NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 2. szám 55–80. | DOI: 10.32561/nsz.2024.2.4

Lendvai Tünde[1]

A Kínai Népköztársaság feltételezett kiberhírszerzési műveleteinek értékelése: eljárások és a nemzetközi hatások áttekintése

Assessment of Presumed Cyber-Intelligence Operations of the People's Republic of China: Overview of Procedures and International Impacts

A tanulmány kutatási célkitűzése, hogy áttekintést adjon a Kínai Népköztársaság kiberhírszerzési tevékenységének nemzetközi relációban megjelenő helyéről és szerepéről, eszközrendszeréről. A szekunder források feldolgozása kvalitatív módszerrel valósult meg, kiegészítve olyan esetpéldák elemzésével, amelyek jól szemléltetik az elmúlt 5–7 év során nyilvánosan attribútált, feltételezhetően kínai kibertéri hírszerző műveletek cél- és eszközrendszerét. Az Egyesült Államokat érő, 2015 után megindított műveleteket (a Marriott Szállodaláncot, az Equifax hitelminősítőt és az Anthem Biztosítót ért incidensek) gazdasági, technológiai és politikai előnyök megszerzése motiválta. A megszerzett adatok felhasználhatók adatigényes technológiák és speciális IoT-eszközök fejlesztési és piackutatási szakaszában. Az incidensek kapcsán az USA nyomozó szervei rávilágítottak egy átfogó kínai kiberhírszerzési kampány eshetőségére. A nemzetbiztonsági kockázatok közt megjelenik a piaci szereplőktől megszerzett adatbázisok kombinálhatósága a szövetségi alkalmazottak személyi ügyeit kezelő hivataltól 2015-ig megszerzett (OPM-adatlopás) érzékeny információkkal és személyes adatokkal.

Kulcsszavak: *Kínai Népköztársaság, KNK, kiberhírszerzés, kiberműveletek, kiberkémkedés*

The research aims to provide an overview of the People's Republic of China's presumed cyber intelligence activities in the international context. It utilizes qualitative analysis of secondary sources and publicly attributed case studies from the past 5-7 years. Operations launched in the US after 2015, such as the Marriott, Equifax,

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

and Anthem incidents, were driven by economic, technological, and political motives. The acquired data might be used for developing data-driven technologies (AI, ML) and IoT tools. US investigative agencies suspect a broader Chinese cyber intelligence campaign, posing national security risks by combining acquired databases with sensitive information and personal data obtained from the Office of Personnel Management of federal employees (OPM data theft) until 2015.

Keywords: *People's Republic of China, PRC, cyber intelligence, cyber operations, cyber espionage*

Bevezetés

Hadtudományi szempontból vizsgálva, a nemzetközi érdekérvényesítés eszközeként kell értelmezni az állami és állam alatti kiberműveleti képességeket, ideértve a fejlett perzisztens fenyegetések[2] (APT vagy fejlett perzisztens fenyegetés) tevékenységét.[3] Ebből kiindulva, a Kínai Népköztársaságot (KNK vagy Kína) vizsgáló biztonság- és védelempolitikai, valamint az orientalisztikai kutatási területek már 2003-tól (az első felderített APT-kampánytól kezdve) vizsgálták az állami és állam alatti kiberegységekhez köthető kiberhírszerzési műveletek stratégiai célrendszerét, a pekingi vezetés globális hatalmi ambíciói kontextusában.[4] Kína kibertéri aktivitása 2012–2015 között ismét jelentős sajtópublicitást kapott (különösen a Snowden-ügy tapasztalatai kapcsán), az időszakban feltárt hírszerzési célú APT-kampányok miatt (lásd az USA köztisztviselőinek személyügyi hivatalát és az Anthem Biztosítót ért incidensek), majd 2017-ben a kínai Nemzetbiztonsági Törvény módosításának okán.[5] Ezen előzmények mellett, 2019-től tovább nőtt a Kínához kapcsolódó (kiber) fenyegetés-percepció a Huawei vállalat szoftverének és egyéb termékeinek integritását és bizalmasságát kétségbe vonó incidensek és a rájuk reflektáló kiberdiplomáciai események

[2] Az *Advanced persistent threat* (APT) jelen kontextusban állami háttértámogatással működő kiberbűnözői csoport. Az APT olyan kibertámadási modell, amelyben a támadó csoport vagy kiberbűnözők rendkívül komplex eljárásokat és fejlett támadó eszközöket alkalmaznak, továbbá hosszú időn keresztül képesek észrevétlenek maradni a célzott hálózatokban, hogy érzékeny információkat szerezzenek meg. Az APT-csoportoknak az ilyen műveletek kivitelezéséhez előzetesen – akár humánalapú technikákat alkalmazva, mint a *social engineering* vagy HUMINT – komoly figyelmet kell fordítaniuk az áldozatok folyamatos megfigyelésére a megfelelő támadási pont meghatározásához (pl. célzott adathalász-támadás kivitelezése), és rendkívül sok erőforrásra a hosszú távú hálózati jelenlét fenntartása érdekében. Ez utóbbi jelentheti a költségek időarányos megtérülését, nehezen hozzáférhető *zero-day* sérülékenységek vagy beszállítói láncok felhasználását és a rendkívül mély szakértelem rendelkezésre állását kormányzati, katonai vagy ipari titkok megszerzése érdekében. Ezen jellemzők és a célorientált feladat-megvalósítás okán feltételezhető, hogy az APT-csoportok tevékenységét állami támogatással hajtják végre. A támadók által alkalmazott TTP-k és célpontkiválasztás utal arra, hogy feltehetőleg mely nemzethez, országhoz köthető a támadás.

[3] Berzsenyi 2023: 19, 99–104, 111–113, 123–125.

[4] Lindsay–Cheung 2015: 58–60.

[5] A 2017-es kínai Nemzetbiztonsági Törvény *(National Intelligence Law)* célja a kínai állam biztonságának védelme és az országban működő szervezetek és egyének felett gyakorolt ellenőrzésének erősítése. A törvény számos kötelezettséget ír elő a szervezeteknek, többek között a kötelező állami adatszolgáltatást és az együttműködést a kínai állambiztonsági hatóságokkal, ami a technológiai multivállalatok üzleti titkainak bizalmasságát és piaci érdekeit is felülírhatja.

miatt.[6] Noha a kibervédelmi szakirodalom jelentős része a technológiai orientáltságú megközelítést alkalmazó CTI-jelentéseken (*cyber threat intelligence* – kiberfenyegetések elleni hírszerzés) alapszik, a kínai hátterű kiberbiztonsági incidenseket stratégiai szinten elemző, kvalitatív értékelést végző kutatócsoportok már 2015-ben és 2020-ban is felhívták a figyelmet publikációikban a kínai technológia- és tudástranszfer-hálózatok kockázataira, valamint a kínai technológiai óriáscégek adatgyűjtő tevékenységére.[7]

A kiberhírszerzés terminológiai és kiberbiztonsági háttere

Napjainkra a kínai hátterű IKT-technológiák és -szolgáltatások infrastrukturális, valamint fogyasztói beágyazottságából eredő fenyegetettségpercepció nem csupán tovább erősödött az euroatlanti szövetségi rendszer katonai és nemzetbiztonsági gondolkodásban, hanem bizonyos mértékben a biztonságiasítás jegyeit is magában hordozza, különösen az 5G-hálózat kiépítéséhez társuló biztonsági aggályok miatt (például hírszerzés- vagy szolgáltatáskiesésben rejlő zsarolási potenciál).[8] Ennek eredményeképp Kína és az euroatlanti szövetségi rendszer közt fennálló kiberdiplomáciai kapcsolatokat bizalmi krízishelyzet dominálja. Ez a jelenség különösen az Amerikai Egyesült Államok és az Egyesült Királyság kiberdiplomáciai kapcsolatait terheli meg, egyrészt a kölcsönösen alkalmazott szankciós politika miatt, amelyek IKT-termékeket és -vállalkozásokat vagy technológia- és tudástranszfer-együttműködéseket sújtanak.[9] Másrészt az utóbbi három évben az amerikai és brit kormányzat egyaránt aktívan alkalmazta a nyilvános attribúciót Kínával szemben, különösen az APT31 tevékenységére visszavezetett események miatt, amelyet közvetlenül a kínai Állambiztonsági Minisztérium állam alatti kiberegységei közé sorolnak.[10] Ennek kiemelendő példája az USA Igazságügyi Minisztériuma által 2024 márciusában nyilvánosságra hozott vádiratkivonat, amelyben a KNK hét állampolgárát vádolják számítógépes behatolásra és elektronikus csalásra irányuló összeesküvéssel, mert részt vehettek az APT31 egyes műveleteiben. A vádak szerint a célpontok között szerepeltek az USA mindkét nagy politikai pártjának kampányain dolgozó munkatársai, a 2018-as félidős választást és a 2020-as elnökválasztást megelőző időszakban. Továbbá érintettek voltak minisztériumi köztisztviselők, szenátorok és házastársaik, valamint amerikai vállalatok és kínai disszidensek is.[11] Az USA Pénzügyminisztériuma és brit tisztségviselők részéről ugyanezen események nyilvános attribúciójának egy másik megtorló formája volt egy kínai hátterű vállalat és két vállalkozó elleni bilaterális szankciók közös bejelentése 2024. március 24-én. London a Kínával kritikus törvényhozók elektronikus levelezési fiókjának feltörési kísérletével vádolja az APT31-ként azonosított csoportot, illetve egy másik

6 Kaska–Beckvard–Minárik 2019.
7 Lindsay–Cheung–Reveron 2015, Hannas–Tatlow 2020.
8 Friis–Lysne 2021.
9 Greig 2024.
10 Értsd: a nyilvános attribúció mint kiberdiplomáciai eszköz olyan eseteket takar, amelyek során az érintett („megtámadott") állam a sajtóban vagy diplomáciai fórumokat felhasználva teszi felelőssé az incidensért vagy kiberműveletért a feltételezett „támadó" államot. A nyilvános attribúció célja a hasonló tevékenység elrettentése, a „leleplezett" hírszerző tevékenység miatti megszégyenítés diplomáciai eszközként való alkalmazása által.
11 US Department of Justice 2024.

kínai hátterű kibertéri fenyegetést tesz felelőssé a brit választási bizottság (választásokat felügyelő szervezet) 2021–2022-es kompromittálásáért.[12] A kínai diplomaták Nagy-Britanniában és az Egyesült Államokban egyaránt alaptalannak minősítették a fenti vádakat.[13]

A brit és amerikai kormányokkal ellentétben, a kínai külpolitika általánosságban tartózkodik a nyilvános attribúció alkalmazásától. Kiberdiplomáciai ellenpólusként, Kínához hasonlóan – a nagyobb euroatlanti kiberhatalmak által ugyancsak gyakorta nevesített – Oroszország is ellenzi a nyilvános attribúció gyakorlatát, és Észak-Korea is a legritkább esetben kommentálja a vádakat. Kína szakpolitikai perspektíváját az alábbi okokra vezette vissza az SIIS *(Shanghai Institutes for International Studies)* és a CEIP *(Carnegie Endowment for International Peace)* amerikai–kínai kutatócsoportja:

