HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 139–161.
DOI: 10.32567/hm.2025.1.8

Lendvai Tünde[1]

Kiberbiztonsági körkép Japánról

Japán kiberbiztonsági reformja és kiberhatalmi ambíciója

Cybersecurity Overview of Japan

Japan's Cybersecurity Reform and Cyberpower Ambition

Absztrakt

Az utóbbi évtizedben Japán jelentős erőforrásokat fektetett kibervédelmi rendszerének fejlesztésébe, amit a regionális ellenfelei – Oroszország, Kína és Észak-Korea – által demonstrált kibertámadó képességekhez kapcsolódó fenyegetéspercepció váltott ki. A szekunder forrásokat elemző kutatás arra irányult, hogy feltárja, milyen országspecifikus sajátosságok teszik lehetővé vagy korlátozzák az ország stratégiai dokumentumaiban előirányzott aktív kibervédelem megvalósítását és az offenzív kiberképességek alkalmazását. A tanulmány amellett érvel, hogy ezt három tényező befolyásolja. Az első a jogszabályi környezetből adódik, ami továbbra is olyan mértékben korlátozza Japán lehetséges válaszlépéseit a kibertérben, hogy a sikermegtagadó elrettentési mechanizmusokat alkalmazó kibervédelem hatékonysága megkérdőjelezhető. A másik két tényező biztonságpolitikai relációban mozdítja elő az offenzív képességek jogszerű alkalmazását. Ennek elemei a nemzetközi kibervédelmi kooperációs hálózat kiépítése és a kiberbiztonsági ökoszisztéma rezilienciáját növelő reformok.

Kulcsszavak: Japán, proaktív kibervédelem, kiberstratégia, offenzív kiberképességek, kiberbiztonság, Önvédelmi Haderő, kibervédelem

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: lendvai.tunde@uni-nke.hu

Abstract

Over the past decade, Japan has invested significant resources in developing its cyber defense system, driven by threat perceptions associated with the demonstrated offensive cyber capabilities of its regional adversaries such as Russia, China, and North Korea. This research, based on secondary source analysis, explores the country-specific factors that enable or limit the implementation of active cyber defense outlined in Japan's strategic documents and the application of offensive cyber capabilities. The study argues that three key factors influence these efforts. The first stems from the legal framework, which continues to constrain Japan's potential responses in cyberspace to such an extent that the effectiveness of cyber defense based on denial-of-success deterrence mechanisms is questionable. However the other two factors, in a security policy context, facilitate the lawful use of offensive capabilities. These include the development of an international cyber defense cooperation network and reforms aimed at enhancing the resilience of the cybersecurity ecosystem.

Keywords: Japan, proactive cyber defence, cybersecurity strategy, offensive cyber capability, cybersecurity, Japan Self Defence Force, cyber defence

Bevezetés

Az utóbbi évtizedben Japán kibervédelmi szakpolitikájának egyik legmegosztóbb dilemmája volt, hogy a pacifista alkotmányos megkötések betartása mellett miként készíthető fel kibervédelmi ökoszisztémája – az államigazgatás, a kritikus infrastruktúrák és a Japán Önvédelmi Haderő – defenzív rendszerekkel és eszközökkel, valamint kizárólag védelmi céllal alkalmazható limitált offenzív képességekkel, az egyre jelentősebb kibertámadó képességekkel rendelkező regionális ellenfelei (Oroszország, a Kínai Népköztársaság és a Koreai Népi Demokratikus Köztársaság) jelentette fenyegetéssel szemben.[2] Noha a japán külpolitika proaktív pacifizmusa jól működik az amerikai–japán szövetség keretében, és összhangban áll az úgynevezett passzív kibervédelem módszereivel, a japán kormányok időről időre keresik a lehetőséget az offenzív kiberképességek jogszerű alkalmazásának előmozdítására, ami – például elrettentési mechanizmusok segítségével – magasabb szintű védelmet tenne lehetővé.[3] A publikáció bemutatja, hogy az elmúlt évtizedben milyen tényezők formálták Japán kibertéri fenyegetéspercepcióját és kiberképességeit, amelyek eredményeképp a tokiói vezetés a passzív védelmi megközelítéstől a 2018-as és 2021-es Kibervédelmi Stratégiában az aktív kibervédelem irányába mozdult el.[4] Az egyes fejezetekben időrendben áttekintjük azon országspecifikus nehézségeket vagy kibervédelmi szakpolitikai reformokat, amelyek napjainkban is hátráltatják az aktív kibervédelem megvalósítását.

[2] Katagiri 2022: 49–51; Bartlett 2020: 93–94; Basu 2024.
[3] Osawa 2024: 74; Najah 2024; Siripala 2024.
[4] Osawa 2024: 71–72; Kosuke 2024.

A témában elérhető, főként szekunder forrásokon alapuló szakirodalom feldolgozása deduktív és leíró kutatási módszerrel valósult meg. A kiberbiztonsági incidensek esetszámának vizsgálatához a szerző a JPCERT/CC japán nemzeti CSIRT (Computer Security Incident Response Team, számítógép-biztonsági incidenskezelő csoport) negyedéves jelentéseiben publikált adatait használta fel, amelyeken idősorelemzést végzett a 2019–2023 közötti időszakban. A kutatás arra irányult, hogy feltárja, milyen elméleti megközelítés és országspecifikus sajátosságok teszik lehetővé vagy korlátozzák Japánban az offenzív kiberképességek alkalmazását, és ezáltal az aktív kibervédelmi stratégia kialakítását (K1). Jelen tanulmány amellett érvel, hogy ez elsősorban három tényezőre vezethető vissza.

H1: Japán kiberbiztonsági fenyegetéspercepcióját a regionális ellenfelei által kifejlesztett és egyre gyakrabban demonstrált offenzív kiberképességek, valamint az ország gazdasági rendszerének és haderejének információs technológiáktól való függősége alakítja.

H2: A kibertérből érkező kihívások ellensúlyozása érdekében Japán újabban egy jóval szélesebb körű – az USA-partnerségen felüli – nemzetközi kooperációs hálózat kiépítésére törekszik.

H3: A japán aktív kibervédelmi stratégia hatékony végrehajtását korlátozza a jogszabályi környezet.

A japán kibervédelmi stratégia jogi korlátai (H3)

A japán kibervédelmi reformfolyamat eredményeinek értékeléséhez elsőként azt fontos megérteni, hogy az alkotmányos megkötések milyen korlátok közé szorítják a kiberstratégiai modellt és az offenzív kiberműveletek önvédelmi célú alkalmazhatóságát. A fejezet a passzív és aktív kibervédelem, valamint az offenzív képességek terminológiája mentén mutatja be, hogy a jogi környezet miként befolyásolja a japán kibererő fejlesztési lehetőségeit.

A passzív kibervédelem és az aktív kibervédelem közötti terminológiai különbségeket Berzsenyi a disszertációjában többféle megközelítésben mutatta be.[5] Amennyiben az elhatárolást a tevékenység típusa és célja mentén kívánjuk ismertetni, a passzív kibervédelem fő ismérve, hogy az aktivitás nem lépi túl a saját hálózat határait, mert az információk és rendszerek védelmét a támadások elhárításával és a sérülékenységek csökkentésével biztosítja. A passzív kibervédelem szinte minden jogrendszerben, így Japán esetében is elfogadott, mivel célja a kiberrendszerek határvédelmének kialakítása (például vírusvédelmi eszközökkel és behatolásészlelő rendszerekkel), illetve támadásokkal szembeni rezilienciájának kiépítése (például *zero-trust* model szerinti rendszertervezési megoldásokkal). Ennélfogva a passzív védelem nem alkalmaz közvetlen válaszlépéseket a támadó infrastruktúra megzavarása vagy megsemmisítése érdekében, ezért nem feltételez támadó, csak önvédelmi szándékot.[6]

[5] Berzsenyi 2023: 77–84.
[6] Berzsenyi 2023: 77–78.

Ezzel összefüggésben elmondható, hogy a japán kormányok évtizedek óta úgy értelmezik az 1946-os Alkotmány híres 9. „békecikkét",[7] miszerint a támadó katonai erő alkalmazásának tilalma nem zárja ki Japán önvédelemhez való alapvető jogát, illetve az annak gyakorlásához szükséges minimális fegyveres erő fenntartását, így a defenzív és offenzív képességeket magában foglaló kibererő felépítése és fenntartása indokolt. Bartlett több kutatásában is kiemeli, hogy a japán Alkotmány önvédelemre vonatkozó megkötése befolyásolja a kibertérben műveleteket végrehajtó egységek határokon belüli és kívüli jogszerű alkalmazhatóságát is.[8] Emiatt – a passzív kibervédelmi stratégiai modellel ellentétben – az aktív kibervédelem Japán számára jogilag és etikailag érzékenyebb terület, abból kifolyólag, hogy noha alapvetően védekező jellegű, a határai elmosódhatnak az offenzív műveletek irányába. Berzsenyi megfogalmazásában: „az aktív kibervédelem olyan közvetlen védelmi tevékenység, ami rombolja, csökkenti vagy megsemmisíti a kiberfenyegetések baráti erőkkel szembeni hatékonyságát."[9] Noha a szakirodalomban nincs konszenzus a tekintetben, hogy milyen megoldások és rendszerek tekinthetők aktív kibervédelmi képességnek, néhány példa következik: a behatolásmegelőző rendszer *(intrusion prevention system)* vagy *honeypot* elhelyezése, valamint a védett hálózaton túli olyan válaszlépések alkalmazása a támadások megelőzésére és megzavarására, mint a C2 szerverek *(command and control)* hozzáférésének blokkolása vagy irányításának átvétele.[10]

