BODA JÓZSEF

A KIBERTÉR BIZTONSÁGA

„A bűnös szándékú próbálkozásokat nem lehet elkerülni, de azokra fel kell készülni!”
Craig Bowlus[1]

1. Bevezetés

Ez a rövid tanulmány nem arról szól, hogyan és milyen programot, appot (alkalmazás) kell telepíteni a tökéletes biztonság érdekében, mert ilyen nem létezik! A valódi biztonságot, az eszközök biztonságtudatos használata jelenti! Mai infokommunikációs világunkban a biztonság a felhasználó tudásán és felkészültségén múlik! Milyen fenyegetésekkel nézünk szembe, és mit tehetünk?

- a személyi számítógépek és honlapok feltörése,
- a vírusok megjelenése és működése az elektronikus eszközökön,
- az adataink ellopása,
- pénzünk ellopása egy távoli számítógéppel,
- a vírusirtók tűzfalak, APP-ok hatékonysága,
- zsarolások az elektronikus eszközökről ellopott fájlokkal,
- a kiberbűnözők eszközei,
- az elektronikus eszközök védelmének lehetőségei,[2]
- a mesterséges intelligencia fejlődésének hatásai.

Mielőtt ezekre a kérdésekre megpróbálom megtalálni a válaszokat, az előtt tisztázni szükséges a témával kapcsolatos alapvető fogalmakat.

1.1. Kibertér

Globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint az e rendszereken keresztül - adatok és információk- formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. A kibertér egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit beleértve az internetet, a távközlési hálózatokat, számítógépes rendszereket, beágyazott processzorokat és vezérlőket, a rajtuk áramló digitális információkat, valamint az ezen információkkal, információs rendszerekkel kölcsönhatásban lépő felhasználókat.[3] A szót William Gibson (amerikai- kanadai) sci-fi szerző alkotta meg, az 1982-ben megjelent Burning Chrome (Égő króm) c. novellájában!

---

[1] Craig Bowlus a dublini székhelyű Aon kockázatmegosztásért felelős ügyvezető igazgatója.
[2] A kibertér biztonsága - avagy vírusok, hackerek, feltört honlapok és Ön : uwsnet.eu (Letöltés ideje: 2023.05.08.)
[3] Rendészettudományi Szaklexikon. Dialóg Campus Kiadó. Budapest, 2019. 316. o.

„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”[4]

1.2. Kiberbiztonság

A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási ismeretek, tudatosságnövelés, valamint a technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a létező kockázatok elfogadható szintjét biztosítva megbízható környezetté alakítják a kiberteret, és akként tartják fenn a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.[5] A kiberbiztonság a kibertérben létezõ kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelõ, valamint technikai eszközök folyamatos és tervszerû alkalmazása, amelyek a kibertérben létezõ kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan mûködéséhez és mûködtetéséhez.[6]

1.3. Biztonság

A többtényezős, komplexfogalom, amely az *állam* és társadalom érdekeinek, az ország területének és lakosságának külső és belső veszélyektől fenyegetéstől mentes állapotát fejezi ki. A létezés és a működés káros befolyásoló hatásaitól és a veszélytényezőktől kellően mentesített, védett állapot. A kellően szükséges *védelem* azt jelenti, hogy a fenyegetéseknek megfelelően ki lettek dolgozva az adminisztratív védelem követelményei és protokolljai, amelynek alapján a rezsimintézkedéseket kiadták, az emberi erőforrásokat felkészítették, rendelkezésre állnak és hatékonyan működnek a szükséges védelmi technológiák és eszközök. A kellő védelem megteremtéséhez szükséges folyamatos környezeti adatgyűjtéssel és *kockázatelemzéssel* a *fenyegetéseket*, veszélyforrásokat azonosítani, a megelőzéshez, a fenyegetés időbeni felismeréséhez és elhárításához, a bekövetkezett *biztonsági esemény* kezeléséhez a szükséges ismereteket, és tapasztalatokat begyűjteni.[7]