1. Egyrészt az eljárás miatt fennáll a hírszerző források és módszerek kompromittálódása, amely révén a kibertámadók korábbi hibáikat javítva még nehezebben lesznek detektálhatók. Objektív bizonyítékok – önkéntes – bemutatásának hiányában pedig megkérdőjelezhető az attribúció hitelessége.
2. Külpolitikai szempontból a nyilvános attribúció diplomáciai feszültséget generál, így csökkentheti a felek rugalmasságát más bilaterális ügyek rendezésében. Alapvetően alkalmatlan politikai eszköz az elrettentésre, ám kedvezőtlenül hat a kereskedelemre és csökkenti a bizalmat az érintett piacok és gazdasági szereplők által használt infrastruktúra és előállított termékek integritásában. Ezen túlmenően fennáll az elítélt ország megtorlásának lehetősége is.
3. Belpolitikai tekintetben a gyakorlat szükségtelen mértékű fenyegetettségérzetet generálhat a társadalomban, amely egyfelől a támadók zavarkeltési és megfélemlítési célját segítheti elő, továbbá teret ad a populizmusnak és a biztonságiasításnak, ami kedvezőtlen biztonságpolitikai környezetet teremthet. Ezzel összefüggésben a társadalom olyan belpolitikai nyomást helyezhet a kormányzatra, amely erősebb megtorló intézkedéseket sürgetve eszkalálja a helyzetet. Emiatt Kína a nyilvánosságot mellőző háttérdiplomáciára helyezi a hangsúlyt az offenzív kibertéri aktivitás kezelésében.[14]

A fentiekben leírt kiberdiplomáciai helyzet hozadékaként, egyre mélyülő külpolitikai érdekellentét figyelhető meg a NATO-szövetségesek körében, aminek fő eredője a tagállamok eltérő mélységű digitális technológiai kooperációja a Kínai Népköztársasággal.[15] Különösen igaz ez Magyarország esetében is, ami a kutatási téma aktualitását adja. A hazai gazdasági és politikai elit – nem reprezentatív kutatásban részt vevő – prominens szereplői többségében üdvözlendőnek tartják a kínai tőkebefektetést és más gazdasági-technológiai együttműködési lehetőségeket.[16]A tanulmány kutatási célkitűzése, hogy áttekintést adjon a Kínai Népköztársaság kiberhírszerzési tevékenységének nemzetközi relációban megjelenő helyéről és szerepéről és stratégiai eszközrendszeréről.

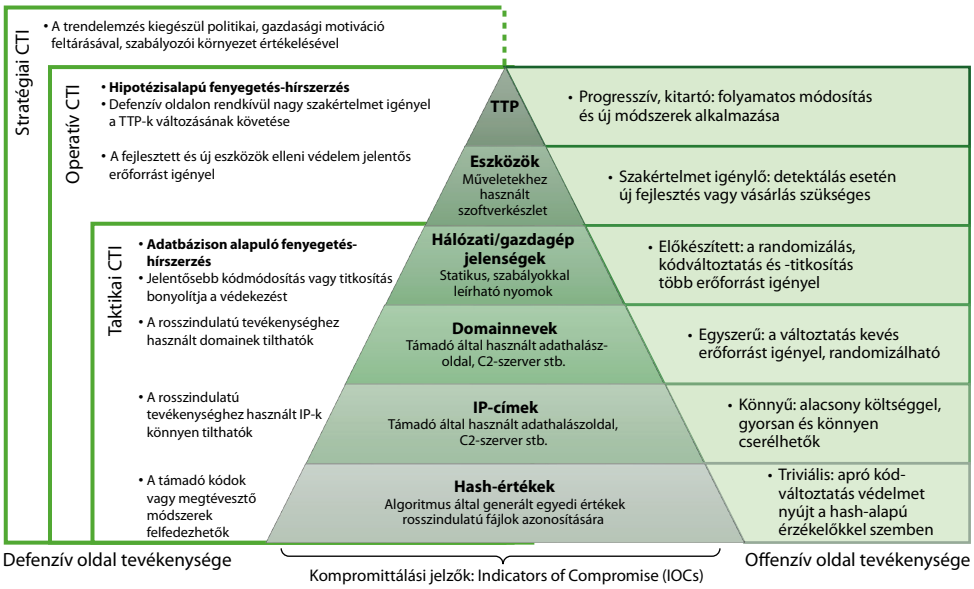
A nemzetbiztonsági tudományág egyik alapvetése, hogy minden nemzet kardinális érdeke a saját védelmét szolgáló hírszerzési információk megszerzése, valamint

12 Macaskill–Pearson 2024.
13 Pearson–Satter–Bing 2024.
14 Yang 2022.
15 Lima da Frota Araujo – Szunomár 2022.
16 Matura et al. 2022.

az ellenérdekelt hírszerzési tevékenység ellensúlyozása. A kibertér által lehetővé tett hírszerzési tevékenységet, a kiberhírszerzést (vagy CYBINT) a szakirodalom hírszerzési szakágként sorolja be, de összadatforrású tevékenységként jellemzi.[17] Ennek oka, hogy egy sikeres kiberműveletet (értsd: információszerző műveletet a kibertérben) ugyancsak megelőzhet más hírszerzési ágakba sorolt tevékenység, például HUMINT (emberi erőforrásokkal folytatott hírszerzés, a kiberbiztonsági szaknyelvben: social engineering, vagyis pszichológiai befolyásolás) vagy OSINT (nyílt forrású hírszerzés).[18] A kiberhírszerzési tevékenység feladatköre azonban kiterjed a kibertéri fenyegetettségek felderítésére is. A szakirodalom a felhasználás szintje szerint háromféle CTI-típust különít el:

1. *Strategic threat intelligence* (stratégiai szintű fenyegetettség-hírszerzés vagy -előrejelzés): A „stratégiai hírszerzés" átfogó jellegű, magas szintű áttekintést nyújt a fenyegetési környezetről *(threat landscape)* egy ország vagy gazdasági ágazat számára. Az incidensek historikus adatait és trendjeit kiegészítő kontextuális adatok, amelyek például a szabályozási környezetet, politikai vagy gazdasági motivációs hátteret jellemzik, egyaránt fontosak a stratégiai hírszerzés szempontjából. Az ilyen metodika mentén elemzett fenyegetésekre vonatkozó technikai attribútumok rávilágítanak a védelmi és detekciós képességek hiányosságai mellett a lehetséges jövőbeli stratégiai célpontokra, támadó eljárásokra.
2. *Operational threat intelligence* (operatív vagy műveleti szintű fenyegetettség-hírszerzés vagy -előrejelzés): Az operatív hírszerzés azokra a konkrét támadástípusokra vagy ágazatspecifikus fenyegetésekre összpontosít, amelyek potenciálisan veszélyt jelentenek az adott szervezetre. Kockázatorientáltan (például bekövetkezés valószínűsége, lehetséges támadási vektorok) kiemeli, hogy az incidenskezelő csapatnak hogyan javasolt priorizálnia egy adott incidenstípust vagy támadási kísérletet, és mely lépések lennének a leghatékonyabbak annak megakadályozásához vagy az informatikai rendszeren belüli terjedés korlátozásához. Az operatív fenyegetés-hírszerzés átfogóbb betekintést nyújt az offenzív aktorok képességeibe és támadásaik időzítésébe, így alkalmazva a stratégiai szintű hírszerzést egy valós élethelyzetre.
3. *Tactical threat intelligence* (taktikai szintű fenyegetettség-hírszerzés vagy -előrejelzés): A taktikai hírszerzés olyan technikai információk megszerzésére összpontosít egy incidens során, hogy támogassa a kiberbiztonsági szakembereket a védelmi intézkedések hatékonyabb koordinálásában, incidens reagálási tervek *(incident response plan)* felépítésében és a védelem rendszerének megtervezésében és konfigurálásában. Ennek értelmében a taktikai szintű fenyegetettség-előrejelzés az egyes incidensek lefolyásának (*cyber kill chain,* kiberbiztonsági modell) – akár valós időben történő – elemzése által szolgáltat információt az egyes támadó aktorok (például APT-k) által alkalmazott taktikai lépésekről, technikákról és eljárásokról (*tactics, techniques and procedures,* TTP) vagy például a támadók tevékenységének észleléséhez szükséges technikai indikátorokról, a kompromittálási jelzőkről (*indicators of compromise,* IOCs).[19]

[17] Szeleczki 2022.
[18] Dobák–Tóth 2021.
[19] Flashpoint Team 2022.



1. ábra: A kiberfenyegetettség-hírszerzés felhasználási szintjei mentén tagolt információforrások sematikus ábrája
Forrás: a szerző szerkesztése Bianco *2013 és* Berzsenyi *2023: 193 alapján*

Az 1. ábra mutatja be a David Bianco kiberbiztonsági és CTI-szakértő által megalkotott „fájdalompiramis" (*Pyramid of Pain,* PoP) nevű fenyegetésmodellt, amelyen az látható, hogy az egyes szinteken megjelenő technikák megváltoztatása mekkora nehézséget okoz a támadónak. Az offenzív tevékenység indikátor-központú skálázása a piramis teteje felé haladva vizualizálja, hogy milyen lehetőségek nyílnak ezen támadó technikák beazonosítására (adatbázison alapuló *[intel based hunting]* és hipotézis alapján *[hypothesis hunting]*), és milyen hatékonysággal csökkenthetők a támadások, amennyiben a védelmi rendszerekbe (például: SIEM, SOAR) becsatornázott riasztásokat és monitorozásból származó adatokat a specifikus IOCs-indikátorok szerint definiáljuk. A modell szemlélteti, hogy a támadó IP-címének blokkolása önmagában nem elegendő egy támadó aktor elrettentésére, azonban a támadó egyedi taktikáinak, technikáinak és eljárásainak (TTPs) célzása az IOCs-eken keresztül lényegesen akadályozhatja a kiberművelet sikeres végrehajtását, miközben az üzemeltetett védelmi megoldások naplófájljaiból a továbbiakban predikcióra (az ábrán *hypothesis hunting*) is felhasználható információ nyerhető ki. (Bianco modelljének elnevezése tehát a támadó aktor erőforrás-veszteségére utal, amely technikák és eszközök egy sikertelen támadási kísérlet esetén a védelmi rendszerek továbbfejlesztését szolgálják.)[20]

A kiberbiztonsági események és incidensek kezelését támogató CTI-rendszerek (értsd: CTI-platform-szolgáltatás) hatékony működésének alapfeltétele a becsatornázható információk minőségétől és pontosságától függ, legyenek azok akár ember, akár gép által olvashatók (adattáralapú). Emiatt a Kínához köthető APT-tevékenység elleni védekezéshez

[20] Bianco 2013.

elengedhetetlen a magán- és közszféra kooperációja az incidensek jelentésében, valamint a kiberbiztonsági szakmai közösség együttműködése a riportok egységes szempontrendszerek mentén történő publikálásában. A közös szabványok és módszertanok (például: MITRE ATT&CK-féle metodológia alkalmazása) lehetővé teszik az elemzések összehasonlítását, a védelmi megoldások hatékonyságának növelését, különösen a fals pozitív riasztások kiszűrése és a támadók felismerése tekintetében. Az új technológiák fejlődése (például AI, ML, IoT) lehetővé teszi a CTI-rendszerek hatékonyabbá tételét, ugyanakkor új kihívásokat is jelenthet a támadási felületek bővülése és az adatok mennyiségének növekedése miatt, különösen az ipari irányítási rendszerek esetén.[21]

Módszertan

A kutatás stratégiája deduktív megközelítést és kvalitatív értékelést alkalmaz, kiegészítve olyan esetpéldák feldolgozásával, amelyek jól szemléltetik az elmúlt 5–7 év során feltárt kínai kibertéri hírszerző műveletek cél- és eszközrendszerét. A kutatásnak módszertani szempontból két limitációja van. Az első, hogy a feltételezhetően állami támogatással megvalósult kiberműveleteket, így különösen az APT-k tevékenységét, az erőforrás-ráfordítás, anyagi haszonszerzés és a megszerzett információ hasznosíthatóságának arányából adódóan lehet kvalitatív módszerrel beazonosítani az esetekről készült technikai jelentések mellett, ezért a források megbízhatósága vitatható. A második, hogy az esetpéldák elemzése és a kínai kibertéri hírszerző tevékenységről nyilvánosan elérhető szakirodalom feldolgozása szekunder adatgyűjtési módszerrel valósult meg.