Japánban a határokon túlnyúló – önvédelmi célú – kiberműveletek jogszerű alkalmazhatósága kérdéses, ám az ország biztonság- és védelempolitikai gondolkodásában már megjelent ennek alapja. Disszertációjában Fábián Emília részletesen bemutatja, hogy a kizárólag védelemorientált megközelítés és a fegyveres erő passzív önvédelmi, avagy reagáló célú alkalmazhatósága által szabott alkotmányos kereteket az Abe-kormány (2012–2020) biztonságpolitikája igyekezett leginkább kitágítani proaktív irányba nemzeti és nemzetközi relációban egyaránt. A kormányzó Liberális Demokrata Párt (a továbbiakban: LDP) a proaktív pacifizmus politikáját többek közt az USA haderejének való kiszolgáltatottsággal és a megváltozott biztonságpolitikai környezetből eredő sokrétű fenyegetéssel indokolta.[11] Nemzetközi relációban a tokiói vezetés amellett érvelt, hogy Japánnak a globális felelősségvállalás jegyében aktívan fel kell lépnie az olyan határokon átívelő fenyegetések ellen, mint a terrorizmus és a kiberbűnözés, ezért növelnie kell szerepvállalását a nemzetközi békemissziókban (a kollektív önvédelmi jog gyakorlása által), amihez az Önvédelmi Haderő képességeinek fejlesztése elengedhetetlen.[12] Katagiri kutatásai is alátámasztják, hogy nemzeti relációban a kabinet álláspontja azt tükrözte, hogy a regionálisan növekvő militarizációs trendek hatása mellett a kibertérből érkező kihívások csökkentése nélkül nem garantálható a nemzetközi kereskedelem zavartalansága, ezáltal a nemzetgazdaság stabilitása.[13]

[7] The Constitution of Japan (Japán Alkotmánya), 9. cikk.
[8] Bartlett 2019: 17–30; Bartlett 2020: 94–96.
[9] Berzsenyi 2023: 78.
[10] Berzsenyi 2023: 80–82.
[11] Fábián 2015: 180–182.
[12] Fábián 2015: 169–174.
[13] Katagiri 2021: 332–336.

A híres 9. cikk mellett Japán jogi környezete több ponton is szigorú korlátok közé szorítja a nemzeti szintű kibervédelmi feladatok egyik fontos elemét, a kibertérben végzett felderítő műveletek és a rádióelektronikai hírszerzés jogszerű végrehajtását.[14] Egyfelől az Alkotmány 21. cikkéből vezethető le a cenzúra tilalma és a távközlési titok védelme, ami mellett a távközlési törvény 4. cikke előírja, hogy a távközlési szolgáltató által lebonyolított kommunikáció bizalmas jellegét tilos megsérteni.[15] Ezt a szabályozást a japán jogrend szigorúbban értelmezi és interpretálja más országokhoz képest, ami megnehezíti a végrehajtó hatalom és a távközlési szolgáltatók számára az adatforgalom megfigyelését, ezzel a kiberműveletek észlelését és a támadó infrastruktúra elemeinek beazonosítását. A japán Büntető törvénykönyv 161. cikke tiltja az elektronikus vagy mágneses feljegyzések jogosulatlan létrehozását, míg a 168. cikk tiltja a jogosulatlan parancsokat tartalmazó elektronikus vagy elektromágneses rekordok készítését, így rendkívül korlátozott módon valósulhat meg az állami szereplők számára a kommunikáció elemzése és visszafejtése a támadó aktor beazonosítása érdekében.[16] Habár belföldön a Védelmi Minisztérium és az Önvédelmi Haderő korlátozott mértékben jogosult a vezeték nélküli kommunikáció megfigyelésére, a vezetékes digitális kommunikáció széles körű megfigyelése nem engedélyezett még nemzetbiztonsági célból sem.[17]

Japánban napirenden lévő jogi kérdés az is, hogy a kiberbűncselekményeket elszenvedő magáncégek kötelezhetők-e arra, hogy bejelentsék az incidenst az állami szerveknek. A kötelező jelentéstétel hiánya miatt a vállalkozások jellemzően elkerülik azon incidensek nyilvánosságra hozatalát, amelyek sikeresen kompromittálták a rendszerüket (viszont a személyes adatokat érintő incidenseket kötelező jelenteni Japánban is).[18] Ez késlelteti a kiberfenyegetésekre, sérülékenységekre és támadási technikákra vonatkozó információk vállalatok közötti kölcsönös megosztását, ami azt eredményezi, hogy az állami és a magánszektor közt sem történik előrelépés a gyakori támadási minták és technikák megértésében, ami szükséges lépés az ellenintézkedések kialakításához.[19]

A kiberműveletek észlelhetőségén túl a támadó infrastruktúra semlegesítésére irányuló erőfeszítéseket is összhangba kell hozni Japán jogosulatlan számítógép-hozzáférést tiltó törvényével (Japan's Act on Prohibition of Unauthorized Computer Access). Osawa kutatásaiban rámutat arra, hogy más államokkal ellentétben a jogosulatlan számítógépes hozzáférés tilalma alól a japán kormányzati szervek nem képeznek kivételt. A támadó infrastruktúra feletti irányítás átvétele mellett a semlegesítés másik módja lehet egy kártékony program *(malware)* küldése a támadás forrására, ami ütközhet a malware létrehozását és alkalmazását büntető törvényekkel, ezért a büntetőjog revíziója is szükséges lenne az aktív kibervédelem kialakításához.[20]

[14] Katagiri 2021: 339–342.
[15] A 2022. évi 70. törvény a japán távközlési vállalkozásokról szóló 1984. évi 86. törvény egyes rendelkezéseinek módosításáról, 4. cikk; Japán Alkotmánya, 21. cikk.
[16] Osawa 2024: 73–74; Onodera–Tanaka–Shimamura [é. n.].
[17] Katagiri 2021: 339.
[18] Siripala 2024; Japan Mulls Requiring Private Sector Operators to Report Cyberattacks on Infrastructure 2024.
[19] Siripala 2024; Alan 2024.
[20] Osawa 2024: 74.

Összességében tehát a távközlési és büntetőjogi megkötések kifejezetten a hírszerzési célú, valamint az offenzív képességek jogszerű alkalmazhatóságát korlátozzák. Ez utóbbi megnyilvánulását érdemes elméleti oldalról is bemutatni. Az amerikai összhaderőnemi megközelítésben alkalmazott terminológia alapján az offenzív kiberműveleti képességek feloszthatók a műveleti tér megtagadására és manipulálására[21] irányuló tevékenységekre. Az ellenfél erőforrásokhoz történő hozzáférését gátló, úgynevezett megtagadó műveletek további három kategóriába sorolhatók hatásuk alapján: degradálás, megzavarás és pusztítás. A degradálás redukálja az ellenfél által használható erőforrásokat, míg a kibertérbeli megzavarás időszakosan ellehetetleníti az ellenfél által használt infrastruktúra hozzáférését, így megakasztja tevékenységét. A tudományos szakirodalom Japán legnagyobb kibervédelmi stratégiai problémájaként azonosítja, hogy az alkotmányos megkötések és a jogi környezet még a legtágabb értelmezésben is összeférhetetlenek egyes offenzív kiberműveletekkel, így például a megtorló elrettentési mechanizmusokat (visszatámadás, *hackback*) alkalmazó kibervédelmi modell megvalósításával.[22] Enélkül azonban kérdéses hatékonysággal vagy egyáltalán nem valósítható meg az aktív kibervédelmi stratégia azon karakterisztikája, amely a védett, saját hálózaton túli ellenlépéseket foglalja magában.[23]

A szakirodalom-elemzés azt mutatja, hogy a meglévő jogrendszer szigorúan a passzív és aktív kibervédelmi stratégiai modellel összehangolt offenzív kiberképességek fenntartását teszi lehetővé. Emiatt a kormányzó LDP-nek feltehetően szándékában áll a kiberbiztonsági jogszabályok revíziója a határokon átnyúló aktív kibervédelemre vonatkozó kormányzati stratégia bevezetése érdekében.[24] Ez lehetővé tenné, hogy a nemzetbiztonsági aggályokat felvető súlyos kibertámadások megelőzhetők legyenek például a támadó aktorok szervereibe való behatolással és azok kiiktatásával.[25] A kormányzati szándékot az támasztja alá, hogy 2023 januárjában a kabinet titkárságán létrehoztak egy hivatalt, amely a kiberbiztonsági szabályozások előkészítésével foglalkozik.[26]

A japán kibervédelmi szakpolitika reformja 2012–2022 között: egy globális kiberhatalom víziója (H1)

Ahogyan a fentiekben is említettük, a hagyományosan passzív kibervédelmi szakpolitika reformját a második Abe-kormány kezdte meg azon törekvésével, hogy a kibertér használatát nemzetbiztonsági politikájának középpontjába emelje, és a 2012–2016 közti védelempolitikai intézkedéseivel stabil alapot teremtsen Japán globális kiberhatalommá válásához.[27] Kallender és Hughes amellett érvelt, hogy a tokiói vezetés kiberhatalmi ambíciójának megvalósításához szükséges reformok nemzeti és nemzetközi

[21] Berzsenyi a következőképp fogalmazta meg a manipulálást: „lényegében az ellenfél rendelkezésére álló információk, információs rendszerek és/vagy hálózatok feletti ellenőrzést és az ezekben – a parancsnok célkitűzései szerint – végrehajtható változtatási képességet jelenti." Berzsenyi 2023: 85.
[22] Katagiri 2021: 335, 339–342; Bartlett 2020; Osawa 2024: 72–74.
[23] Berzsenyi 2023: 80–84.
[24] Siripala 2024.
[25] Kosuke 2024.
[26] Osawa 2024: 74.
[27] Gady 2017: 24–28.

