosz SVR (Cozy Bear / APT29)**	**Állami hírszerzés**
2022	**Ukrajnai kibertámadások (HermeticWiper, Viasat, DDoS)**	**A 2022-es orosz invázió részeként Ukrajnát kiterjedt kibertámadások érték, köztük törlőprogramok, műholdas zavarás és dezinformáció. A cél az ellenállás gyengítése és a koordináció akadályozása.**	**Orosz GRU (Sandworm, APT28, UNC2589)**	**Multidomain katonai művelet – kiberkomponens**
2023	Storm-0558 – Microsoft támadás	A kínai Storm-0558 APT-csoport titkosítókulcs megszerzésével kompromittálta kormányzati emailfiókokat. A támadás kifinomult technikai módszerekkel történt és hónapokig észrevétlen maradt.	Kína (APT – Storm-0558)	Katonai hírszerzés
2025	CyberAvia támadás – ukrán légiközlekedés megbénítása	Az orosz GRU-hoz köthető támadás célba vette Ukrajna légiközlekedési és irányító infrastruktúráját. A támadás zavart keltett a katonai utánpótlásban és polgári forgalomban is.	Orosz GRU (Sandworm csoport gyanúja)	Multidomain katonai művelet – kiberkomponens

Kiberhadviselés | Kiberháborús incidensek – esettanulmányok

Legjelentősebb Orosz-Ukrán kibertámadások, kiemelten a háború éveiben

Év	Esemény	Leírás	Elkövető	Jelleg
2014	Telebots / BlackEnergy előkészítés	A Krím félsziget annektálását követően indultak célzott kiberműveletek ukrán állami célpontok ellen. Ezek hírszerzési célt szolgáltak és megalapozták a későbbi, destruktívabb támadásokat.	GRU (Sandworm)	Felderítés, destabilizáció
2015	Ukrán áramszünet – BlackEnergy	Több mint 230 000 ukrán maradt áram nélkül, amikor a támadók ICS rendszereket manipuláltak. Ez volt az első ismert sikeres kibertámadás egy elektromos hálózat ellen.	GRU (Sandworm)	Kritikus infrastruktúra elleni támadás
2016	Industroyer / CrashOverride	Az Industroyer malware célzottan támadta Ukrajna energiahálózatát, új típusú ipari protokollokat kihasználva. A támadás fejlettebb volt, mint a 2015-ös, de kisebb hatású.	GRU (Sandworm)	ICS rendszerek célzása
2017	NotPetya	A NotPetya malware adatok helyreállíthatatlan törlésére készült, de zsarolóvírusnak álcázták. Elsődleges célpont Ukrajna volt, de globálisan is milliárdos károkat okozott.	GRU (Sandworm)	Pusztító logisztikai támadás
2022	HermeticWiper	A HermeticWiper nevű törlőprogrammal több ukrán minisztériumot és pénzügyi intézményt támadtak meg az invázió előestéjén. A cél az állami működés megbénítása volt.	GRU / UNC2589	Invázió előkészítése – IT infrastruktúra
2022	Viasat műhold elleni támadás	A KA-SAT műholdas internetes hálózatot támadták meg, lekapcsolva katonai és polgári kommunikációs csatornákat. A támadás a szárazföldi inváziához volt időzítve.	GRU (Sandworm)	Multidomain támadás
2022	WhisperGate, CaddyWiper stb.	Többféle wiper és támadó kódot vetettek be az orosz oldalon. Ezek célja a zavarkeltés, adatok megsemmisítése és a védekezés megbénítása volt.	GRU / APT28 / UNC2589	Tömeges romboló támadások
2022	Killnet és Xaknet DDoS hullám	Oroszbarát hacktivisták túlterheléses támadásokat indítottak ukrán banki és állami oldalak ellen. A cél pszichológiai nyomásgyakorlás és dezinformáció volt.	Oroszbarát hacktivisták	Információs művelet
2023	FakeApp / frissítéses kampányok	Ukrán felhasználókat hamis szoftverfrissítésekre vettek rá, amelyek valójában kártevők voltak. A cél a rendszerekbe való bejutás és adatlopás volt.	APT29 + civil támogató hálózat	Kémkedés, hozzáférésszerzés
2025	CyberAvia – légiforgalom zavarása	A CyberAvia támadás során a repülésirányítási rendszerek megbénítása történt, több órára leállítva a forgalmat. A cél a logisztika és katonai mozgások zavarása volt.	GRU (Sandworm – feltételezett)	Multidomain katonai művelet