1.4. Mesterséges intelligencia (MI)

Gép, program, mesterségesen létrehozott tudat által képviselt, az emberi gondolkodás, tanulás, reagálás reprodukálására törekvő intelligencia. Informatikai téren a számítástudománynak az a területe, amely emberi intelligenciát igénylő feladatokat megoldó számítógépes programok készítésével foglalkozik.[8]

[4] Magyarország Nemzeti Kiberbiztonsági Stratégiája. Magyar Közlöny 2013/47. 6339. o.
[5] Rendészettudományi Szaklexikon. i.m. 315. o
[6] Magyarország Nemzeti Kiberbiztonsági Stratégiája
[7] Rendészettudományi Szaklexikon. i.m. 66. o.
[8] Rendészettudományi Szaklexikon. i.m. 389. o

2. Rövid/vázlatos történeti áttekintés

Mint minden technikai újdonság, a számítástechnika is a katonai alkalmazás során jelentkezett először. Az angol titkosszolgálat Alan Turing matematikus vezetésével 1943-ban megépítteti a Colossust, ez szintén relés alapon épült fel, és a II. világháborús német katonai rejtjelezőkód megfejtését segíttette. 1949-ben jelent meg az EDVAC (Electronic Discrete Variable Automatic Computer, elektronikus diszkrét változós automata számítógép), amely Neumann János (1903–1957) magyar matematikus elvei alapján, az ő közreműködésével készült.

Az első kereskedelemben kapható számítógép az UNVAC I. 1951-ben került forgalomba, majd 1964-ben ismerkedhettünk meg az IBM 360-as általános használatú géppel. Az első hazai számítógép – amely még „jelfogós" rendszerű volt -, a MESZ-1 (1955) tervezése és megépítése Kozma László villamosmérnök (1902-1983) nevéhez fűződik, akinek munkássága a telefonközpontok területén is rendkívül jelentős.[9]

Az eszközök katonai alkalmazásának és fejlesztésének lehetőségei fontos szerepet töltöttek be mind a nyugati hadseregek, mind a Szovjetunió és a Varsói Szerződés csapatainál. Már 1970-ben a Zrínyi Katonai Kiadónál megjelent V. A. Bokarev. Kibernetika és Hadügy című könyve, amelynek talán legérdekesebb része „A fegyveres erők automatizálásának új szakasza és az automatizálás hatékonyságának kritériuma".

A nagy fordulat 1971-ben következett be, amikor John Blankenbaker megépítette az első személyi számítógépet a Kenbak I-t. 1975-ben Bill Gates és Paul Allen kifejlesztette az első magas szintű programozási nyelvet és megalapították a MICROSOFT nevű céget. A következő nagy fordulatot az 1989-es év hozza, amikor is az Apple bemutatta a régóta várt hordozható Macintosh-t. A Poqet az első zsebben hordozható MS-DOS operációs rendszerrel rendelkező számítógépével jelentkezett. A Grid pedig létrehozza a laptop számítógépet. Megjelentek az operációs rendszerek, szerverek. 1993-tól megkezdődött az internetcsomagok magánszemélyek részére történő árusítása, majd lehetővé vált az internetes böngészés, és a következő évtől megjelentek a játék-konzolok. Létrejött tehát egy globális információs hálózat a számítógépek összekapcsolásával. 1996-ban megjelent a kizárólag webes alapú, ingyenes levelezőrendszer, a Hotmail. 1997 a 3D gyorsítási képességgel rendelkező kártyák elterjedésének kezdete volt. 2010-től jelentek meg a felhőalapú számítástechnikai rendszerek, és azóta sincs megállás! Újabb és újabb alkalmazások, fejlesztések kerülnek alkalmazásra, katonai és polgári célokra egyaránt!