pillérét alkotó intézkedéseket egy újfajta, szekurizációs elemeket is magában hordozó védelempolitikai narratíva is kísérte. Ezt támasztja alá, hogy az LDP már 2012 februárjában – közvetlenül a kormányra jutása után – a *Javaslat az információbiztonságról* című dokumentumban a nemzetbiztonság kritikus elemének nyilvánította a kibertér biztonságának megtartását.[28] Ezen túlmenően az Abe-kormány első, 2013. évi Kiberbiztonsági Stratégiája nóvumként részletezte a japán Védelmi Minisztérium és a Japán Önvédelmi Haderő szerepét a „külföldi kormányok által fegyveres támadás részeként végrehajtott kibertámadások és más olyan nemzeti szintű kibertámadásokra adott válaszreakciókban, amelyekben külföldi kormányok részvétele feltételezhető".[29] Ennek megfelelően az Önvédelmi Haderőt jelölték ki felelősnek a kiberműveletek elhárításáért, ha azok fegyveres támadások részét képezik, és felhatalmazták a Védelmi Minisztériumot, hogy hozzon létre egy védelmi célú mandátummal rendelkező kiberegységet a haderőben (Kibervédelmi Csoport, Cyber Defense Unit vagy Cyber Defence Group).[30]

A szekurizációra vonatkozó érvelést erősíti Soesanto kutatásának eredménye, ami rávilágít arra, hogy az LDP a kibertérből érkező fenyegetés kezelésére egyre militarizáltabb intézkedéseket hozott, és centralizáló reformokat indított meg a kritikus információs infrastruktúrákra fókuszálva, amivel politikai szinten is reagált két jelentős, 2011-ben nyilvánosságra került incidensre.[31] Az egyik esetben, 2011 júliusában, a japán képviselőház szervereit kompromittálta egy kínai hátterű fejlett perzisztens fenyegetés (a továbbiakban APT) az Icefog nevű interaktív kémprogrammal *(backdoor)*.[32] A másik eset ugyanezen év augusztusában történt, amikor az ország egyik legjelentősebb hadiipari és nehézipari vállalatát, a Mitsubishi Heavy Industries ellen követtek el összehangolt hírszerzési célú kampányt, noha a vállalat álláspontja szerint titkos dokumentumok nem szivárogtak ki.[33] A Kabinet szekurizációs törekvéseiben feltehetően olyan nemzetközi események is szerepet játszottak, mint az iráni atomprogram elleni Stuxnet-művelet és a 2011-es dél-koreai kereskedelmi bankok, továbbá a védelmi ipari vállalatok és kormányzati szervek weboldalait érő, észak-koreai DDoS-támadás.[34]

A defenzív képességfejlesztési irányban 2019-ben következett be újabb változás, amikor a Mitsubishi Co.-t újfent sikeresen kompromittálta egy állami hátterű aktor, ezúttal az APT41 csoport.[35] Ezen fejlett perzisztens fenyegetés tevékenységét gyakran azonosítják a Kínai Népköztársaság (a továbbiakban KNK) állam alatti kiberegységeinek műveleteivel.[36] Az állami hátterű offenzív kibertéri jelenlét növekedése miatt a tokiói vezetés végül amellett kötelezte el magát, hogy 2023-ig felülvizsgálja, miként alakíthatók offenzív elemeket magában foglaló kiberműveleti képességgé az Önvédelmi

[28] Kallender–Hughes 2016: 127.
[29] Japán Információbiztonsági Politikai Tanács 2013: 42.
[30] Kallender–Hughes 2016: 128.
[31] Soesanto 2020: 8, 11, 30.
[32] Kaspersky Lab 2013: 14.
[33] Soesanto 2020: 8.
[34] Koo 2013.
[35] Paganini 2020.
[36] Lásd például MITRE [é. n.]; Malpedia [é. n. a].

Haderőben meglévő kapacitásai.[37] Mivel Japán jogi környezete korlátok közé szorítja a katonai erő alkalmazását, a kiberegységek offenzív képességeit úgy limitálták, hogy azokat katonai konfliktus keretében a hálózatok és számítógépes rendszerek megzavarására alkalmazhassák, nem pedig arra, hogy fizikai rendszerekben kárt okozva vagy a kibertér adottságait fegyverként felhasználva támadást indítsanak más államok ellen.[38] Ezt a szakpolitikai álláspontot tükrözi Japán legutóbbi, 2021-es Kiberbiztonsági Stratégiája (Cybersecurity Strategy), amely a nemzetbiztonsági érdekből végzett tevékenységek és az ország gazdasági stabilitása szempontjából közelíti meg a kibertér biztonságát. A stratégia a „szabad, tisztességes és biztonságos kibertér" alapelveinek garantálásához a nemzetközi együttműködés szükségességét hangsúlyozza az USA, Ausztrália és India irányába, valamint az ASEAN-tagállamok részére nyújtott kibervédelmi kapacitásépítő programok folytatását az ellátási láncok megbízhatóságának megőrzéséhez. A dokumentum belföldre fókuszáló hatókörében Japán védelmi, elrettentő és helyzetfelismerési képességeinek erősítését jelölte ki elsősorban. Ezenfelül az LDP a humán erőforrás képzésének és digitális kompetenciáinak egyéni fejlesztésére irányuló programok további finanszírozását is megerősítette a stratégiai célok közt.[39] Gazdasági-társadalmi vonatkozásban a vállalati szféra innovációs képességének és digitális transzformációjának támogatása jelent meg politikai célkitűzésként.[40]

A Kisida-kormány 2022 decemberében három fontos védelmi dokumentumot hagyott jóvá, amelyek együttesen alkotják Tokió átfogó védelempolitikáját: a Nemzeti Biztonsági Stratégiát (National Security Strategy), a Nemzeti Védelmi Stratégiát (National Defense Strategy), amely a védelmi célokat és az elérésükhöz szükséges eszközöket határozza meg, valamint a Védelmi Fejlesztési Programtervet (Defence Buildup Plan), amely tartalmazza a 2023–2027-es védelmi kiadásokat és az eszközbeszerzések volumenét.[41] A Nemzeti Biztonsági Stratégia nóvumként említi a megelőző célú kiberműveletek végrehajtását még olyan esetekben is, amelyek nem minősülnek fegyveres támadásnak, azonban súlyos nemzetbiztonsági aggályokat vetnek fel a kormányzat és a létfontosságú, kritikus infrastruktúrák érintettsége miatt.[42] Ez valójában a jogi korlátok jelentette problémát nem rendezi, csak politikai felhatalmazást jelent a japán kormány számára, hogy utasítást adjon a potenciális támadó infrastruktúrájába való behatolásra annak semlegesítése érdekében. Vagyis sikermegtagadó elrettentési mechanizmusként az ellenfél képességeinek degradálását és megzavarását teszi lehetővé, megtorló lépéseket nem.[43] Noha a 2022-es Nemzeti Biztonsági Stratégia elsősorban a rakétavédelem kontextusában nevesítette az ellencsapás lehetőségét, ezzel párhuzamosan a japán biztonságfelfogásban elméleti lehetőség nyílt az Önvédelmi Haderő offenzív kiberképességeinek szélesebb körű alkalmazhatóságára az aktív kibervédelmi stratégia keretében.[44] A Nemzeti Védelmi Stratégia az Önvédelmi Haderő szerepének bővítését tűzte ki a következő tízéves időtávra a tekintetben, hogy a katonai

[37] Japán Védelmi Minisztérium 2019: 229.
[38] Bartlett 2020: 96.
[39] Japán Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központja 2021: 6–7.
[40] Japán Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központja 2021: 3–4, 7, 10.
[41] Lottaz 2023.
[42] Hideshi 2023.
[43] Berzsenyi 2023: 80–85.
[44] Hideshi 2023.

hálózaton kívüli entitások biztosításával hozzájáruljon Japán teljes kiberterének védelméhez is. Ehhez a politikai célkitűzéshez igazodva a 2022-es Védelmi Fejlesztési Programterv a 2027-es pénzügyi évre előirányozta az Önvédelmi Haderő újonnan létrehozott Kibervédelmi Parancsnokságának (Cyber Defence Command, korábban Cyber Defence Unit) bővítését mintegy 4000 főre, és a teljes kibervédelmi állomány létszámának növelését 20 000 főre.[45]

Összességében a proaktív pacifizmus irányvonalát a Szuga-kormány (2020–2021) és a Kisida-kormány (2021–2024) is követte. A sokrétű fenyegetéspercepció kezelésére Tokió olyan stratégiát alkalmaz, amellyel nem engedi műveleti előnyhöz jutni a létszámában és a rendszeresített eszközök mennyiségében fölényben lévő kínai haderőt. Ezért a japán hosszú távú haderő-modernizáció[46] a korábbi sikermegtagadás-alapú elrettentési stratégia mellett – amelynek célja, hogy az elérendő katonai célhoz képest túl sok erőforrást emésszen fel egy támadás – a megtorlásalapú elrettentéshez szükséges képességek kiépítésére törekedett az elmúlt 15–20 évben, amivel akár kínai vagy észak-koreai támaszpontok megsemmisítése is lehetséges egy támadás esetén.[47] Mindezek eléréséhez elsősorban az alkotmány értelmezésének megváltoztatására volt szükség, amivel lehetővé vált a védelempolitikai reformok végrehajtása valamennyi műveleti tér, így a fentiekben részletezett *kiberdomain* és kibererő vonatkozásában is.