Kiberhadviselés | Kiberháborús incidensek – esettanulmányok

Stuxnet - 2010

Típus: Katonai kiberfegyver (célzott ipari kártevő)

Célpont: Irán, natanzi urándúsító létesítmény

Elkövető: Feltehetően USA és Izrael (Operation Olympic Games)

Főbb jellemzők:

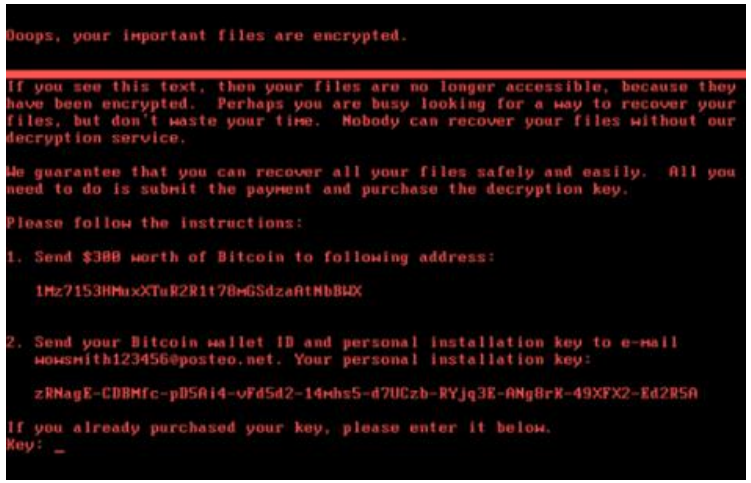
- Először azonosított, fizikailag romboló malware
- Négy 0-day sérülékenységet használt
- Terjedt USB-n és hálózaton
- Megfertőzte a Siemens SCADA rendszereket
- Centrifugák meghibásodását idézte elő anélkül, hogy a kezelők észrevették volna

Jelentősége:

- Mérföldkő a kiberműveletek történetében
- Ipari vezérlőrendszerek (ICS/SCADA) sebezhetőségének nyilvánvalóvá tétele
- Kiberháborús precedens: célzott, államilag támogatott művelet

Kiberhadviselés | Kiberháborús incidensek – esettanulmányok

NotPetya - 2017



Típus: Katonai kiberfegyver
Zsarolóvírusnak álcázott wiper (megsemmisítő malware)

Célpont: Elsődlegesen Ukrajna, de globálisan is elterjedt

Elkövető: Feltételezhetően orosz GRU (APT28)

Főbb jellemzők:

