HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 4. szám 131–151.
DOI: 10.32567/hm.2022.4.9

Lendvai Tünde[1]

Kiberbiztonsági körkép Tajvanról[2]

Cybersecurity Overview of Taiwan

A Tsai-adminisztráció kibervédelmi reformjai mentén Tajvan egy alapvetően defenzív berendezkedésű hatalomból mára jóval szélesebb körű, proaktív védelmi eszközkészlettel is rendelkező entitássá vált. A szerző azt elemzi, hogy milyen lehetőségeket nyújt, illetve milyen korlátok jelentkeztek az elrettentési koncepció mentén felépülő kibervédelmi stratégia alkalmazásával. A tanulmány azzal a konklúzióval zárul, hogy a jelenlegi tajvani vezetés stratégiai autonómia felépítésére törekszik a kibertérben, amely visszatükröződik a kiberdiplomáciai aktivitásban és a 2021–2024-es Nemzeti Kiberbiztonsági Programban előirányzott célokban. A minél ütőképesebb és széles körűbb – offenzív és defenzív – képességekkel rendelkező kibertéri erő kialakításával és folyamatos korszerűsítésével a diplomáciai erőfeszítések elérhetik, hogy Tajvan más védelmi szektorban is kimozduljon a kínai diplomáciai nyomás alól, vagy kiegyensúlyozottabb erőviszonyokon alapuló szoros-menti kapcsolatokat tartson fenn.

Kulcsszavak: **Tajvan, proaktív kibervédelem, kiberbiztonság, kiberelrettentés, kibervédelem, kiberdiplomácia**

Along the cyber defence reforms of the Tsai administration, Taiwan has evolved from a principally defensive power to a much broader entity with proactive defence capabilities. The academic problem studied by the author analyses the opportunities and constraints that Taiwan has encountered by applying a cyber defence strategy based on the concept of deterrence. The study concludes that the current Taiwanese leadership is seeking to build strategic autonomy in cyberspace, which is reflected in its cyber diplomacy activities and the goals envisaged in the National Cyber Security Program 2021–2024. By developing and continuously upgrading a cyber force with the most effective and extensive, both offensive and defensive, capabilities, diplomatic efforts could bring Taiwan out from Chinese diplomatic pressure in other defence sectors or maintain more balanced relations based on alignment of power.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: tunde.lendvai@uni-nke.hu
[2] A tanulmány az Innovációs és Technológiai Minisztérium ÚNKP-21-3-I-NKE-124 kód-számú „új nemzeti kiválóság" programjának szakmai támogatásával készült.

Keywords: **Taiwan, proactive cyber defence, cybersecurity, cyber deterrence, cyber defence, cyber diplomacy**

1. Bevezetés

A 2000-es évektől kezdődően Tajvan (Kínai Köztársaság, a továbbiakban Tajvan) az IT-területen, különösen az információ- és kommunikációtechnológiai (IKT-) szektorban, lenyűgöző innováción ment keresztül, aminek eredményeképpen napjainkra globális viszonylatban szinte megkerülhetetlen gyártói és fejlesztői szerepkörbe került. Különösen érzékelhető a tajvani ellátási láncok jelentősége a chipgyártásban, ami a közeljövőben egyre komolyabb nehézségek árán tudja majd kiszolgálni a többek közt a hazánkban is stratégiai jelentőségű autóipar növekvő igényeit. A jelenlegi tajvani vezetés biztonságpolitikai alapvetése egy potenciális katonai megszállás esetére, hogy a Kínai Népköztársaság (a továbbiakban Kína) aszimmetrikus erőfölényét csak az ellátási láncokban betöltött szerepével és hadereje elrettentő képességének folyamatos fejlesztésével képes ellensúlyozni. Tsai Ing-wen (蔡英文), elnök asszony 2018-ban akképp írta le a *de facto* állam politikai szuverenitásának kulcsát, hogy Tajvannak „nélkülözhetetlenné és pótolhatatlanná kell válnia a világban" biztonságának garantálásához.[3] Az olyan bizalmi garanciákra érzékeny gazdasági szektorok, mint a microchipek, félvezetők (például TSMC vállalat, Taiwan Semiconductor Manufacturing Co.) és más IT-termékek meghatározó világpiaci gyártójaként a tajpeji döntéshozók számára a kibertér védelme ugyanolyan magas politikai prioritást élvez, mint a hagyományos hadszínterek.[4] A tanulmány kutatási célja, hogy átfogó jelleggel mutassa be, miként alakítja Tajvan kibervédelmi felfogását geostratégiai és biztonságpolitikai helyzete.

1.1. Kutatási kérdések és hipotézis

Tajvan biztonságpolitikáját regionális szinten két tényező befolyásolja. Az első az Egyesült Államok és Kína regionális szembenállása, a második a kelet-ázsiai biztonsági komplexumban tapasztalható militarizációs trendek, amelyek érvényesülnek a kibertérben is. A kelet-ázsiai régióban kialakult fegyverkezési verseny a folyamatos észak-koreai fegyverkísérletek okozta fenyegetésre és az USA elrettentését célzó kínai haderőfejlesztésből eredő biztonsági dilemmára vezethető vissza. A Kínai Népi Felszabadító Hadsereg (People's Liberation Army, PLA) képességeinek átalakítása a biztonsági komplexum legtöbb államát (különösen az ellentmondásos és konfliktussal terhelt szoros-menti kapcsolatokkal rendelkező Tajvant) védelmi stratégiája területvédelmi célú megreformálására és haderőfejlesztésre késztette.[5] Japánhoz hasonlóan, a tajvani

[3] Tajpej Képviseleti Iroda (Magyarország) 2018.
[4] Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzott előadások alapján.
[5] Bartók–Wagner 2020.

haderőfejlesztési program másik prioritása, a területvédelem mellett, a kiberbiztonsági készültségi szint emelése.[6]

A Tsai-elnökség (2016–2020; 2020–2024) fő védelempolitikai irányelve az „eltökélt védelem és több hadszínteret érintő elrettentés" *(resolute defence, multidomain deterrence)* megvalósítása. A koncepcióban megjelenő, úgynevezett első védelmi réteget *(the first layer of deterrent force)* a kibertérben kell megvalósítani, hiteles elrettentést megjelenítő kiberképességek adaptációjával. A kormányokon átívelő kibervédelmi reformok mentén Tajvan egy alapvetően defenzív berendezkedésű hatalomból mára már jóval szélesebb körű, aktív védelmi eszközkészlettel is rendelkező entitássá vált a kibertérben. A tanulmány első kutatási kérdése arra keresi a választ, hogy milyen lehetőségeket nyit, illetve milyen korlátok jelentkeztek Tajvan kiberdiplomáciai mozgásterében az elrettentési koncepció mentén felépülő kibervédelmi stratégia alkalmazásával párhuzamosan (KK1)? Ehhez kapcsolódóan azt a hipotézist állítottam fel, hogy Tajvan kiberdiplomáciai mozgásterének növelése érdekében arra törekszik, hogy további militarizálás nélkül, kooperatív eszközökkel növelje kiberbiztonsági szintjét, mivel stratégiai érdeke, hogy a régiós biztonsági dilemma ne terjedjen tovább a kibertérben (H1). 2021 novemberében Jyan Hong-wei (簡宏偉), az Ügyvezető Jüan (Kormány) Kiberbiztonsági Osztályának (Department of Cyber Security, 資通安全處) volt igazgatója, parlamenti meghallgatásán megközelítőleg napi 5 millió, kormányzati szektort érintő hálózati behatolási kísérletről számolt be, amelyek közel feléről feltételezik az attribúciót követően, hogy Kína területéről indult, vagy Kínához köthető infrastruktúrát használtak fel hozzá. A tajvani kibervédelmi szervek álláspontja szerint, az állami szektort érő, világszinten is kiemelkedő mennyiségű támadás összefüggésben van Tsai Ing-wen 2016-os és 2020-as újraválasztásával.[7] A kiemelkedő incidensszám összetételét tekintve főként dezinformációs kampányokról, kormányzati weboldalak és hírportálok eltorzításáról (úgynevezett *defacement* támadás) és szolgáltatásmegtagadó (DoS, DDos) támadásokról tettek jelentést a kibervédelmi szervek. E támadások időzítése, tartalma, TTP- *(tactics, techniques, practices)* elemzése arra engedte következtetni a tajvani szakembereket, hogy azok a *de facto* állam függetlenedését vagy a kínai szeparatizmust promulgáló kijelentésekre adott válaszreakciók.[8] Ugyanakkor az utóbbi öt évre visszamenően a tajvani szervek APT- *(advanced persistent treat)*[9] jelenlétre utaló bizonyítékokat találtak az állami szektor elleni sikeres támadások közt.[10] A kínai diplomácia következetesen tagadja állami érintettségét. Önálló, önérdek vezérelte kiberbűnözői tevékenységként tekint az incidensekre, más esetben felületesen elvégzett attribúción alapuló, a tajpeji vezetés vagy az Egyesült Államok által generált lejáratókampányokra figyelmezteti a nemzetközi közösséget.[11] Kérdéses, hogy a Taj-

6 Yau 2020.

7 AFP 2021; Strong 2021. A jelenlegi elnök a Kínai Népköztársaságtól való elhatárolódást és Tajpej függetlenedését szorgalmazza külpolitikájában, ellentétben a korábbi Koumintang-adminisztráció politikájával, amely az anyaországhoz való közeledést szorgalmazta. Az irányváltás fokozta a szoros-menti politikai ellentéteket és növelte az erődemonstrációs katonai aktivitást.