Japán kiberbiztonsági ökoszisztémája és a centralizáló reformok áttekintése

Az Abe-kormány (2012–2020) kiberhatalmi ambíciója megvalósításának nemzeti (belföldre irányuló) pillére egy jogilag jól szabályozott, centralizált felelősségi körökkel működő kiberbiztonsági igazgatási rendszer kialakítására irányult, amely szakpolitikai háttértámogatást nyújt a kabinet legfőbb biztonságpolitikai döntés-előkészítő szerve, a Nemzetbiztonsági Tanács (National Security Council) részére.[48] Ennek alapjait a 2014-től hatályos Kiberbiztonsági kerettörvény (Basic Act on Cybersecurity)[49] fekteti le, amelyben a japán törvényhozás regionális viszonylatban úttörőként határozta meg a kibervédelem alapfeladatait és államigazgatásra vonatkozó stratégiai céljait (amelyeket 2016-ban, 2019-ben és 2022-ben felülvizsgált), továbbá rendelkezett a kibervédelmi ökoszisztémát koordináló szervezetek létrehozásáról.[50]

A japán kibervédelmi szervek hierarchiájának tetején egy miniszteri szintű koordinációs szerv, a Kiberbiztonsági Stratégiai Központ (Cybersecurity Strategic Headquarters) helyezkedik el, amelyben állandó szakértői testületek működnek, például a kritikus infrastruktúrákat, az emberi erőforrásokat és információbiztonsági tudatosítást, valamint a technológiai fejlesztési programokat érintő ügyekben. A központ alárendeltségében 2015-től működik a Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központ

[45] Osawa 2024: 72; Japán Védelmi Minisztérium 2022a: 26; Japán Védelmi Minisztérium 2022b: 11–12.
[46] Az elmúlt 15–20 évben Japán haditengerészeti (például kékvízi hajóegységek és fedélzeti rakétaelhárító rendszerek) és 4–5. generációs légierő-részképességek minőségi fejlesztésével (és elegendő mennyiség rendszeresítésével) kezdte ellensúlyozni a KNK haderejének mennyiségi fölényét.
[47] Szakértői interjú, podcast alapján készült. FIXTV HUNGARY 2024.
[48] Bartlett 2019: 26.
[49] Japán Kiberbiztonsági kerettörvénye (The Basic Act on Cybersecurity) [2014. évi 104-es törvény].
[50] Basu 2024.

(National Centre for Incident Readiness and Strategy for Cybersecurity, NISC), amely a Japán Önvédelmi Haderő és a rendőrség mellett működve koordinálja a kibervédelmi szakpolitika végrehajtását és a kibervédelmi operatív egységek irányítását. A konkrét incidensekre reagáló, műveleti kiberegységek a Kormányzati Biztonsági Műveleti Koordinációs Csoport (Government Security Operation Coordination Team, GSOC) és a Kiberincidens Mobil Segédcsapat (Cyber Incident Mobile Assistant Team, CYMAT) keretei közt folytatják tevékenységüket. Japán kibervédelmi ökoszisztémájának további fontos szerve a Kiberbiztonsági Tanács (Cybersecurity Council), amelynek fő funkciója, hogy a köz- és magánszféra szereplői közt biztosítsa az információátadást, és korai előrejelzést adjon kibervédelmi kihívások és fenyegetések felmerülése esetén a Kiberbiztonsági Stratégiai Központnak.[51]

A Kiberbiztonsági Stratégiai Központ mellett a kiberbiztonsági szakpolitika tervezésének második ágát (2021-től) a Digitális Ügynökség (Digital Agency) tevékenysége határozza meg. A Digitális Ügynökség a kormányzási funkciók digitális transzformációjának kivitelezéséhez nyújt projektmenedzsment-támogatást (például a társadalmi célcsoport tudatosítása kapcsán), továbbá iránymutatást ad a kormányzati szervek részére az infrastruktúra rezilienciájának növeléséhez (például piaci szférában bevált innovatív technológiák adaptációja kapcsán).[52] A szakpolitikai tervezés harmadik ága a kritikus infrastruktúrák védelme, ennek érdekében Japán rendszeresen ad ki akcióterveket. Jelenleg ezen akciótervek negyedik kiadása hatályos (2022-es kiberbiztonsági politika a kritikus infrastruktúrák védelmére, Cybersecurity Policy for Critical Infrastructure Protection). Az akcióterv célkitűzései közül kiemelendő a kockázatmenedzsment-folyamatok standardizálása, az érintett ágazatok számára releváns fenyegetésekről szóló információmegosztó *(threat intelligence)* folyamatok megalapozása és folyamatos fejlesztése, valamint az a törekvés, hogy nemzeti szintű incidenskezelő szervezeteket hozzanak létre, amelyek kifejezetten ezzel a speciális (értsd: nemcsak IT, hanem ipari környezetet is működtető) területtel foglalkoznak.[53]

A centralizáló reformok nemcsak az államigazgatási szerveket érintették, hanem az Önvédelmi Haderőt is. A jelenlegi struktúrában a szárazföldi, a haditengerészeti, valamint a légi- és űrerők összhaderőnemi együttműködését a Központi Parancsnoki Rendszer (Central Command System, CCS) és a Védelmi Információs Infrastruktúra (Defense Information Infrastructure, a továbbiakban DII) biztosítja, amelynek működtetését és karbantartását egy dedikált parancsnokság (C4 Rendszerek Parancsnoksága, C4 Systems Command) felelősségi körébe rendelték. A DII a japán Védelmi Minisztérium és a haderő közös információs és kommunikációs hálózata, amely az egyes bázisokat és helyőrségeket köti össze, két részre osztva: nyílt rendszerre (kapcsolat az internettel) és zárt rendszerre (titkosított adatok kezelése céljából, ami nem csatlakozik külső hálózatokhoz). A C4 Rendszerek Parancsnoksága két egységet foglal magában: a hálózatüzemeltetési csoportot *(network operation group)* és a központi parancsnoki rendszer működtetéséért felelős egységet *(central command post operations unit)*.[54]

[51] *National center of Incident readiness and Strategy for Cybersecurity NISC*. About NISC. [n.d.].
[52] Japan Digitális Ügynökség [é. n.].
[53] Japán Információbiztonsági Politikai Tanács 2014: 22–28; Japán Kiberbiztonsági Stratégiai Központ (NISC) 2022: 12–35.
[54] Soesanto 2020: 22–23.

A fentiekben említett kibervédelmi egység (Cyber Defence Unit) is ezen parancsnokság alárendeltségébe tartozott 2022-ig,[55] azonban a legfrissebb Védelmi Fejlesztési Programterv önálló parancsnoksági státuszba emelte. Ez a változás célzottan arra irányul, hogy a 2023 márciusában 540 fős létszámmal megalakuló Japán Kibervédelmi Parancsnokság (Cyber Defence Command) már egy agilisabb és autonómabb struktúrában legyen képes reagálni a kibertérben jelentkező fenyegetésekre, valamint hatékonyabban integrálhassa az offenzív képességeket és a védelmi műveleteket.[56] A Kibervédelmi Parancsnokság (Cyber Defence Command) napjainkra mintegy 800 fős állománya önállóan felel a kiberfenyegetések felderítéséért, a DII védelméért, és biztosítja az Önvédelmi Haderő hálózatának folyamatos védelmi felügyeletét.[57] A fentiekben bemutatott jogi megkötések és stratégiai dokumentumok aktív kibervédelemre vonatkozó célkitűzéseivel összhangban a Kibervédelmi Parancsnokság hatáskörébe tartozik az operatív kiberműveletek végrehajtása.[58]

Kibervédelmi és kiberdiplomáciai célok megjelenése a külpolitikában (2012–2022)

Japán kiberhatalmi ambíciója megvalósításának nemzetközi pillére két területen kívánt eredményeket elérni. Ezen területek egyike az USA-val való kooperáció további bővítése, noha a két nemzet minisztériumi és ügynökségi delegációi már 2013-tól évenként egyeztettek a Japán–USA Kiberdialógus (Japan-US Cyber Dialogue) keretében, a kétoldalú operatív együttműködés és a kibervédelmi szakpolitika összehangolása érdekében.[59] A második Abe-kormány – a Japán és az USA közötti kiberdialógus napirenden tartása mellett – elsősorban arra törekedett, hogy az Egyesült Államokkal fennálló védelmi garanciákat kiterjesszék a *kiberdomainre,* és elmélyítsék a két nemzet kooperációját a kibertéri fenyegetések felderítésében. Kallender és Hughes amellett érvelt, hogy a japán szakpolitikai vezetés e tekintetben sikereket ért el, mert a kétoldalú Védelmi Irányelvek (Defence Guidelines) 2015-ös kiegészítésében a két kormány rögzítette az együttműködését a kritikus infrastruktúrák és azon szolgáltatások védelme érdekében, amelyektől az Önvédelmi Erők és az Egyesült Államok Fegyveres Erői küldetésük teljesítése során függenek. Ennek keretében a japán fél elsődleges felelősségi és hatáskörébe delegálták a szigetország területét vagy az Önvédelmi Haderőt érő kibertéri műveletekre adott defenzív válaszlépés műveleti tervezését és kivitelezését, amihez az USA hadereje támogatást nyújt. Ezzel a feladatmegosztással közel egyenlő súlypontra igyekeztek terelni a partnerségi viszonyt.[60] Fontos aspektus volt, hogy a nukleáris védőernyőhöz hasonlatosan, az amerikai fél vállalta az elrettentő célú kibertéri offenzív műveleti támogatást.[61] A kooperáció elmélyítését mutatja, hogy a Védelmi Irányelvek tartalmazza

[55] A kibervédelmi egység megalakulásakor nagyjából 90 fős volt, 2021-ben 220–290 fősre becsülték. Lásd Katagiri 2021: 339.
[56] Japan's SDF Launches New Cyber-Defense Unit 2022.
[57] Strategic Command 2024.
[58] Japan's SDF Launches New Cyber-Defense Unit 2022.
[59] Japán Külügyminisztérium 2013; Japán Külügyminisztérium 2024; Soesanto 2020: 30.
[60] Kallender–Hughes 2016: 136–137; Japán Külügyminisztérium 2015: 22.
[61] Kallender–Hughes 2016: 138.