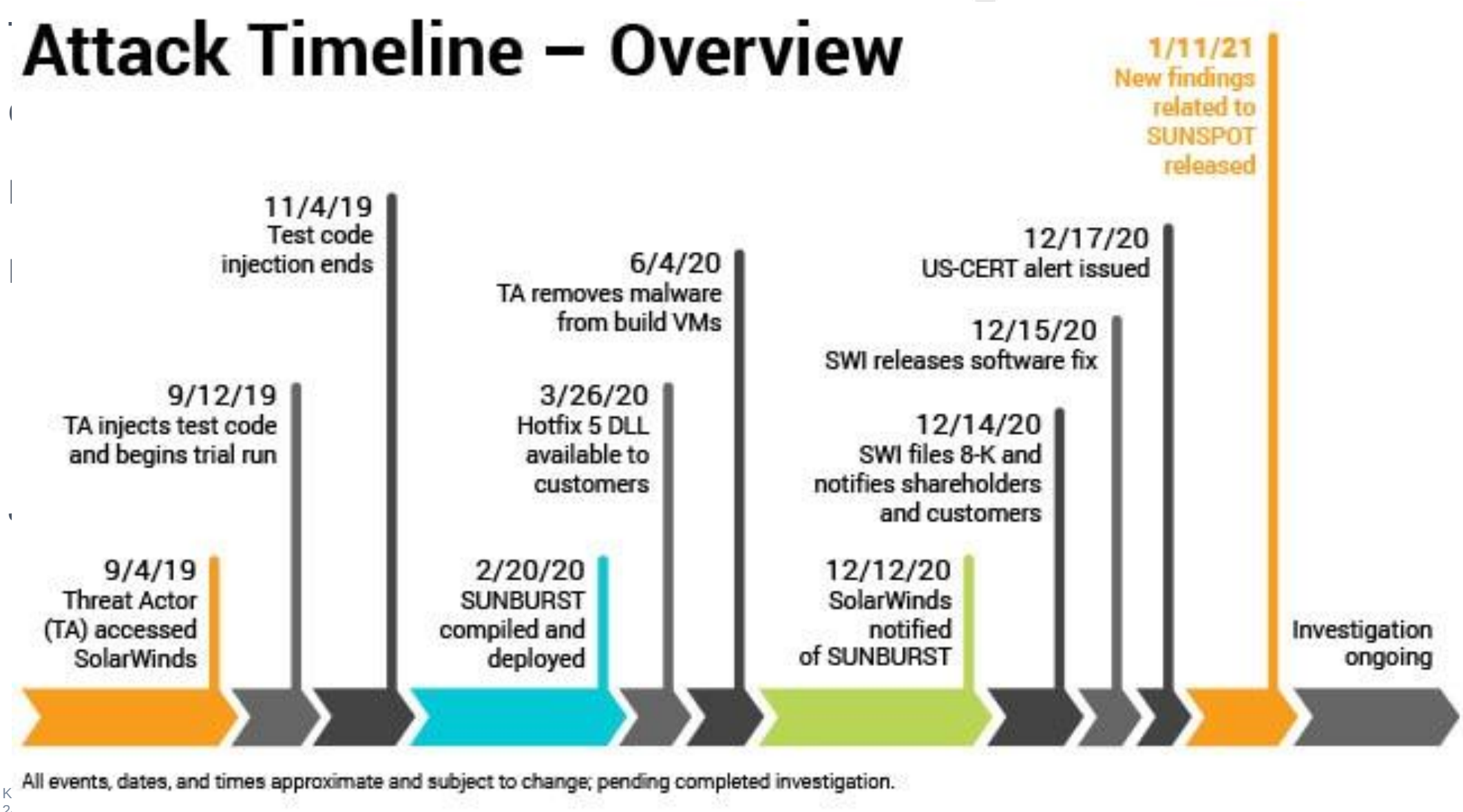
- M.E.Doc ukrán könyvelőszoftveren keresztül terjedt
- SMB-vulnerabilitásokat használt (EternalBlue, EternalRomance)
- Adatokat titkosított, de a visszafejtés lehetetlen volt – célja nem pénzszerzés
- Nagyvállalatok is érintettek: Maersk, Merck, FedEx, Rosneft

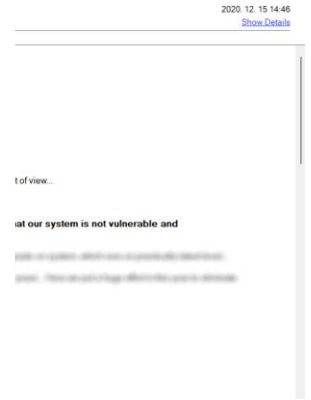
Jelentősége:

- Gazdasági károk >10 milliárd USD
- Példa a kiberháborús eszközként bevetett, félrevezető malware-re
- Hibrid hadviselés egyik tipikus példája

Kiberhadviselés | Kiberháborús incidensek – esettanulmányok

Sunburst (SolarWinds supply chain támadás, 2020)





Kiberhadviselés | Kiberháborús incidensek – esettanulmányok

Viasat KA-SAT műhold elleni támadás - 2022

Típus: Katonai kiberfegyver
Műholdas kommunikáció elleni fizikai hatású kibertámadás

Célpont: KA-SAT műholdi hálózat (Viasat), Ukrajnában és Európában

Elkövető: Feltételezhetően orosz GRU

Főbb jellemzők:

- Az invázió első napján történt (2022. febr. 24.) – Gen5 Warfare
- Támadók a műholdmodemek firmware-jét módosították
- Következmény: több ezer modem offline állapotba került
- Hatás: ukrán haderő kommunikációja is megbénult

Jelentősége:

- Klasszikus multi-domain műveletként is értelmezhető, különösen, ha az űr- és kibertér integrációját, valamint a földi katonai műveletek támogatását is figyelembe vesszük.
- Polgári szolgáltatások is leálltak (pl. szélessáv az EU-ban)
- NATO és EU is vizsgálta, mint potenciálisan 5. cikkely alá tartozó aktust