8 A tajvani *Webinar on Digital Governance* című (2022. június 21-i) konferencián elhangzott előadások alapján.

9 Az APT-k tevékenységét államilag támogatott hacker- vagy kiberbűnözői csoportok tevékenységéhez szokás kötni, a szofisztikált módszereik, jelentős infrastrukturális erőforrásaik és hosszan tartó hálózati jelenlétük miatt, amelyek főleg rendkívül érzékeny információk, minősített adatok megszerzésére vagy károsítására irányulnak.

10 Huang 2018.

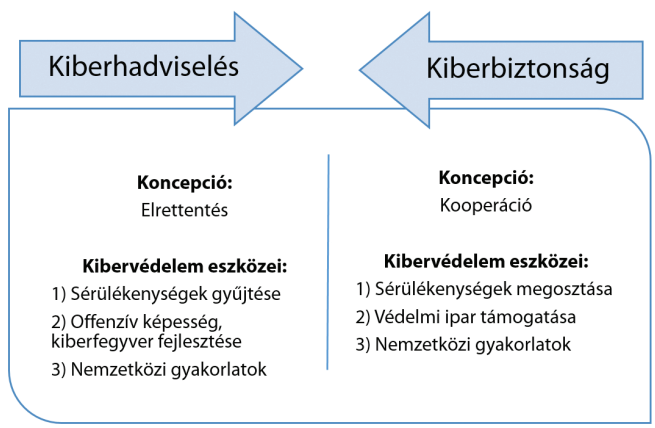
11 Yu–Blanchard 2018; Cheung–Ripley–Tsai 2021; Kínai Népköztársaság Külügyminisztériuma 2022.

vant érő kibertámadásokat lehet-e információs műveletekként (INFOOPS) értékelni (KK2). A tanulmány második hipotézise, hogy jelenleg a tajpeji külpolitikai fordulatra reagáló, a hibrid műveletek közé sorolható szürke zónás tevékenység tapasztalható a KNK részéről, amely nem minősül információs műveletnek (H2).

1.2. Módszertan

A kutatási módszereket tekintve a tanulmány deduktív megközelítést alkalmaz, esettanulmány feldolgozásán és dokumentációelemzésen alapuló kutatási stratégia mentén. Az elsődleges forrásból származó adatgyűjtés módszere szakértői interjú lefolytatásával valósult meg. A szerzőnek lehetősége nyílt kérdéseket feltenni az Ügyvezető Jüan Kiberbiztonsági Osztálya volt igazgatója részére, a magyarországi Tajpej Képviseleti Iroda közreműködésével, és részt venni a Taiwan International Cooperation and Development Fund (ICDF) International Human Resource Development Workshop programsorozata keretében, a 2022. június 21-i *Webinar on Digital Governance* című konferencián. Ezt kiegészítve, a másodlagos forrásokon alapuló adatgyűjtés sajtóhírek, publikus tajvani kormányzati jelentések és a vonatkozó szakirodalom feldolgozásával valósult meg.

2. A tajvani kibervédelmi stratégia témakörében rendelkezésre álló szakirodalom áttekintése



1. ábra: A nemzeti kibervédelem kiépítésének elrettentésen és kooperáción alapuló koncepciói
Forrás: a szerző szerkesztése Taddeo 2018 és Yau 2020 alapján

A tudományos probléma, amely a tajvani kiberképesség-fejlesztés kapcsán körvonalazódik, azt veti fel, hogy amennyiben egy állam – esetünkben *de facto* állam – kibertéri védelmét elrettentő koncepcióra alapozza abból a célból, hogy növelje kiberbiztonsági szintjét, ellentétes hatást érhet el a nemzetközi kapcsolatok realista szemléletmódja alapján. Az elrettentési koncepción alapuló nemzeti kibervédelem kiépítése során

kiberhadviselési eszközöket is felhasznál (lásd 1. ábra), amelyek más államokat késztethetnek ugyanerre, így biztonsági dilemma vagy fegyverkezési verseny alakulhat ki, csökkentve az adott régió és állam kiberbiztonsági szintjét. Az offenzív képességek – lehetnek akár magas vagy alacsony technológiai fejlettségi szinten – a politikai szándékot is figyelembe véve fenyegetettségérzetet kelthetnek a környező országokban, katonai és egyéb nemzetközi szövetségekben. A kelet-ázsiai biztonsági komplexum államainak védelempolitikai gondolkodásában rendkívül elterjedt az elrettentéskoncepció, amely célnak megfelelő kibertéri alkalmazhatósága számos kritikát vet fel elméleti oldalról.[12]

A kiberelrettentés-elmélet kritikusai szerint a kiberbiztonsági szintet valójában csökkenti és nem emeli a koncepció megvalósításának eszközkészlete. Először is, a nemzetközi vagy bilaterális gyakorlatokon (*red team* és *blue team* típusú szimulációk) való részvétel erődemonstrációvá válik a nemzetközi közösség számára. Másodszor, a malware-ek és más támadó programok fejlesztése, a célpontkiválasztás fényében kiberfegyverként értékelhetők, különösen, ha kontrollálhatatlanná válik terjedésük a hálózatokban. Harmadszor, az offenzív képességek fejlesztésének előfeltétele, hogy az állami aktor a felfedezett sérülékenységeket ne publikálja a gyártó vagy a nyilvánosság részére, hanem gyűjtse a későbbi kihasználás érdekében. Ez a gyakorlat végső soron csökkenti az adott állam kiberdiplomáciai mozgásterét, a piaci és állami szereplők közti bizalmat, valamint a szoftver- és hardvergyártók termékeibe vetett fogyasztói bizalmat, ami különösen fontos a világszinten kiemelkedő IKT-technológiai iparral rendelkező Tajvan számára.[13]

Tajvan esetében, a már említett kiemelkedő számú kormányzati és állami szerveket érintő incidensszám mellett, a kibertéri fenyegetések széles skálája fordul elő, amelyek a kognitív dimenziót célzó műveletektől kezdve a kritikus információs infrastruktúrát érő incidensig terjednek. E tényezők mellett a tajvani kiberbiztonsági stratégiai gondolkodást jelentős mértékben alakítja a kínai megszálláshoz kapcsolódó fenyegetettségpercepció. Ebben a kiberbiztonsági és biztonságpolitikai környezetben, 2018 szeptemberében a Nemzetbiztonsági Tanács közzétette első nemzeti kiberbiztonsági stratégiai jelentését, amely kiterjesztette a nemzetbiztonság értelmezését a kiberbiztonságra *(cybersecurity as national security)*. 2019-ben a tajpeji vezetés elérte a nemzeti biztonsági törvény módosítását, amellyel jogi felhatalmazást biztosított az állami szervek, köztük a hadvezetés részére, hogy offenzív képességekkel biztosítsák Tajvan kibertéri védelmét. A 2019-es Nemzeti Védelmi Jelentésében *(The 2019 National Defense Report)* a Tsai-elnökség offenzív és defenzív képességek adaptációjával kívánta felépíteni a hiteles kibertéri elrettentő erőt.[14] A szakértői interjú során megerősítették, hogy az e mögött álló kibervédelmi stratégiai elképzelés az, hogy a válaszcsapás lehetősége rettenti el a támadó aktorokat (például a támadó infrastruktúra ellehetetlenítésével), és egyelőre nem fogalmazódott meg politikai szándék egyéb alkalmazási célokra vonatkozóan, például a megelőző csapásmérés lehetőségével kapcsolatban. Ebben a nézőpontban a *passzív védelmi képességek,* vagyis a korai észlelési és detekciós képességek, a fejlett incidenskezelés

[12] Yau 2020. 11.
[13] Taddeo 2018.
[14] Yau 2020. 2.

annyira megnövelhetik a védelem áttöréséhez szükséges erőforrás-ráfordítást, hogy az már nem lesz összhangban az elérni kívánt eredmény nyújtotta előnyökkel. Ez eltérítheti a legtöbb kevésbé szofisztikált módszerekkel és szerényebb technológiai háttér-infrastruktúrával rendelkező támadó aktort, azonban nagy valószínűséggel az állami hátterű csoportokat nem. Elméletben az „ellentámadás" megindításának lehetősége, vagyis az *aktív kibervédelem* alkalmazása eltántoríthat egy állami szereplőt. Ilyen esetben a megtámadott fél, offenzív képességeit a támadó infrastruktúra vagy akár bármely más célpont ellen is bevetheti. Az ellentámadásnak pont a megfelelő mértékű, hálózati és kinetikus károkat kell okoznia (Stuxnet) kontrollált, például földrajzilag korlátozható kiterjedésben. Az elmélet alapján ez a károkozási képesség tántoríthatja el szándékától a potenciális állami hátterű támadókat, aminek hitelességét alá kell támasztani (például egy szimulációs gyakorlat alkalmával vagy éles demonstrációval).[15] A kibertéri elrettentéselmélet hatékony alkalmazhatósága több problémát is felvet. Egyrészt a válaszcsapás könnyen eszkalálhatja a konfliktust, vagy elmarasztaló reakciót válthat ki a nemzetközi közösségből, akár diplomáciai elszigeteltséghez is vezethet. Másrészt azon offenzív képességek, amelyek ilyen hatás kiváltására képesek, már túlmutathatnak a nemzetközi jogban bevett arányos fellépés és önvédelem esetpéldáin. Sokkal inkább értelmezhetők kiberfegyverként.[16]