a bilaterális fenyegetés-hírszerző hálózat fenntartását, vagyis a kibertéri fenyegetésekről és feltárt sérülékenységekről való kormányközi információmegosztást, ami kiterjedhet a magánszektor irányába is, továbbá a szakképzések és a kiberképességek fejlesztésével kapcsolatos jó gyakorlatok átadását.[62] A kibertér védelmére irányuló megállapodás hatóköre miatt szükségszerű volt a két haderő műveleti egységei és kiberképességei közti interoperabilitás megteremtésére, ezért a Védelmi Irányelvekben a felek a közös katonai kibergyakorlatok megtartása mellett kötelezték el magukat.[63] Ezzel összhangban a USINDOPACOM (U.S. Indo-Pacific Command) és a japán Védelmi Minisztérium 2019-től napjainkig legalább éves szinten szervezett – a térségbeli szövetségeseik aktív részvételével vagy megfigyelők delegálása mellett – többdimenziós *(multidomain)* szimulációs gyakorlatot *(tabletop)*.[64] Például az Indo-Pacific Critical Infrastructure Workshop[65] és a Cobra Gold (az USA, Japán és Dél-Korea közti multilaterális kibervédelmi gyakorlat komponense) elnevezésű szimulációk középpontjában a kritikus infrastruktúrákat vagy a katonai és polgári rendszerek összekapcsolódási pontjait érintő kiberműveletekkel szembeni koordinált válaszlépések és közös fellépési stratégiák tesztelése állt.[66]

A kiberhatalmi ambíció megvalósításához vezető út második meghatározó területe Japán kibervédelmi kapacitásépítő tevékenysége, amely (az USA-val való együttműködés elmélyítésével párhuzamosan) már a 2009–2013-as időszakban egyre jelentősebbé vált.[67] Bartlett kutatásában feltárta, hogy Japán – kezdetben az ASEAN közvetítésével – szerepet vállalt azon délkelet-ázsiai államok lakosságának tudatosításában, kormányzati területen dolgozó kibervédelmi szakembereinek képzésében és kritikus infrastruktúrájának rezilienciáját növelő szakpolitikák megvalósításában, amelyre saját ipara beszállítóként vagy piacként támaszkodott.[68] Emiatt a kibervédelmi kapacitásépítő szakpolitika célkitűzése elsősorban az lehetett, hogy stabil gazdasági környezetet biztosítson a japán vállalatok számára Délkelet-Ázsiában, másodsorban az, hogy diverzifikálja az USA-n kívüli biztonsági kapcsolatait, és ellensúlyozza a katonai és gazdasági területen felemelkedő Kínai Népköztársaság térségbeli pozícióit.[69] A tokiói vezetés külpolitikájában csak később, 2016-tól jelent meg célként, hogy technológiai kompetenciák átadására irányuló kiberbiztonsági kapacitásépítő támogatással piacot teremtsen a japán kibervédelmi vállalati szféra számára az ASEAN-tagállamokban.[70]

Japán mint újonnan felemelkedő kiberhatalom képét tükrözi egy 2020-as harvardi kutatói jelentés is, amely számos technológiailag fejlett országot hasonlít össze a kibervédelem területén az erőforrások alkalmazásának képessége és a kormányzati szándék céljai alapján (például hírszerzés, destruktív műveletek, kibererő

[62] Japán Külügyminisztérium 2015: 21–23.
[63] Japán Külügyminisztérium 2015: 21–23.
[64] Bartlett 2020: 97.
[65] Amerikai Egyesült Államok Indo-csendes-óceáni Parancsnokság 2024.
[66] Brunson–Chick 2024.
[67] *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation* 2013.
[68] Bartlett 2023: 479–482.
[69] Bartlett 2023: 495–497.
[70] Bartlett 2023: 495; Bartlett 2018.

finanszírozása, információk felügyelete stb.). A tanulmány Japánt 2020-ban kiemelkedő eredményekkel értékelte a nemzeti kiber- és kereskedelmi technológiai kompetencia, a védelemi képességek fejlesztése területén, illetve a részvételét nemzetközi szakmai szervezetek kiberteret érintő normaalkotási és technikai standardizációs törekvéseiben, ezért világszinten a tíz legjelentősebb kiberhatalom közé sorolta.[71] A legfrissebb, 2022-es jelentésben Japán pozíciója némileg változott, így a nemzeti kiberhatalmi index (National Cyber Power Index) szerinti globális összesítésben a 16. helyre került, például Ausztrália, Vietnám, Dél-Korea, Irán, Ukrajna, Kanada, Észak-Korea és Spanyolország előretörése okán. Azonban Japán a 2022-es mérésben is megőrizte kiemelkedő szerepét a kiber- és kereskedelmi technológiai kompetencia kategória mindkét ágában *(commerce category),* ahol globális összesítésben 6. helyet ért el, míg a képességpontszám szerinti ágban a 4. helyen jegyezték).[72]

Japán kibervédelmi szakpolitikájának aktuális kihívásai (H2)

Japán kurrens biztonságpolitikai környezetéből eredő kiberbiztonsági fenyegetéspercepcióját elsősorban az orosz–ukrán háborúban demonstrált kiberműveletek és a Tajvani-szoros körüli feszültséggel összefüggésben álló kínai dezinformációs tevékenység befolyásolja (ami kiemelten éri Okinava lakosságát).[73] Ezenkívül hatással vannak rá a kínai hátterű hírszerzési kampányok növekvő volumene[74] és Észak-Korea főként pénzügyileg motivált kiberbűnözői aktivitása,[75] valamint az orosz–észak-koreai technológiai kooperációban rejlő fenyegetések.[76]

Japánban a kínai hátterű fenyegetések aktivitására a dezinformáción kívül a kiberkémkedés vált jellemzővé, ami fenyegetést jelent Japán ipari bázisára.[77] Különösen az olyan korszerű iparágak szellemi tulajdonát és üzleti titkait veszik célba, mint például a védelmi ipar, a légi közlekedés, a hightech gyártókapacitás és a gyógyszeripar.[78]A közelmúltban ezen állami hátterű fenyegetések többek közt a Fujitsut,[79] Japán űrkutatási és fejlesztési ügynökségét (vagy más néven JAXA), a repüléstechnológiai gyártó Aviation Electronics vállalatot kompromittálták.[80] A legsúlyosabb hatást kiváltó incidensről, amely után Tokió úgy döntött, 4000 főre emeli a Kibervédelmi Parancsnokság létszámát, az USA Nemzetbiztonsági Ügynöksége (NSA) tájékoztatta 2023-ban a nyilvánosságot a *The Washington Post*on

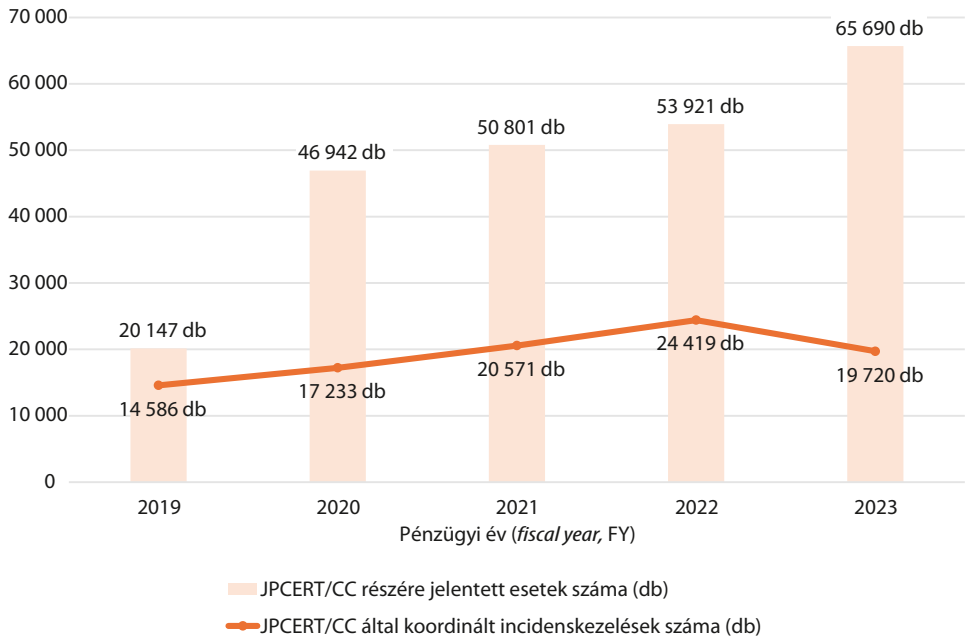
[71] Voo et al. 2020: 6–12.
[72] Voo–Hemani–Cassidy 2022: 10–11, 27.
[73] Johnstone–Klaas 2024: 7–9; és szakértői interjú, podcast alapján készült: Center for Strategic & International Studies 2024.
[74] Martin 2023.
[75] Greig 2024.
[76] Smith 2024.
[77] Osawa 2024: 65–66.
[78] Sinha 2024: 3–4.
[79] Notice Regarding Results of Security Incident Investigation 2024.
[80] A JAXA tájékoztatása alapján az eset rakétatechnológiát és műholdakra vonatkozó információt nem érintett. Sinha 2024: 3–4.

keresztül. Az amerikai információk alapján 2020-tól egy feltehetően kínai hátterű fenyegetés volt jelen Japán védelmi szférájának bizalmas hálózatában.[81] Ezenfelül 2023-ban adatszivárgáshoz vezető tevékenység sújtotta a Japán Külügyminisztériumot és a Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központot,[82] illetve ugyanezen évben a támadók a Tokiói Egyetem 2003–2022-es évfolyamain tanuló diákjainak adataihoz fértek hozzá, és a LockBit zsarolóvírussal tesztelhették a nagoyai kikötő infrastruktúrájának védelmét, noha Kína Külügyminisztériuma tagadta a japán hatóságok erre irányuló attribúcióját.[83] A japán kormányzati CERT (JPCERT/CC) 2024 első felében a MirrorFace elnevezésű, kínai hátterű APT10 csoport aktivitását észlelte.[84] Az APT10 a LODEINFO és NOOPDOOR malware-család tagjait használva kezdetben médiavállalkozásokat, politikai intézményeket, valamint egyetemeket és *think-tankeket* célzott, 2023-tól azonban a technológiai gyártóegységeket és kutatóközpontokat érintette a tevékenysége.[85]

