



VIKMAN LÁSZLÓ

A NÉMET KIBERBIZTONSÁGI
SZISZTÉMA ÁTTEKINTÉSE
SZERVEZETI KERETEK, KÜLÖNÖS
TEKINTETTEL A NEMZETBIZTONSÁGI
SZOLGÁLATOK ÉS A HADSEREG SZEREPÉRE
ÉS KAPCSOLATÁRA, VALAMINT A
SZABÁLYOZÁSI HÁTTÉR ALAKULÁSÁRA

MILITARY AND INTELLIGENCE CYBERSECURITY RESEARCH PAPER

2021/2.



Németország hazánk számára Szent István kora óta jelentős viszonyítási pont, nem csak gazdasági szempontból, de védelem- és biztonságpolitikai aspektusok és jogfejlesztési trendek mentén is. Ebben a tanulmányban a német szövetségi kiberbiztonsági rendszerről, annak legfontosabb alapidokumentumairól és szereplőiről adunk áttekintést, külön figyelemmel a katonai szervezetekre. A szabályozási háttér rövid feldolgozásánál kitérünk az éppen folyamatban lévő jogalkotási projektekre, melyek várhatóan tovább növelik a nemzeti kibervédelmi hálózat hatékonyságát.

Kulcsszavak: kibertér, kritikus infrastruktúrák, hírszerzés, szabályozás, együttműködés

Germany is a significant point of reference for Hungary since the time of St. Stephen, not just from an economic perspective, but along defence policy aspects and legislative development trends as well. This study aims to give an overview about the German federal cybersecurity system, its most important ground documents and actors with special regard to the military organisations. At the short elaboration of the regulatory field the paper touches upon the ongoing legislative projects and processes which expectedly will further improve the effectiveness of the national cybersecurity network.

Keywords: cyberspace, critical infrastructure, intelligence, regulation, cooperation

BEVEZETÉS

A kibertér és az abban felmerülő fenyegetések jelentőségét egyértelműen, korszakváltó módon jelezte, amikor az Észak-atlanti Szerződés Szervezete (a továbbiakban: NATO) a 2014. szeptemberi wales-i csúcstájékoztatóján először mondta ki, hogy a nemzetközi jogot a kibertérben is alkalmazandónak tekinti, és egy

hagyományos fegyveres támadás szintjét elérő akciót a virtuális közegben ugyanúgy alkalmasnak lehet értékelni az alapító szerződés 5. cikkelyének felhívására, mint egy konvencionális eszközökkel végrehajtott agressziót.¹ Ezt követően logikus és szükségszerű lépés volt, hogy Varsóban két évvel később a NATO tagok vezetői a kibertér az ötödik hadszíntérként, domain-ként azonosították.² Ezek a változások aztán a

¹ <https://ccdcoe.org/incyber-articles/nato-summit-updates-cyber-defence-policy/>

² Példaként lásd: Michael N. SCHMITT (eds.): *Tallinn Manual On The International Law Applicable To Cyber Warfare*. New York, Cambridge University Press, 2013.; Michael N. SCHMITT (eds.): *Tallinn Manual 2.0 On The International Law Applicable To Cyber Warfare*. New York, Cambridge University Press, 2017.; Rain LIIVOJA - Maarja NAAGEL - Ann VÄLIATAGA: *Autonomous Cyber Capabilities under*

International Law. Tallinn, CCD CoE, 2019.; Samuele DE TOMAS COLATIN - Ann VÄLIATAGA: *Data as a Weapon: Refined Cyber Capabilities Under Weapon Reviews and International Human Rights Law*. Tallinn, CCD CoE, 2020.; CCD CoE: *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit* (letöltve: 2021.04.18., <https://ccdcoe.org/incyber-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/>).

kutatói közösséget is gondolkodásra sarkallták, úgy a NATO, mint a hazai viszonylatban.³

Németország, mint az Európai Unió egyik tagállama, és a NATO fontos tagja a szövetségi szintű változásokhoz is alkalmazkodott tehát, mikor a kiberbiztonság terén fejlesztésekre szánta el magát. Fontos azonban, hogy nemzeti szinten, csúcstechnológiájú és innováció-alapú ipara, valamint magasan fejlett civil infrastruktúrái miatt sem engedheti meg magának, hogy lemaradjon és sérülékennyé váljon a kibertérben. Ezért a német döntéshozók természetesen számos szabályozási és állam-szervezési intézkedéssel is igyekeztek az elmúlt időszakban és igyekeznek napjainkban is folyamatosan adekvát válaszokat adni a felmerülő kiberbiztonsági kihívásokra. Hogy a feladat még egy élen járó országban sem könnyű és komoly útkereséssel jár, azt jól jelzi, milyen sűrűséggel változnak az egyes regulatív és organizációs megoldások Németországban⁴. A szövetségi állami

létből fakadó hozzáadott komplexitás mellett az általános kép áttekintését az sem könnyíti meg, hogy a kibertérből származó fenyegetésekkel érintett állami szervezetek – azaz gyakorlatilag szinte az összes – megalkotta már a saját szakterületi illetékessége és feladatköre szerint szükségesnek ítélt megoldásait.

A Stiftung Neue Verantwortung think tank (a továbbiakban: SNV) által készített alábbi ábra⁵ az EU, a szövetségi és a tagállami szintű szereplőket foglalja össze, elég egy pillantást rávetni a képre, hogy kívülállóként feltegyük azt a kérdést: egy rendszer egyes elemeinek valamely összetett feladatra adott önálló válasza milyen ponttól vált át szofisztikáltból bénítóan fragmentálttá? Természetesen a német szervezési és együttműködési kultúra számára ez a kép nem feltétlenül tűnik problémásnak, az egyes szervezetek részletesebb kifejtésénél látható lesz, hogy a működési rendbe illesztett számos kooperációs és koordinációs elem milyen komoly szerepet játszik abban, hogy a

³ Példként lásd: KELEMEN Roland - FARKAS Ádám: *To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare*. In Szabó Marcel – Gyeney Laura – Láncos Petra Lea (eds.): *Hungarian Yearbook of International Law and European Law* (2019). Den Haag, Eleven International Publishing, 2020, 203-226. o.; FARKAS Ádám: *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai*. In Jog Állam Politika 2019/2. szám, 63-79. o.; KELEMEN Roland - SIMON László: *A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái*. In FARKAS Ádám - VÉGH Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások*. Budapest, Zrínyi Kiadó, 2020, 150-170. o.; KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése*. In Honvédségi Szemle 2020/4. szám, 65-81. o.; KELEMEN

Roland: *A kibertámadások nemzetközi jogi olvasata és a NATO értelmezése, különös tekintettel a válaszlehetőségekre*. In FARKAS Ádám (szerk.): *Az állam katonai védelme az új típusú biztonsági kihívások tükrében*. Budapest, Nemzeti Köszolgálati Egyetem, 2019, 29-50. o.