Az esetpéldák időtartam szerinti lehatárolását az offenzív kibereszközkészlet és -technikák folyamatos fejlődése és elavulása indokolta. Emellett a feltárt esetek napjainkra értek a nyilvános attribúciót követő, hivatalos nyomozati és bírósági szakaszba, így arányaiban több magasabb hitelességű forrás áll rendelkezésre. Az incidensek kiválasztásban további szempont volt azok kiberdiplomáciai jelentősége, ami abból a politikai célból eredeztethető, hogy az incidenst elszenvedő állam (a vizsgált esetekben az USA) nyilvánosan attributál kínai hátterű APT-*tevékenységet (public cyber attribution)* amellett, hogy a digitális nyomokat elemző *(digital forensics)* állami szervezetek vagy kiberbiztonsági vállalatok kínai hátterű tevékenységre utaló jeleket is feltártak publikált jelentésükben. Emiatt a tanulmány a kiberbiztonsági szakterület terminológiáját[22] és szempontrendszerét alkalmazza a kiberhírszerzési esetek feladatmegvalósítás-szempontú vizsgálata során.

A hadtudomány a kibertér által lehetővé tett hírszerzési tevékenységek célrendszerét a társadalmi érdekek nemzetbiztonsági artikulációja mentén vizsgálja, valamint az aktuális biztonság- és védelempolitikai helyzet, illetve külpolitikai relevanciája szerint értékeli. Kína esetében mindezen indikátorok a Kínai Kommunista Párt (KKP) ázsiai geopolitikai célkitűzéseinek változásában, a nagyhatalmi ambíciók előtérbe kerülésében és a kettős felhasználású csúcstechnológiák fejlesztési versenyének kiéleződésében mutatkoznak meg,

[21] Gyebnár 2023.

[22] A szerző szinonimaként használja az incidens kifejezést az ún. kiberbiztonsági eseményekre (értsd: sikeres kompromittáció).

ezáltal új prioritásokat behozva az ország külföldi célpontokra irányuló kibertéri információszerző tevékenységébe. A tanulmányban mindezeket áttekintő jelleggel mutatom be.

A KNK feltételezett kiberhírszerzési tevékenységének áttekintése 2003–2015 között

Az első Kínához köthető APT-csoportot a Mandiant kiberbiztonsági vállalat kutatói azonosították 2003-ban. A kutatók által feltárt Titan Rain kódnévvel ellátott műveletek során az APT1-es csoport számos amerikai kormányzati és katonai intézménybe hatolt be, illetve ezek ellátási láncába tartozó védelmi és technológiai iparágba tartozó szervezetek rendszereit kompromittálták, több terabyte-nyi érzékeny adatot zsákmányolva. A Titan Rain kampány feltárása diplomáciai feszültséget okozott az Obama- és Hszi-kormányzatok között, ám egyúttal jelentős hatást gyakorolt az amerikai szervezeti rezilienciát erősítő intézkedések bevezetésére és a nemzetközi kiberbiztonsági együttműködések növelésére. Az Egyesült Államok csatlakozott a Nemzetközi Kibervédelmi Ügynökséghez (*International Cyber Security Protection Alliance,* ICSPA),[23] és megosztotta a Titan Rain kampányról szerzett technikai információkat más országokkal. A kínai ipari kémkedés és hírszerzés akkori volumenét és az ellene fellépő nemzetközi kooperáció kiterjedtségét jól szemlélteti, hogy 2006–2007 között az Egyesült Királyság, Németország és Új-Zéland kormányai közösen hozták nyilvánosságra számos Kínához köthető kiberművelet technikai részleteit.[24] A Kínához köthető kiberhírszerzési tevékenység újabb mérföldkövének tekinthető a 2010-es Aurora kódnevű támadás, amely a Google forráskódjának megszerzése érdekében több különböző egyesült államokbeli vállalat rendszereibe is bejutott. Emellett említésre méltó a McAfee kiberbiztonsági szolgáltató 2011-ben publikált elemzése, amelyben a kutatók által Shady RAT kampánynak elnevezett behatolásokról 5 évre visszamenően tártak fel Kínához köthető APT-tevékenységet. Az incidensjelentésben az USA kormányzati szervei, magáncégek, valamint olyan nemzetközi szervezetek kompromittálódását hozták nyilvánosságra, mint az ENSZ és a Nemzetközi Olimpiai Bizottság.[25]

Inkster, továbbá Lindsay és Cheung is kiemelik kutatásaikban, hogy a haditechnikai eszközök mérnöki visszafejtése révén szerzett információ sokkal könnyebben adaptálható a védelmi ipari gyártásban és kutatásban, mint a digitálisan megszerezhető információk, amelyek például kutatási részadatként vagy gyártási „jó gyakorlatként" hasznosíthatók a releváns szakértelem hiányában. Emellett a haderő- és támogató infrastruktúra modernizációjában a kettős felhasználású technológiák vagy egyéb modern technikák terén a kutatási és technológiatranszfer-hálózatok legális és illegális felhasználása arányaiban sokkal számottevőbb a kiberműveletekhez képest (például Kína japán gyorsvasútterveken alapuló vasúthálózat-fejlesztése.

[23] A brit kezdeményezésre létrejött ICSPA a kiberbűnözés elleni nemzetközi fellépést segíti, valamint az ipari és kormányzati információmegosztásokon alapuló együttműködés keretét biztosítja.
[24] Lindsay–Cheung 2015: 58.
[25] Lindsay–Cheung 2015: 59–60.

1. táblázat: Kínai fegyverrendszerek külföldi technológiai függősége (Chinese Weapons System Dependence on Foreign Technology)

Platform (Platform)	**Sector** (Haderő-nem)	**Country of origin** (A technológia származási országa)	**Foreign content** (Az alkalmazott külhoni technológia aránya és kritikussága)	**Illicitly obtained material** (Jogellenesen megszerzett technológia és komponensek)
J-11B	Légierő	Oroszország	5 – Magas	Igen: Su-27SK mérnöki visszafejtése (reverse engineering)
J-16	Légierő	Oroszország	5 – Magas	Igen: Su-30MK2 mérnöki visszafejtése (reverse engineering)
J-15	Légierő	Oroszország	5 – Magas	Igen: Su-33 mérnöki visszafejtése (reverse engineering)
Donghai-10 LACM	Űrerők	Oroszország, Ukrajna, USA, Németország, Franciaország	5 – Magas	Igen: rakétatechnológia mérnöki visszafejtése (reverse engineering)
LuyangII romboló, 052C típus	Hadi-tengerészet	Oroszország, Ukrajna, USA	2 – Alacsony-közepes	Igen: német motortechnológia
Changzheng hordozórakéta	Űrerők	USA, Oroszország	1 – Alacsony	Igen: USA motortechnológia

Forrás: Lindsay–Cheung 2015 alapján kivonat és magyar fordítás

A kutatók ezen érvelését támasztja alá az 1. táblázat (Lindsay és Cheung adatgyűjtésének kivonata), amely a haditechnikai és védelmi ipari célpontokra irányuló kiberhírszerzési műveletek (beleértve az APT-tevékenységet is) haderőfejlesztésben való szerepét helyezi kontextusba azáltal, hogy öt fokozatú „magas–alacsony" skálán értékeli a kínai haderő egyes fegyverrendszereinek feltételezhető kitettségét a „külhoni" technológiáknak. A kutatók által vizsgált adatsor kivonata a 2015-ig hadrendbe állított eszközpark azon fegyverrendszereit jeleníti meg, amelyek technológiája vagy egyes komponensei tekintetében illegális információszerzés merült fel (és az incidens ténye nyílt forrásként elérhető).[26] A haditechnika megszerzésére irányuló tevékenység egyik leghírhedtebb esetpéldáját egy 2009 áprilisában kiadott jelentés tárta fel, amelyben a kínai hátterű APT-csoport 2007–2008 között hozzáfért az F-35-ös vadászgép titkosítatlan tervezési adataihoz, a Lockheed Martin, a Northrop-Grumman és a BAE technológiai konzultációinak és értekezleteinek megfigyelésével. Érdekesség, hogy ezen adatlopás miatt a kínai hatóságok vállalták a felelősséget. A katonai célpontokat érintő kiberhírszerzési műveletek másik kiemelkedő esetpéldája az „RSA-incidens", ami ugyancsak a beszállítói láncot kompromittálta. A Nemzetbiztonsági Ügynökség (NSA) kiber szakágazatát irányító Keith Alexander tábornok 2013-ban tett jelentést az úgynevezett RSA biztonsági rendszer[27]

[26] Lindsay–Cheung 2015: 59–60 és Inkster 2015.

[27] Ezt a rendszert használják azok a cégek, amelyek a Pentagon minősített dokumentumaival dolgoznak.

SecureID tokenjeinek 2012-es kompromittálódásáról. Az esetet az amerikai hatóságok és kormányzat egy 2011-ig visszanyúló behatolás visszafejtésével kínai aktorokhoz attribuálta. Keith tábornok megerősítette, hogy a beszállítói láncot érő adatlopási incidens (supply chain attack) tette lehetővé 2011 májusában (két hónappal az RSA kompromittálódását követően) a Lockheed Martin rendszereinek feltörését.[28]

A Kínához köthető állam alatti hackercsoportok tevékenységének felderítésében 2013 jelentett újabb fordulópontot. Ekkor a Mandiant kiberbiztonsági szolgáltató publikálta egy Sanghajba telepített PLA-egység (UNIT 61398) lokációját, amelyet az amerikai hatóságok 2006-ig visszamenően több angol nyelvterületen elkövetett adatlopásért és hálózati behatolásért tettek felelőssé. Habár az épületet rövidesen kiürítették, az esetet követően magas szintű egyeztetések és kiberdiplomáciai kapcsolatfelvétel indult az USA és Kína között, aminek keretében elnöki találkozó (Obama és Hszi elnökök) volt, illetve felállítottak egy kiberbiztonsági munkacsoportot a USA–Kína Stratégiai és Gazdasági Dialógus *(U.S.–China Strategic and Economic Dialogue)* gondozásában.[29] A Washington–Peking bizalomépítési kezdeményezéseket vizsgáló Inkster elemzésében a Snowden-botrány kirobbanására vezeti vissza ezen kiberbiztonsági kezdeményezés megrekedését. A kutatás alapján az eset beigazolta a kínai fél fenyegetéspercepcióját, és egyúttal betekintést engedett a Five Eyes együttműködés mélységébe és kiterjedtségébe, megerősítve a kínai felet abban, hogy az USA technológiai fölényével visszaélve épít ki hegemóniát a kibertérben, miközben diplomáciai szempontból kettős mércét alkalmaz és helyez nyomást a pekingi vezetésre.[30]