Az észak-koreai hátterű aktív jelenlét kapcsán a japán állami CERT 2023 és 2024 októbere közti jelentésében a Lazarus (és annak JokerSpy néven nyilvántartott affiliációja), valamint a Kimsuky elnevezésű fejlett perzisztens fenyegetések tevékenységét detektálta.[86] A JPCERT/CC 2024 márciusában ezen Kimsuky APT-csoport folyamatban lévő célzott adathalász-kampányára hívta fel a japán vállalkozások figyelmét. A Kimsuky-kampány támadási vektorát adó e-mailt egy biztonsági vagy diplomáciai szervezet nevében küldték el, ami kettős kiterjesztésű EXE-fájlokkal kezdte meg a VBS-fájlok végrehajtását. A VBS-fájlok közül az egyik az adatlopást eredményező *keylogger* volt, a másik a rendszerindításkor rejtett perzisztenciát (értsd: jelenlétet) biztosító PowerShell szkriptet töltötte le.[87] Az észak-koreai kibertéri aktivitásra jellemző pénzügyi motiváció Japán esetében is jelentős. Az amerikai Szövetségi Nyomozóiroda (FBI) és a Japán Rendőrség közös attribúció után megerősítette, hogy a Lazarus affiliációjába tartozó TraderTraitor elnevezésű csoport volt felelős a 2024-es év legnagyobb kriptorablásáért, amely során 308 millió USA-dollárt loptak el a DMM nevű japán platformról.[88]

Összességében megállapítható, hogy a japán védelempolitikának és az Önvédelmi Erő Kibervédelmi Parancsnokságának folyamatosan adaptálódnia kell egy olyan fenyegetési környezethez, amelyben kínai és észak-koreai állam alatti kiberegységként is azonosítható APT-tevékenység is jelen van. Japán kibertéri fenyegetettségi környezetét jól szemlélteti az 1. ábra, amely a kormányzati incidenskezelő központ (CERT) 2019–2023-as pénzügyi években mért tevékenységét mutatja be. A JPCERT/CC a belföldről bejelentett incidensek számát és ezen belül azon esetek darabszámának változását publikálta, amelyek az incidensmenedzsment folyamatát koordinálták.[89]

[81] Nakashima 2023; Faguy 2023.
[82] Martin 2023.
[83] Antoniuk 2024.
[84] Malpedia [é. n. b].
[85] Tomonaga 2024a.
[86] Tomonaga 2024b.
[87] Telychko 2024.
[88] Greig 2024.
[89] JPCERT/CC 2024: 5–6.



1. ábra: A JPCERT/CC részére bejelentett incidensek számának és a szervezet által koordinált incidensmenedzsment-folyamatok darabszámának változása 2019–2023 között
Forrás: a szerző szerkesztése a JPCERT/CC 2024: 5–6 alapján

Katonai képességfejlesztés a technológiai dependencia árnyékában

Japánnak az állami hátterű kiberfenyegetések aktivitása mellett a kibervédelmi ökoszisztéma technológiai függőségének kezelésére is ki kellett dolgoznia egy stratégiát. A Kishida-kabinet védelempolitikája keretében több olyan program is megindult 2023-ban, amely Japán hazai védelmi ipari bázisának támogatására fókuszált. Ezen piaci szegmens amiatt került a kabinet fókuszába, mert az elmúlt 20 évben a vállalatok nem tudtak a fejlesztési költségekkel arányos nyereséget termelni, ezért napjainkig több mint 100 jelentős japán védelmi vállalat leépítése vagy kivonulása következett be. Ennek kompenzálása érdekében a japán Védelmi Minisztérium önálló fejlesztéspolitikai tervet publikált a védelmi ipari termelés és technológiai bázis fejlesztéséhez (Basic Policy for Improving Defense Production and Technology Bases), ami a hazai infrastruktúra megerősítését célozza a védelmi szektorbeli vállalatoknak nyújtott nemzeti támogatás révén. A fejlesztési politika egyúttal megteremti a lehetőséget a védelmi ipari termelők beszállítói láncának magasabb szintű felügyeletére például egy specifikus, önálló klasszifikációs rendszer adaptálásával, ami a fejlesztési információk védelmét szolgálja.[90]

[90] Matsuo 2024.

Az államigazgatás és a haderő információs és kommunikációs technológiai függőségéből eredő fenyegetéspercepció kezelése érdekében hirdette meg 2022 decemberében a japán Védelmi Minisztérium a Digitális Transzformációs Programját. A minisztérium a program keretében jelentette be a digitális kormányzás közép- és hosszú távú tervét, amelynek digitális transzformációs célja, hogy előmozdítsa a minisztériumi háttérintézmények és az Önvédelmi Haderő részére fejlesztett rendszerek felügyeletének központosítását, például a Digitális Ügynökség által kifejlesztett kormányzati felhőrendszer felhasználásával. A szakpolitika ugyancsak prioritásként kezeli a felhőtechnológia bevezetését az Önvédelmi Haderő és a Védelmi Minisztérium szervezetközi kommunikációjának észszerűsítése érdekében, amely a 2022-es stratégiai dokumentumok kiadásakor főként az elektronikus levelezésen alapult a jelentős késedelemmel létesíthető távoli hozzáférések miatt. Hasonló kollaborációs és adattovábbítási problémával néz szembe a japán védelmi beszerzésekért felelős ügynökség (Acquisition, Technology & Logistics Agency, ATLA) a magánszférában működő védelmi ipari beszállítóival. A kihívás kezelése érdekében a kabinet amellett kötelezte el magát, hogy 2024 márciusáig létrehoz egy integrált, a köz- és a magánszféra által használt felhőkörnyezetet (*defense security gateway,* DSG), amely biztosítja az érzékeny adatok védelmét és megosztását a védelmi beszerzések lebonyolításáért felelős ügynökség (ATLA) és a kapcsolódó szervezetek között.[91]

A 2023–2027 közti ötéves védelmi reformcélok megvalósításához a kabinet összesen 43500 milliárd jen (JPY) értékű forrást különített el (ami 2022. december 16-i árfolyamon megközelítőleg 318 milliárd dolláros [USD], körülbelül 121 395 milliárd forint [HUF] összeget jelentett).[92] Azonban a védelempolitika irányvonalát és a haderő-finanszírozást jelentősen befolyásolhatja, hogy Kishida miniszterelnök lemondása után a kormányzó Liberális Demokrata Párt és annak koalíciós partnere (Komeito) elvesztette többségét a Parlament alsóházában a 2024. októberi előrehozott választásokon. Emiatt Ishiba Shigeru (2024–) korábbi védelmi miniszter számára kérdésessé vált, hogy a kisebbségbe került kormánykoalícióval milyen mértékben tudja realizálni a kampányában hangsúlyozott védelempolitikai elképzeléseit. Ishiba az USA-val való védelmi együttműködés kapcsán az egyenrangú mechanizmusok kialakítását szorgalmazta, amit álláspontja szerint például a műveleti tervezés területén és a katonai erő állomásoztatása kapcsán kellene előmozdítani.[93] Emellett az LDP hosszú távú biztonságpolitikai célkitűzése kiemelendő, amely egy, a NATO-ról mintázott, többoldalú szövetségi védelmi szervezet létrehozását veti fel a kelet-ázsiai régióban. A japán elképzelés szerint egy ilyen szervezet képes lehetne Kína és Észak-Korea katonai elrettentésére, valamint összefogná a már létező biztonságpolitikai integrációt, például az USA – Dél-Korea – Japán trilaterális együttműködést a Fülöp-szigetekkel és Tajvannal, valamint a Quad-államok (Japán, India, Ausztália, USA) közti információmegosztó mechanizmusokat.[94]

[91] Matsuo 2024.
[92] Japán Védelmi Minisztérium 2022b: 49.
[93] Ishiba azzal kampányolt, hogy az okinavai támaszponthoz hasonlóan a japán katonák is állomásozhatnának az USA csendes-óceáni támaszpontjain, például Guamon.
[94] Szakértői interjú, podcast alapján készült. *Hit Rádió* 2024.

A nemzetközi kibervédelmi kooperáció elmélyítése

Japán mint feltörekvő kiberhatalom jelentőségét tükrözi a NATO-val való partnerségi viszonyának átalakulása a 2023-as évtől. A tokiói vezetés, építve az USA katonai kibererőivel és kiberképességeivel való kooperáció eredményeire, már 2018-ban csatlakozott a NATO Kibervédelmi Kiválósági Központjához (CCDCOE), és részt vett például a Locked Shields szimulációkon és a Cyber Coalition éves kibervédelmi gyakorlatokon.[95] Az éves gyakorlatokon való aktív részvétel stratégiai jelentősége abban mutatkozik meg, hogy egyrészt műveleti szinten támogatja a kiberfenyegetések elleni közös felkészülést és információmegosztást, másrészt politikai dimenzióban lehetőséget ad a tokiói vezetés kollektív önvédelmi jog gyakorlását előtérbe helyező diplomáciájának népszerűsítésére. A NATO és Japán 2023-ban újabb szintre emelte az együttműködést az Egyedi Partnerségi Program (Individually Tailored Partnership Programme, ITPP) keretében, amely külön prioritásként kezeli a kibervédelmet.[96] A felek célként jelölték meg, hogy közösen dolgozzanak a kiberfenyegetések elleni technológiai és információmegosztási rendszerek fejlesztésén, miközben a stratégiai kommunikáció, a hibrid hadviselés elleni fellépés, valamint az úgynevezett feltörekvő és bomlasztó technológiák (*emerging and disruptive technologies,* EDTs)[97] jelentette kihívásokra való felkészülés[98] területén is szorosabbra fűzik együttműködésüket.[99] Japán hozzájárulása különösen értékes az új generációs kommunikációs technológiák, például az Open RAN hálózatok fejlesztésében, valamint az ázsiai régió kiberfenyegetéseivel kapcsolatos tapasztalatok megosztásában. Összességében az Egyedi Partnerségi Program együttműködési területei az információcsere mellett a közös kutatások és képzések, amelyek célja az ellenálló képesség növelése és a NATO-partnerekkel való interoperabilitás erősítése.