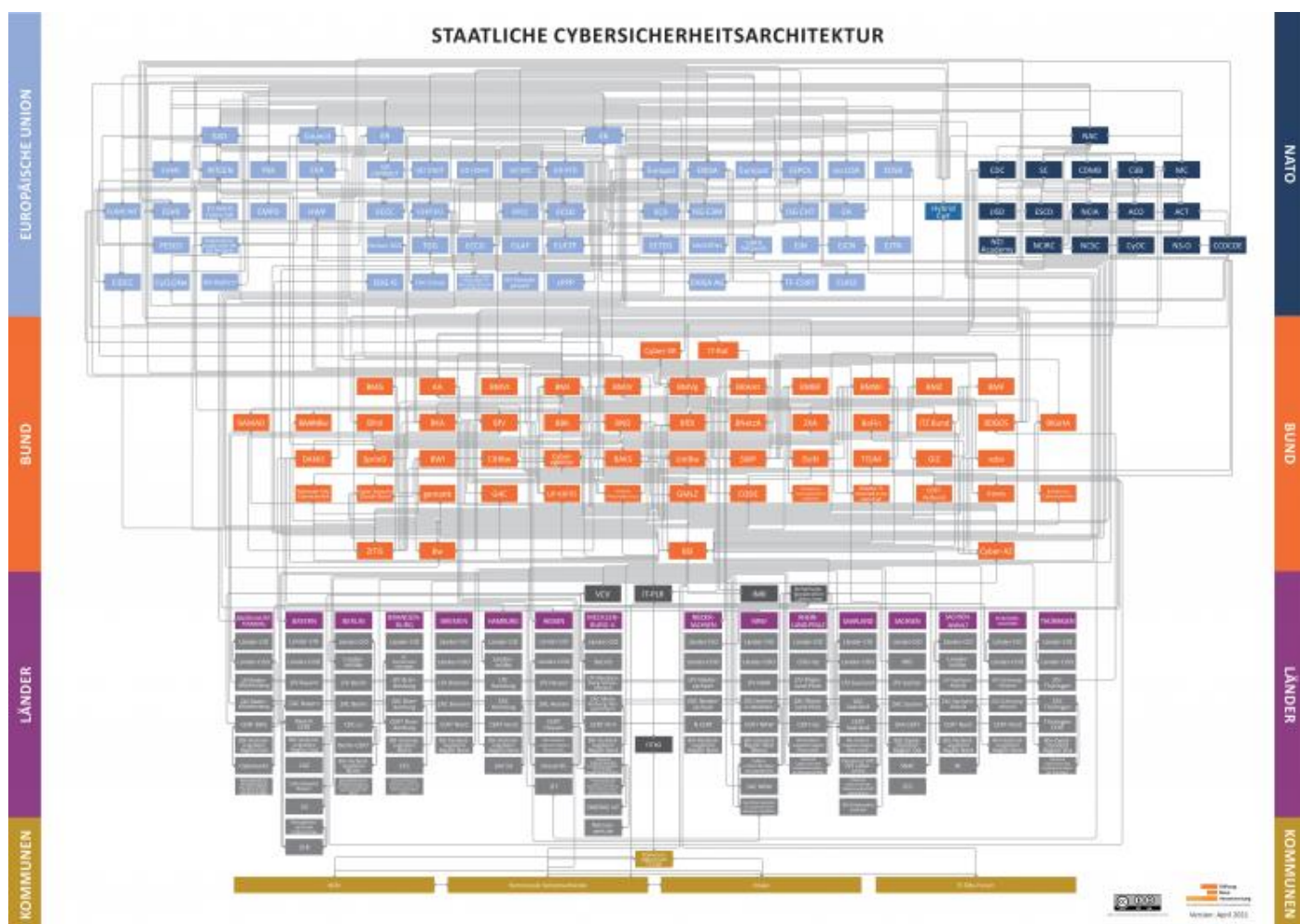
⁴ 2018 év elejéről származó alapos tanulmányában Molnár Dóra is elvégezte ezt az áttekintő munkát, lásd: MOLNÁR Dóra: *Kiberbiztonság Németországban – pillanatkép a német digitális térről*. In *Nemzet és Biztonság*, 2018/1. szám, 142-156. o. (letöltve: 2021.03.27.,

nemzetesbiztonsag.hu/cikkek/neb_2018-01-09_molnar_dora_-_kiberbiztonsag_nemetorszagban-pillanatkep_a_nemet_digitalis_terrol.pdf)

⁵https://www.stiftung-nv.de/sites/default/files/deu_visualisierung-deutschlands_staetliche_cybersicherheitsarchitektur_april_2021.pdf

rendszerük a fenti példánál maradva kifinomult és ne bürokratikus töredezett legyen⁶. Azonban a folyamatban lévő reformok tervezett irányából és a rendszert érő kritikákból az is látszik, hogy a kibertér által kikényszerített gyors reakciókészség megköveteli, hogy a döntéshozók a jövőben a védelmi rendszer és szervezése alakításakor központosítottabb megoldásokat keressenek és így hatékonyabb megközelítések vannak előkészületben. Jelen áttekintésben – az

angolszász fejlesztési irányokkal⁷ való párhuzamos elemzés, illetve e szervezetek kiemelt védelmi és biztonsági jelentősége miatt – elsősorban a nemzetbiztonsági szervezetek és a hadsereg szerepére fókuszálunk majd, igyekezve ezeket kontextusukban elhelyezni, és említést teszünk a folyamatban lévő egyes reformfolyamatokról is, melyeknek jelentős hatása lehet a kibervédelem területén.



⁶ Bár vannak olyan kritikus hangok, amelyek központosítottabb megoldásokat látnának szívesen: <https://www.dbwv.de/aktuelle-themen/newsbeitrag/viele-koeche-beim-it-brei-die-cyberabwehr-in-deutschland/>

⁷ FARKAS Ádám: *Hírszerzés és hadművelet metszésében? Gondolatok az angol National Cyber Force kapcsán*. In Military and Intelligence Cybersecurity Research Paper 2021/1., Budapest, Nemzeti Közszerzési Egyetem, 2021.

STRATÉGIAI HÁTTÉR

A német kiberbiztonsági stratégia⁸

Az első német kiberbiztonsági stratégiát 2010-ben fogadták el, a jelenleg hatályos szöveg 2016-ban készült el. Ennek irányelvei szerint Németország tevékenységi szabadságát és szuverenitását a digitalizáció korszakában is biztosítani kell, ezt egy jövőorientált kiberbiztonsági politikával kell elérni, amely a fejlődéshez kapcsolódó jelentős lehetőségek és állami érdekek mellett uralja a kapcsolódó kockázatokat is.

A szabadság és biztonság garantálása az állam feladata a kibertérben is, így az innen érkező fenyegetések, mint például a kiberbűnözés elhárítása is. A stratégia szerint egy állam csak akkor látja el helyesen a feladatait, ha képes a gazdaság és a társadalom részére a kibertérben is védelmet és biztonságot nyújtani a fejlődéshez és ehhez a saját rendszereit is kiterjedten óvja. A kiberbiztonság elsősorban a kockázathoz igazított viselkedésen és a biztonságos rendszerek alkalmazásán múlik az üzemeltetők és a felhasználók részéről. A támadások megelőzéséhez a felismerésen, hozzárendelésen, elhárításon és nyomon követésen kívül a szoros kooperáció és koordináció is elengedhetetlen. Az állam, a gazdaság, a tudomány és a társadalom a kibertér biztonságaért közös felelősséget

visel⁹. Ezen felül a gyakran határokat átlépő függőségek és fenyegetések kapcsán uniós és nemzetközi egyeztetés is nélkülözhetetlen a vonatkozó kül- és biztonságpolitikai szempontok szerint.

Ezek alapján a stratégiában a szövetségi kormány a következő tevékenységi területeket és az ezeket tovább részletező – időnként más területre is átnyúló – intézkedéseket határozta meg:

1. Biztonságos és autonóm tevékenység egy digitalizált környezetben
 - minden alkalmazó/felhasználó esetében a digitális kompetenciaszint emelése
 - a digitális hanyagság/gondatlanság csökkentése
 - a biztonságos elektronikus kommunikáció és online tér előfeltételeinek megteremtése
 - biztonságos elektronikus identitások
 - a tanúsítás és engedélyeztetés erősítése – IT-biztonságot igazoló jelzés bevezetése
 - a digitalizáció biztonságos alakítása
 - IT-biztonsági fejlesztések ösztönzése
2. A kiberbiztonság az állam és a gazdaság közös feladata
 - kritikus infrastruktúrák biztosítása
 - németországi vállalkozások védelme
 - a német IT gazdaság erősítése

⁸ Bundesministerium des Innern: *Cyber-Sicherheitsstrategie für Deutschland*, 2016, 8-11. o., (letöltve: 2021.03.27., https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf)

⁹ Ennek hazai szakmai, tudományos, gazdasági szereplők által történt közelmúltbeli rögzítése

kapcsán lásd: SZÉPVÖLGYI Enikő: *Kiberbiztonság – mindannyiunk felelőssége*. In Katonai Jogi és Hadijogi Szemle 2021/1. szám, 183-190. o.; *Kulcskérdéssé vált a kiberbiztonság* (letöltve: 2021.03.27., <https://uni.sze.hu/kulcskerdesse-valt-a-kiberbiztonsag>)