3. Milyen fenyegetésekkel nézünk szembe, és mit tehetünk?

3.1. A személyi számítógépek és honlapok feltörése

Napjainkra kialakult egy elkövetői réteg, melyet csak komputerunderground-nak neveznek. Steven Mizrach szerint a következő elkövetők sorolhatóak e kategóriába:

- Hackerek, crackerek (a crackerek annyiban különböznek a hackerektől, hogy jellemzően haszonszerzési célból törnek be védett rendszerekbe),
- Phreakek (telefonvonalakba, illetve rendszerekbe próbálnak technológiai eszközökkel bejutni),

[9] A számítástechnika története. Tények Könyve. Kézikönyvtár. Forrás: arcanum.com (Letöltés ideje: 2023.05.28.)

- Vírusírók (olyan személyek, akik olyan kódokat írnak, melyek megpróbálnak behatolni más rendszerekbe, s gyakran mellékhatásokat is produkálnak),
- Kalózozok (a crackerek közül váltak ki, szoftverek védelmi rendszereit feltörő személyek, akik e tört-szoftvereket terjesztik is),
- Cypherpunkok (olyan programokat terjesztenek, melyekkel bárki adatait erős kódolással láthatja el – nagy teljesítményű számítógépekkel is komoly feladat feltörni az ilyen erősen kódolt adatokat),
- Anarchisták (törvénysértő, vagy legalábbis morálisan kétes megítélésű információkat terjesztő személyek – pl.: bomba készítés stb. Anarchista a komputerundeground tekintetében olyan személy, aki minden olyan kísérletet, rendelkezést elutasít, amely akadályozná az információ szabad áramlását),
- Kiberpunk (általában a fentiek valamilyen kombinációja).

3.2. Adataink ellopása

A hackerek elsősorban azért igyekeznek ellopni a személyes adatainkat, mert azok segítségével bankszámlát nyithatnak, átutalásokat és online vásárlásokat végezhetnek a nevünkben. Ezekben az esetekben az áldozatok akkor szokták észrevenni a lopást, amikor megkapják a számlát. Általában egy mindenki által használt cég nevében kapjuk az üzeneteket, ami lehet a bank, a posta, a Netflix vagy egy kisebb telefonos szolgáltató.

Mi a teendő, ha valaki ellopja az adatainkat? Ha olyan kérést kapunk telefonon, e-mailen vagy üzenetben, amiben személyes, bizalmas vagy pénzügyi adatokat kérnek, akkor ne adjunk meg semmilyen adatot. Ha azonban már rákattintottunk arra a gyanús linkre, és megadtuk az adatainkat, akkor ezt érdemes jelenteni a rendőrségen. A legfontosabb, hogy azonnal fel kell hívnunk a bankot, hogy zárolni tudjuk a számlánkat, bár a legtöbb telefonos applikációban ez bármikor megtehető.

3.3. A vírusirtók, tűzfalak, APP-ok (alkalmazások) hatékonysága

A különböző támadók átlagosan másodpercenként 39-szer próbálnak behatolni a gyanútlan felhasználók számítógépeibe.[10] A tűzfalak célja, hogy a kimenő és bejövő adatcsomagokat megvizsgálják, majd a beállított szabályok alapján megakadályozzák a gyanús csomagok beérkezését, így megóvva gépünket és hálózatunkat a támadóktól.

Habár a tűzfalak kiemelten fontosak elemei az informatikai biztonságnak, a legtöbb esetben szükség van még a vírusirtó csomagok által nyújtott plusz védelemre is. Ez különösen igaz akkor, ha gyakran csatlakozunk nyílt, nem titkosított, nyilvános wifi-hálózatokhoz.

3.4. Zsarolások az elektronikus eszközökről ellopott fájlokkal

A zsarolóprogramok olyan kártevők, amelyek titkosítják a fájljait, vagy meggátolják a számítógép használatát, amíg nem fizeti ki a megfelelő összeget (váltságdíjat) a feloldásukhoz. Ha a számítógép egy hálózatra csatlakozik, a zsarolóprogram a hálózat többi számítógépére vagy tárolóeszközére is átterjedhet.

[10] Mi az a tűzfal, és hogyan nyújthat teljes védelmet 2023-ban? Forrás: safetydetectives.com (Letöltés ideje: 2023.05.28.)