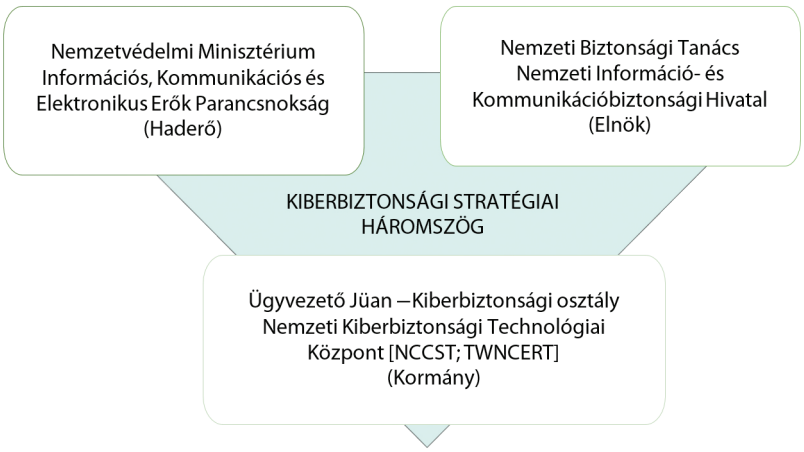
A szakirodalom alapján Tajvan és Kelet-Ázsia számára az alternatívát egy olyan együttműködésre építő stratégia jelenti, amelyben a hasonló fenyegetettségpercepcióval és kiberdiplomáciai célokkal rendelkező, közel azonos értékek mentén gondolkodó országok összehangoltan erősítik meg védelmi technológiai képességeiket. A kooperáció mélységétől függően a gyakorlati területek a kiberbiztonsági termékek fejlesztését, malware-elemzések és sérülékenységek publikálását és a felfedezett szoftveres sebezhetőségek kijavításával kapcsolatos információmegosztást foglalhatják magukban (lásd. 1. ábra). Ezek a lépések összességében emelik bármely ország vagy régió kiberbiztonsági szintjét és rezilienciáját.[17]

3. A kibervédelem szerkezeti felépítése és stratégiai háttere

A tajvani vezetés már 1999-ben megtapasztalta a kibertérből érkező fenyegetések lakosságra gyakorolt káros kognitív hatásait[18] és ezzel együtt felismerte az átfogó nemzeti kibervédelmi intézményrendszer és C3I-struktúra (*command, control, communications and intelligence*, parancsnokság, irányítás, kommunikáció és hírszerzés) kiépítésének szükségességét, az információs hálózatok folyamatos korszerűsítésének fontosságát.[19] Tajvanon a kibervédelmi keretrendszer és intézményi struktúra alapjait a 2000-es évektől kezdték kiépíteni, elsősorban a digitális információk védelmét célozva. A 2001-ben létrehozott Nemzeti Információs és Kommunikációs Munkacsoport

[15] Yau 2020. 7.
[16] Taddeo 2018.
[17] Yau 2019.
[18] 1999-ben számos kormányzati szerv weboldala szenvedett el defacement támadást azt követően, hogy Li Tenghui elnök „különleges államközi kapcsolatnak" nevezte a Tajvan és Kína közi viszonyt.
[19] Rawnsley 2005.

(National Information and Communication Task Force) feladata, hogy összefogja a minisztériumokon, kormányhivatalokon és egyéb állami szerveken belüli kiberbiztonsági részfeladatokat ellátó munkacsoportok tevékenységét.[20] Ezt az alapstruktúrát egészíti ki a Nemzeti Kiberbiztonsági Technológiai Központ (National Center for Cyber Security Technology) – amelyen belül a tajvani CERT (TWNCERT, kormányzati eseménykezelő központ) működik –, amely technológiai biztonsági szolgáltatásokat nyújt.[21]



2. ábra: A tajvani kiberbiztonsági szervek elhelyezkedése a védelmi szempontból releváns (elnök, kormány, hadsereg) államigazgatási területeken
Forrás: a szerző szerkesztése Huang 2018. 101. alapján

A stratégiai horderejű védelmi reformokat tekintve, Ma Ying-jeou (2008–2016, Kuomintang) elnöki ciklusa során, 2015-ben állítottak fel egy kiberhírszerzésre szakosodott szervezeti egységet a nemzetbiztonsági hivatalon belül. A Tsai-elnökség 2016-os beiktatását követő egyik első intézkedése volt a Nemzeti Információ- és Kommunikációbiztonsági Irodának a felállítása a Nemzeti Biztonsági Tanácson belül, amely az elnök közvetlen tanácsadó testülete. Ugyanebben az évben az Ügyvezető Yüan (a kormány) is felállította végrehajtó szervezetrendszerén belül a Kiberbiztonsági Osztályt, amelyhez tartozó munkacsoportok felelősek többek közt a kritikus információs infrastruktúra védelméért, a szabályozási és standardizálási előírások megalkotásáért és fejlesztéséért. 2017-ben a haderőszervezési reform keretében állították fel a tajvani hadsereg negyedik parancsnokságaként a Nemzetvédelmi Minisztérium irányítása alatt az Információs,

[20] Például az Oktatásügyi Minisztériumon belül működik a tudatosító képzésekért és tehetséggondozásért felelős csoport (Awareness Education and Talents Cultivation Group) az Igazságügyi és Belügyminisztériumok közös felügyelete alatt működik a kiberbűnözés felderítéséért és megelőzéséért felelős csoport (Cybercrime Protection and Control Group), míg a Nemzeti Kommunikációs Bizottság alatt az ún. Információs és kommunikációs ökoszisztéma és az internetes tartalom biztonsági csoport (Information and Communication Environment and Internet Content Security Group).

[21] Például általános tervezés és stratégiai elemzés (oktatás, jogi és szabályozási ügyek), incidensbejelentés és incidenskezelés (*monitoring, forensics* szolgáltatás is), adatelemzés, kutatás-fejlesztés, *penetration testing* (offenzív vizsgálatok) stb. A két szervezet tevékenységi köre magyar relációban a Nemzeti Infokommunikációs Szolgáltató Zrt. és a Nemzeti Kibervédelmi Intézet feladatköréhez hasonlítható.

Kommunikációs és Elektronikai Hadviselési Parancsnokságot, amely égisze alatt megkezdődhetett az offenzív kiberképességek kiépítése. Hsini Huang tajvani kiberbiztonsági szakember arról értekezett, hogy a kibervédelmi szervezetrendszer átalakítását érintő reformokban is megfigyelhető a Kuomintang-adminisztrációt jellemző, fenntartható Kína-kapcsolatok megtartása miatti óvatosabb, provokációt kerülő védelmi átszervezés. Ezzel szemben a jelenlegi elnökséget adó Demokratikus Progresszív Párt, a kiberbiztonsági környezet változását (növekvő incidensszám és APT-jelenlét) is kihasználva, képes volt keresztülvinni a katonai szervezetrendszert érintő reformokat. Emellett új stratégiai irányt hirdetett – amely a nemzeti biztonság részének tekinti a kiberteret, továbbá elrettentésre és offenzív technológiákra építi védelempolitikáját –, és a korábbiaktól eltérő megközelítést alkalmazva a hazai kiberbiztonsági iparág támogatásával kívánta korszerűsíteni a kiberbiztonsági infrastruktúrát. A Tsai-elnökség védelempolitikai elképzeléseihez illeszkedő szervezeti struktúrát „kiberbiztonsági stratégiai háromszög"-nek (lásd 2. ábra) nevezték el a szakirodalomban, mert integrálja a védelmi stratégiai tervezéshez és reagáláshoz szükséges három államigazgatási kulcsterületet: a hadvezetést, az elnöki tanácsadó testületet és a kormányzatot.[22]