- együttműködés az IT szolgáltatókkal
 - IT-biztonsági szolgáltatók bevonása
 - a megbízható információcseréhez szükséges platform létrehozása
3. Hatékony és tartós összkormányzati kiberbiztonsági architektúra
- a Nemzeti Kiber-elhárítási Centrum (Nationale Cyber-Abwehrzentrum, NCAZ) továbbfejlesztése
 - a helyszíni elemzés és reakció képességének erősítése
 - a kibertéri bűnüldözés erősítése
 - a kiber-kémkedés és -szabotás elleni hatékony küzdelem
 - a külföldről érkező kiber-támadások elleni korai előrejelző rendszer
 - központi kiberbiztonsági tudáscentrum alapítása (ZITiS)
 - a kiberbiztonság védelmi aspektusainak erősítése
 - a németországi CERT-szervezetek erősítése
 - a szövetségi közigazgatás biztosítása
 - szoros együttműködés a szövetségi és szövetségi tagállami szint közt
 - további erőforrások bevonása, megfelelő tudású személyzet megnyerése és fejlesztése
4. Németország aktív pozicionálása az európai és nemzetközi kiberbiztonsági politikában
- aktív részvétel egy hatékony európai kiber-biztonságpolitika kialakításában
 - a NATO kibervédelmi politikájának továbbfejlesztése
 - a nemzetközi kiberbiztonság alakításában való aktív részvétel
 - kétoldalú és regionális alapú együttműködések és támogatás kiber-képességek fel- és kiépítésére
 - a nemzetközi bűnüldözés erősítése

A stratégia jelenleg éppen felülvizsgálat alatt áll, és a tervek szerint a felülvizsgált változatot 2021. közepéig fogadja el a kormány. Fő változtatási irányként az egyes intézkedések hatékonyságának növelését és mérhetővé tételét tették. Hangsúlyos szerepet kapna a „security by design”-elv erősítése (az IT termékekbe előre betervezett biztonság), és még inkább elmélyítenék a kapcsolatokat a tudományos és a gazdasági szféra irányában. A vállalkozások fokozott védelme szintén erősítendő, ahogy az is, hogy az üzemeltetők mellett a gyártók és beszállítók szerepét is figyelembe kell venni biztonsági kérdésekben. A kritikus infrastruktúrák erősebb bevonása mellett emelni szükséges az összkormányzati kiberbiztonsági architektúra színvonalát, és a minél hatékonyabb fellépése érdekében megfelelően kell pozicionálni a Szövetségi Információtechnikai Biztonsági Hivatalt (BSI).¹⁰

¹⁰ Dennis-Kenji KIPKER: *Cybersecurity Regulierung 2021: Update*, (letöltve: 2021.03.27.,

https://www.researchgate.net/publication/348365761_Cybersecurity-Regulierung_2021_Update

Fehér könyv a biztonságpolitikáról és a Bundeswehr jövőjéről¹¹

Ez a programadó alapidokumentum több fontos lényeges újítást hozott a német biztonság- és védelempolitikába, meghaladva többek közt olyan korábbi tabukat, mint a nemzeti hadseregben való szolgálat megnyitása más uniós államok polgárai előtt¹².

Az elektronikus térből érkező fenyegetéseknek nem csak a mennyisége, hanem a minősége is érezhetően megváltozott az elmúlt időszakban az egyszerű vírusoktól az APT¹³-kig. Mivel a széles körben használt szoftvertermékek könnyen és olcsón hozzáférhetők, ezért a támadók köre nem korlátozódik kizárólag az állami szereplőkre, hanem terrrorszervezetek, szervezett bűnözői csoportok és akár egyének is képesek lehetnek relatíve kis ráfordítással jelentős károkat okozni. A nemzetközileg is kikényszeríthető jogi szabályozás vagy a különböző bizalom- és biztonságépítő intézkedések bevezetése és alkalmazása azonban e területen még mondhatni gyerekcipőben jár, így fokozott nyomás nehezedik a nemzetállami szintű védelmi entitásokra.

Az államok és kritikus infrastruktúráik elleni támadások már régen nem a fikció birodalmába tartoznak, és jellemző, hogy az értékes célpontokkal szemben mindig testreszabott

megoldásokat alkalmaznak. Úgyszintén jelentős kihívást jelent a pluralisztikus berendezkedésű társadalmakban a közvélemény befolyásolására használt digitális kommunikáció kezdve a közösségi oldalakon folytatott, irányított vitáktól egészen a hírportálokon megjelenő manipulált hírekig. Ezek természetesen a hibrid hadviselésben is jelentős szerepet kapnak, mivel a kiber- és információs térből érkező támadások könnyen álcázhatók, ami megnehezíti ezen aktivitások attributálását. Ezzel a konvencionális elrettentő eszközök hatékonysága csökken, miközben a kibertámadások akár a valós térben bekövetkezett támadások szintjét is elérhetik, és valós eskalációhoz vezethetnek. A kiber- és információs műveletek már jelenleg is fontos részét képezik minden fegyveres összeütközésnek, illetve befolyásolási törekvésnek, amivel a virtuális tér nem hogy hadszínterré, de egy határtalan nemzetközi és stratégiai jelentőségű színterré fejlődött.

A fentiek miatt a nemzetközi jog alkalmazásának megegyezésen alapuló értelmezésére való törekvés mellett nagyon fontos a nemzeti reagáló- és ellenállóképesség, valamint a kibertámadások és információs műveletek megelőzésére és elhárítására irányuló képességek fokozása¹⁴. A kibertérre jellemző attribúció-probléma miatt jelentős a bizalomépítés és konfliktus kezelő mechanizmusok kiépítése az esetleges

¹¹ Weissbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr, 36-38. o. (letöltve: 2021.03.27., <https://www.bundesregierung.de/resourcer/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-data.pdf>)

¹² U.o. 120. o.

¹³ APT – Advanced Persistent Threat – folyamatos és szofisztikált hacker támadás valamely rendszerhez való hozzáférés megszerzésére

¹⁴ Mindezen képességek fejlesztését persze épp úgy kell értelmezni, ahogy maga a kiberfenyegetés is megjelenik, kölcsönhatásban a klasszikus kihívásokkal és ez által a klasszikus védelmi és elhárító funkciókkal.

eszkálációk elkerülésére. A kibervédelem összkormányzati feladat, amelyhez a német felfogás szerint természetesen a kritikus infrastruktúrák védelme is hozzátartozik. A feladatok meghatározása a kiberbiztonsági stratégiában történik, amely a Belügyminisztérium koordinációjával készül el. Az összkormányzati kiberbiztonság védelmi aspektusai azonban a Védelmi Minisztériumhoz, operatív szinten a Bundeswehr-hez illetve a BAMAD-hoz tartoznak, miközben a nemzetközi kiberbiztonsági politikában való részvétel a Külügyminisztérium feladata.

A Bundeswehr koncepciója¹⁵

A már tárgyalt Fehér Könyv irányelvei alapján kidolgozott és 2018 nyarán elfogadott koncepció a német hadseregről természetesen tovább konkretizálta az operatív kibervédelem területén végrehajtandó feladatokat és célkitűzéseket.

A koncepció szerint az összkormányzati biztonság és integritás a kiber- és információs térben és az ehhez szükséges katonai informatikai rendszerek reziliens alkalmazása, üzemeltetése és védelme alapfeladat. A Bundeswehr szerepe és feladatai az aktuális német kibervédelmi stratégiából, illetve egyes aspektusok a hadsereg alkotmányban meghatározott országvédelmi feladataiból eredeztethetőek. Ide sorolható a kritikus infrastruktúrák védelme, vagy támadások esetén a műveleti képesség megőrzése a kibertérben. A kiberbiztonság védelempolitikai vonatkozásai és ezek

nemzetközi kontextusú értelmezése kapcsán a Bundeswehr a NATO keretekhez orientálódik.

A hadseregnek a jövőben készen állnia komplex kibertámadások elhárítására, defenzív és offenzív képességekre is szüksége van, melyeket folyamatosan készenlétben kell tartania és fejlesztenie kell. Az innovációs sebesség és a fenyegetések globális minősége is megköveteli a nemzeti és nemzetközi partnerekkel való együttműködést a gazdasági, tudományos és innovációs szférából. Annak érdekében, hogy a hadsereg a feladatait elláthassa, szükséges

- az összkormányzati képességek kiépítése, a kiterjedt kooperáció, a partneri hálózatok kiépítése a tudománnyal, iparral és más kulcsszereplőkkel,
- a hadsereg saját képességeinek kiépítése, a saját IT-rendszer konszolidációja, és a kibertérből érkező támadásokkal szembeni ellenállóképességének kiépítése,
- megfelelő információellátás céljából a megfelelő IT technológia alkalmazásával a saját elemző- és értékelő-képesség kifejlesztése,
- az egyes fegyverrendszerektől a kritikus területeket ellátó beszerzési láncokig a nemzeti kulcs-technológiák igénybevételének erősítése,
- kooperáció és partnerségi kapcsolatok kiépítése a gazdasági és ipari szférával,
- az eddig fragmentált felelősségi körök és struktúrák egyesítése robosztus képességfejlesztéssel a

¹⁵ *Konzeption der Bundeswehr*, 29-30., 43-44., 52. o. (letöltve: 2021.03.27).