Többek között az alábbi módokon fertőződhet meg zsarolóprogramokkal:

- Nem biztonságos, gyanús vagy hamis webhelyek felkeresése.
- Olyan fájlmellékletek megnyitása, amelyeket nem várt, vagy amelyeket ismeretlen személyektől kapott.
- E-mailekben, a Facebookon[11], a Twitteren[12] és egyéb közösségimédia-bejegyzésekben, illetve csevegésekben vagy SMS[13]-ekben levő rosszindulatú vagy hibás hivatkozások megnyitása.

A hamis e-mailek és weblapok gyakran felismerhetők a szövegben található helyesírási hibákról vagy a szokatlan kinézetükről.

3.5. A kiberbűnözők eszközei

A kiberbűnözők nagyon kreatívak, ha a felhasználók pénzének elcsalásáról van szó. Áldozataikat a legkülönfélébb módszerekkel célozzák meg, kezdve különböző kormánytisztviselők megszemélyesítésétől egészen a csaló online piacterek létrehozásáig. Újra és újra bebizonyosodik, hogy gyorsan alkalmazkodnak, és eszközeiket sokszor az aktuális hírekhez igazítják. A gyanútlan áldozatok megcélzásának egyik leggyakoribb módja az online vásárlással kapcsolatos csalás. Másik kedvelt taktikájuk az aukciós átverés. Ebben az esetben egy nem létező terméket bocsájtanak aukcióra, vagy lemásolják egy valóban eladásra kínált tárgy hirdetését, mintha az a sajátjuk lenne.

Money mule átverések, avagy az online pénzmosás. A "money mule" átverések különböző formákat ölthetnek, a mögöttük álló bűnözők célja azonban mindig ugyanaz: tiltott tevékenységből származó pénz mozgatása nyomon követhetőség nélkül.

Az előlegdíjas csalások kategóriájába tartozó lottó- és nyereménycsalások általában azzal kezdődnek, hogy a potenciális áldozat egy kéretlen e-mailt, telefonhívást vagy SMS-t kap, melyben azt állítják, hogy egy nagyobb összeget vagy valamilyen luxusnyereményt nyert, amely átvételéért csak korlátozott ideig tud jelentkezni.

Adócsalások: ezek az átverések általában - de nem csak - az adóbevallási időszakok környékén ütik fel a fejüket. A befektetési csalások általában a magas nyereség és gyors megtérülés ígéretéről vagy a "hiteles forrásból származó" szigorúan bizalmas tippekről ismertek.[14]

3.6. Az elektronikus eszközök védelmének lehetőségei

Vegyük figyelembe, hogy mindannyian potenciális célpontjai vagyunk a számítógépes bűnözőknek! Az egyéni védelmi lehetőségek: Gondosan válasszuk ki a jelszavainkat, és minden webhelyre más jelszót állítsunk be. Ezeket ne hozzuk mások tudomására, és ha lehet, ne írjuk le olyan helyre, ahonnan azok ellophatók!

- Soha ne hagyjuk őrizetlenül az elektronikus eszközeinket, ha rövid időre is távozunk zárjuk azokat be! Ha érzékeny adatokat tárol egy adathordozón, azt is zárja el!

[11] Amerikai alapítású közösségi hálózat.
[12] Közösségi hálózat és mikro-blog szolgáltatás rövid üzenetek küldésére.
[13] Short Massage Servise: rövid-üzenet szolgáltatás.
[14] Miről felismerhetőek a kiberbűnözök – interaktív- és mobilmédia hírek – mediainfo - Médiások médiája (Letöltés ideje: 2023.07.31.)

- Legyünk óvatosak, ha e-mail mellékletre, vagy linkre kattintunk, mert ezt a módszert is gyakran használják a hackerek!
- Banki utalásokat, egyéb vásárlást csak olyan eszközön végezzünk, amelyik a mienk, és a hálózat is biztonságos!
- Rendszeresen készítsünk magunknak biztonsági másolatot a fontos dokumentumokról, adatokról!
- Vegyük figyelembe, hogy a fertőzések, mástól kapott elektronikus adathordozókról, és okos telefonokkal is terjedhetnek!
- Figyeljünk arra is, hogy mit osztunk meg magunkról a közösségi hálózatokon!