A fentiekben is bemutatott incidensekből visszafejthető adatok alapján az amerikai és más nemzetek kormányzati szervei (például CSIRT, GovCert-ek) és kiberbiztonsági magáncégek[31] számos különböző cél- és eszközrendszerrel rendelkező kínai hátterű hackercsoport tevékenységét különítették el, amelyek közül napjainkra megközelítőleg 120–130 önálló tevékenységet (kampányt vagy incidenst) tartanak nyilván APT-fenyegetésként.[32] A legjelentősebb APT-csoportok közül számos esetben megfigyelhető volt a hírszerzési célú tevékenység,[33] amelyekre az alábbi lista mutat be tipizálható jellemzőket:

1. Az APT1 csoport (más néven *Comment Crew*) tevékenysége elsősorban katonai és politikai célpontokat érintett, többek között az USA, Japán és India kormányzati szerveit is célba vették. Az APT1 tevékenységét a Mandiant hozta

28 Greenberg 2021.
29 USA White House 2015.
30 Inkster 2015: 42–47.
31 Például FireEye, Kaspersky, Mandiant, McAfee, MITRE, CrowdStrike.
32 Electronic Transactions Development Agency 2022a és Malpedia adatbázisa, lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/apt1
33 Említésre méltó, hogy az APT10 csoport (más néven Codoso) célpontjai a védelemi, a telekommunikációs és a légi közlekedési szektorba tartoznak. Az APT17 csoport (más néven DeputyDog) tevékenysége főként az Egyesült Államok és Dél-Korea kormányzati szerveit, valamint az amerikai hadsereget célozta meg. Az APT19 csoport (más néven Deep Panda) tevékenysége elsősorban a védelmi iparba és az energiaszektorba sorolható vállalatokat érintette, továbbá a gyógyszeripar szereplőit. Az APT27 csoport (más néven Emissary Panda) az ázsiai régióra összpontosított, fő célja katonai és politikai információk megszerzése volt a kormányszervek, a régió államainak nemzetbiztonsági szervei, valamint a védelmi ipari és telekommunikációs szolgáltatók kompromittálásával. Electronic Transactions Development Agency 2022a és 2022b.

összefüggésbe a Népi Felszabadító Hadsereg vezérkari hivatala (*General Staff Department*, GSD) 3. osztályának 61398-as[34] egységével.[35]

2. Az APT30 csoport (más néven *Elise*) tevékenysége legalább 2005 óta érinti az ASEAN-tagállamokat, aktivitását Tajvan, Malajzia, a Fülöp-szigetek, Vietnám és Kína területén is detektálták, utóbbi esetben kiberbűnözői csoportként. A Mandiant által gyűjtött CTI-információk alapján feltételezhető, hogy az APT30 tagjai felváltva dolgozhatnak egy kollaboratív környezetben, és koherens fejlesztői terv mentén módosítják és adaptálják az általuk használt malware-ek (SHIPSHAPE, SPACESHIP, FLASHFLOOD) forráskódját. A csoport fő célpontjai közt kormányzati szerveket, nemzetbiztonsági szerveket, védelmi ipari vállalatokat, tudományos kutatóintézeteket és energiaipari vállalatokat tartanak számon.[36] Érdekesség, hogy az APT30 tevékenységét átfedésbe helyezik a Naikon néven számontartott, fejlett perzisztens fenyegetéssel, amely aktort a rendelkezésre álló nyílt információk alapján ugyancsak kínai hátterű entitásként tartják számon, és a hadsereg 78020-as számú egységéhez kötik. Berzsenyi értekezésében így jellemzi a Naikon mandátumát: „vélhetően kiterjed a regionális számítógépes hálózati műveletekre, rádiójelfelderítésre és politikai elemzésre a Délkelet-Ázsiával határos nemzetek kapcsán, azon belül is azokra, amelyek az energiahordozókban gazdag Dél-kínai-tenger területi vitáiban érintettek."[37]
3. Az APT31 csoport hírszerző tevékenységéhez olyan applikációkban található sebezhetőségeket használt ki, mint például a Java és az Adobe Flash. A Mandiant adatbázisa alapján az APT31 kormányzati és nemzetközi pénzügyi intézményeket, űrkutatási és védelmi szervezeteket, valamint csúcstechnológiai, építőipari és mérnöki vállalatokat, távközlési, továbbá médiaipari és biztosítási szolgáltatókat is kompromittált. A célpontok ezen széles skálája alapján feltehető, hogy a hírszerzési tevékenység célja, hogy rövid és középtávon hasznosítható információt szerezzenek politikai, gazdasági és katonai előnyök megszerzéséhez.[38]
4. Az APT40 csoport jellemzően az Övezet és Út kezdeményezés *(Belt and Road Initiative)* szempontjából stratégiailag fontos országokat veszi célba. A csoport kampányai elsősorban olyan globális szervezetekre fókuszálnak, amelyek a védelmi ipari vagy mérnöki vertikumban tevékenykednek. Emellett a Mandiant adatai alapján legalább 2013-tól kezdve egyre jelentősebb mértékben érintettek vegyipari, kutató- és oktatási intézmények, kormányzati és technológiai szervezetek is, valamint hajózási és légi közlekedési célpontok. Állam alatti kiberegységként értelmezve az APT40 tevékenységét a stratégiai cél az lehet, hogy a megszerzett

---

34 A kínai haderőben számok jelölik az egységeket (military unit cover designator, MUCD). Lásd Berzsenyi 2023: 94.

35 Electronic Transactions Development Agency 2021.

36 Mandiant 2021. Advanced Persistent Threat (APT) groups & threat actors. APT31. (Bővebben lásd: www.mandiant.com/resources/insights/apt-groups) és Malpedia adatbázisa: Fkie, F. [n.d.]. APT30 [Threat Actor], bővebben lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/apt30), Electronic Transactions Development Agency 2022a és 2022b.

37 Berzsenyi 2023: 94 és Malpedia adatbázisa: Fkie, F. [n.d.]. Naikon (Threat Actor), bővebben lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/naikon

38 Malpedia adatbázisa: Fkie, F. [n.d.]. APT31 (Threat Actor), bővebben lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/apt31

információ által Kína előnyösebb pozíciót szerezzen meg a globális tengeri kereskedelemben, és megkönnyítse a katonai és polgári célra is alkalmazható kikötők létesítését. Emellett a csoport műveletei a kínai haditengerészeti erők eszközparkjának modernizálására is irányulhatnak, vagy a polgári célú hajózást fejlesztő projektek technológiájának megszerzésére (járművek és felszerelés).[39]

5. Az APT41 kettős műveleti célrendszerben működő, kémkedésre és finanszírozásra összpontosító csoportként olyan iparágakat vesz célba, mint a szerencsejáték, az egészségügy, a csúcstechnológia, a felsőoktatás, a távközlés és az utazási szolgáltatások.[40] Az APT41 gyorsan alkalmazkodik a célpontok IT-környezetében bekövetkező változásokhoz és észlelésekhez, és gyakran az incidensre reagáló személyek tevékenységét követően néhány órán belül újrakompilálja (gépi nyelvre történő módosítás) a rosszindulatú programokat. Több alkalommal észlelték, hogy az APT41 a közelmúltban nyilvánosságra hozott sebezhetőségeket is felhasználta, gyakran napokon belül létrehozta a specifikus sérülékenységet kihasználó támadó programokat *(weaponizing)* és alkalmazta a kártevőket *(exploiting)*.[41]

A fejezetben ismertetett incidensek historikus adatai alapján megállapítható, hogy a kínai kiberműveletek fő célpontjai 2015-ig a védelmi ipar, a mérnöki és csúcstechnológiai kutatásokat végző piaci és állami szféra vertikumába tartoztak. Emögött feltehetően olyan stratégiai célok húzódhattak meg, mint a haderő transzformációja és az eszközpark modernizációja, különösen a haditengerészeti, stratégiai támogató erők (kiberképességek idesorolandók), űrerők és légierő képességfejlesztése miatt. A vizsgált időszakban, a külpolitikai célok megvalósítását támogató kiberhírszerzési kampányok olyan nemzetközi szervezeteket érintettek (például: ASEAN és részes államok), amelyek a pekingi vezetés akkori geopolitikai célkitűzéseinek érdekszférájába estek bele. Ilyen cél volt például Kína regionális nagyhatalmi pozíciójának globális hatalmi státuszba emelése, a dél-kínai-tengeri kereskedelem (és útvonalak) feletti kontroll bővítése által és erőkivetítési képesség növelésével. Továbbá az ország napjainkra elért kiberhatalmi státuszát megalapozó csúcstechnológiai ipar gyártó- és tervezőkapacitásának kiépítését támogató információk megszerzése (akár legális és illegális eszközökkel), illetve az IKT-technológiákat érintő tudásmenedzsment-hálózatok létrehozása.

A KNK kiberhírszerzési képességei a nemzetközi színtéren: feladatrendszer és támogató infrastruktúra elemzése

A kiberhírszerzési feladatokat végrehajtó szervezeti háttér feltérképezésében kiemelten fontos a kínai katonai és polgári szolgálatok tevékenységi körének behatárolása, a magánszférában meglévő képességek integrálhatóságának, az együttműködési területeknek

[39] Plan et al. 2024.
[40] MITRE Corporation [n.d.] Groups. és Mandiant [n.d.]. APT41 Chinese Cyber Threat Group 04. 29. Bővebben lásd: www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation
[41] Pennino–Bromiley 2022.

célirányos vizsgálata. Kína esetében mindezeket az ország külpolitikai célkitűzéseinek és a nemzetközi közösségben képviselt álláspontjának tükrében szükséges értelmezni.

A KNK kiberbiztonsági környezete: a hatalmi játszma a digitális világban

A legtöbb kiberbiztonsági trendkutatás hangsúlyozza, hogy globális viszonylatban a feltételezhetően Kína támogatását élvező aktorok egyre növekvő számú és szofisztikáltságú kiberműveletben érintettek, amelyek közt adatlopási kampányok, és újabban, noha nem számottevő arányban, a kritikus infrastruktúrák elleni támadások is fellelhetők. Ennek jelentősége, hogy a Kínához köthető APT-csoportok képességfejlődése lehetővé teszi, hogy a tevékenységük során kinyert információ mennyiségét és minőségét tekintve egyre komplexebb nemzetbiztonsági célokat szolgáljon ki. Továbbá az ipari kémkedés és technológiatranszfer-hálózatok jogszerűtlen kihasználása mellett – a fejlesztésre fordítandó költségek és humántőke-befektetés kihagyásával – piaci versenyelőnyhöz juttathatják a kínai vállalatokat, vagy hozzáférést biztosíthatnak katonai és kettős felhasználású technológiákhoz. Mindezek mellett, a kínai külügy képviselői évek óta sikeresen közvetítik a KKP azon álláspontját, miszerint az ország sokkal inkább tekinthető a kibertérből érkező fenyegetések áldozatának, semmint kiváltó szereplőjének. Az alábbiakban részletezett körülmények kontextusba helyezik Kína kiberbiztonsági környezetét és infrastruktúráját, feltárva annak okát, hogy mi teszi Kínát kelet-ázsiai viszonylatban az első számú, leggyakrabban támadott célponttá, és miként reprezentálható a világviszonylatban is kimagasló, kiberbűnözői tevékenységre visszavezethető anyagi károkat elszenvedő országként.[42]