A kibervédelmi fejlesztések politikai prioritásának kormányokon átívelő kontinuitása figyelhető meg abban, hogy 2001-től folyamatosan publikálták a négyéves ciklusra meghatározott kibervédelmi és kiberbiztonsági környezetet fejlesztő programokat. Két fejlesztési programot határoztak meg 2001–2004 és 2005–2008 között Nemzeti információs és kommunikációs infrastruktúra-biztonsági mechanizmusterv *(National Information and Communication Infrastructure Security Mechanism Plan)* néven. A 2005–2008 közötti fejlesztési időszakban kialakítottak egy nemzeti szinten működő kiberbiztonsági műveleti központot (Security Operation Center, SOC), amelynek feladata az incidensek megelőzése, detektálása és figyelmeztetések kiadása. Ezt követően – illeszkedve a nemzetközi trendekhez – a fejlesztési programokat új néven hirdették meg, a kiberbiztonság és kibervédelem szélesebb fogalmi értelmezése miatt, amely figyelembe veszi a pszichológiai hatások kiváltását az információs és kommunikációs technológiák felhasználásával. Ennek fényében négy további ciklusra vonatkozó Nemzeti Stratégiát adtak ki a Kiberbiztonság Fejlesztési Tervéről *(National Strategy for Cybersecurity Development Plan)*, amely legutóbbi, hatodik szakaszát a 2021–2024-es időszakra tervezték. A 2013–2016-as időszaktól kezdődően fokozatosan tovább bővült a nemzeti SOC rendszere, ami révén napjainkra kialakították az úgynevezett Nemzeti Közös Védelmi Rendszert (National Joint Defence System), amely ISAC- (Information Sharing and Analysis Center, információmegosztó és elemző központ) és CSIRT- (Computer Security Incident Response Team, számítógép-biztonsági incidenskezelő csoport) képességeket is integrál.[23] A reformsorozat növelte a nemzeti helyzetfelismerő képességet az úgynevezett domain szintű speciális nagyvárosi önkormányzati *(domain level)* és helyi önkormányzati, úgynevezett szolgáltató szinteken *(service provider level)* nyújtott felügyeleti szolgáltatások információinak becsatornázásával. A 2017–2020-as fejlesztési program egyik fő eleme a legmagasabb biztonsági osztályba sorolt állami szervek érettségi szintjének növelése és a hazai kiberbiztonsági piacot

[22] Huang 2018. 101–103.
[23] *Taiwan National Computer Emergency Response Team Annual Report 2021.* 2022.

támogató akcióterv megvalósítása volt. Emellett a teljes körű ISAC, SOC és CERT kiépítésének megkezdését irányozta elő a kritikus infrastruktúrában.[24]

A 2020-ban kiadott, 2021–2024-es Nemzeti Kiberbiztonsági Program (National Cyber Security Program) három fő célterületet határozott meg a víziójában a „biztonságos és ellenálló intelligens nemzet" *(smart country)* felépítéséhez:

- a kiberbiztonsági kutatás és képzés központjává válni az ázsiai és csendes-óceáni térségben;
- felépíteni egy proaktív védelmi alapokon nyugvó infrastruktúra-hálózatot;
- köz- és magánszféra közötti partnerség megteremtésével megfelelő ökoszisztémát létrehozni a kiberbiztonsági szint növelése érdekében.

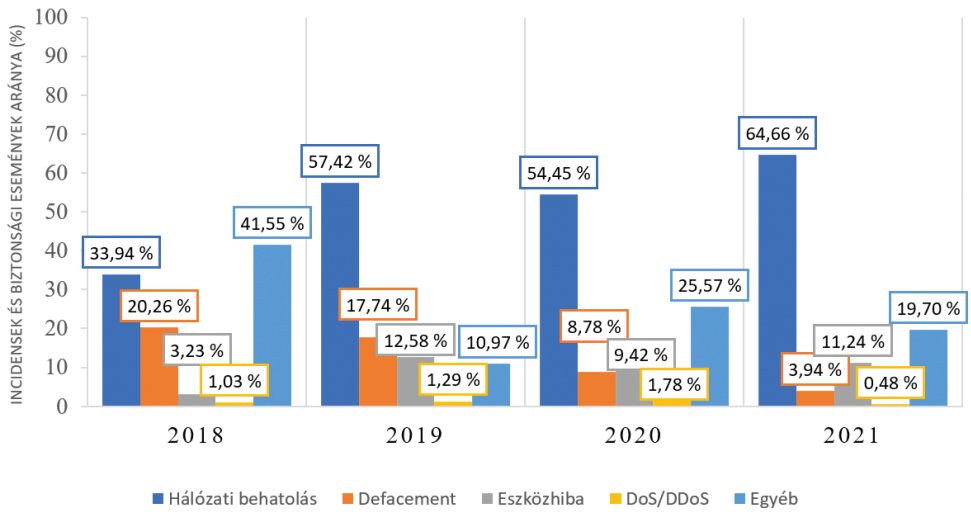
Az első célterülethez kapcsolódóan növelik a gyakorlati szakemberek számára elérhető tehetséggondozó lehetőségeket, és megnövelték a felsőoktatásban a kiberbiztonsági kutatási erőforrások és oktatók létszámának kvótáját, továbbá megnyitják a kormányzati szolgálati hálózat (Government Service Network, GSN) egy részét a gyakorlati oktatás részére. Emellett Kiberbiztonsági Kiválósági Központot (Cybersecurity Center of Excellence) hoznak létre az akadémiai kutatások és kritikai „jövőkutató" előrejelzések *(critical cybersecurity prospective research)* elvégzésére. A tervek szerint a központ csereprogramokat fog indítani és nemzetközi kutatókat is fogad majd. A második célterület a kritikus infrastruktúrák ellenállóképességének növelésére, valamint a kormányzati infrastruktúra felderítő képességei fejlesztéséhez fogalmaz meg intézkedéseket. Ilyen a kritikus infrastruktúra-szolgáltatók rendszeres auditálása és az egységes védelmi mechanizmus továbbfejlesztése (információmegosztás, értesítés az incidensekre adott válaszokról, kiberbiztonsági felügyelet). Fontos célkitűzés a CISO-k kinevezése és a biztonsági alapszint *(cyber security baseline)* kiépítése a létfontosságú infrastruktúra-szolgáltatóknál. A harmadik, magán- és állami szféra kooperációját növelő célterület főleg az infokommunikációs chipek gyártására fókuszál, valamint az 5G infrastruktúra biztonságának növelésére (Tajvan is biztonsági előírásokra vonatkozó megállapodást írt alá az Egyesült Államokkal: Joint Declaration on 5G Security).[25] Ennek keretében a kiszervezett szolgáltatások ellátási láncára vonatkozó kockázatkezelési rendszer megerősítését tűzte ki, és előrevetíti egy állami megfelelőségi tanúsítás *(compliance certificate)* kidolgozását az IoT-eszközök részére. Emellett fontos szegmens a lakosság tudatossági szintjének növelése a dezinformáció kiszűrése érdekében, amelyben célprogramokkal aktívan részt vesz a magánszféra, például a Google tajvani képviselete is.[26]

Arra a kérdésre, hogy védelempolitikai kérdésekben a tajvani vezetés mennyire tartja fontosnak a kibertér védelmét a haditengerészeti és légvédelemhez képest, a megkérdezett szakértő elmondta, hogy mindhárom domain egyforma fontosságú,

[24] Huang–Li 2018.
[25] Her 2021.
[26] Az információk alapjául a szakértői interjú és a Taiwan International Cooperation and Development Fund (ICDF) International Human Resource Development Workshop programsorozata keretében, a 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzottak szolgáltak. Lásd még a tajvani Nemzeti Kiberbiztonsági Technológiai Központ weboldalán megjelent összefoglalót: National Center for Cyber Security Technology 2022. (A program teljes szövege angol nyelven itt elérhető.)

mivel a biztonság és védelem értelmezését kiterjesztették a fizikai térről a kibertérre is, a támadások által kiváltható hatásokra tekintettel. Ebben a kérdésben Tajvanon konszenzus van a közvéleményben és a politikai diskurzusban.

4. Kibertéri fenyegetések



3. ábra: Kormányzati szervek által jelentett kiberbiztonsági incidensek százalékos megoszlása a TWNCERT éves jelentései alapján (2018–2020)

Forrás: a szerző szerkesztése a Taiwan National Computer Emergency Response Team Annual Report 2018–2021. alapján

A TWNCERT részére bejelentett biztonsági események és incidensek évenkénti megoszlásának százalékos arányát mutatja meg a 3. ábra.[27] Az éves részadatok 7709 db, 2022. január 31-én felügyelet alá tartozó intézménytől származtak, amelyek központi vagy helyi kormányzati szervek, kritikusinfrastruktúra-szolgáltatók, állami vállalatok és alapítványok. Az összesítő táblázat 2021-es „Hálózati behatolás" adatcsoportjára vonatkozik a sajtóhírekben megjelent, összességében 7709 intézményt érő, napi 5 milliós ártó szándékú esetszám, amelybe egyaránt beletartozik a sérülékenységeket kereső hálózati letapogatás *(scan)* és a támadás *(incidens),* valamint ez utóbbi sikeressége esetén az irányítás megszerzése *(control)*.[28] A CyCraft tajvani kiberbiztonsági

[27] Mivel a TWNCERT jelentéseiben használt címszavak pontos definíciói, a konkrét számadatok és háttérszámítások nem ismert, érzékeny információk, ezért csak korlátozott pontosságú megállapítások vonhatók le. Fontos megjegyezni továbbá a sajtóhírekben megjelent állami szerveket érő nagyszámú támadás – havi 30-40 millió hálózati behatolási kísérlet – kapcsán, hogy a tajvani kormányzati közleményekben a biztonsági eseményekre és incidensekre használt definíciók különbözhetnek az egyes nemzetközi szervek, az akadémiai és a civil szféra által használt munkadefinícióktól, emiatt a különféle forrásokban eltérőek lehetnek a vonatkozó számadatok.