Konklúzió

Számos szakértő közt konszenzus van abban, hogy Japán az elmúlt évtizedben egyre nagyobb erőfeszítéseket tett az infrastruktúrája és a társadalom kibertéri ellenálló képességek fejlesztése, valamint a kiberbiztonsági stratégia finomítása érdekében.[100] A japán vezetés kibertérből jelentkező fenyegetésekre adott válaszlépései a 2012–2016-ig tartó időszakban tapasztalt szekurizáció eredményeképp egyre inkább militarizált formát öltöttek, ami hozzájárult a jelenlegi centralizált kibervédelmi igazgatási rendszer és az Önvédelmi Haderő Kibervédelmi Parancsnokságán belüli kiberképesség kialakításához.[101] Noha az USA-val fennálló szövetség – továbbá a NATO-partnerség – kiberműveleti területen való elmélyítése előmozdította az aktív kibervédelmi stratégiai

[95] Pernik 2023.
[96] NATO 2023.
[97] Például AI, autonóm rendszerek, kvantumtechnológia, robotika, nanotechnológia stb.
[98] Például a felelős fejlesztés irányelveinek promotálása által.
[99] NATO 2023; NATO 2025.
[100] Katagiri 2022; Bartlett 2019; Kallender–Hughes 2016.
[101] Kallender–Hughes 2016: 125–127, 136.

modell alkalmazásához szükséges offenzív képességek fejlesztését, Japánban továbbra is limitált maradt ezek jogszerű alkalmazhatósága. Ennek kapcsán kiemelendő, hogy az aktív kibervédelem terminológiájának nem feltétlenül része a védett hálózaton túli offenzív kiberműveletek alkalmazása. Ez magyarázza, hogy Japán sikermegtagadó elrettentési mechanizmusokat épített be aktív kibervédelmi stratégiájába, megtorlásalapú elrettentést viszont nem.[102]

A tanulmány amellett érvelt, hogy Japán aktív kibervédelmi stratégiáját elsősorban három tényező befolyásolja: a jogszabályi keretrendszer megkötései, az USA-val és további partnerekkel fennálló védelmi szövetség, valamint a regionális ellenfelei által alkalmazott offenzív kiberképességekhez kapcsolódó fenyegetéspercepció. A kutatás eredményeképp a bevezetésben részletezett hipotézisek pontosítására volt szükség, így a tézisek a következők.

H1–T1: A centralizáló reformok és a militarizált kibervédelmi szakpolitika ellenére csak korlátozott mértékben csökkentek azok a kockázatok, amelyek Japán gazdasági rendszerének és haderejének információs technológiáktól való függőségéből erednek. Emiatt ez a tényező továbbra is a fenyegetéspercepció részét képezi, és jelentős kihívás elé állítja az ország kiberbiztonsági ökoszisztémáját. Japán feltehetőleg a délkelet-ázsiai kibervédelmi kapacitásépítő tevékenységének folytatásával igyekszik elősegíteni regionális beszállítói láncának rezilienciáját.

H2–T2: Az ország regionális ellenfelei (Kína, Észak-Korea és Oroszország) által kifejlesztett és egyre gyakrabban demonstrált offenzív kiberképességek fokozott fenyegetést jelentenek az ország nemzetbiztonságára nézve. Az ehhez kapcsolódó fenyegetéspercepció ellensúlyozása érdekében a defenzív és limitált offenzív kiberképességek fejlesztése mellett Japán manapság egy jóval szélesebb körű – az USA-partnerségen felüli – nemzetközi kooperációs hálózat kiépítésére törekszik. Ezen új partnerségek célja a regionális fenyegetésfelismerő képesség javítása, a sérülékenységekről és kibertéri fenyegetésekről rendelkezésre álló információ megosztásával.

H3–T3: A „kizárólag védelemorientált" jogrendszer és biztonságpolitika továbbra is olyan mértékben korlátozza Japán lehetséges válaszlépéseit, hogy emiatt megkérdőjelezhető a jelenlegi sikermegtagadó elrettentési mechanizmusokat alkalmazó aktív kibervédelmi stratégiai modell hatékonysága. Emiatt feltehetően felértékelődik a bilaterális és multilaterális kibergyakorlatok jelentősége, az USA kibererejével való interoperabilitás és a műveleti tervezésben történő együttműködés javítása érdekében.

Felhasznált irodalom

Alan, J. (2024): Japan Considers Measures To Mandate Private Sector Cybersecurity Incident Reporting. *The Cyber Express,* 2024. augusztus 6. Online: https://thecyberexpress.com/japan-mandatory-cybersecurity-reporting

Antoniuk, Daryna (2024): Japan Sees Increased Cyberthreats to Critical Infrastructure, Particularly From China. *The Record,* 2024. február 16. Online: https://therecord.media/japan-critical-infrastructure-cyberthreats

[102] Osawa 2024; Katagiri 2021, 2022.

Amerikai Egyesült Államok Indo-csendes-óceáni Parancsnokság (2024): *ASD(A) Cyber Warfare, USINDOPACOM, JFHQ-DODIN join forces to host second Indo-Pacific Critical Infrastructure Workshop.* 2024. november 6. Online: www.pacom.mil/Media/News/News-Article-View/Article/3957555/asda-cyber-warfare-usindo-pacom-jfhq-dodin-join-forces-to-host-second-indo-pacif/

Bartlett, Benjamin (2018): Government as Facilitator: How Japan Is Building Its Cybersecurity Market. *Journal of Cyber Policy,* 3(3), 327–343. Online: https://doi.org/10.1080/23738871.2018.1550522

Bartlett, Benjamin (2019): How Japanese Cybersecurity Policy Changes. *Harvard Program on U.S.-Japan Relations Occasional Paper Series,* (1), 1–39. Online: https://projects.iq.harvard.edu/files/us-japan/files/19-01_bartlett.pdf

Bartlett, Benjamin (2020): Japan: An Exclusively Defense-Oriented Cyber Policy. *Asia Policy,* 15(2), 93–100. Online: https://dx.doi.org/10.1353/asp.2020.0013

Bartlett, Benjamin (2023): Why Do States Engage in Cybersecurity Capacity-Building Assistance? Evidence From Japan. *The Pacific Review,* 37(3), 475–503. Online: https://doi.org/10.1080/09512748.2023.2183242

Basu, Pratnashree (2024): From Reactive to Proactive: Japan's Advances in Cybersecurity and Cyber Defence Strategies. *Observer Research Foundation,* 2024. március 17. Online: www.orfonline.org/expert-speak/from-reactive-to-proactive-japan-s-advances-in-cybersecurity-and-cyber-defence-strategies

Berzsenyi Dániel (2023): *Különleges kiberműveletek. A kiber különleges műveleti képesség és kialakításának vizsgálata.* Doktori (PhD-) értekezés. Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2023.012

Brunson, Xavier – Chick, Cody (2024): How Cobra Gold Helps the US Strengthen its Indo-Pacific Partnerships. *The Diplomat,* 2024. május 14. Online: https://thediplomat.com/2024/05/how-cobra-gold-helps-the-us-strengthen-its-indo-pacific-partnerships/

Center for Strategic & International Studies [@csis] (2024): What to Expect from Japan's New Leader? *YouTube,* 2024. október 3. Online: www.youtube.com/watch?v=sFrSzgDBG4A

Fábián Emília (2015): *Az átalakuló normák hatása a japán biztonságpolitikára. Yoshidától az Abe-doktrínáig- az antimilitarista normától a proaktív pacifizmusig.* PhD-értekezés. Budapest: Budapesti Corvinus Egyetem Nemzetközi Kapcsolatok Doktori Iskola. Online: https://doi.org/10.14267/phd.2016016

Faguy, Ana (2023): China Hacked Japanese Military Networks, Report Says. *Forbes,* 2023. augusztus 7. Online: www.forbes.com/sites/anafaguy/2023/08/07/china-hacked-japanese-military-networks-report-says/

FIXTV HUNGARY (FIX) [@fixhdtv] (2024): Enigma – Bizonytalan Japán háborúra készül. *YouTube,* 2024. december 13. Online: www.youtube.com/watch?v=PcDUPWjMQxY

Gady, Franz-Stefan (2017): *Japan: The Reluctant Cyberpower.* Paris–Brussels: Institut français des relations internationales. Online: www.ifri.org/en/papers/japan-reluctant-cyberpower

Greig, Jonathan (2024): FBI Attributes Largest Crypto Hack of 2024 to North Korea's TraderTraitor. *The Record,* 2024. december 25. Online: https://therecord.media/fbi-largest-crypto-hack-2024-tradertraitor

Hideshi, Tokuchi (2023): Japan's New National Security Strategy and Contribution to Networked Regional Security. *Center for Strategic and International Studies,* 2023. június 23. Online: www.csis.org/analysis/japans-new-national-security-strategy-and-contribution-networked-regional-security

Hit Rádió [@hitradiobudapest] (2024): Létrehozná az ázsiai NATO-t Japán? – Bartók András. *YouTube,* 2024. november 3. Online: www.youtube.com/watch?v=OMR1B1QNsI0

Japan Mulls Requiring Private Sector Operators to Report Cyberattacks on Infrastructure. *The Japan Times,* 2024. augusztus 4. Online: www.japantimes.co.jp/news/2024/08/04/japan/japan-cybersecurity-reporting/