A Kínai Népköztársaság kiterjedt digitális piaca és elektronikus államigazgatási ökoszisztémája széles támadási felületet eredményez, ezenfelül kritikus hálózati rendszere számos külföldi (főként az ország számára kihívást jelentő amerikai és vele szövetséges országok gyártóihoz köthető) kibervédelmi és egyéb technológiai megoldástól függ. További kihívásokat generál, hogy Kína kiberbiztonsági szabályozói környezete továbbra is elmaradottnak tekinthető az Európai Unió és az Egyesült Államok szabályozási rendszereihez képest. A pekingi vezetés ezen kockázatok kezelését prioritásként jelölte meg a 2019-es védelmi fehér könyvben, és folyamatosan támogatja a hazai digitális ipart és a védelmi megoldások fejlesztését.[43] Azonban a 2019–2021 között kiadott jogi normák ellenére is, az ország digitális infrastruktúrájának védelmét célzó jogi szabályozói környezet és adatvédelmi normarendszer még nem átfogó jellegű,[44] így teret ad a Kínai Kommunista Párt és a hazai technológiai óriásvállalatok közti konfliktusnak, ami az utóbbiak adatvesztési botrányai, valamint az adatgyűjtés és -felhasználás mértéke miatt szélesedett ki az elmúlt két-három évben.[45]

A kínai K+F+I-szektor módszeres állami támogatása az 5G, mesterséges intelligencia és kvantumszámítási technológia tekintetében ugyancsak piaci, nemzetbiztonsági és katonai megrendelők igényeit is kielégíti. Mindemellett Peking még nem tudott domináns státuszt elérni az ázsiai régióban (a pekingi külügy olvasatában biztonságot nyújtó

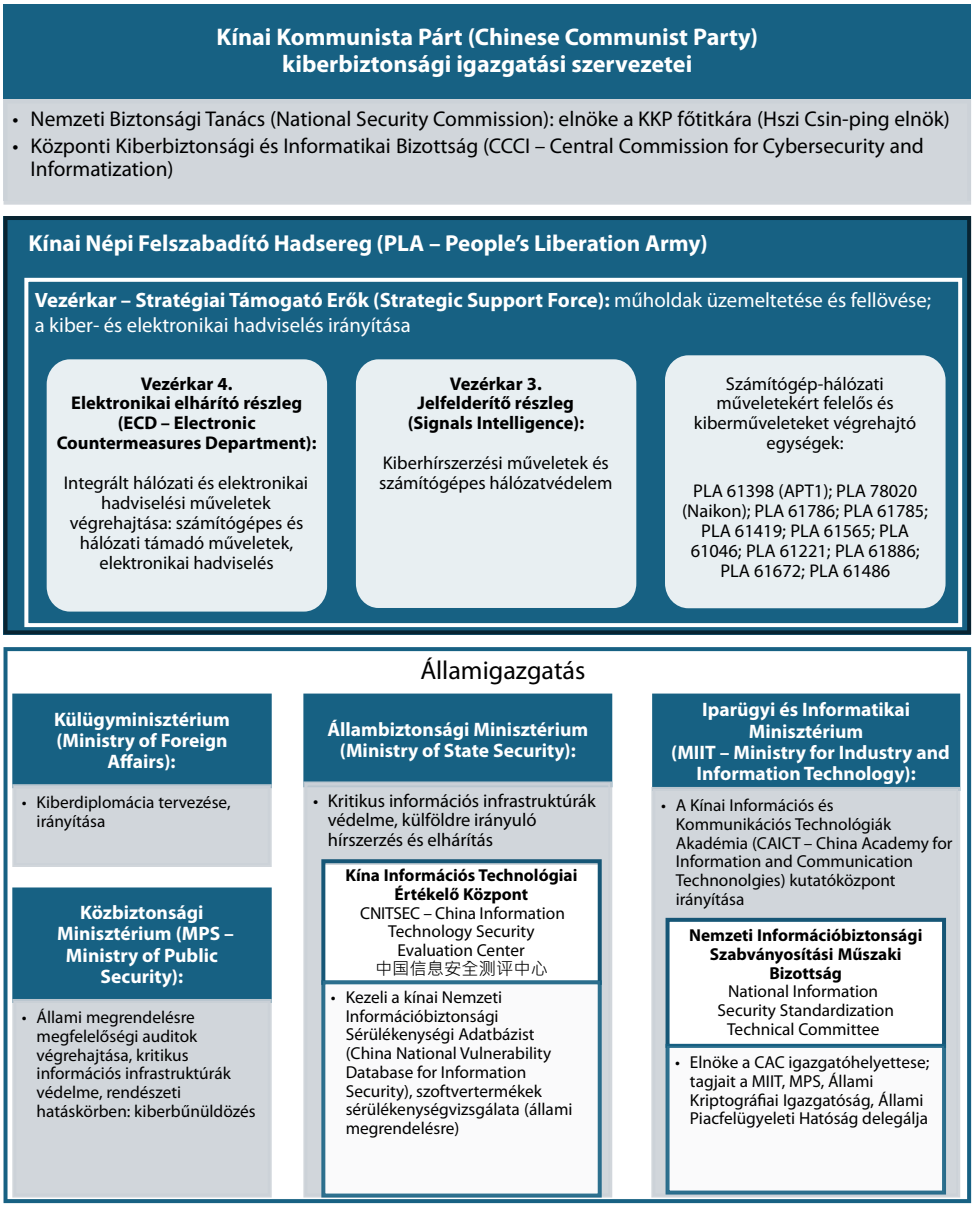
42 Lusthaus–Bruce–Phair 2020.
43 Segal 2020.
44 Kaszián 2021.
45 Mészáros 2021.

képességi szintet) az USA és szövetségesei kibertéri műveleti képességei és kiberbiztonsági technológiai iparával szemben. Egy ázsiai regionális konfliktus korai szakaszában az információs fölény megszerzése érdekében Peking képes lenne arra, hogy zavaró vagy pusztító célú kiberműveleteket indítson, különösen ellenfele parancsirányítási rendszerei, műholdas és kommunikációs hálózata ellen, amennyiben a katonai és a polgári hírszerzés vagy APT-csoportok tevékenysége révén megfelelően fel tud készülni.[46] A kínai katonai gondolkodásban egy olyan kibertéri művelet, amely hosszan tartó, jelentős zavarokat képes okozni a banki és telekommunikációs rendszerekben, stratégiai elrettentő hatással bírhat, mivel ezen szektoroktól való függőségük miatt képes lehet gátolni az USA vagy ázsiai regionális partnereinek beavatkozását egy fegyveres konfliktusba. A politikai és katonai vezetés azonban valószínűleg túl nagy kockázatnak tartja, hogy Kína legalább ugyanennyire sebezhető és kitett a fentiekhez hasonló megtorló vagy ellentámadásoknak, így konfliktus esetén katonai célpontok ellen indított műveletek vagy kiberfegyver alkalmazására kevesebb esélyt látnak a szakértők a kínai hálózati felderítés hatékonyságától függetlenül. Ezen ellentámadások miatti dilemma fenntartását célozza kibervédelmi fejlesztéseiben a kelet-ázsiai régió számos olyan állama – köztük Tajvan, Japán, Dél-Korea és Vietnám –, amelyek biztonságpolitikájában megjelenik a kínai kibertéri fenyegetettségpercepció. Az offenzív képességek növekedésével párhuzamosan várhatóan a következő években is jellemző lesz a kínai digitális piac terjeszkedése és a kritikus hálózatok sebezhetősége, amit a KKP fejlesztési támogatásokkal, valamint intézményesítési és szabályozási tevékenységgel igyekszik javítani. Az erősségek és gyengeségek ezen kombinációja azt eredményezi, hogy Kína elsősorban kiberkémkedési és dezinformációs kampányok általi fenyegetést jelent az ázsiai csendes-óceáni térségre.[47]

A kiberhírszerzési tevékenységet és információfeldolgozást támogató intézményi háttér

A Kínai Népköztársaság számos szervezete játszik fontos szerepet az ország digitális irányítási ökoszisztémájában. A 2. ábra szemlélteti azon államigazgatási szervezeteket, köztük a Népi Felszabadító Hadsereget (PLA), amelyek hatásköre kiterjed a digitális kormányzás valamely szegmensére (minisztériumok és háttérszerveik), vagy állami és pártfunkciójukon keresztül a kiberteret érintő igazgatási és szakpolitikai felelősségük van, ezáltal koordinálhatják a kiberhírszerzési feladatokat vagy az információk felhasználását. Kiemelendő, hogy valamennyi szervezet döntéshozatali struktúrájának a legfelsőbb szintjén a közvetlen elnöki hatalom és felügyelet jelenik meg. Sok más államhoz hasonlóan Kína esetében sem lehet egyértelműen szétválasztani a kiberhírszerzési és az elhárítási funkciókat, amelyek integráltan működnek az Állambiztonsági Minisztérium *(Ministry of Public Security)* szervezetében. Emiatt a felelősségiterület- és feladatkör-alapú szétválasztás mentén sorolták fel a külföldre irányuló hírszerzést végző szervezeteket. Az Állambiztonsági Minisztériumban két iroda végzi a külföldre irányuló hírszerzést: az első iroda felelősségébe tartozik a külföldre utazó diákok, akadémikusok és üzletemberek által megszerezhető technológiai

[46] Smith 2022.
[47] Segal 2020.



2. ábra: A Kínai Népköztársaság digitális és kibertéri igazgatásának legfontosabb intézményi szereplői
Forrás: a szerző szerkesztése Lee *2022 alapján*

és tudástranszfer, míg a második iroda a külföldi tartózkodási engedéllyel rendelkező állampolgárok által megvalósítható hírszerzést koordinálja. A kiberműveleti képességek a kínai haderőn belül a stratégiai támogató erők alá tartoznak. A katonai hírszerzési ágazat a PLA vezérkarán *(General Staff)* belül működik: a második részleg (2/PLA) koordinálja a védelmi attasék tevékenységét a nyilvános adatok megszerzése tekintetében, míg a harmadik úgynevezett Jelfelderítő részleg (3/PLA) felelős a SIGINT-tevékenységért, továbbá a számítógépes hálózatvédelemért és a kiberkémkedési tevékenység koordinálásáért. A negyedik úgynevezett Elektronikai elhárító részleg (4/PLA) hatáskörébe tartoznak a számítógépes és hálózati támadó műveletek. (A vezérkar negyedik részlegének offenzív kiberműveleti tevékenységét a kínai műveletszervezés integráltan kezeli az elektronikai hadviseléssel és Integrált Hálózati és Elektronikai Hadviselés [*Integrated Network Electronic Warfare,* INEW] tevékenységnek nevezi).[48]

Az információfeldolgozó és értékelő szervezetek közül két, közvetlenül a KKP-hoz köthető államigazgatási intézmény és egy közigazgatási testület emelhető ki. Az elmúlt évek politikai hatalomkoncentrációjának eredményeképpen a legszélesebb feladat- és hatáskört a Kibertér-igazgatási Hivatal (*Cyberspace Administration of China,* CAC) vonta magához, így Kína legfontosabb kiberbiztonsági hatósága, amely felelős az internetes tartalmak felügyeletéért és DNS-alapú szabályozásáért, a Kritikus Információs Infrastruktúrák (CII) felügyeletéért, valamint a kínai személyes adatok védelméről szóló törvény (*Personal Information Protection Law,* PIPL) gyakorlati implementációjáért, így szabályozói és felügyeleti hatásköre a piaci szereplőkre is kiterjed. A CAC helyettes igazgatójának irányítása alatt áll Kína szabványügyi és kriptográfiai kontrollszervezete, a Nemzeti Információbiztonsági Szabványosítási Műszaki Bizottság (*National Information Security Standardization Technical Committee,* más néven TC260). A CAC tevékenységét a Központi Kiberbiztonsági és Informatikai Bizottság (*Central Commission for Cybersecurity and Informatization,* CCCI) koordinálja, amelyet a kínai kormány 2014-ben hozott létre. A CCCI feladata a kiberbiztonsági stratégia kidolgozása, a kibertér-irányítás és a kínai kiberbiztonsági politika koordinálása, valamint a különböző kiberbiztonsági problémák kezelése. A CCCI vezetője az ország miniszterelnöke, és tagjai között szerepelnek a kínai legfőbb kormányzati szervek vezetői, a vezérkari főnök és más magas rangú tisztségviselők. A szervezet egyéb hatáskörei közé tartozik a kiberbiztonsági törvények és előírások kidolgozása, valamint a kínai kibertér fejlesztésével és védelmével kapcsolatos nemzetközi együttműködés koordinálása.[49]