[28] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzottak alapján.

vállalat, a *Taiwan News*-ra hivatkozva átlagosan heti 2644 támadásról (incidensről) írt blogbejegyzésében, így számításaik szerint 2020-ról 2021-re 38%-kal nőtt a tajvani állami szférában tapasztalt incidensek száma. A heti 925 támadásra tehető globális átlagtól való eltérés okát a CyCraft elemzői Tajvan egyedülálló geopolitikai helyzetére, csúcstechnológiás gazdaságára és kiforrott kommunikációs infrastruktúrájára vezetik vissza.[29] Tovább árnyalják az összképet a tajvani kormányzat által publikált, sikeres incidensek számára vonatkozó adatok, amelyek alapján 2019-ben 310 sikeres hálózati behatolás történt, 2020-ban 525 és 2021-ben 642 eset. A kihasznált sérülékenységek leggyakoribb eredői a gyenge jelszavakra, a *social engineering* technikákra és a frissítések hiányára *(unpatch)* vezethetők vissza.[30]

4.1. A dezinformáció esetpéldái

A 2021-es World Press Freedom Index Ázsián belül a másodikként (Dél-Korea mögött), világszinten negyvenhatodikként értékelte (180 vizsgált államból) a tajvani média diverzitását és a szólásszabadság biztosítottságát. 2020-as statisztika alapján a háztartások 99,99%-a rendelkezik digitális televízióval, továbbá 252 online és nyomtatott sajtószolgáltató, 32 hírügynökség, valamint 64 kábel- és 105 műholdas csatorna érhető el.[31] Ebben a médiakörnyezetben a kormányzati szereplők és a kiberbiztonsági szakértők egyaránt a dezinformáció mértékét tartják a Tajvant érő legsúlyosabb kihívásnak.[32] A dezinformáció elleni küzdelem részeként 2019-ben a Nemzetvédelmi Minisztérium politikai hadviselés elleni irodája (Political Warfare Bureau) bejelentette egy álhírekre adott válaszreakciókért felelős gyors reagálású csoport létrehozását, továbbá azt, hogy a Nemzeti Biztonsági Tanács big data elemzési technológiát alkalmazva elemzi a Kínai Kommunista Párt narratívájával egyező álhírek terjesztési taktikáit a megfelelőbb, technológiaalapú válaszlépések kidolgozásához. Ezzel párhuzamosan a kormányzat egyik új megközelítésében a köztisztviselők kreativitására bízta, hogy az „internet nyelvén", vagyis mémekkel reagáljanak az álhírekre, amely technikát a tajvani digitalizációért felelős miniszter, Audrey Teng egy 2019-es beszédében „a humorral a híresztelés ellen" ('humor over rumor', *meme engineering*) mechanizmusként írt le. A minisztériumokban olyan csoportokat alakítottak ki, amelyek feladata, hogy az álhírekre 1 órán belül reagáljanak, legfeljebb 20 szavas címet és 200 karakternyi szöveget tartalmazó tisztázó mémüzenet közzétételével a közösségimédia-felületeken. A kezdeményezés mögött olyan felmérés áll, amely alátámasztotta, hogy azon felhasználó, aki látta a tisztázó üzenetet, többé nem osztotta meg a kapcsolódó álhíreket, így gyors kiszűrés esetén rövid időn belül képesek visszaszorítani annak terjedését.[33] A módszer sikerének előfeltétele, hogy a lakosság magas digitalizáltsági mutatókkal és tudatossági szinttel

[29] CyCraft Technology Corp 2022.

[30] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián Jyan Hong-Wei (Végrehajtó Jüan Kiberbiztonsági osztályának volt igazgatója) *National Cyber Security Program of Taiwan* című előadása alapján.

[31] Tajvan Külügyminisztériuma 2022.

[32] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzottak alapján.

[33] Blanchette et al. 2021. 16–17.

rendelkezzen, továbbá a kormányzati kommunikációs csatornáknak széles elérési hálója legyen a társadalomban.

Az álhírek terjedéséről a tajpeji The DoubleThink Lab nevű kutatólabor végzett nagyszabású felmérést annak apropóján, hogy nagyszámú hamis vagy félrevezető információ jelent meg a tajvani médiában 2020-ban, ami a koronavírus okozta pandémia kiindulása mellett az elnökválasztás éve is volt. A támadók azt sugallták, hogy Tajvanon megbukott a demokrácia, és ezt a koronavírussal kapcsolatos hamis állításokra is visszavezették. Ezzel próbáltak megosztottságot generálni a lakosságban, csökkenteni a kormányzat iránti bizalmat, valamint megzavarni a politikai folyamatokat olyan eszközökkel, amelyek úgynevezett hír- és információs visszhangkamrákba[34] szorítják az egyes társadalmi csoportokat. A hamis vagy félrevezető információt tartalmazó közösségimédia-posztokon vizsgált indikátorok, amelyek a dezinformáció eredetét, célját, hatását, célközönségét és terjesztésének módját elemezték, összehangolt tevékenységre és pekingi narratívára vezethetők vissza. A The DoubleThink Lab elemzése feltárta, hogy a támadók szoros együttműködést kezdeményeztek célországbeli (nem csak Tajvan), valós online influencerekkel (véleményformálók), akiket arra próbáltak rávenni, hogy megosszák az álhíreket nagy elérésű platformjaikon. A kutatólabor összességében nagyszabású információs műveletként értékelte a 2020-as dezinformációs kampányt, amelyért állításuk szerint a Kínai Kommunista Párt tehető felelőssé. Megoldási javaslatukban jogi normák meghozatalát vagy módosítását és tartalomszabályozási intézkedéseket ajánlottak a tajpeji vezetés részére.[35] Fontos megjegyezni, hogy Magyarország és euroatlanti szövetségesei tágabban értelmezik az információs műveleteket a *Tallinn Manual* (*Tallinni kézikönyv,* a kiberháborúra alkalmazandó nemzetközi jog tallinni kézikönyve) alapján. A pszichológiai műveletek (PSYOPS) és a számítógép-hálózati műveletek mellett – amelyet a dezinformációs kampány érint – beletartoznak a fogalomba a képi és rádióelektronikai felderítés (IMINT, SIGINT) és az elektronikai hadviselés műveletei. Annak megállapításához, hogy Tajvant érik-e információs műveletek Kína részéről, komplexebb képet kell vizsgálni az euroatlanti katonai gondolkodásmód alapján.

Maradva a dezinformáció esetpéldáinál, a tajvani rendőrség csúcstechnológiás bűnözéselleni központja (High-tech Cybercrime Center)[36] 2020 és 2021 folyamán az alábbi két jelentős, állami hátterű dezinformációs támadásról számolt be. Az első eset 2021 áprilisában történt, amikor a Twitteren egy hamis állami dokumentumról készült fotó kezdett el terjedni, amely azt tartalmazta, hogy Tajvan nukleáris anyagokkal szennyezett vizet vesz át Japántól. Az álhíreket tartalmazó eredeti posztot közzé tevő fiókok lenyomozása után megállapították, hogy a felhasználó IP-címe kínai szolgáltatóhoz van regisztrálva, továbbá már korábban is használták támadások során. A második esetpéldában az összehangolt hiteltelen magatartás *(coordinated inauthentic behaviour)*

[34] Egy jelenség, amelyet a keresőmotorok és a közösségi hálózati oldalak üzemeltetői által működtetett hírválogatási algoritmusok (például a felhasználó által beállított szempontok vagy egyedi aktivitás) szűrőbeállításai okoznak. Emiatt a felhasználó a teljes médiakörnyezet helyett csak korlátozott, megszűrt híreket és hírforrást ér el közösségimédia-felületén vagy a keresőmotorokban, ami nem feltétlenül fedi a valóságot. GÁLIK 2019.

[35] Allen-Ebrahimian 2021.

[36] A központ és annak digitális igazságügyi laboratóriuma (digital forensics lab) rendelkezik ISO/IEC 17025 Windows Program Analysis Operating Procedures tanúsítvánnyal.

technikáját fedték fel 2021 szeptemberében egy tajvani kiberbiztonsági céget érintő dezinformációs kampányban. A támadás első hullámában egy japán hírmegosztási szolgáltatást nyújtó weboldalon keresztül jelenítettek meg álhíreket szeptember 17-én, amelyeket négy napig terjesztettek a tajvani közösségi médiában. Szeptember 25-én, a második hullám kezdetén a támadók által létrehozott felhasználó hamisnak nevezte a kiberbiztonsági cég hivatalos magyarázatát, két nappal később ugyanaz a japán weboldal a Kaspersky Lab japán kirendeltségének bejegyzésére hivatkozva újabb hamis információt közölt, amelyet a korábban is használt felhasználói fiókon keresztül terjeszteni kezdtek a közösségi médiában. Szeptember 30-án a Kaspersky Lab Japan közzétette hivatalos oldalán a helyesbítést, és elismerte, hogy a támadók megszemélyesítették. A támadók identitására többek közt a bejegyzésekben használt egyszerűsített kínai írásjegyek (ezeket Kínában használják hivatalosan, míg Tajvanon a régies, komplexebb írásjegyeket) is utaltak, a nyomozás végén a tajvani rendőrség két elkövető személyt azonosított.[37]

4.2. APT-jelenlét esetpéldái

Az egyértelmű politikai indíttatás miatt említésre méltó az Apple Daily tajvani hírszolgáltatót 2014-ben érő támadások sorozata, amely a szolgáltató hongkongi „esernyős forradalom" tüntetéssorozatról szóló, kínai kormányzatot elítélő hangvételű riportjaira adott válaszreakciók voltak.[38] Jelentős eseményként tartják számon a tajvani szakemberek a Közszolgálati Minisztériumot ért 2019. júniusi adatszivárogtatást, amely a közszolgálatot ellátók személyes adatait érintette.[39]