<https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384>

CIR (Cyber und Informationsraum) doménben,

- az IT-képességek összefogása a Bundeswehr digitalizációjára.

Az egyes dimenziók értékelésénél a már Fehér Könyvben is érintett információs hadviselés és propaganda mellett szóba kerül az Internet határokat átlépő jellege, az adatfeldolgozó rendszerek elosztott, nemzetközi jellegű működése¹⁶. Úgyszintén megemlíti a koncepció a elektromágneses spektrum, mint közeg, illetve az ennek felhasználásában szerepet játszó technológiák¹⁷, illetve a terület magasan képzett szakemberek és a folyamatos emberi erőforrás utánpótlás iránti „éhségét”. Végezetül kulcsfontosságú kérdés a korszerű fegyverrendszerek egyre szélesebb körű digitalizációja is.

A NÉMET KIBERVÉDELMI RENDSZER FONTOS SZEREPLŐI

A bevezetőben már említett SNV több éve gondozza és frissíti a kibervédelemben német szempontból jelentős szerepet játszó szervezetek "szakmai katalógusát"¹⁸. Az ebben felsoroltak közül most – némileg önkényesen – a legfontosabbnak értékelt

szereplőket írjuk le röviden. A stratégiai szintű platformokat követően a kibertérben jelentős feladatokat vállaló egyes minisztériumokat vesszük sorra, majd a nemzetbiztonsági és katonai háttérű aktorokkal foglalkozunk részletesebben, áttekintve releváns tevékenységüket, feladatrendszerüket. Zárásként említés teszünk a területen kiemelten fontos tudás-háttérrel biztosító oktatási-kutatási szervezetekről.

Központi koordinációs platformok

IT-Tervtanács (IT-Planungsrat)¹⁹: A tanács a szövetségi szintű együttműködés központi grémiuma az információtechnológia területén. IT kérdésekben koordinálja a szövetség és a tagállamok tevékenységét, határozatokat hoz szakterületek feletti vagy azokon átnyúló interoperabilitási- vagy biztonsági ügyekben, e-közigazgatási projekteket vezet és irányítja a hálózatok fejlesztését. A szövetségi és tagállami kormányzatok információtechnológiai képviselőiből áll, tanácskozási joggal települési önkormányzatok szövetségei által delegált képviselők, valamint adatvédelemmel és információszabadsággal foglalkozó

¹⁶ Ennek geopolitika szerepéről lásd: Amael CATTARUZZA: *A digitális adatok geopolitikája. Hatolom és konfliktusok a big data korában*. Budapest, Pallas Athéné Books, 2020.; FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amael Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei*. In SmartLaw Research Group Working Paper 2021/1. szám (letöltve: 2021. március 27., http://smartlawresearch.hu/storage/app/media/Kia dvanyok/slrgrp_1-2021.pdf).

¹⁷ Ennek honvédelmi jelentősége a magyar szabályozásban is megjelent a kibertér műveletek mellett. A téma kapcsán áttekintésül. Vö: FARKAS

Ádám: *A kortárs technológia-fejlődés és innováció viszonya a honvédelmi szabályozással*. In MTA Law Working Papers 2021/4. szám (letöltve: 2021. április 25., <https://jog.tk.hu/mtalwp>).

¹⁸ Dr. Sven HERPIG, Rebecca BEIGEL: *Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten*. Oktober 2020.2, 5. Auflage, (letöltve: 2021.03.27. <https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik>)

¹⁹ https://www.it-planungsrat.de/DE/Home/home_node.html

szakértők is részt vehetnek az üléseken. További meghívottak lehetnek az egyes érintett szakminisztériumok munkatársai is. Az elnökölés joga évente felváltva illeti meg a tagállamokat és a szövetséget. A tanács részét képezi az információbiztonsági munkacsoport (AG InfoSic). Ez a munkacsoport 2011 óta azért felel, hogy célkitűzéseket dolgozzon ki a közigazgatás számára, ideértve az ezek eléréséhez szükséges stratégiákat is. A szövetségi kancellár hivatalának vezetője és a tagállami kancelláriák vezetői minden évben jelentést kapnak a tanács tevékenységéről, és tájékozódnak a nemzeti e-közigazgatási-stratégia továbbfejlesztéséről.

IT-Tanács (IT-Rat)²⁰: Az IT-tanács, mint politikai-stratégiai testület, a szakterületek feletti digitalizációs témák és a szövetségi közigazgatás IT szektorának felelőse. Elnöke a szövetségi kancellária vezetője, helyettesei a szövetségi digitalizációs kormány megbízott és a szövetségi kormányzati IT kormány megbízott. Kiberbiztonsági Tanács (Cyber-Sicherheitsrat)²¹

A nemzeti Kiberbiztonsági Tanácsot 2011-ben a kiberbiztonsági stratégiával összefüggésben hozták létre abból a célból, hogy a szövetségi kormányzat stratégiai tanácsadójaként azonosítsa a hosszútávú teendőket és a kiberbiztonsági trendeket, továbbá ösztönözze az ezeknek megfelelő válaszokat. Tagjai közt a szövetségi kormányzat, és a tagállami képviselők

mellett a jelentős gazdasági szereplők is megtalálhatók. A 2016-os új kiberbiztonsági stratégiát követően a tanács belső összetételét átalakították, jelenleg a tanácsban lévő állami szervezetek a szövetségi szintről a kancellária, a belügyminisztérium, a külügyminisztérium, a védelmi minisztérium, a gazdasági- és energiaügyi minisztérium, az igazságügy, a pénzügy, az oktatási tárca és a közlekedési és digitális infrastruktúra minisztérium, a tagállamokat Niedersachsen és Hessen tartomány szakértői képviselik.

UP KRITIS (Umsetzungsplan Kritische Infrastrukturen)²²: Az UP KRITIS program a köz- és privátszféra közötti kooperációs feladatot látja el a kritikus infrastruktúrák működésének biztosítása kapcsán, melyben az érintett állami szereplők mellett a kritikus infrastruktúrák üzemeltetői és szakmai szövetségeik képviselői vesznek részt, mivel működésükben az IT és kommunikációs technológiák egyre nagyobb szerepet játszanak. Az állam részéről a kooperáció elsődleges résztvevői a belügyminisztérium, információtechnológiai nemzetbiztonsági szolgálatként a BSI (Bundesamt für Sicherheit in der Informationstechnik) és a lakosságvédelemért és katasztrófaelhárításért felelős BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe).

²⁰https://www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/IT-Rat_node.html;jsessionid=120F286E6A0F4D8D631F3647D08D241A.2_cid350

²¹<https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-sicherheitsrat>

²² https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/UPKOrganisation/upk_organisation_node.html;jsessionid=CAAB2F9E7BCCF6E6C3AF26C705F8EED7.1_cid320

Operatív kibervédelmi szervezetek

Nemzeti Kiberelhárító Központ (Nationales Cyber-Abwehrzentrum, NCAZ)²³: A központ feladata a kibertérben lévő különböző kibertéri fenyegetésekre tekintettel az egyes állami szereplők közötti operatív együttműködés optimalizálása és a megfelelő védelmi- és elhárítási lépések koordinálása. Ennek érdekében a BSI-nél települő incidenskezelő központ minden az IT-infrastruktúra elleni kibertámadásokról szóló információt összefog. A központ kooperációs platformként is szolgál a BSI, a BBK, a szövetségi rendőrség, a szövetségi bünyügyi hivatal (BKA), az alkotmányvédelem (Bundesamt für Verfassungsschutz, BfV), a szövetségi hírszerzés (Bundesnachrichtendienst, BND), a vámügyi és pénzügyi bünyügyi szervek, valamint a katonai elhárítás (Bundesamt für den Militärischen Abschirmdienst, BAMAD) számára. Éves jelentését a Kiberbiztonsági Tanácsnak adja, koordinátora a BKA, helyettes koordinátorai az alkotmányvédelem és hadsereg kibervédelmi parancsnoksága. Minden résztvevő szervezet köteles összekötőket küldeni a központba.