A KNK feltételezett kiberhírszerzési műveleteinek áttekintése 2015-től napjainkig

Az elmúlt években több jelentős, kritikusinfrastruktúra-elemeket célzó esetet is feltártak, amelyeket az USA igazságszolgáltatási szervei vagy a megbízott kiberbiztonsági magáncégek a Kínai Népköztársasághoz köthető APT-csoportokhoz kapcsoltak. Fontos

[48] Campbell 2021 és Berzsenyi 2023: 92–96.
[49] Lee 2022.

azonban megjegyezni, hogy az ilyen szofisztikáltságú támadások során használt rosszindulatú programok (malware-ek) vagy ezek kódrészleteinek kinyerése esetén is nehéz bizonyítani, hogy melyik konkrét ország vagy APT-csoport felelőssége feltételezhető. A kiberbűnözők és állami aktorok egyaránt törekszenek nyomaik elrejtésére (például saját kódjának törlésére programozott malware-rel) és meghamisítására, például más kiberbűnözői csoportoktól vagy etikus hackerektől, vállalatoktól megszerzett támadó eszközök használatával. A bemutatott esetpéldák hasonló célpont- és eszközrendszere átfogó jellegű, kínai kiberhírszerzési APT-kampányra utalnak.[50]

A kampány egyik eleme a 2015-ben feltárt Anthem-adatlopási incidens, amelyet az amerikai egészségügyi iparágban bekövetkezett egyik legjelentősebb volumenű támadásként jegyeznek. A Deep Panda nevű APT-csoport 2014 decemberében mintegy 78,8 millió személy érzékeny adatait[51] szerezte meg az Anthem Inc. háttéradatbázisaiból, az Egyesült Államok egyik legnagyobb egészségbiztosító vállalatától. A belépési pont egy célzott adathalász-támadás volt, míg az incidens támadási vektora a Derusbi malware nevű kártékony szoftveren alapult, amelynek segítségével a támadók laterálisan (oldalirányban) mozogtak az Anthem hálózatán belül, és végül több mint 50 munkavállalói fiókhoz és 90 különböző rendszerhez jutottak hozzá. Az Anthem-adatlopás becslések szerint 260 millió dolláros kárt okozott a vállalatnak, amely összeg magában foglalta a rekordmértékű HIPAA-büntetést (16 millió USD)[52] és több száz millió dolláros jogi költségeket (például a 15 millió dolláros csoportos peres megállapodás), továbbá az ügyfelek tájékoztatására elkülönített kommunikációs költségeket, valamint a remediációs és helyreállítási intézkedések anyagi erőforrásait és a kiberbiztonsági szakértői díjazást.[53] Kérdéses, hogy a támadás politikai vagy gazdasági okokból történt-e, mindazonáltal további nemzetbiztonsági kockázatokat jelent, hogy a zsákmányolt adatok továbbértékesíthetők és felhasználhatók, például az érintettek célzott megfigyelésére, hamisított dokumentumok készítéséhez vagy más támadások kivitelezésére (például célzott adathalász-támadásra való felkészülés, megszemélyesítés).

Egyértelműbb kiberhírszerzési célpont volt az amerikai kormányzati szervek emberierőforrás-menedzsmentjével foglalkozó Személyzeti Menedzsment Hivatalát (Office of Personnel Management, OPM) ért támadás. Az adatlopás 2015. júniusi felfedezéséig mintegy 22 millió felhasználó személyes adatait szerezték meg olyan háttéradatbázisokból, amelyeken ujjlenyomatokat és olyan kitöltött űrlapokat tároltak, amelyek a kormányzati biztonsági engedélyekhez szükséges háttérvizsgálatok során gyűjtött személyes információkat tartalmaztak. Az incidensről kiadott hivatalos kongresszusi jelentésben a támadás idővonalát és a támadók tevékenységét csak részben sikerült visszafejteni, többek közt a behatolási pont sem volt egyértelműen beazonosítható, ám kiderült, hogy akár több különböző támadó aktor is jelen lehetett eltérő időpontban. Először 2013 novemberében törték fel az OPM egyes rendszereit, ekkor üzemeltetési kézikönyveket és a rendszer-architektúra

50 Krebs 2015.

51 Például nevek, születési adatok, társadalombiztosítási számok, egészségügyi ellátási azonosítószámok, kapcsolattartási adatok (pl. e-mail- és lakcím) és jövedelmi adatok. A támadók azonban nem fértek hozzá egészségügyi leletek adataihoz vagy fizetési és bankkártyaadatokhoz.

52 Az USA Egészségbiztosítási Portabilitási és Felelősségi Törvénye *(Health Insurance Portability and Accountability Act).*

53 Young 2021.

feltérképezéséhez felhasználható információkat szereztek meg. Egy hónappal később kísérelték meg az USIS és a KeyPoint feltörését, amelyek a kormányzati háttérellenőrzést és átvilágítást végző alvállalkozókként aktív hozzáféréssel rendelkeztek az OPM személyes adatokat tartalmazó szervereihez. A kongresszusi jelentés kiemeli, hogy az OPM IT-biztonsági személyzete azért nem tett lépéseket a támadók kizárására – amikor 2014 márciusában észlelték jelenlétüket egy olyan hálózatban, amely nem tartalmazott érzékeny adatokat –, mert így ellenhírszerzést végezve feltérképezhették egy potenciális APT-aktor tevékenységét. Az OPM szakemberei végül 2014 májusában kényszerítettek ki egy rendszerátállítást, amely végleg kizárta volna a támadókat, akik elkezdtek keyloggereket telepíteni a személyzeti adatbázisok adminisztrátorainak munkaállomásaira. Az OPM adatvesztését végül a beszállítói láncuk sérülékenysége okozta. Ugyanis még a rendszerátállítást megelőzően, feltehetőleg egy másik támadó aktor, észrevétlenül hitelesítő adatokat szerzett meg a KeyPoint vállalattól.

Ezeket felhasználva a korábbiaktól eltérő belépési pontot létesítettek az OPM rendszerében, és valósnak tűnő hozzáférési jogosultságot szereztek, amelyet a rendszerfrissítés érintetlenül hagyott. Így a támadók képessé váltak egy olyan malware telepítésére, amely a rendszerfrissítés ellenére hátsó kaput nyitott *(backdoor)*. 2014 nyarán ezen az útvonalon keresztül exfiltrálták a kormányzati háttérellenőrzések eredményeit tartalmazó adatbázisokat. A kongresszusi jelentésben nem tárták fel, hogy az első és második kiberművelet elkövetője ugyanaz az aktor lehetett-e, ám feltételezhető, hogy kooperáltak a rendszer-architektúrára vonatkozó és az üzemeltetési kézikönyvekből kinyerhető információk felhasználásával. 2014 októberére a támadók privilegizált AD-jogosultság-eszkaláció révén *(Active Directory privilege escalation)* telepítették a távoli irányítást *(remote control)* biztosító Sakula malware-t, illetve egy PlugX malware-változatot, amely távoli hozzáférést *(remote access)* biztosított, és lehetővé tette az OPM rendszereiben való navigálást, adatok tömörítését és kiszivárogtatását. Átjutva az OPM környezetén feltörték az amerikai belügyminisztérium egyik szerverét, így az év végére újabb adatokat loptak el a kormányzat személyzeti nyilvántartásaiból, majd 2015 márciusában exfiltrálták az ujjlenyomatokat tartalmazó adatbázisokat. Az OPM biztonsági szakemberei 2015 áprilisában, a titkosított SSL-forgalom ellenőrzésének alkalmával tárták fel jelenlétüket a rendszereikben a gyanús adatforgalom alapján. Az incidens nyilvános attribúciója 2018-ban volt, amikor az NSA képviselője a KNK-t nevezte meg a támadás felelőseként. Konkrét vádemelés ekkor még nem történt, mert az OPM-ügyben beazonosított eszközök, az Equifax-adatlopással és Marriott-incidenssel összehasonlítva, rávilágítottak egy átfogó kínai kiberhírszerzési kampány eshetőségére.[54]

Az Equifax Inc. hitelminősítő céget 2017-ben érte adatlopási támadás, amely mintegy 143 millió ügyfél olyan személyes adatait érintette (a felhasználók teljes neve, lakcíme, születési dátuma, vezetői engedélye, bankkártyaszáma, társadalombiztosítási száma), amelyek felhasználhatók megszemélyesítéshez, illetéktelen tranzakciók végrehajtására, vagy további megfigyelésre és profilozáshoz. Az Amerikai Igazságügyi Minisztérium hivatalosan 2020 februárjában emelt vádat négy kínai katonai tiszt ellen az Equifax-adatlopás miatt. A vádirat ismertetésekor azonban az esetet nyíltan összekapcsolták a Marriott

[54] Fruhlinger 2020a.

elleni és az OPM-támadással egy nagyobb művelet részelemeiként.[55] Fruhlinger kiberbiztonsági szakértő elemzésében a vádemelést meglehetősen szokatlan lépésként értékelte, mivel az Egyesült Államok ritkán indít büntetőeljárást külföldi hírszerzők ellen, hogy elkerülje az amerikai ügynökökkel szembeni megtorlást. Ebben a narratívában a feltárt APT-kampány kiberdiplomáciai hatása rávilágít arra, hogy az amerikai kormány mennyire súlyos nemzetbiztonsági incidensként értékelte a támadásokat.[56]

A Marriott-adatlopás kapcsán a *New York Times* és a *Washington Post* hírportálok 2018 decemberében egy névtelenséget kérő kormányzati kontaktra hivatkozva számoltak be a KNK tevékenységének gyanújáról, ám a kormányzati szervek ekkor még nem tettek közzé részletekbe menő hivatalos technikai jelentést.[57] A Marriott Szállodalánc szakemberei 2018 szeptemberében egy szokatlan adatelérési kérést *(unusual database query)* észlelő felügyeleti eszköz riasztása miatt indítottak kivizsgálást, a korábban a Starwood vállalathoz tartozó hotelek (például a Westin, Sheraton, St. Regis és W hotelek) foglalásait kezelő belső rendszerben. A digitális nyomelemzés másfél hónappal később visszafejtette, hogy valamikor 2014-ben törhették fel a Starwood IT-infrastruktúráját, amikor az még különálló vállalatként működött.[58] A négy év során megközelítőleg 500 millió vendég foglalási adatait titkosították és exfiltrálták egy olyan adminisztrátori fiók segítségével, amely felett átvették az irányítást egy távoli hozzáférést biztosító trójai vírus (*Remote Access Trojan,* RAT) és egy etikus hackerek által is használt nyílt forráskódú eszköz, a Mimikatz[59] segítségével, amelyek a támadás vektoraiként értékelhetők.[60] Az elkövetkező években további technikai részletet is publikáltak, 2022-ben a CrowdStrike szakértője, Ryan Cornateanu, egy e-mail-hamisítási technikára *(email spoofing)* vezette vissza a belépési pontot, amely adathalász-támadást tehetett lehetővé.