A tajvani kritikus információs infrastruktúrát 2020 májusában érte zsarolóvírus *(ransomware)* általi kibertámadás. A célpont a nemzeti olajvállalat – a CPC Corp – volt, amely az olajtermékek szállításáért és a cseppfolyósított földgáz (LNG) importjáért felelős. A tajvani hatóságok a támadási lánc első eseményét 2018 júliusára vezették vissza, amikor a támadók *malware-t* helyeztek el az áldozatok weboldalán. A támadók 2022. március végén kezdték meg a műveletet, ekkor a weboldal abnormális csatlakozást kezdeményezett az intranet irányába, majd négy nappal később a hackerek behatoltak a domainszerverre és nagyszámú csatlakozási kérést generáltak, ami riasztást váltott ki. Másnap a támadók két számítógépre helyeztek el programot *(backdoor)*, amely utat nyitott a rendszerbe történő behatoláshoz. Ezt a trójai típusú támadást tekinthetjük a behatolási pontnak *(intrusion point)*. Negyvenkét nappal később, a munka ünnepe miatti három napos hosszú hétvégét kihasználva, május 4-én a támadó átvette az irányítást a rendszergazda fiókja felett, és bejelentkezve az AD-szerverre, a csoportházirendek (GPO) segítségével szétterítette szervezeti szinten a zsarolóvírust,

[37] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián, Rufus Lin (Belügyminisztérium Nemzeti Rendészeti Ügynökség Információ Menedzsment Irodájának Igazgatója) *Fighting High Tech Crime Experience in Taiwan* című előadása alapján.

[38] Yang–Chung 2014.

[39] Huang 2018.

majd hajnalban aktiválta a programot, így az titkosította az adatokat.[40] Bár a támadás nem érintette a vállalat energiatermelését, egyes ügyfelek esetében megzavarta a vállalat által kiadott kártyákkal lebonyolított fizetési tranzakciókat.[41] A CyCraft Technology Corp elemzésében az APT10 tevékenységére utaló bizonyítékokat talált, amely több hátsó kaput, köztük a *CobaltStrike backdoor*-t kihasználva juttathatta be a rendszerbe a *ColdLock* zsarolóvírust. A vállalat malware-elemzésének eredményei alapján a ColdLock eltávolította az összes fizetési információt, a kapcsolattartó e-mail-címét és az RSA nyilvános kulcsot, amelyek mind információként szolgálhattak volna a titkosítás feloldásához.[42] 2020 májusában zsarolóvírus-támadás ért 10 másik kritikusinfrastruktúra-üzemeltető szervezetet is, köztük a Chunghwa Telecom-ot.

2020 augusztusában legalább 10 kormányzati intézményt ért támadásra derült fény: a *Waterbear malware* mintegy 6000 e-mail-címet kompromittált, így bizalmas információk és személyes adatok is érintettek voltak. A tajvani kiberbiztonsági nyomozó osztály attribúciója két kínai hátterű hackercsoport – az úgy nevezett Blacktech (APT10) és Taidoor csoportok – tevékenységére talált bizonyítékot. A nyomozóhivatal igazgatóhelyettese, Liu Chia-zung egy 2020-as interjúban elmondta, hogy a támadók céljaként, az adatlopás mellett, a bizalmas adatok kiszivárogtatása sem kizárható. A hálózati behatolás legkorábbi időpontját ebben az esetben is 2018-ra vezették vissza a szakemberek. A kampányban legalább négy tajvani technológiai cég is érintett volt, amelyek mind kormányzati beszállítók voltak.[43]

5. Nemzetközi együttműködések és gyakorlatok

Tajvan számos nemzetközi kooperációs platformon van jelen, sokrétű technikai jellegű tevékenységgel, így kiberdiplomáciai mozgásterének alapját is ezek a képességei adják, főként a Nemzeti Kiberbiztonsági Technológiai Központ, a TWNCERT és a kormányzati Kiberbiztonsági Osztály munkája nyomán. Tajvan nemzetközi kiberbiztonsági együttműködési lehetőségeinek egyik fő sarokköve az APCERT- (Asia Pacific Computer Emergency Response Team) tagság, amelyen keresztül nemzetközi szimuláción vett részt 2018 májusában (Data Breach via Malware on IoT),[44] 2019 júliusában (Catastrophic Silent Draining in Enterprise Network)[45] és 2020 márciusában (Banker doubles down on Mining).[46] Az együttműködés másik területe a technikai képzések megtartása az APCERT Képzési Munkacsoportjában (Training Working Group), amelyben Tajvan minden évben részt vett oktatóként a TWNCERT 2018–2021-es éves beszámolói alapján.[47]

[40] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián, Jyan Hong-wei (Végrehajtó Jüan Kiberbiztonsági osztályának volt igazgatója) *National Cyber Security Program of Taiwan* című előadása alapján.
[41] Lyngaas 2020.
[42] Cycraft Technologies Corp 2021.
[43] Lee 2020; CyCraft Technology Corp 2020.
[44] *Taiwan National Computer Emergency Response Team Annual Report 2018.* 2019. 8.
[45] *Taiwan National Computer Emergency Response Team Annual Report 2019.* 2020. 8.
[46] *Taiwan National Computer Emergency Response Team Annual Report 2020.* 2021. 9.
[47] *Taiwan National Computer Emergency Response Team Annual Report (A TWNCERT éves beszámolói.)* 2022.

Az államközi együttműködések kapcsán a megkérdezett szakértő kiemelte, hogy Tajvan minden évben megrendezi a Cyber Offensive and Defensive Exercise (CODE) gyakorlatot, amely kétévente (2019-ben és 2021-ben) egy alkalommal nemzetközi résztvevőket is fogad, általában a támadó fél szimulálásához. Az interjúalany azt is megerősítette, hogy Tajvan, az irányába mutatott nyitott és barátságos hozzáállású, bármely nemzetközi szervezettől és országtól érkező együttműködési lehetőségre nyitott. Jellemzően a közös védelem *(joint defence)* jegyében valósulnak meg az együttműködések, amelyben Tajvan szívesen megosztja a fenyegetésekről gyűjtött információit és az általuk szerzett tapasztalatokat, például a CODE-gyakorlatok alkalmával.

Egyes sajtóorgánumok szalagcímei „kiberháborús gyakorlatként" emlegették a 2019. novemberi négynapos 2019 CODE multinacionális, hálózatbiztonsági gyakorlatot, amelyet az Amerikai Intézettel (American Institute in Taiwan, az USA képviseleti szervezete) együtt szerveztek meg Tajvanon. A gyakorlat közös megtartása azért is jelentős diplomáciai előrelépésnek számított, mert Tajvan mégsem kapott meghívást az Egyesült Államok által szervezett 2018. tavaszi Cyber Storm nemzetközi gyakorlatra. A korábbi helyzetgyakorlatoktól eltérően a 2019-es CODE teljes körű szimuláció volt, amelyet pénzügyi kiberbiztonsági környezetre terveztek. A nemzetközi résztvevők a tajvani pénzügyi szervezetek szakembereivel alkottak integrált csapatokat, hogy fejlesszék mindkét szerepkör technikai és reagáló képességeit.[48] A TWNCERT 2019-es jelentése alapján a gyakorlaton részt vevők 4 támadó csapatot *(Red team)* alkottak, közülük egyet-egyet Malajzia (MyCERT) és a Cseh Köztársaság (NCISA) alkotott, kettőt pedig a tajvani kormányzati ügynökségek. A két védekező csapat *(Blue team)* 14 tajvani banki alkalmazottból állt.[49]

A 2020-as évben a TWNCERT részt vett az Iszlám Együttműködés Szervezete (OIC-CERT) által tartott gyakorlaton (Cyber Drill), valamint a CyberEx gyakorlaton, amelyet a Spanyol Nemzeti Kiberbiztonsági Intézet (INCIBE-CERT) vezetett.[50] Feltehetőleg a 2020. májusi CPC Corp energiavállalatot ért támadástapasztalat feldolgozásának jegyében, a 2020-as évhez hasonlóan, a TWNCERT 2021-es Cyber Offensive and Defensive Exercise (CODE 2021) nemzetközi gyakorlatán ismét energiaipari létfontosságú információs infrastruktúrát (CII) érő támadást szimuláltak. A CODE 2021-en 20 nemzetből érkeztek résztvevők, így összesen 31 állami és magánszervezet vett részt Red vs. Blue team felállásban. Az interjúalany hozzátette, hogy tíz különböző állam csatlakozott hivatalosan az eseményhez, az érkező szakemberek három támadó csapat felállítását tették lehetővé. A TWNCERT belföldi (úgynevezett Nemzeti Kiberbiztonsági Gyakorlat) helyzetgyakorlatokat is tartott a kormányzati szervek részére, amelyek közt a *social engineering* szimulációt és az incidensreagáló képességek fejlesztését célzó gyakorlatot nevesítették.[51]

Arra a kérdésre, hogy miként reagáltak a régió országai Tajvan offenzív kiberképességek kiépítésére irányuló erőfeszítéseire, a szakértő elmondta, hogy Tajvan nem offenzív képességként tekint a fejlesztésre, hanem proaktív védelemként, amellyel céljuk, hogy megállítsák a támadást annak folyamatában, vagy mielőtt kifejtené

[48] Department of Information Services, Executive Yuan 2019; BBC News 2019.
[49] National Center for Cyber Security Technology 2019. 7.
[50] *Taiwan National Computer Emergency Response Team Annual Report 2020.* 2021. 9.
[51] *Taiwan National Computer Emergency Response Team Annual Report 2021.* 2022. 7.

károkozó hatásait. Az utolsó interjúkérdés arra kereste a választ, hogy Tajvan miként látja szerepét a nemzetközi közösségben, milyen kiberdiplomáciai célkitűzései vannak. Az interjúalany elsősorban az ország kibertéri védelmét növelő eszközként tekint a kiberdiplomáciai lehetőségeikre. Ezt kiegészítve a konferencia házigazdája, a tajvani Nemzeti Chengchi Egyetem Közigazgatási Karának professzora úgy írta le Tajvan nemzetközi látásmódját, miszerint nagyon komolyan számol a kiberháború veszélyével és lehetőségével.