A központot nem azzal a szándékkal hozták létre, hogy aktív ellentevékenységet végezzen, pl. az USA által alkalmazott megközelítéssel szemben a „hackback” módszereket nem alkalmazzák, aminek az is nyilvánvaló oka lehet, hogy egy német szereplő külföldön üzemeltetett szerverét

éri támadás. Ilyenkor a joghatósági kérdések igen bonyolulttá tudnak válni, hiszen a német bünyldöző szervek nem tehetnek aktív lépéseket. Emiatt a német elhárítási filozófia alapvetően decentralizált és védelem-központú, igyekszik a kritikus infrastruktúrák üzemeltetőit is a rendszereik megfelelő védelmére ösztönözni²⁴.

Egyes szakmai kritikusai szerint nagyobb létszámú személyzetre lenne szüksége, és a kiberbünyözés üldözéséhez nagy segítséget jelentene egy speciálisan erre szakosodott ügyész szerv létrehozása²⁵.

Szövetségi CERT (CERT-Bund)²⁶: A CERT-Bund Németország nemzeti szintű kibervészhelyzeti csapata (Computer Emergency Response Team) és minden szövetségi hivatal és szervezet támogatója bármely IT-biztonsági esemény bekövetkezésekor. A csapatnak a BSI ad otthont, és együttműködik a tagállami szintű CERT-csapatokkal is.

A fenti szervezeteken kívül az aktuális fenyegetettségi helyzet nyomán követésére szintén a BSI-nél létrehozták a **Nemzeti IT-Helyzetkövető Központot (Nationales IT-Lagezentrum, LZ)**²⁷. Éjszaka ennek feladatait a BBK-ban működő **Együttes Jelentési- és Helyzetkövető Központ (Gemeinsames Melde- und Lagezentrum, GMLZ)**²⁸ látja el, ami napi jelentéseket is készít. Kifejezetten **katonai jellegű helyzetkövető szervezet is létezik**

²³https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

²⁴<https://www.bpb.de/politik/hintergrund-aktuell/327385/nationales-cyber-abwehrzentrum>

²⁵<https://www.bpb.de/veranstaltungen/dokumentation/286397/podiumsdiskussion-politik-und-kontrollmoeglichkeiten-von-cyber-aktivitaeten>

²⁶<https://www.cert-bund.de/about>

²⁷https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/nationales-it-lagezentrum_node.html

²⁸https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/GMLZ/GMLZ_node.html

*(Gemeinsames Lagezentrum Cyber- und Informationsraum, GLZ CIR)*²⁹, amelynek felállításában a Bundeswehr Kibervédelmi Parancsnoksága mellett a BWI GmbH, mint a hadsereg informatikai beszállítója is részt vett, és saját, mesterséges intelligenciával is megtámogatott rendszereivel gyűjti és rendszerezi a katonai szempontból releváns információkat a kiber- és információs térből.

A kibervédelemben kiemelten szerepet játszó minisztériumok

Kancellária Hivatala (Bundeskanzleramt, BKAm)³⁰: A szövetségi kancellárt támogató munkaszervezet a tükör-referatúrái segítségével szoros kapcsolatban van minden minisztériummal. A kiberbiztonsághoz közvetlenül az ide alárendelt szövetségi hírszerzésen (Bundesnachrichtendienst, BND) és finanszírozási kérdéseken keresztül kapcsolódik és képviselteti magát a Kiberbiztonsági Tanácsban is.

Külügyminisztérium (Auswärtiges Amt, AA)³¹: A Külügyminisztérium alapfeladatából adódóan a kiberbiztonságban is a nemzetközi- és külpolitikai témákra koncentrált, így különösen az általános emberi jogok érvényesülésére a kibertérben, vagy a digitalizáción keresztül elérhető gazdasági fejlődés lehetőségeire. 2011-ben a szakterület felügyeletére létrehoztak egy

koordinációs stábot is (Koordinierungsstab für Cyber-Außenpolitik, KSCA). A minisztérium részt vesz a Kiberbiztonsági Tanács munkájában, és felváltva a védelmi tárccal felváltva kinevezi a kiber témában is jelentős oktatóhelynek számító Szövetségi Biztonságpolitikai Akadémia vezetőjét.

Védelmi Minisztérium (Bundesministerium der Verteidigung, BMVg)³²: Németország katonai védelme a kibertérben a védelmi tárca feladatkörébe tartozik. Ehhez a legkülönbébb nemzeti és nemzetközi együttműködésekben vesz részt, pl. a NATO Kibervédelmi Kiválósági Központ munkájában. A minisztérium kiber- és információtechnológia részlege felel a védelmi kérdésekért is, és részt vesz a Kiberbiztonsági Tanácsban. Irányítja a Bundeswehrt, és a BAMAD-ot, amelyek az operatív képességeket nyújtják.

Belügyminisztérium (Bundesministerium des Innern, für Bau und Heimat, BMI)³³: A belügy felel a kibertér polgári jellegű biztonságáért, a minisztérium által 2016-ban előterjesztett Kibervédelmi Stratégia adja a szövetségi kormányzat szakterületeken átnyúló stratégiai kereteit ebben a szférában. A Kiberbiztonsági Tanács elnöki posztját is betöltő információtechnológiáért felelős kormány megbízott koordinálja a stratégia végrehajtását. A minisztériumhoz tartozik a szövetségi rendőrség, a BKA, a BSI, a BfV és a BBK. Rendelettel hozta létre a központi

²⁹<https://www.bmvg.de/de/aktuelles/lagezentrum-cyber-und-informationsraum-19284>

³⁰<https://www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt>

³¹<https://www.auswaertiges-amt.de/de/aussenpolitik/themen/cyber-aussenpolitik>

³²<https://www.bmvg.de/de/themen/cybersicherheit>

³³<https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/it-und-cybersicherheit-node.html>

informatikai tudásközpontként működő ZITIS-t, és többek közt aktív résztvevő az UP KRITIS kezdeményezésben.

Szövetségi szintű polgári állami szervezetek

Szövetségi Információtechnikai Biztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik, BSI)³⁴: A BSI feladata az ország IT biztonságának erősítése, mint hatóság magas technikai szakértelemmel ösztönzi az információ- és kiberbiztonságot a közigazgatásban, gazdaságban és általában a társadalomban különböző kooperációkon és kezdeményezéseken keresztül. Országszerte rendelkezik kirendeltségekkel a regionális beágyazottsága elérése érdekében, 2019-ben pedig egy második telephelyet kapott Drezdában, amelyet Saarlandban követ majd egy kifejezetten mesterséges intelligenciákra összpontosító harmadik is. A Belügyminisztériumhoz tartozó szervezet, és annak keretei közt otthont ad a Nemzeti Kiberelhárító Központnak és a CERT-Bundnak. Minden évben széles fókuszú részletes jelentést tesz közzé a német kibervédelem helyzetéről³⁵.

Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz, BfV)³⁶: A BfV elsősorban arra fókuszál, hogy a szélsőségesek, terroristák, más államok hírszerzése milyen új technikai

lehetőségeket tud kihasználni Németországban kémkedés, politikai dezinformáció vagy számítógépes szabotázs céljából. A BfV igyekszik elhárítani és felderíteni az állami- és magáncélpontok elleni kibertámadásokat. A hivatal a belügy irányítása alatt áll, részt vesz a NCAZ munkájában, szerepet vállal a gazdaságvédelemben és gyakran igénybe veszi a ZITIS szakértői háttérét.

Szövetségi Hírszerző Szolgálat (Bundesnachrichtendienst, BND)³⁷: A külföldi hírszerzésért felelős BND már külföldön törekszik a német érdekek elleni kibertámadások, -kémkedés és -szabotázs elhárítására és figyelmezteti az érintett belföldi aktorokat, hogy a megfelelő ellenintézkedéseket tegyék meg. Ezt a tevékenységét a SSCD – SIGINT Support to Cyber Defense rövidítéssel jelöli. A BND a Kancelláriához tartozik, részt vesz a gazdaságvédelemben és az NCAZ tevékenységében is.

Szövetségi Rendőrség (Bundespolizei, BPol)³⁸: A kiberbűnözés növekedésével és a „hagyományos bűnözés” egyre gyakoribb információtechnológiát igénybevevő trendjével a rendőrségnek is lépést kellett tartania. A szövetségi rendőrségnek csak CERT csapata van (CERT Bpol), amely a saját rendszereit védi. Természetesen a belügy portfóliójához tartozik és részt vesz a NCAZ-ban is, szükség esetén pedig igénybe veszi a ZITIS támogatását.