A csoportos kártérítési igények mellett a szállodaláncra 23,8 millió dolláros bírságot szabtak ki a GDPR[61] megsértése miatt, továbbá kötelezettséget vállalt az érintettek útlevélcsere-költségeinek átvállalására.[62] Fruhlinger kiberbiztonsági szakértő elemzésében rávilágít arra, hogy az incidens, hasonlóképpen az OPM-adatlopáshoz, azon tények alapján utalt állami kiberhírszerzési műveletre, hogy nem találtak arra utaló jeleket, hogy a megszerzett személyes adatokat tartalmazó csomagokat[63] eladásra kínálták volna a dark weben, vagy felhasználták volna anyagi haszonszerzés céljából megszemélyesítésre, ahogy egy kiberbűnözői csoport tette volna. Emellett a Marriott Szállodalánc az amerikai kormányzat és hadsereg egyik legnagyobb szállásadó partnere, így a zsákmányolt útlevél

55 BBC (2020).

56 Fruhlinger 2020a.

57 Nakashima–Timberg 2018 és Sanger et al. 2018.

58 A Marriott 2016-ban vásárolta fel a Starwoodot, de majdnem két évvel később a korábbi Starwood Szállodák (például a Westin, Sheraton, St. Regis és W hotelek) még nem kerültek át a Marriott saját foglalási rendszerére, és továbbra is a Starwoodtól örökölt IT-infrastruktúrát használták, lásd Fruhlinger 2020b.

59 A Mimikatz Microsoft-alapú végpontokon képes kivonni a rendszermemóriából a felhasználónév-jelszó párokat. Soare 2022.

60 Fruhlinger 2020b.

61 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.

62 Hollander 2023.

63 Az adatcsomagok olyan információkat tartalmaztak, mint: név, születési dátum, nem, levelezési és e-mail-cím, telefonszám, útlevélszám, Starwood Preferred Guest (SPG) számlaadatok, érkezési és távozási adatok, foglalási dátum és kommunikációs preferenciák. Hollander 2023.

és személyazonosító igazolványok számai vagy bankkártyaadatok az OPM-adatlopás során szerzett információkkal kombinálhatók. Az így létrehozott big data adatbázis elemzésével lehetővé válhat a kormányzati alkalmazottak (köztük hírszerzők) és hivatásos személyek mozgásának nyomon követése.[64] Említésre méltó, hogy a szállodaláncot 2020-ban és 2022-ben is érték további, önálló incidensek, amelyeket azonban még nem attribuáltak.[65]

A SolarWinds vállalat Orion rendszerének egy másik sérülékenységét kihasználó támadás mögött kínai állami érdekről jelentek meg sajtóközlemények 2022-ben. Felügyeleti rendszerként a SolarWinds Orion terméke privilegizált hozzáféréssel rendelkezik az informatikai rendszerekhez, hogy napló- és rendszerteljesítmény-adatokat használhasson fel, így értékes célponttá vált. A Reuters hírügynökség az FBI folyamatban lévő nyomozására hivatkozva publikálta, hogy a feltételezhetően kínai aktorok a Sunburst nevű malware-t felhasználó támadással (amelyet orosz aktorokra attribuáltak 2020-ban) egy időben használták ki a SolarWinds rendszer sérülékenységét. Ezen második támadás alkalmával használt rosszindulatú programot a SolarWinds vállalat Supernova néven azonosította. A Reuters jelentése szerint a feltételezett kínai aktorok az Egyesült Államok Mezőgazdasági Minisztériumának egyik bérszámfejtő ügynökségét, a Nemzeti Pénzügyi Központot vették célba, amely megközelítőleg 600 ezer munkavállaló adatát kezeli, és több mint 160 ügynökségnek nyújt szolgáltatást. Arról azonban nincs információ, hogy történt-e kompromittálódás. Az újabb SolarWinds-eset is kiemelkedő jelentőségű, mert rávilágít arra, hogy az offenzív szereplők ismételten képesek voltak az Orion szoftvert támadó eszközzé formálni. A sajtóban megjelent vádakat a kínai külügyminisztérium is kommentálta, miszerint Kína határozottan ellenzi, és eltökélten küzd a kibertámadások és adatlopások minden típusa ellen, áll a Reuters által is idézett közleményben. A külügyminisztérium emellett hangsúlyozta azon igényét, hogy az amerikai kormányzat minden vádat konkrét bizonyítékokkal támasszon alá, utalva a technikai attribúció komplexitásából fakadó bizonytalansági tényezőkre.[66]

Noha az Anthem-adatlopási incidens, az Equifax – OPM – Mariott-kampány, valamint a SolarWinds-Orion szoftver kompromittálása különböző vertikumban elhelyezkedő intézmények elleni műveletek, párhuzamosságként azonosítható, hogy a megszerzett adatok lehetővé tehetik az Egyesült Államok kormányzati tevékenységének komplex megfigyelését, elemzését és befolyásolását, a szervezeti infrastruktúraelemek feltérképezése és a személyi állományról elérhető háttérinformációk révén. A fejezetben ismertetett kiberhírszerzési eseteket és a bevezetőben tárgyalt választási és általános politikai információszerzésre irányuló kiberműveleteket egyaránt az a stratégiai cél motiválhatta, hogy olyan háttér-információkhoz juttassák a kínai döntéshozókat, amelyek révén képesek finomhangolni az ország nemzetközi befolyásának növekedésére tett nonkonfrontatív erőfeszítéseket és konfrontatív – például választások eredményére ható – érdekérvényesítő képességét. Az ilyen célú kiberhírszerzési tevékenység napjainkra egyre mérvadóbbá vált a Kína nagyhatalommá válását közvetlenül megelőzően fennálló nemzetközi rendszert

64 Fruhlinger 2020b.
65 McGarry 2022.
66 Bing et al. 2021.

leginkább domináló országokban, amelyek jellemzően a globális „Nyugat" országai (az USA és az EU legnagyobb katonai-gazdasági befolyással rendelkező tagállamai).

Az USA mellett az európai régió célponttá válását helyezi kontextusba P. Szabó elemzése a kínai „kétvágányos" külpolitikai cél-, érték-, érdek- és eszközrendszerről, és magyarázatot ad arra, hogy a napjainkban tapasztalható befolyásolási törekvések – amelyek akár a kibertér által is megvalósulhatnak – milyen stratégiai hátrányok leküzdésére irányulnak. Az érintett államok társadalmának jelentős része – ideértve a domináns politikai erőket is – kritikus Kínával szemben. Ez egyrészt abból ered, hogy értékrendbeli ellentét áll fenn a pekingi vezetéssel a szocialista pártállami rendszer miatt, másrészt potenciális katonai fenyegetésnek értékelik Kínát. Harmadrészt, ezen államok lakosságának zöme úgy vélekedik, hogy rövid és középtávú gazdasági érdekei ellentétesek Kína IKT-technológiai és kereskedelmi befolyását növelő törekvéseivel.[67]

Összességében elmondható, hogy a kínai külpolitika – ideértve a nyilvános attribúcióhoz fűződő álláspontját – igyekszik eloszlatni az általa jelentett (katonai) fenyegetéssel kapcsolatos percepciót, mert az jelentősen korlátozza kiberhatalmi státuszának felépítését és nemzetközi érdekérvényesítő képességének növekedését (aminek stratégiai célja egy Kína által jelentősen befolyásolt vagy Kína által dominált világrend kiépítése). Annak ellenére, hogy napjainkra a kínai állami és állam alatti kiberegységek (APT) tevékenysége egyre konfrontatívabbá válik, és ezáltal egyre jelentősebb külkereskedelmi és kiberdiplomáciai szankciós intézkedést váltanak ki a „nyugati" nagyhatalmak részéről, Kína mindeddig tartózkodott az olyan mértékű, kritikusinfrastruktúra-elemeket érő károkozástól, amely az orosz vagy az észak-koreai állami aktivitást jellemzi.

Összegzés és konklúzió

Azon APT-csoportokról, amelyek feltehetően kiberbűnözői és kínai hátterű, állam alatti kiberegységként is tevékenységet folytatnak, globális viszonylatban megállapítható, hogy az általuk elkövetett – 2015 óta egyre gyakoribb – sikeres incidensek és behatolási kísérletek fő stratégiai célja a védelmi ipari és csúcstechnológiákra vonatkozó információk, továbbá a kínai geopolitikai célokat támogató hírszerzési adatok megszerzése. Napjainkban a kínai tevékenységre nyilvánosan attribútált kiberhírszerzési esetek jelentős arányban politikai befolyásszerzés céljából végrehajtott kiberműveletek (míg például Észak-Korea esetében az anyagi haszonszerzés a fő motiváció, és a célpontok többsége a pénzügyi vertikumban található szervezet). A kínai állam alatti (APT-) és állami (PLA-) kiberegységek offenzív kiberműveletei várhatóan tovább erősödnek az USA elnöki, európai uniós parlamenti és további tagállami választások közeledtével.

A védelmi technológiák fejlődése és az információmegosztás (például CTI-platformok és kormányközi kezdeményezések) ellenére, továbbra is nehézséget okoz csak technikai adatokra és a korábban feltárt – feltehetően kínai hátterű – kiberhírszerzési esetekre alapozva objektíven bizonyítani egy-egy támadás mögött meghúzódó állami érdekeltséget. Esetenként a támadás során feltárt geolokációs adatok (vagy IP-címek), programozási nyelv és a korábban publikált támadó eszközök (egyéb könnyebben reprodukálható offenzív

[67] P. Szabó 2020.

technikák és támadó kódrészletek) újbóli felhasználása miatt, a kielemzett digitális nyomok még évekig nem tudnak kielégítő bizonyítékot szolgáltatni a vádemeléshez és a kiberdiplomáciai szempontból kockázatos nyilvános attribúcióhoz. A bemutatott esetekből is látszik, hogy az egyes APT-csoportokra jellemző TTP-k beazonosítása (amelyek szintén fejlődnek az évek során), így a támogató állam beazonosítása is, referenciaként felhasználható vagy összehasonlítható incidensek bekövetkezése esetén lehetséges.

Összességében megállapítható, hogy a kiberhírszerzési tevékenység fő célja a gazdasági, technológiai és politikai előnyök megszerzése. A 2015 után megindított APT-műveletek célpontkiválasztása főként személyes adatok megszerzésére (Marriott-, Equifax- és Anthem-incidensek) irányult, amelyek tovább értékesíthetők vagy felhasználhatók adatigényes egészségügyi vagy pénzügyi intelligenciák (AI vagy ML) vagy speciális IoT-eszközök (IoMT – *internet of medical things,* az orvosi tárgyak internete) fejlesztési és piackutatási szakaszában. A kínai APT-csoportok rendkívül fejlett támadó eszközökkel és olyan szakértelemmel rendelkeznek, amit jól szemléltetnek az USA-ból származó esetpéldák, rámutatva arra, hogy a kínai hátterű APT-k képesek behatolni más országok hadiipari vállalatainak és védelmi minisztériumainak hálózataiba (RSA-incidens), vagy kompromittálni a személyi állomány adatbázisát (OPM-incidens), továbbá információkat gyűjteni a legújabb technológiákról és hadiipari fejlesztésekről (SolarWinds-incidens újabb sérülékenységének kihasználása). A kínai kiberhírszerzési tevékenység összetett, integrált rendszert alkot az Állambiztonsági Minisztérium és a hadsereg között.