6. Összegzés és konklúzió

A szakértői interjún kapott válaszok alapján az a következtetés vonható le, hogy Tajvan a kibertérből érkező fenyegetéseket akképp igyekszik csökkenteni kiberdiplomáciai eszközökkel, hogy nemzetközi információmegosztáson (riasztási információk, *threat intel, forensics* és malware-elemzések megosztása) alapuló hálózatot épít régión belüli partnereivel és az USA-val. A Kínához fűződő speciális helyzete ellenére az utóbbi öt évben részt tudott venni nemzetközi kiberbiztonsági szimulációs gyakorlatokon, amelyek mellett az általa rendszeresen megszervezett CODE nemzetközi gyakorlatokon folyamatosan képes az állami szervek szakemberállományának technikai készségeit emelni. Tajvannak más irányba is bővítenie kell kiberdiplomáciai mozgásterét, amire a 2021–2024-es Nemzeti Kiberbiztonsági Program tudásmenedzsmentre vonatkozó célkitűzései alkalmasak lehetnek. A tervben előirányozottak sikeres megvalósítása regionális szintű (és világszínvonalú) tudásközponttá emelnék Tajvant, amiből a belföldi IKT-ipar és az akadémiai szféra is profitálna a tervezett Kiberbiztonsági Kiválósági Központon keresztül.

A belföldi kiberbiztonsági piac támogatása egyrészt a nemzeti infrastruktúra korszerűsítését szolgálja, másrészt a Nemzeti Kiberbiztonsági Programban körvonalazott állami megfelelőségi tanúsítvány bevezetése az IoT-eszközökre és a rendszeres állami auditok további bizalmi garanciákat adhatnak a tajvani félvezető- és chipgyártók fogyasztóinak, valamint az IKT-szektor piacának. Ezen intézkedések hatására erősít rá a Tajvan által képviselt diplomáciai szerepkör, amelyben a regionális kiberbiztonsági szintnövelés egyik előmozdítójaként kíván megjelenni, az információmegosztást és kooperációt promulgáló szereplőként. Tajvan emellett felhasználja a dezinformációs kampányok kezeléséből és a kormányzatot érő támadásokból származó tapasztalatát, és incidenskezelési kompetenciáját helyezi a kiberdiplomáciai kapcsolatok megindításának mérlegére.

A kibervédelmi reformok és a kiberdiplomáciai aktivitás értékelése alapján az a konklúzió vonható le, hogy a Tsai-elnökség stratégiai autonómiára törekszik a kibertérben, amellyel célja, hogy ebben a védelmi ágazatban Kína ne tudja nemzetközileg elszigetelni, így akadályozva képességeinek korszerűsítését. Tajvan számára a kibertér védelme egyet jelent a szürke zónás és hibrid fenyegetések elleni felkészültséggel és a nemzetgazdasági húzóágazatok prosperálásával, míg a nemzetközi közösség számára Tajvan kibertéri biztonsága összefonódik a különböző gazdasági szektorokkal, például az elektronikai és autóipari ellátási láncokban betöltött szerepe okán. Ennélfogva Tajvan védelmi ipari fejlesztési lehetőségeit és korlátait figyelembe

véve, katonai szempontból a kibertér jelentheti azt az ágat, amelyben önerejére és, érdekegyezés alapján, a nemzetközi közösség segítségére is számíthat a területvédelemhez szükséges hiteles elrettentési képesség felépítésére. Ez is jól mutatja, hogy a tajvani védelempolitikai stratégia, „*Eltökélt védelem, több dimenzióra kiterjedő elrettentés*" koncepciójának első védelmi rétegeként miért a kibertér van megnevezve. A minél ütőképesebb és szélesebb körű – offenzív és defenzív – képességekkel rendelkező kibertéri erő kialakításával és folyamatos korszerűsítésével a diplomáciai erőfeszítések elérhetik, hogy Tajvan más védelmi szektorban is kimozduljon a kínai diplomáciai nyomás alól, vagy kiegyensúlyozottabb erőviszonyokon alapuló szoros-menti kapcsolatokat tartson fenn.

KK1:

A tanulmány első kutatási kérdése arra vonatkozott, hogy Tajvan elrettentési koncepció mentén felépülő kibervédelmi stratégiája milyen lehetőségeket nyit, és milyen korlátokat szab Tajpej kiberdiplomáciai mozgásterének. A tajvani IT-ipari termékek jelentősége, a kiberbiztonsági szakemberek incidenskezelési tapasztalata és szakértelme kiegészülve a proaktív védelmi képességekkel komoly nemzetközi figyelmet irányított Tajpejre. A tajvani diplomácia azt a tőkét, amelyet a technikai képességek nemzetközi gyakorlatokon való demonstrálásával, valamint a szaktudás szakmai fórumokon és képzéseken történő átadásával halmozott fel, kibertéri fenyegetettségekkel kapcsolatos hírszerzési és elemzési információkra tudta váltani, ám politikai, stratégiai értékű együttműködést még nem tudott megvalósítani regionális partnereivel vagy az USA-val, a bonyolult Kína-kapcsolatok miatt.

H1:

Ebben a kontextusban vizsgálva az első hipotézist, miszerint Tajvan kiberdiplomáciai mozgásterének növelése érdekében arra törekszik, hogy további militarizálás nélkül, kooperatív eszközökkel növelje kiberbiztonsági szintjét, mivel stratégiai érdeke, hogy a régiós biztonsági dilemma ne terjedjen tovább a kibertérben, csak részben tekinthető helytállónak. A kooperatív eszközök, mint amelyeket a 2021–2024-es Nemzeti Kiberbiztonsági Program tudásmenedzsment céljaiban, illetve az állami és magánszféra IKT-ipar, valamint kiberbiztonság területein megvalósuló kooperációjának előmozdítására tett intézkedésekben fektetett le, ugyanúgy hozzájárulnak a kiberdiplomáciai mozgástér bővítéséhez, mint a gyakorlati képességek a proaktív védelemi stratégia adaptációjával. Mindkét módszer szükséges a kibervédelmi stratégiai autonómia eléréséhez. Emellett lényeges az a politikai narratíva is, amelyre a szakértői interjú hívta fel a figyelmet, hogy Tajvan az offenzív képességeit proaktív védelemként definiálja, habár az magában hordozza a csapásmérés lehetőségét is. Összességében a kiberhadviselési képességek bármelyike indukálhatja a kelet-ázsiai biztonsági komplexumban a kibertér militarizálását, ami végső soron geopolitikai okok miatt csökkenti a kibertér biztonsági szintjét. Az északkelet-ázsiai biztonsági

szubkomplexum militarizációs trendjei és fenyegetettségpercepciói már jelenleg is érvényesülnek a kibertérben, így a folyamat öngerjesztővé válhat, ami kedvezőtlen a régió összes államára nézve, amelyek IT-ipari nagyhatalmak. Tajvan viszont akár előnyére is fordíthatja ezt a helyzetet, mivel gazdasági húzóágazatai – a félvezetők és a microchipek gyártása – alaptermékként szolgálnak például Kína IT-iparának. Ezt a gondolatmenetet támasztja alá Tsai Ing-wen elnök asszony niche piac (réspiac) erősítésére utaló beszédének részlete, miszerint Tajvannak „nélkülözhetetlenné és pótolhatatlanná kell válnia a világban" biztonságának garantálásához.

KK2:

A második kutatási kérdés arra kereste a választ, hogy értékelhető-e a Tajvant érő kibertámadások volumene és összetétele információs műveletekként. Tekintettel a kutatás azon korlátjára, miszerint az információs műveletek fogalmába beletartozó képi és rádióelektronikai felderítés, valamint elektronikai hadviselés esetpéldáiról, továbbá ezek súlyosságának mértékéről nem áll rendelkezésre részletes, publikus információ, nem lehet objektív választ alkotni. Mindazonáltal a dezinformációs kampányok okozta fenyegetés és az APT-jelenlét esetpéldái önmagukban nem tekinthetők információs műveleteknek, annak ellenére, hogy súlyosan érintik a pszichológiai dimenziót és állami hátterű, szofisztikált számítógép-hálózati műveletek voltak.