³⁴https://www.bsi.bund.de/DE/Home/home_node.html

³⁵<https://www.bmi.bund.de/SharedDocs/download/s/DE/veroeffentlichungen/2020/bsi-lagebericht-cybersicherheit-2020>

³⁶ <https://www.verfassungsschutz.de/en/fields-of-work/cyber-attacks>

³⁷https://www.bnd.bund.de/EN/Mission-areas/Cybersecurity/cybersecurity_node.html

³⁸https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

Pénzügyi Szolgáltatások Szövetségi Felügyelete (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin)³⁹: A felügyelet feladata egy működőképes, megbízható és stabil pénzügyi rendszer biztosítása Németországban. A gazdasági bűnözés területén a „hagyományosabb”, pl. pénzmosási műveletek üldözése mellett egyre komolyabb feladatot jelentenek a biztosítók, pénzügyi szolgáltatók és bankok a kibertérből érő fenyegetések. A szervezet a pénzügyi tárcához tartozik, és képviselteti magát az NCAZ-ban.

Szövetségi Lakosságvédelmi és Katasztrófaelhárítási Hivatal (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK)⁴⁰: A belüghöz tartozó BBK a kiber területen elsősorban a kritikus infrastruktúrák érintő esetleges támadásokkal és kockázatokkal foglalkozik. Természetesen tagja az NCAZ-nak és működteti a folyamatosan ténykedő Együttes Jelentési- és Helyzetkövető Központot és jelentős szereplője az UP KRITIS kezdeményezésnek.

Szövetségi Bűnügyi Hivatal (Bundeskriminalamt, BKA)⁴¹: A BKA szintén a belügyminisztérium irányítása alatt van, és magasan szervezett, kiemelt jelentőségű bűnügyek kapcsán a kibertérben is tevékeny. Külön dedikált kiberbűnözési részleggel is rendelkezik, ahol az ilyen bűncselekményekkel kapcsolatos kompetenciák és információk összefutnak. Használja a ZITIS támogatását, részt vesz a

NCAZ-ban, és képviseli Németországot az Europolban.

Katonai szervezetek

Miután 2017 áprilisában a kiber- és információs teret a hadsereg legújabb szervezési területeként azonosították (a hagyományosnak tekinthető szárazföld, légvédelmi és tengeri területek mellett), 2021-es határidővel kialakították a Bundeswehr új feladatának ellátásához szükséges szervezeti hátteret is, tervezetten 14.500 fős állománnyal. A doménfelelősség keretében el kell látni a hadsereg belföldi és missziós IT-rendszereinek védelmét, biztosítani kell a szükséges felderítést és üzembiztosságot, a szükséges geoinformációs adatokat, és a szakterületi kapcsolattartást más kiber témában felelős szervekkel. Le kell szögezni azonban, hogy a nemzeti szintű védelmi képességfejlesztés és megóvás szempontjából kulcsfontosságú a Bundeswehr viszonylatában a BAMAD támogatása és feladatellátása a haderő nemzetbiztonsági jellegű védelmének és stabilitásának erősítése érdekében. A hadsereg informatikai képességeit egy vezető és két alárendelt parancsnokszághoz osztották be.

Kiber- és Információstér Parancsnokság (Kommando Cyber- und Informationsraum, KdoCIR)⁴²: A KdoCIR 3 csillagos tábornoki szintű vezetési szint, feladatai a kiber-,

³⁹https://www.bafin.de/DE/Startseite/startseite_no_de.html

⁴⁰<https://www.bbk.bund.de/SubSites/Kritis/DE/Publikationen/Sektoruebergreifend/Leitfaeden/Sicherheit%20und%20Verantwortung%20im%20Cyber-Raum.html>

⁴¹https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html

⁴²<https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum>

információs tér és stratégiai felderítés, a hadsereg geoinformációs tevékenysége és az operatív kommunikáció. Elsődleges mégis a CIR domén strukturálása és a vezetés. Helyettesként koordinálja a NCAZ működését.

Információtechnikai Parancsnokság (Kommando Informationstechnik, KdoITBw)⁴³: A 2013-ban felállított parancsnokság tényleges, „műveleti” képességet nyújt, hat IT-zászlóaljba szervezve biztosítja, hogy a Bundeswehr műveletein az IT eszközök beüzemelése, működtetése és biztonsága garantált legyen. A hadsereg kiberbiztonsági központjából Incident Response Team-ek rendelkezésre bocsátásával nyújt szükséges reakcióképességet valamely kibertámadás esetére.

Stratégiai Felderítési Parancsnokság (Kommando Strategische Aufklärung, KdoStratAufkl)⁴⁴: A parancsnokság feladata a hadsereg információigényének kielégítése meghatározott tevékenységekből származó adatokkal. Ezek a műholdas képalkotás, a távérzékelés és elektronikai felderítés, az elektronikai harc, objektumanalízis. Folyamatosan fejleszti hálózati műveleti képességeit, és üzemelteti a hadsereg kiber-műveleti központját, ami támogatást nyújt katonai kiberműveletek tervezéséhez, előkészítéséhez, vezetéséhez és végrehajtásához.

Szövetségi Katonai Elhárítási Hivatal (Bundesamt für den Militärischen Abschirmdienst, BAMAD)⁴⁵: A BAMAD Németország katonai nemzetbiztonsági szolgálata, 2017-ben rendelték közvetlenül a védelmi minisztérium alá. A szervezetben 2019-ben egy reorganizációt, és egy 400 fős létszámbővítést hajtottak végre (összlétszám nagyságrendileg 1200 fő). Az elnököt egy nagyobb törzs valamint egy civil és egy katonai elnök-helyettes támogatja a munkában. Mindketten saját szakterületi portfólió felett rendelkeznek, a kiber témáért is felelős „T részleg” a katonai ágba tartozik.⁴⁶ A központ Kölnben található, nyolc további kirendeltséggel rendelkezik országszerte, illetve állomáshelyekkel külföldön. A BAMAD feladatkörének jellege elsősorban alkotmányvédelmi. Törvényben⁴⁷ foglalt feladatai közé tartozik a szélsőséges- és terrorista-elhárítás mellett a (kiber-) kémkedés és -szabotázs elleni küzdelem is. Ezen felül természetesen folyamatosan követi a belföldi támaszpontok és a német missziók biztonsági helyzetét, és részt vesz ezek védelmében, továbbá végrehajtja a szükséges személyi biztonsági ellenőrzéseket, végül a védelmi minisztérium szervezeti körében az elektromágneses leárnyékolásért is felel. A már említett „T részleg” több korábbi képesség koncentrálásával jött létre, és folyamatosan törekszik az IT technikai

⁴³<https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-informations-technik-der-bundeswehr>

⁴⁴<https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung>

⁴⁵<https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/mad-bundesamt-fuer-den-militaerischen-abschirmdienst>

⁴⁶<https://www.bundeswehr.de/de/mad-jahresbericht-2019-250908>

⁴⁷<https://www.gesetze-im-internet.de/madg/BJNR029770990.html>

menedzsment, a hírszerzési technikák és a leányékolás területén a jövőbemutató fejlesztésekre. A szervezet exkluzív rész képességeivel a titok- és szabotázs védelem, illetve a robbanóeszközök hatástalanítása területén komolyan hozzájárul a védelmi terület erőfeszítéseéhez⁴⁸. A BAMAD állandó tagja a NCAZ-nak.

Jelentős oktatási intézmények, tudományos műhelyek

Szövetségi Biztonságpolitikai Akadémia (Bundesakademie für Sicherheitspolitik, BAKS)⁴⁹: A védelmi minisztériumhoz tartozó felsőoktatási intézmény a szükséges szakember-utánpótláson kívül több együttműködésben is érdekelt, a kiber témában is. Ilyen a „Berliner Forum zur Cyber-Sicherheit” című rendezvénysorozat is.

Bundeswehr Egyetem (Universität der Bundeswehr München, UniBw)⁵⁰: A hadsereg tisztképzésének központja. A kínált stúdiumok között van informatikai, kiberbiztonsági, mérnöki és gazdaságinformatikai képzés is.

Kibervédelmi Kutatóintézet (Forschungsinstitut Cyber Defence, CODE)⁵¹: A Bundeswehr Egyetemen működő intézet célja kifejezetten a hadsereg számára az

adatvédelem, a szoftverek és rendszerek területén innovatív technikai újítások megvalósítása, amellet, hogy hagyományos kutatóműhelyként is funkcionál, a ZITIS közvetlen közelében.