3.7. Kormányzati védelmi szervezetek

Az Országgyűlés 2013-ban – figyelembe véve Magyarország Biztonsági Stratégiáját, Magyarország Nemzeti Kiberbiztonsági Stratégiáját, valamint ez utóbbit is megalapozó Európai Unió kiberbiztonsági stratégiáját – megalkotta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.), amely 2013. július 01-jén lépett hatályba.

A szervezetrendszer stratégiai szintű eleme a Nemzeti Kiberkoordinációs Tanács, amelynek feladata a stratégia kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése, valamint a magánszféra szakmai véleményének kormányzati döntéshozatalba történő becsatornázására létrehozott Kiberbiztonsági Fórum. A szervezetrendszer operatív elemei:

- a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó információbiztonsági hatóság,
- a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó eseménykezelő központ, valamint
- az informatikai rendszerek gyenge pontjainak feltárását, a rendszer védelmi képességek tesztelését (sérülékenység vizsgálat) végző szerv.

Az Ibtv. 2015. évi módosítása eredményeként az állami és önkormányzati szervezetek információs rendszerei tekintetében a fenti operatív feladatok működtetésére a Nemzetbiztonsági Szakszolgálat (NBSZ) kerül kijelölésre, amelynek szervezetén belül 2015. október 1-jével létrehozásra került a Nemzeti Kibervédelmi Intézetet (NKI). A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet a 2019. január 1-jén hatályba lépett jogszabály-módosítások eredményeként ellátja

- az eseménykezelési feladatokat a létfontosságú információs rendszerek és rendszerelemek, valamint
- az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben meghatározott bejelentés-köteles szolgáltatást – úgymint online piactér, internetes keresőszolgáltatás, valamint felhőszolgáltatás – nyújtó szolgáltatók esetében az eseménykezelési, valamint a hatósági felügyeletet.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet jogszabályi feladatai közé tartozik továbbá az ún. „nemzeti kapcsolattartó pont” működtetése, amelynek feladata az

Európai Unión belüli nagy hatású kiber-incidensek hazai koordinálása, az incidensekkel kapcsolatos jelentések fogadása, küldése a nemzetközi partner-szervezetek irányába.[15]

4. A mesterséges intelligencia fejlődésének hatásai

A mesterséges intelligencia fejlődésének hatását minden területen érzékelhetjük: katonai/titkosszolgálati téren, valamint polgári alkalmazása során az üzleti életben, a munkaerő toborzásában, kiválasztásában, a termékek és szolgáltatások megtervezésében és kivitelezésében, a vásárlókkal való kommunikációban, az üzleti innovációban, az adminisztrációban stb. Nyugodtan kijelenthetjük, hogy nincs olyan terület, melyre ne lenne hatással a mesterséges intelligencia fejlődése!

Az Európai Unió kezdeményezésére Magyarországon is indult olyan kezdeményezés, mely a mesterséges intelligencia gyakorlati alkalmazását segíti elő. Az innovációs és technológiai miniszter kezdeményezésére alakult meg 2018. október 8-án a Mesterséges Intelligencia Koalíció egyetemek, nemzetközi és hazai cégek, tudományos műhelyek, szakmai és közigazgatási szervek részvételével. A Koalíció alapvető célkitűzése a mesterséges intelligencia fejlesztési kereteinek és irányvonalainak meghatározása szakmai fórum keretein belül, részt vesz Magyarország mesterséges intelligencia stratégiájának kialakításában, valamint a mesterséges intelligencia által generált gazdasági és társadalmi hatások elemzésében.[16]

2023 júniusában az Európai Parlament elfogadta tárgyalási álláspontját a mesterséges intelligenciára vonatkozó törvénnyel kapcsolatban – ez a világ első átfogó szabályrendszere a mesterséges intelligencia kockázatainak kezelésére.