H2:

A kutatás fent említett korlátait figyelembe véve, a tanulmányban felsorakoztatott esetpéldák, valamint a kiemelkedően magas incidensszám összetevőinek elemzése részben alátámasztja a második hipotézist, amely a tajpeji politikai fordulatra reagáló, szürke zónás műveletek közé sorolja a KNK kibertéri aktivitását. Ezzel kapcsolatban az a kiegészítés tehető, hogy a szürke zónás műveletek volumene és az általuk generált konfliktus intenzitása igen magas, amit súlyosbít a PLA aktív katonai tevékenysége a tajvani szorosban és az ukrajnai háborúval kapcsolatos helytelen párhuzamok, amelyeket mindkét fél tagad.[52]

Tajvan kiberbiztonsági körképének megismerése nyomán Magyarország az alábbi ajánlások mentén profitálhat:

- A tajvani Nemzeti Közös Védelmi Rendszerhez hasonló nemzeti SOC-, CSIRT- és ISAC-képességeket integráló struktúra kialakításának megkezdése.
- A fentiekhez kapcsolódó tudás- és tapasztalatcsere érdekében, a diplomáciai érdekek vizsgálata mellett, megfontolandó a magyar nemzeti kiberbiztonsági szervezetek és a tajvani szervezetek közti technikai és akár más területen megvalósuló kooperáció előmozdítása, valamint az akadémiai, gyakorlati és kutatói tudásmenedzsment-lehetőségek és -kezdeményezések kiaknázása.

[52] Portfolio 2022.

- A tajvani Nemzeti Kiberbiztonsági Programban és fejlesztési tervekben megfogalmazott célok átültetése a magyar kiberbiztonsági struktúrába és környezetbe.
- A tajvani dezinformáció elleni kezdeményezések magyarországi megvalósíthatóságának vizsgálata és alkalmazása.

Felhasznált irodalom

AFP (2021): Taiwan Government Faces 5 Million Cyber Attacks Daily: Official. *The Guardian,* 2021. november 10. Online: https://guardian.ng/news/world/taiwan-government-faces-5-million-cyber-attacks-daily-official/

Allen-Ebrahimian, Bethany (2021): Report: Beijing Flooded Taiwan with Coronavirus Disinformation. *Axios China,* 2021. május 24. Online: www.axios.com/2021/05/24/report-beijing-taiwan-coronavirus-disinformation

Bartók András – Wagner Péter (2020): A kínai A2/AD és a válaszreakciók Kelet-Ázsiában (1). In *KKI-elemzések* E-2020/69. szám. Budapest, Külügyi és Külgazdasági Intézet. 3–12. Online: https://kki.hu/wp-content/uploads/2020/08/E-2020_69_kina-kelet_azsia.pdf

BBC News: US and Taiwan Hold First Joint Cyber-War Exercise. *BBC,* 2019. november 4. Online: www.bbc.com/news/technology-50289974

Blanchette, Jude – Livingston, Scott – Glaser, Bonnie – Kennedy, Scott (2021): Protecting Democracy in an Age of Disinformation: Lessons From Taiwan. *CSIS,* 2021. január 27. Online: https://apo.org.au/node/310698

Cheung, Eric – Ripley, Will – Tsai, Gladys (2021): How Taiwan Is Trying to Defend Against a Cyber ‚World War III'. *CNN Business,* 2021. július 23. Online: https://edition.cnn.com/2021/07/23/tech/taiwan-china-cybersecurity-intl-hnk/index.html

CyCraft Technology Corp (2020): *China Implicated in Prolonged Supply Chain Attack Targeting Taiwan Financial Sector,* 2022. február 22. Online: https://medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525

CyCraft Technologies Corp (2021): *China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware*. (2021. június 2.) Online: https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

Department of Information Services, Executive Yuan (2019): *Taiwan and US Co-hosting Multinational Cybersecurity Exercise.* (2019. november 9.). Online: https://english.ey.gov.tw/Page/61BF20C3E89B856/0f357b66-7ed3-4123-98c6-b91097b82536

Gálik Mihály (2019): A hálózati hírmédia sajátosságai különös tekintettel a visszhangkamra- és a szűrőbuborék-jelenségre. *In Medias Res*, 2019. december 19. Online: https://media-tudomany.hu/2019/12/19/a-halozati-hirmedia-sajatossagai-kulonos-tekintettel-a-visszhangkamra-es-a-szurobuborek-jelensegre/

Her, Kelly (2021): Defending Cyberspace. *Taipei Times,* 2021. május 1. Online: https://taiwantoday.tw/news.php?unit=8&post=200638&unitname=Economics-Taiwan-Review&postname=Defending-Cyberspace

Huang, Hsini (2018): A Collaborative Battle in Cybersecurity? Threats and Opportunities for Taiwan. *Asia Policy, National Bureau of Asian Research,* 15. évf. 2. sz. 101–106. Online: https://doi.org/10.1353/asp.2020.0015

Huang, Hsini – Li, Tien-Shen (2018): A Centralised Cybersecurity Strategy for Taiwan. *Journal of Cyber Policy,* 3. évf. 3. sz. 344–362. Online: https://doi.org/10.1080/23738871.2018.1553987

Kínai Népköztársaság Külügyminisztériuma (2022): *Zhao Lijian szóvivő nyilatkozata a 2022. április 15-i rendes sajtótájékoztatón.* (2022. április 15.). Online: http://cy.china-embassy.gov.cn/eng/fyrth/202204/t20220415_10668556.htm

Lee, Yimou (2020): Taiwan Says China Behind Cyberattacks on Government Agencies, Emails. *Reuters,* 2020. augusztus 19. Online: www.reuters.com/article/us-taiwan-cyber-china-idUSKCN25F0JK

Lyngaas, Sean (2020): Taiwan's State-Owned Energy Company Suffers Ransomware Attack. *CyberScoop,* 2020. május 5. Online: www.cyberscoop.com/cpc-corp-ransomware-attack-taiwan-trend-micro/

Portfolio (2022): Dől a következő dominó? Menekül a tőke Tajvanból. *Portfolio,* 2022. március 8. Online: www.portfolio.hu/uzlet/20220309/dol-a-kovetkezo-domino-menekul-a-toke-tajvanbol

Rawnsley, Gary D. (2005): Old Wine in New Bottles: China–Taiwan Computer-Based 'Information Warfare' and Propaganda. *International Affairs,* 81. évf. 5. sz. 1061–1078. Online: https://doi.org/10.1111/j.1468-2346.2005.00502.x

Strong, Matthew (2021): Taiwan Government Departments Targeted by Hackers 5 Million Times per Day. *Taiwan News,* 2021. november 10. Online: www.taiwannews.com.tw/en/news/4340699

Taddeo, Mariarosaria (2018): How to Deter in Cyberspace? *Strategic Analysis.*

Taiwan National Center for Cyber Security Technology Annual Report 2019. 2020. Online: www.twncert.org.tw/Download/NCCST%20Annual%20Report%202019.pdf

Taiwan National Center for Cyber Security Technology (2022): *About NCCST: 6th Phase of National Cyber Security Program*, 2022. augusztus 30. Online: www.nccst.nat.gov.tw/About?lang=en

Taiwan National Computer Emergency Response Team Annual Report 2018. 2019. Online: www.twncert.org.tw/Download/TWNCERT%20Annual%20Report%202018.pdf

Taiwan National Computer Emergency Response Team Annual Report 2020. 2021. Online: www.twncert.org.tw/Download/TWNCERT%20Annual%20Report%202020.pdf

Taiwan National Computer Emergency Response Team Annual Report 2021. 2022. Online: www.twncert.org.tw/Download/TWNCERT%20Annual%20Report%202021.pdf

Tajpej Képviseleti Iroda (Magyarország) (2018): *Tsai elnök asszony ígérete egy erősebb Tajvan építésére nemzeti napi beszédében.* Taipei Representative Office in Hungary – Taiwan Today, 2018. november 9. Online: www.roc-taiwan.org/hu_hu/post/1919.html

Tajvan Külügyminisztériuma (2022): *Fact Focus. Mass Media.* Online: www.taiwan.gov.tw/content_11.php

Yang, Yuan-ting – Chung, Jake (2014): Apple Daily Slams Hack Attack. *Taipei Times,* 2014. június 19. Online: www.taipeitimes.com/News/front/archives/2014/06/19/2003593115

Yau, Hon-min (2019): A Critical Strategy for Taiwan's Cybersecurity: A Perspective From Critical Security Studies. *Journal of Cyber Policy,* 4. évf. 1. sz. 35–55. Online: https://doi.org/10.1080/23738871.2019.1604782

Yau, Hon-min (2020): *Evolving Toward a Balanced Cyber Strategy in East Asia: Cyber Deterrence or Cooperation? Issues & Studies,* 56. évf. 3. sz. Online: https://doi.org/10.1142/S1013251120400111

Yu, Jess Macy – Blanchard, Ben (2018): Chinese Cyber Attacks on Taiwan Government Becoming Harder to Detect. *Reuters,* 2018. június 15. Online: www.reuters.com/article/us-taiwan-china-cybersecurity-idUSKBN1JB17L