Japán Digitális Ügynökség [é. n.]: Organisational Background of Estabilishment. Online: www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/ed91c288-7d40-4a9b-9d86-1007f256ada6/c83a6759/20240528_en_organization_outline.pdf

Japán Információbiztonsági Politikai Tanács (2013): *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace.* Online: www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf

Japán Információbiztonsági Politikai Tanács (2014): *The Basic Policy of Critical Information Infrastructure Protection (3rd Edition).* Online: www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

Japán Kiberbiztonsági Stratégiai Központ (2022): *The Cybersecurity Policy for Critical Infrastructure Protection.* Cybersecurity Strategic Headquarters. Online: www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf

Japán Külügyminisztérium (2013): *Joint Statement Japan-U.S. Cyber Dialogue.* 2013. május 10. Online: www.mofa.go.jp/region/page22e_000001.html

Japán Külügyminisztérium (2015): *The Guidelines for Japan-U.S. Defense Cooperation.* 2015. április 27. Online: www.mofa.go.jp/mofaj/files/000078188.pdf

Japán Külügyminisztérium (2024): *The 9th Japan-US Cyber Dialogue.* 2024. június 27. Online: www.mofa.go.jp/press/release/pressite_000001_00394.html

Japán Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központja (2021): *Japan's Cybersecurity Strategy 2021 (Overview).* Online: www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou-en.pdf

Japán Védelmi Minisztérium (2019): *Defense of Japan 2019.* Online: www.mod.go.jp/en/publ/w_paper/wp2019/pdf/DOJ2019_Full.pdf

Japán Védelmi Minisztérium (2022a): *National Defense Strategy.* 2022. december 16. Online: www.mod.go.jp/j/approach/agenda/guideline/strategy/pdf/strategy_en.pdf

Japán Védelmi Minisztérium (2022b): *Defense Buildup Program.* 2022. december 16. Online: www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf

Japan's SDF Launches New Cyber-Defense Unit. *Kyodo News,* 2022. március 17. Online: https://english.kyodonews.net/news/2022/03/2009b0fac163-japans-sdf-launches-new-cyber-defense-unit.html?utm_source=chatgpt.com

Johnstone, Christopher B. – Klaas, Leah (2024): *Combating Disinformation. An Agenda for U.S.-Japan Cooperation.* Washington, DC: Center for Strategic and International Studies. Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-07/240708_Johnstone_Combating_Disinformation.pdf

Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation. 2013. szeptember 13. Online: www.asean.org/wp-content/uploads/images/Statement/final_joint_statement%20asean-japan%20ministerial%20policy%20meeting.pdf

JPCERT/CC Incident Handling Report January 1, 2024–March 31, 2024. 2024. április 18. Online: www.jpcert.or.jp/english/doc/IR_Report2023Q4_en.pdf

Kallender, Paul – Hughes, Christopher W. (2016): Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies,* 40(1–2), 118–145. Online: https://doi.org/10.1080/01402390.2016.1233493

Kaspersky Lab (2013): *The 'Icefog' APT: A Tale of Cloak and Three Daggers.* Online: https://media.kaspersky.com/en/icefog-apt-threat.pdf.

Katagiri, Nori (2021): From Cyber Denial To Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations? *Asian Security,* 17(3), 331–348. Online: https://doi.org/10.1080/14799855.2021.1896495

Katagiri, Nori (2022): Assessing Japan's Cybersecurity Policy: Change and Continuity From 2017 to 2020. *Journal of Cyber Policy,* 7(1), 38–54. Online: https://doi.org/10.1080/23738871.2022.2033805

Koo, Soo-Kyung (2013): Cyber Security in South Korea: The Threat Within. *The Diplomat,* 2013. augusztus 19. Online: https://thediplomat.com/2013/08/cyber-security-in-south-korea-the-threat-within/

Kosuke, Takahashi (2024): Why Japan Is Lagging Behind in Cyber Defense Capabilities. *The Diplomat,* 2024. május 24. Online: https://thediplomat.com/2024/05/why-japan-is-lagging-behind-in-cyber-defense-capabilities/

Lottaz, Pascal (2023): Japan's New Security Strategy, Part 2: The Ongoing Debates. *The Diplomat,* 2023. június 8. Online: https://thediplomat.com/2023/06/japans-new-security-strategy-part-2-the-ongoing-debates/

Malpedia [é. n. a]: *APT41.* Online: https://malpedia.caad.fkie.fraunhofer.de/actor/apt41

Malpedia [é. n. b]: *MirrorFace.* Online: https://malpedia.caad.fkie.fraunhofer.de/actor/mirrorface

Martin, Alexander (2023): Japan's Cybersecurity Agency Breached by Suspected Chinese Hackers: Report. *The Record,* 2023. augusztus 29. Online: https://therecord.media/japan-cybersecurity-agency-breached-report

Matsuo, Miki (2024). Unaddressed Challenges for Defense Policy Reform in Japan. *Center for Strategic and International Studies,* 2024. május 9. Online: www.csis.org/analysis/unaddressed-challenges-defense-policy-reform-japan

MITRE [é. n.]: *APT41.* Online: https://attack.mitre.org/groups/G0096/

Najah, Redouan (2024): Japan's NSS in the Age of Cyber Warfare: A Historical Transformation. *Japan Up Close,* 2024. július 8. Online: https://japanupclose.web-japan.org/policy/p20240708_1.html

Nakashima, Ellen (2023): China Hacked Japan's Sensitive Defense Networks, Officials Say. *The Washington Post,* 2023. augusztus 8. Online: www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/

NATO (2023): *Individually Tailored Partnership Programme between NATO and Japan for 2023–2026.* Online: www.nato.int/cps/en/natohq/official_texts_217797.htm.

NATO (2025): *Emerging and Disruptive Technologies.* Online: www.nato.int/cps/fr/natohq/topics_184303.htm?selectedLocale=en

Notice Regarding Results of Security Incident Investigation. *Fujitsu,* 2024. július 9. Online: www.fujitsu.com/global/about/resources/news/notices/2024/0709-01.html

Onodera, Yoshifumi – Tanaka, Hiroyuki – Shimamura, Naoto [é. n.]: Cybersecurity 2024: Japan. In *Chambers Global Practice Guides.* Online: https://org-www.morihamada.com/en/insights/publications/2024-60

Osawa, Jun (2024): Direction of Japan's New Cybersecurity Policy. *Asia-Pacific Review,* 30(3), 63–78. Online: https://doi.org/10.1080/13439006.2023.2295707

Paganini, Pierluigi (2020): Mitsubishi Electric Corp. Was Hit by a New Cyberattack. *Security Affairs,* 2020. november 20. Online: https://securityaffairs.com/111201/hacking/mitsubishi-electric-cyberattack.html

Pernik, Piret (2023): NATO-Japan Deepening Cooperation in Cybersecurity and Critical Technologies. *Japan Up Close,* 2023. március 24. Online: https://japanupclose.web-japan.org/policy/p20230324_2.html

Sinha, Sharat (2024): Japan Cyber Threat Landscape, Elevandi & Future Matters Center of Excellence. Online: www.elevandi.io/hubfs/custom-video-thumbnails/Japan%20Cyber%20Threat%20Landscape%20-%20Sharat%20Sinha%20-%20March%202024.pdf

Siripala, Thisanka (2024): Japan's Rush to Play Cyber Defense Catchup. *The Diplomat,* 2024. június 14. Online: https://thediplomat.com/2024/06/japans-rush-to-play-cyber-defense-catchup/

Smith, Sheila A. (2024): How Japan is Viewing the North Korea-Russia Alliance. *Council on Foreign Relations,* 2024. június 27. Online: www.cfr.org/expert-brief/how-japan-viewing-north-korea-russia-alliance

Soesanto, Stefan (2020): *Japan's National Cybersecurity and Defense Posture. Policy and Organizations.* Zürich: Center for Security Studies (CSS), ETH Zürich. Online: https://doi.org/10.3929/ethz-b-000437790

Strategic Command (2024): Strategic Command Shares Cyber Expertise With Japan. *Gov.uk,* 2024. február 20. Online: www.gov.uk/government/news/strategic-command-shares-cyber-expertise-with-japan?utm_source=chatgpt.com

Telychko, Veronika (2024): Kimsuky APT Campaign Detection Targeting Japanese Organizations. *SOC Prime,* 2024. július 10. Online: https://socprime.com/blog/kimsuky-apt-campaign-detection-targeting-japanese-organizations

Tomonaga, Shusei (2024a): MirrorFace Attack against Japanese Organisations. *JPCERT/CC Eyes,* 2024. július 16. Online: https://blogs.jpcert.or.jp/en/2024/07/mirrorface-attack-against-japanese-organisations.html

Tomonaga, Shusei (2024b): Recent Cases of Watering Hole Attacks, Part 1. *JPCERT/CC Eyes,* 2024. december 19. Online: https://blogs.jpcert.or.jp/en/2024/12/watering_hole_attack_part1.html

Voo, Julia et al. (2020): *National Cyber Power Index 2020. Methodology and Analytical Considerations. China Cyber Policy Initiative Reports*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs. Online: www.belfercenter.org/sites/default/files/2024-09/NCPI_2020.pdf

Voo, Julia – Hemani, Irfan – Cassidy, Daniel (2022): *National Cyber Power Index 2022*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs. Online: www.belfercenter.org/publication/national-cyber-power-index-2022

Jogi források

Japán Alaptörvénye (The Constitution of Japan). 1946. május 3. Online: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html

2014. évi 104. Kiberbiztonsági kerettörvény (The Basic Act on Cybersecurity). Online: www.japaneselawtranslation.go.jp/en/laws/view/4618

2022. évi 70. törvény a japán távközlési vállalkozásokról szóló 1984. évi 86. törvény egyes rendelkezéseinek módosításáról (revised Telecommunications Business Act). Online: www.japaneselawtranslation.go.jp/en/laws/view/3648/en