A mesterséges intelligencia segíthet az egészségügyi ellátás fejlesztésében, az autók biztonságosabbá tételében, testre szabott, olcsóbb és tartósabb termékeket és szolgáltatásokat lehet létrehozni a segítségével. Megkönnyítheti az információkhoz, az oktatáshoz és a képzéshez való hozzáférést is - ez különösen most, a távoktatás előtérbe kerülésével fontos. A mesterséges intelligencia a robotok segítségével biztonságosabbá teheti a munkahelyeket is, és új munkahelyeket teremthet, hiszen az MI segítségével működő iparágak folyamatosan fejlődnek és növekednek.

A mesterséges intelligenciát a bűnmegelőzésben és az igazságszolgáltatás során is egyre többet alkalmazzák, mivel a tömeges adathalmazok gyorsabban feldolgozhatók, a fogvatartottak menekülési kockázatai pontosabban felmérhetők, a bűncselekmények vagy akár a terrortámadások is megjósolhatók és megelőzhetők. Online platformok már most is használják az illegális online magatartás észlelésére. A honvédelem és a nemzetbiztonsági munka során a mesterséges intelligencia felhasználható hírszerző tevékenységre, és hackelés, adathalászat elleni védekezési és támadási stratégiákra is.

5. Befejezés

Mára a kibertérben való jelenlét mind az egyén, mind a vállalkozások, és a kormányzati szereplők számára elengedhetetlenül szükséges! A fő kérdés az, hogyan tudjuk a biztonságos jelenlétet, és működést biztosítani. Jelen cikkben megpróbáltam az egyén

[15] Nemzeti Kibervédelmi Intézet - NBSZ (gov.hu), Letöltve: 2023. 07. 31.

[16] Nagy Adrienn: A mesterséges intelligencia és a digitalizáció jelentősége és lehetséges hasznosítási területei az igazságszolgáltatásban. INFOKOMMUNKIÁCIÓ ÉS JOG 2020/2. 75. o. e-különszám. Forrás: infojog.hu (Letöltés ideje: 2023.07.31.)

szempontjából legfontosabb kockázatokat és azok csökkentésének lehetőségeit felvázolni. Terjedelmi okokból nem tértem ki részletesen a katonai és nemzetbiztonsági területeken jelen lévő kockázatokra, és lehetőségekre!

További ajánlott irodalom

1. Steven Mizrach: Létezik-e „hackeretika" a 90-es években, Replika 2000/41-42. 303-305. o.
2. Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó. Budapest, 2005.
3. Haig Zsolt: Információ- Társadalom – Biztonság, NKE Szolgáltató Kft. Budapest, 2015.
4. Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó. Budapest, 2018.
5. Török Bernát – Ződi Zsolt (szerk.): Az internetes platformok kora. Ludovika Egyetemi Kiadó. Budapest, 2022.
6. Török Bernát- Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest, 2021.
7. Kovács László: A kiberbiztonság stratégiai megközelítése, MTA Doktori Értekezés. Budapest, 2018.
8. Kovács Zoltán: Az infókommunikációs rendszerek nemzetbiztonsági kihívásai. Ludovika Egyetemi Kiadó. Budapest, 2021.
9. Munk Sándor: Katonai informatika a XXI. század elején. Zrínyi Kiadó. Budapest, 2007.
10. Boda József – Dobák Imre: A nemzetbiztonság technikai kihívásai a 21. században. Egyetemi Jegyzet. NKE, Budapest, 2015.
11. Resperger István (szerk.): Nemzetbiztonsági alapismeretek. Dialóg Campus Kiadó, Budapest, 2018.
12. Resperger István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó. Budapest, 2018. (Nemzetbiztonsági Szemle 2014/Különszám 30-39. o.)
13. Aldrich J. Richard: GCHQ The Uncensored Story of Britain's most Secret Intelligence Agency, 2011
14. Glenn Greenwald: A Snowden- ügy, korunk legnagyobb nemzetbiztonsági botránya. HVG Kiadó Zrt. Budapest, 2014.
15. V. A. Bokarev: Kibernetika és hadügy. Zrínyi Katonai Kiadó. Budapest, 1970.