Biztonsági Információtechnikai Központ (Zentrale Stelle für Informationstechnik im Sicherheitsbereich, ZITIS)⁵²: A központ a biztonsági területen végzett fejlesztő- és kutatómunka mellett támogatást nyújt a különböző biztonsági szervezetek számára a digitális nyomozás, -megfigyelés, kriptográfia és big data elemzések területén. Emellett a bűnüldözés, fenyegetések elhárítása és kémkedés megelőzése témáinak technikai vonatkozásaival is foglalkozik. Az UniBw kampuszán található.

A KIBERBIZTONSÁG SZABÁLYOZÁSI HÁTTERÉNEK ALAKULÁSA

A német kiberbiztonság központi szereplőjeként a BSI 1991-ben kezdte el a tevékenységét⁵³ az ún. BSI Errichtungsgesetz alapján⁵⁴, ennek előkészítését pedig egy 1989-es szövetségi koncepció képezte, amely új felfogással közelítette meg az információpolitikát. Irányelvvé vált, hogy minden érintettet és érdekeltet fel kellett készíteni az IT kockázatairól és a szükséges óvintézkedésekről, és 1993-ra - az internet szélesebb elterjedésével - nyilvánvalóvá

⁴⁸<https://www.bundeswehr.de/resource/blob/250916/8b3aab4ba0ceb87d592b6c74bd569c52/mad-report-2019-data.pdf>

⁴⁹ <https://www.baks.bund.de/>

⁵⁰ <https://www.unibw.de/home>

⁵¹ <https://www.unibw.de/code>

⁵²https://www.zitis.bund.de/DE/Home/home_node.html

⁵³https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html

⁵⁴ Teljes címén: „Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik” (letöltve: 2021.03.27., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges_pdf.pdf?__blob=publicationFile&v=1)

vált, hogy ez milyen előrelátó megközelítés volt.

A BSI tevékenységét irányító hatályos törvény jelenleg a BSIG⁵⁵, ami 2009-ben lépett hatályba, és azóta több módosításon is átesett, ezen kívül az energiapolitika- és a telekommunikáció területén szintén vannak törvényi szabályok, amelyek a szervezetnek feladatokat szabnak. A BSI alaprendeltetésének tekintették a kezdetektől a kormányzati hálózatok és a központi csomópontok védelmét, 2009-től ehhez - a BSIG egyik novellájának felhatalmazásával – már a szövetségi szervezetek számára kötelező érvényű biztonsági szabványokat is kiadhatott az IT beszerzések és üzemeltetés területén. A BSI a német közigazgatás jelentési központja lett kiberbiztonság témában, annak érdekében, hogy IT krízisekben információkkal és elemzésekkel támogassa a kormányzatot. A gazdaság, tudomány és a társadalom számára pedig mint kompetens kormányzati partnerként és tanácsadóként állt rendelkezésre.

A 2015-ben hatályba lépő IT-Sicherheitsgesetz⁵⁶ tovább szélesítette a feladat- és hatásköröket, és a kritikus infrastruktúrák üzemeltetői számára meghatározott kötelező minimumelvárások megfogalmazásával tovább emelte az IT biztonság szintjét olyan területeken, ahol az esetleges üzemzavar, vagy -kiesés drámai következményekkel járna a gazdaság, állam vagy a társadalom számára. Ezen felül a

kritikus infrastruktúrák üzemeltetői számára bevezették a BSI felé IT biztonsági események kapcsán a jelentési kötelezettséget is.

A már több, mint két éve készülő IT-Sicherheitsgesetz 2.0 2021-re tovább bővítené a BSI felhatalmazásait és digitális fogyasztóvédelem központjává kívánja tenni. Egy IT-biztonságot igazoló címke bevezetésével – és nyilván az ehhez kapcsolódó vizsgálati- és hitelesítési folyamattal – kívánják biztosítani, hogy a fogyasztók tisztában legyenek az igénybevett technológiák, termékek, szolgáltatások és médiajánlatok kockázataival. A központi közigazgatás vonatkozásában is további feladatokat kapna, a kormányzati hálózatokat érintő ellenőrzési- és nyomozati jogkörökkel, valamint a jelentős IT-fejlesztésekbe való kötelező bevonásával.

A Belügyminisztérium gondozásában készülő tervezetet a német sajtó már "lex Huawei"-ként is aposztrofálja, mivel a fogyasztóvédelmi szempontok erősítésének egyik fő oka az 5G technológia erősítése, amiben a feltehetően kínai állami befolyás alatt álló cég világszerte vezető szerepet játszik, különösen a hálózati eszközök terén.

Az IT-SiG 2.0 javaslat lényegi pontjai⁵⁷:

A BSI vonatkozásában

- a BSI nemzeti kiberbiztonságtanúsító hatósági jogkörrel való felruházása,

⁵⁵ Teljes címén: „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik“ (letöltve: 2021.03.27., https://www.gesetze-im-internet.de/bsig_2009/BjNR282110009.html)

⁵⁶ Teljes címén: „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (letöltve:

2021.03.27., https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#_bgbl_%2F%2F%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1616825336632)

⁵⁷ In: Dennis-Kenji KIPKER

- azonosítási és autentikációs eljárások fejlesztése és kiértékelése,
- központi információszolgáltatás az IT termékek biztonsági szempontú technikai színvonaláról,
- a BSI általános IT-biztonsági jelentési központtá alakítása,
- a szövetségi krízisreakció fejlesztése, BSI együttműködés a polgári védelemmel és katasztrófaelhárítással a krízistervek felállítására,
- jelentős zavarok esetén adatbekérési és beavatkozási jog bármely IT rendszerbe annak helyreállítása érdekében,
- felhatalmazás biztonsági kockázatok aktív felderítésére,
- központi tudásbázis kiépítése az IT-biztonság területén,
- emelkedő pénzbírságok.

Új kötelezettségek a kritikus infrastruktúrák szolgáltatói esetében

- korai, támadásokat előrejelző rendszerek telepítése (Security Incident & Event Management System),
- részletes rendszerleírás a BSI számára minden, az üzemmenet szempontjából lényeges IT-eszközzel,
- a kritikus infrastruktúrákra vonatkozó kötelezettségek kiterjesztése bizonyos közérdekből jelentős vállalkozásokra.

A gyártókra vonatkozó új szabályok:

- önkéntes nemzeti IT-biztonsági címke bevezetése,

- kritikus komponensek esetén gyártói garanciák megkövetelése (lásd Huawei-5G vita).

A tervezettel szemben számos kritika is felmerült már:

- mi alapján állapítják meg a kritikus infrastruktúrákra vonatkozó felelősségi szintet más, közérdekből fontos vállalkozásoknál, mely ismérvek szerint lehet ebbe a személyi körbe kerülni?
- a begyűjtésre kerülő nagy információmennyiség kapcsán jogosan merülhetnek fel adatvédelmi aggályok,
- a sérülékenység-vizsgálat eljárási részletei még nem tisztázottak,
- jogbiztonságot és a precizitás igényét sértheti, hogy bizonyos pontokon még elnagyolt a szövegezés,
- egyes kritikák szerint nem tisztázott, hogy a BSI mit fog tenni a feltárt biztonsági rések esetén, nem tart-e vissza információkat állami érdekre hivatkozva⁵⁸,

A 2020-as évben a másik igazán jelentős kiberbiztonsági téma nem defenzív jellegű volt, inkább a német kormányzat nemzetbiztonsági tevékenységével volt összefüggésben. A világ legforgalmasabb Internet csomópontja a frankfurti DE-CIX⁵⁹, amely már napi 91 terabit adatot is továbbított. Nem meglepő módon a német hírszerzés (BND) is figyelemmel kíséri ezt a csomópontot – és sokáig lényegi korlátozások nélkül tette mindezt.