Kiberhadviselés | Kiberháborús incidensek – esettanulmányok

Összefoglalás

A várt kiber-armageddon elmaradt

- Sokan teljes kiberkáoszra számítottak (pl. elektromos hálózatok, pénzügyi rendszer összeomlása)
- Teljeskörű multidomain hadszíntér helyett: taktikai, célzott kibertámadások domináltak
- Digitális Mohács

Jelentős kiberműveletek mégis történtek

- **KA-SAT támadás** (Viasat, 2022. febr. 24.):
- Egyéb támadások: wiper malware-ek (HermeticWiper, CaddyWiper), DDoS az ukrán kormány ellen

Információs, kognitív hadszíntéren aktív műveltek

- Aktív orosz dezinformációs kampányok:
  - Ukrajnai veszteségek eltagadása vagy eltúlzása
  - Hamis narratívák terjesztése a NATO-ról, „biolaborokról”
- Veszteségek Friss „hivatalos” adat (2024 vége):
  - Orosz / Ukrán kommunikáció: 30 – 40 ezer fő
  - USA becslés: Orosz: 120–150 ezer fő, ukrán: 70–100 ezer fő

Tartalomjegyzék

Kiberhadviselés | Kitekintés: A jövő kiberháborúja

Mesterséges intelligencia katonai alkalmazása

Felderítés, adatfeldolgozás

Döntéselőkészítés

- Cselekvési változatok súlyozása

War gaming/hadijáték

Személyzet/kezelő nélküli járművek

- felderítés, információszerzés, megfigyelés
- logisztika
- harc/fegyver platform

Kiképzés, felkészítés, szimuláció (eseményvezérlés)

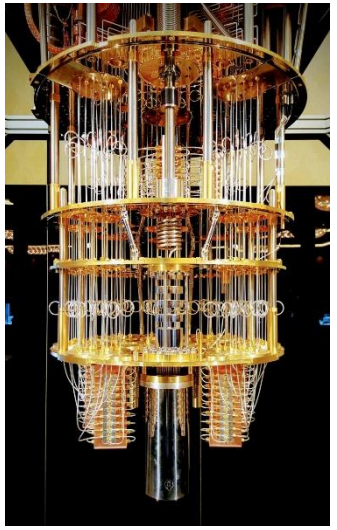
- Nagy adatmennyiség (öntanuló) feldolgozása
- Cyber Threat Intelligence (CTI)
- Indicator of Compromise (IoC)
- Course of Actions (CoA)

Halálos autonóm fegyverrendszerek (LAWS – Lethal Autonomous Weapon Systems)

- célpontok azonosítása és támadása emberi beavatkozás nélkül
- drónrajok autonóm szárazföldi egységek, robotplatformok
- etikai, jogi és katonai kockázatok („ember a döntési láncban?” kérdés)

Kiberhadviselés | Kitekintés: A jövő kiberháborúja

Kvantum technológia, kvatumszámítógép



Új architektúra, algoritmusok, gyors számítási kapacitás

Poszt-kvantum kriptográfia (PQC)

- A kvantumszámítógépek (pl. a Shor-algoritmus révén) képesek lehetnek pár perc alatt feltörni a mai elterjedt titkosításokat (pl. RSA, ECC).
- Új típusú titkosítási módszerekre lesz szükség (már most folynak a NIST versenyek a szabványosításra).

Kvantumkommunikáció (QKD – Quantum Key Distribution)

- Cél a lehallgathatatlan kommunikáció kvantumállapotokon keresztül (pl. fotonok polarizációja)
- Toshiba Quantum: QKD & Quantum Security Solutions

Kvantumradar

- Elméleti technológia, amely alacsony észlelhetőséggel képes objektumokat detektálni, pl. lopakodó repülőgépeket vagy tengeralattjárókat.

Következtetések

- **A 21. század a kiberhadviselés kora**
- **Kinetikus támadások maradnak a központban multi-domain műveletekkel**
- Új és régi rendszerelemek egyidejű használata
- A háború tapasztalatai: az energiaszektor az elsődleges célpont
- Fizikai védelem vs. Kibervédelem
- Veszély-előrejelzés (CTI)
- Kihívások: MI és QC
- Oktatás, képzés, felkészítés, tudatosság
- Katonai képességek fejlesztése
- Nemzetközi együttműködés

Köszönöm a figyelmet!

K&V*

*: *Maple, beszéljük meg!*