A PLA képességeinek átalakítása és a haderőfejlesztési programok offenzív kiberképességek kialakítására tett erőfeszítései (például a Stratégiai Támogató Erők és a Vezérkar állományán belül) regionális szinten kiemelkedő katonai erővé emelték Kínát, ám növelték a digitális rendszerektől való függőségét is. Nemzetbiztonsági és katonai relevanciával is bír az utóbbi évek egyre erősödő trendje, hogy a kínai tehetségek fokozatos átáramlása tapasztalható a nemzetközi gyakorlatok és „hackerkonferenciák" résztvevői közül a hazai versenyek és platformok (például 2017-től a Tianfu Cup) irányába, mert ez a képességek tudatos elrejtésére való törekvést is jelentheti. Emiatt az offenzív képességekkel rendelkező kínai szakemberek tudásszintjének felmérése és nemzetközi összehasonlítása nehezebbé válik, továbbá az általuk használt szofisztikált támadó vagy sérülékenységeket feltáró programok eredményességéről is nehezebb tapasztalatokat és objektív visszajelzést kapni. Körülményesebbé és nehezebbé válik a védelmi rendszerek felkészítése és továbbfejlesztése.[68]

Felhasznált irodalom

BBC (2020): Equifax: US Charges Four Chinese Military Officers Over Huge Hack. *BBC,* 2020. február 11. Online: www.bbc.com/news/world-us-canada-51449778

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

[68] Cimpanu 2021.

Bianco, David (2013): *Pyramid of Pain: A Model for Prioritizing Which Indicators of Compromise To Address First.* Online: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Bing, Christopher et al. (2021): Exclusive: Suspected Chinese Hackers Used SolarWinds Bug to Spy on U.S. Payroll Agency – Sources. *Reuters,* 2021. február 2. Online: www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8

Campbell, Caitlin (2021): *China's Military: The People's Liberation Army (PLA).* Congressional Research Service, 2021. június 4. Online: https://crsreports.congress.gov/product/pdf/R/R46808

Cimpanu, Catalin (2021): Windows 10, iOS 15, Ubuntu, Chrome Fall at China's Tianfu Hacking Contest. *The Record,* 2021. október 17. Online: https://therecord.media/windows-10-ios-15-ubuntu-chrome-fall-at-chinas-tianfu-hacking-contest/

Dobák Imre – Tóth Tamás (2021): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle,* 69(2), 195–212. Online: https://doi.org/10.38146/BSZ.2021.2.2

Electronic Transactions Development Agency (2021): Threat Group Cards: A Threat Actor Encyclopedia – APT Group: Comment Crew, APT 1. Online: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=b99367ed-e483-40a3-98d0-8d3a2102a4ab

Electronic Transactions Development Agency (2022a): Threat Group Cards: A Threat Actor Encyclopedia – All Groups from China. Online: https://apt.etda.or.th/cgi-bin/listgroups.cgi?c=China

Electronic Transactions Development Agency (2022b): Threat Group Cards: A Threat Actor Encyclopedia – APT Group: APT 19, Deep Panda, C0d0so0. Digital Service Security Center, ETDA. Online: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=58c7e347-341c-4446-bf03-81fc1f7d9254

Flashpoint Team (2022): *Guide to Cyber Threat Intelligence: Elements of an Effective Threat Intel and Cyber Risk Remediation Program.* Online: https://flashpoint.io/blog/guide-to-cyber-threat-intelligence/

Friis, Karsten – Lysne, Olav (2021): Huawei, 5G and Security: Technological Limitations and Political Responses. *Development and Change,* 52(5), 1174–1195. Online: https://doi.org/10.1111/dech.12680

Fruhlinger, Josh (2020a): The OPM Hack Explained: Bad Security Practices Meet China's Captain America. *CSO,* 2020. február 12. Online: www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Fruhlinger, Josh (2020b): Marriott Data Breach FAQ: How Did It Happen and What Was the Impact? *CSO,* 2020. február 12. Online: www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

Greenberg, Andy (2021): The Full Story of the Stunning RSA Hack Can Finally Be Told. *Wired,* 2021. május 20. Online: www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/

Greig, Jonathan (2024): Us Sanctions Alleged Chinese State Hackers for Attacks on Critical Infrastructure. *The Record,* 2024. március 25. Online: https://therecord.media/us-sanctions-chinese-hackers-infrastructure-attacks

Gyebnár Gergő (2023): *The Future of Industrial Threat Intelligence.* Black Cell Magyarország Kft. Online: https://web.archive.org/web/20230419093133/https://blackcell.io/blog/2023/04/19/the-future-of-industrial-threat-intelligence/

Hannas, William C. – Tatlow, Didi Kristen szerk. (2020): *China's Quest for Foreign Technology. Beyond Espionage.* London: Routledge. Online: https://doi.org/10.4324/9781003035084

Hollander, Jordan (2023): Marriott Data Breach FAQ: What Really Happened? *HotelTechReport,* 2023. február 16. Online: https://hoteltechreport.com/news/marriott-data-breach

Inkster, Nigel (2015): The Chinese Intelligence Agencies – Evolution and Empowerment in Cyberspace. In Lindsay, Jon R. – Cheung, Tai Ming – Reveron, Derek S. (szerk.): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford University Press, 29–50. Online: https://doi.org/10.1093/acprof:oso/9780190201265.003.0002

Kaska, Kadri – Beckvard, Henrik – Minárik, Tomáš (2019): *Huawei, 5G and China as a Security Threat.* NATO Cooperative Cyber Defence Center for Excellence (CCDCOE), 1–26. Online: https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/

Kaszián Ábel Gergő (2021): A GDPR kínai „unokatestvére" – avagy a kínai adatvédelmi törvény megszületése és várható hatásai. *Jogi Fórum,* 2021. szeptember 20. Online: www.jogiforum.hu/publikacio/2021/09/20/a-gdpr-kinai-unokatestvere-avagy-a-kinai-adatvedelmi-torveny-megszuletese-es-varhato-hatasai/

Krebs, Brian (2015): Catching Up on the OPM Breach. *Krebs on Security,* 2015. június 15. Online: https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

Lee, John (2022): Cyberspace Governance in China: Evolution, Features and Future Trends. *Asie Visions*, (129). Ifri. 2022. július 29. Online: www.ifri.org/en/publications/notes-de-lifri/asie-visions/cyberspace-governance-china-evolution-features-and-future

Lima da Frota Araujo, Carlos Raul – Szunomár Ágnes (2022): Kelet-Közép-Európa a digitális selyemúton? Lehetséges politikai gazdaságtani magyarázatok. *Közgazdasági Szemle*, 69(3), 367–388. Online: https://doi.org/10.18414/KSZ.2022.3.367

Lindsay, Jon R. – Cheung, Tai Ming (2015): From Exploitation to Innovation: Acquisition, Absorption, and Application. In Lindsay, Jon R. – Cheung, Tai Ming – Reveron, Derek S. (szerk.): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford University Press, 51–86. Online: https://doi.org/10.1093/acprof:oso/9780190201265.003.0003

Lindsay, Jon R. – Cheung, Tai Ming – Reveron, Derek S. szerk. (2015): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford University Press. Online: https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

Lusthaus, Jonathan – Bruce, Miranda – Phair, Nigel (2020): *Mapping the Geography of Cybercrime: A Review of Indices of Digital Offending by Country.* 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 2020. szeptember 7–11. Online: https://doi.org/10.1109/EuroSPW51379.2020.00066

Macaskill, Andrew – Pearson, James (2024): Britain Says China Hacked Electoral Watchdog, Targeted Lawmaker Emails. *Reuters,* 2024. március 25. Online: www.reuters.com/world/uk/uk-deputy-pm-set-address-lawmakers-chinese-cyber-security-threat-2024-03-24/

Matura Tamás et al. (2022): *Risky Business? Assessing Political Economic and Technological Risk Perceptions of Relations between the People's Republic of China and Hungary.* Budapest: Central and Eastern European Center for Asian Studies.

McGarry, Pat (2022): Lessons Learned from the Marriott Hack of 2022. *Threater,* 2022. június 9. Online: www.threatblockr.com/blog/lessons-learned-from-the-marriott-hack-of-2022

Mészáros R. Tamás (2021): Annyi adatot gyűjtöttek, hogy a Kínai Kommunista Párt is megijedt tőle. *G7,* 2021. július 25. Online: https://g7.hu/vilag/20210725/annyi-adatot-gyujottek-hogy-a-kinai-kommunista-part-is-megijedt-tole/

Nakashima, Ellen – Timberg, Craig (2018a): U.S. Investigators Point to China in Marriott Hack Affecting 500 million guests. *Washington Post,* 2018. december 12. Online: www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/

Pearson, James – Satter, Raphael – Bing, Christopher (2024): US, UK Accuse China of Cyberespionage That Hit Millions of People. *Reuters,* 2024. március 25. Online: www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25/

Pennino, Alex – Bromiley, Matt (2022): GAME OVER: Detecting and Stopping an APT41 Operation. *Mandiant,* 2019. augusztus 19. Online: www.mandiant.com/resources/blog/game-over-detecting-and-stopping-an-apt41-operation

Plan, Fred et al. (2024): *APT40: Examining a China-Nexus Espionage Actor. Mandiant.* Online: www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor

P. Szabó S. (2020): A Kínai Népköztársaság „kétvágányos" külpolitikája. In P. Szabó Sándor – Horváthné Varga Polyák Csilla (szerk.): *Lehetőségek és kihívások a magyar–kínai kapcsolatok területén. I. kötet. Politikai kapcsolatok.* Budapest: Ludovika, 9–28.

Sanger, David E. et al. (2018): Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing. *New York Times,* 2018. december 11. Online: www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

Segal, Adam (2020): China's Pursuit of Cyberpower. In Segal, Adam et al.: The Future of Cybersecurity across the Asia-Pacific. *Asia Policy,* (15)2, 60–66. Online: https://doi.org/10.1353/asp.2020.0034

Smith, Zhanna Malekos (2022): Emerging Cyber Threats: No State Is an Island in Cyberspace. *CSIS,* 2022. március 23. Online: www.csis.org/analysis/emerging-cyber-threats-no-state-island-cyberspace

Soare, Bianca (2022): What is Mimikatz? What Can It Do and How to Protect. *Heimdal,* 2022. december 7. Online: https://heimdalsecurity.com/blog/mimikatz/

Szeleczki Szilveszter (2022): A kiberhírszerzés értelmezése és helye a nemzetbiztonságban. *Nemzetbiztonsági Szemle,* 10(4), 17–29. Online: https://doi.org/10.32561/nsz.2022.4.2

USA White House, Office of the Press Secretary (2015): *FACT SHEET: President Xi Jinping's State Visit to the United States. Cybersecurity.* Online: https://obamawhitehouse.

archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

US Department of Justice (2024): *Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians*. 2024. március 25. Online: www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived

Yang, Fan (2022): The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective. In Levite, Ariel E. et al. (szerk.): *Managing U.S.-China Tensions Over Public Cyber Attribution*. Washington, D.C: Carnegie Endowment for International Peace, 6–14. Online: https://carnegieendowment.org/files/Perkovich_et_al_Cyber_Attribution_web.pdf

Young, Kelli (2021): Cyber Case Study: Anthem Data Breach. *Coverlink*, 2021. szeptember 27. Online: https://coverlink.com/case-study/anthem-data-breach/