⁵⁸<https://www.golem.de/news/expertenanhoerung-das-unsicherheitsgesetz-2-0-2103-154592.html>

⁵⁹<https://www.theeuropean.de/sven-lilienstroem/cybersicherheit-in-deutschland/>

2020. május 19-ig döntésében a német Szövetségi Alkotmánybíróság kimondta, hogy a külföldi állampolgárok külföldi telekommunikációs forgalmát ugyanúgy megilleti a telekommunikációs titok védelme, ezért az addig folytatott kiterjedt megfigyelési programját a BND-nek le kellett állítania, és az döntésnek megfelelő fokozottabb felügyelet mellett és korlátok között 2021. végéig kell a törvényhozásnak az alkotmánnyal konform új szabályozást megalkotnia.⁶⁰

ÖSSZEGRÉS

Németországban a kibervédelem összkormányzati tevékenység. Az ország közigazgatása tartományi, szövetségi és EU-szinten is aktív a témában, minden jelentősebb állami szerv foglalkozik a területtel, saját felelősségi területén a szükséges szakkompetenciákat kialakította már. Minden hagyományos védelmi és biztonsági funkcionál és szervezetenél folyamatosan és egyre nagyobb büdzsével zajlik a képesség-fejlesztés és innováció, de kiemelt szerepe van a nemzetbiztonsági és a katonai szereplőknek, ami törvényben rögzített feladataikból és hagyományos szerepkörükből is fakad. Jól alátámasztható ez az egyes szervezeteket érintő átszervezések és létszámnövelések tényével is.

A polgári-katonai párhuzamosság, és a kormányzati szerveken is túlnyúló hálózatosság a német rendszerben is alapvetés a kiberbiztonság terén, a szakterületek és a szereplők közötti szoros kooperációval. Az egyes szervezetek és

szférák (állami, gazdasági és civil) között több koordinációs és kooperációs megoldás is biztosítja a rendelkezésre álló információk megosztását, a legjobb gyakorlatok terjedését. Különösen nagy hangsúlyt kap a lényegi tudás összegyűjtése, rendszerezése, és azok eljuttatása az érintettekhez a legkülönbözőbb csatornákon keresztül.

A német kibervédelmi felfogás kifejezetten defenzív alapállású, az idegen rendszerekbe történő behatolásra – hivatalosan - csupán korlátozott körben, az attribúció megállapítása, vagy bűnüldözési, forenzikus szempontok miatt kerülhet sor. A rendszer magas szinten szabályozott és stratégiai dokumentumok segítségével is irányított, ezeket rendszeresen felülvizsgálják és törekszenek a valós kihívásokhoz igazítani, azaz a képességek fejlesztése mellett a német modellben a szabályozás és a kapcsolódó központi közigazgatás és politikai döntéshozatal folyamatos szervezeti fejlesztése is alapvetés. A folyamatban lévő reformokon látható, hogy a biztonsági szempontokat nagy hangsúllyal, lehetőség szerint már az alkalmazott IT-eszközökben még alkalmazás előtt garantálva szeretnék biztosítani, és a minden jelentős rendszer üzemeltetőjének üzemmenetébe kívánják kódolni. A fejlődés felelőse és letéteményese a BSI, a további polgári szolgálatok pedig saját szakterületeik szerinti tevékenységükre koncentrálnak.

A Bundeswehr parancsnokságai és a BAMAD a (katonai) kibervédelemre koncentrálnak, a haderő szerepköre pedig a NATO fejlesztésekkel is szoros szinkront mutat és a kiberen túl az információs

⁶⁰<https://www.bundesverfassungsgericht.de/Share/Docs/Pressemitteilungen/DE/2020/bvg20-037.html>

műveletekkel is összekapcsolódik. Látni kell azonban a tagállami és szövetségi szintű kormányzati irányítás, illetve a koordináció rendszeréből, továbbá a parancsnokságok és a BAMAD alapfeladataiból, hogy ez a képességfejlesztés nem önálló működést hoz létre, hanem egy komplex összkormányzati, ez által politikai-igazságügyi-nemzetbiztonsági-katonai mátrixban megjelenő fontos részrendszerként írható le.

FELHASZNÁLT FORRÁSOK

- [1] CATTARUZZA, Amael: *A digitális adatok geopolitikája. Hatolom és konfliktusok a big data korában*. Budapest, Pallas Athéné Books, 2020.
- [2] CCD CoE: *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit* (letöltve: 2021.04.18., <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/>)
- [3] DE TOMAS COLATIN, Samuele - VÄLJATAGA, Ann: *Data as a Weapon: Refined Cyber Capabilities Under Weapon Reviews and International Human Rights Law*. Tallinn, CCD CoE, 2020.
- [4] FARKAS Ádám: *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai*. In Jog Állam Politika 2019/2. szám, 63-79. o.
- [5] FARKAS Ádám: *A kortárs technológia-fejlődés és innováció viszonya a honvédelmi szabályozással*. In MTA Law Working Papers 2021/4. szám (letöltve: 2021. április 25., <https://jog.tk.hu/mtalwp>)
- [6] FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amael Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei*. In SmartLaw Research Group Working Paper 2021/1. szám (letöltve: 2021. március 27., http://smartlawresearch.hu/storage/app/media/Kiadvanyok/slrgrp_1-2021.pdf).
- [7] FARKAS Ádám: *Hírszerzés és hadművelet metszésében? Gondolatok az angol National Cyber Force kapcsán*. In Military and Intelligence Cybersecurity Research Paper 2021/1., Budapest, Nemzeti Közszerzői Egyetem, 2021.
- [8] HERPIG, Dr. Sven - BEIGEL, Rebecca: *Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten*, Oktober 2020.2, 5. Auflage, (letöltve: 2021.03.27. <https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik>)
- [9] KELEMEN Roland - FARKAS Ádám: *To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare*. In Szabó Marcel – Gyeney Laura – Láncos Petra Lea (eds.): *Hungarian Yearbook of International law and European Law* (2019). Den Haag, Eleven International Publishing, 2020, 203-226. o.
- [10] KELEMEN Roland - SIMON László: *A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái*. In FARKAS Ádám - VÉGH Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások*. Budapest, Zrínyi Kiadó, 2020, 150-170. o.

- [11] KELEMEN Roland: *A kibertámadások nemzetközi jogi olvasata és a NATO értelmezése, különös tekintettel a válaszlehetőségekre*. In FARKAS Ádám (szerk.): *Az állam katonai védelme az új típusú biztonsági kihívások tükrében*. Budapest, Nemzeti Közszerológati Egyetem, 2019, 29-50. o.
- [12] KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése*. In Honvédségi Szemle 2020/4. szám, 65-81. o.
- [13] KIPKER, Dennis-Kenji: *Cybersecurity Regulierung 2021: Update*, (letöltve: 2021.03.27., https://www.researchgate.net/publication/348365761_Cybersecurity-Regulierung_2021_Update)
- [14] LIIVOJA, Rain - NAAGEL, Maarja - VÄLJATAGA, Ann: *Autonomous Cyber Capabilities under International Law*. Tallinn, CCD CoE, 2019.
- [15] MOLNÁR Dóra: *Kiberbiztonság Németországban – pillanatkép a német digitális térről*. In Nemzet és Biztonság, 2018/1. szám, 142-156. o. (letöltve: 2021.03.27., nemzetesbiztonsag.hu/cikkek/neb_2018-01-09_molnar_dora_-_kiberbiztonsag_nemetorszagban-pillanatkép_a_nemet_digitalis_terről.pdf)
- [16] SCHMITT, Michael N. (eds.): *Tallinn Manual On The International Law Applicable To Cyber Warfare*. New York, Cambridge University Press, 2013.
- [17] SCHMITT, Michael N. SCHMITT (eds.): *Tallinn Manual 2.0 On The International Law Applicable To Cyber Warfare*. New York, Cambridge University Press, 2017.
- [18] SZÉPVÖLGYI Enikő: *Kiberbiztonság – mindannyiunk felelőssége*. In Katonai Jogi és Hadijogi Szemle 2021/1. szám, 183-190. o. (letöltve: 2021.03.27., http://www.hadjog.hu/wp-content/uploads/2021/04/Katonai-szemle-2021_1_final.pdf)



Military and Intelligence CyberSecurity Research Paper 2021/2.

Szerző(k) / Author(s):

Dr. Vikman László

Kézirat lezárásának ideje / Manuscript closing time:

2021.04.25.

Szerkesztők / Editors:

Dr. Farkas Ádám PhD

Dr. Magyar Sándor PhD

Kiadó / Publisher:

Nemzeti Közsolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer
Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:

Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:

<https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper>

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:

2786-3778

A borító <https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security> címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at <https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security>.

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.

The opinions and resolutions included in each issue of the series reflect the authors' own opinions. They should not be construed as an official point of view of either the publisher or the institutions employing the author.