HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 1. szám 143–176.
DOI: 10.32567/hm.2024.1.8

Lendvai Tünde[1]

Észak-Korea kiberképességei az északkelet-ázsiai régió műveleti környezetében

North Korean Cyber Capabilities in the Operational Environment of the Northeast Asian Region

Absztrakt

A tanulmány bemutatja a Koreai Népi Demokratikus Köztársaság (továbbiakban KNDK vagy Észak-Korea) kiberképességeinek szervezeti felépítését és feltételezhető kiberhadviselési stratégiáját. A kutatás célja, hogy átfogó képet adjon Észak-Korea offenzív kibertéri tevékenységének biztonságpolitikai összefüggéseiről az északkelet-ázsiai régió vonatkozásában, különös tekintettel a Kínai Népköztársasággal történő stratégiai együttműködés jelentette kockázatokra. A kutatás szekunder adatgyűjtésre épült a rendelkezésre álló szakirodalom, sajtóhírek és esetpéldák elemzésével.

Kulcsszavak: Észak-Korea, kiberműveletek, kiberstratégia, kiberhadviselés, KNDK

Abstract

The paper discusses the organisational structure of cyber capabilities and a hypothetical cyber warfare strategy of the Democratic People's Republic of Korea (hereinafter referred to as the DPRK or North Korea). It aims to provide a holistic view of North Korean offensive cyberspace activities in the context of security policy in the Northeast Asian region, with a particular focus on the risks posed by strategic cooperation with the People's

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

Republic of China. The research was based on secondary data collection through analysis of academic literature, press reports and publicly available case studies.

Keywords: North Korea, cyber operation, cyber strategy, cyberwarfare, DPRK

Bevezetés

Biztonság- és védelempolitikai megközelítésben a kiberműveleti képesség a nemzeti érdekérvényesítés eszköztárának egyik elemeként is értékelhető.[2] Napjainkig több kutatás is felvázolta a jelentős politikai hatást kiváltó incidensek alapján a Koreai Népi Demokratikus Köztársaság (a továbbiakban Észak-Korea vagy KNDK) kiberstratégiájának célrendszerét a phenjani rezsim biztonság- és külpolitikai érdekeinek kontextusában. A kutatások rávilágítottak arra, hogy Phenjan egyre fejlettebb kiberképességeivel képes pénzügyi erőforrásokhoz jutni, valamint a kiberműveletek általi provokációval politikai és stratégiai előnyöket kikényszeríteni a nemzetközi közösségből, amivel stratégiai célja, hogy elősegítse a Kim-rezsim fennmaradását. Észak-Korea nemzetközi helyzetében a kiberképességek oly módon is bevethetők a katonai értelemben vett szürkezónában, hogy még aszimmetrikus helyzetben[3] is (költség)hatékonyan alkalmazhatók politikai célú erődemonstrációra, hírszerzésre vagy a haderőfejlesztést finanszírozó anyagi javak megszerzésére, számottevő konfliktuseszkalációs kockázat nélkül.[4]

Noha a kiberképességek katonai alkalmazásáról Észak-Korea még nem publikált hivatalos, stratégiai szintű dokumentumot, a vezetők politikai nyilatkozatai alapján felvázolható az információs és kibertéri műveletek szerepe a hadászati gondolkodásban. Például a 2003-as iraki háború után Kim Dzsongil a következőket mondta katonai vezetőkhöz intézett beszédében:

„A hadviselés mindeddig a töltényekről és az olajról szólt, a 21. században azonban már az információ felhasználásáról. Az dönti el, hogy ki nyeri meg és ki veszíti el a háborút, hogy békeidőben melyik fél fért hozzá nagyobb mértékben az ellenség katonai technológiájával kapcsolatos információhoz, milyen hatékonyan képes megzavarni ellenfele vezetés-irányítási csatornájában az információáramlást, és milyen hatékonysággal használja fel saját információit."[5]

Kim Dzsongun 2012-ben úgy jellemezte a Koreai Néphadsereg Központi Felderítő Irodájának (Reconnaissance General Bureau, a továbbiakban: Központi Felderítő Iroda vagy RGB) számítógép-hálózati műveleti képességét, mint egy minden célra bevethető kardot, amely a nukleáris fegyverekkel és hordozórakétákkal együtt lehetővé teszi a rezsim számára a folyamatos csapásmérést.[6] Mindkét vezető összességében azt

[2] Berzsenyi 2023: 19; 99–104; 111–113; 123–125.

[3] Észak-Korea és az Egyesült Államok között aszimmetrikus helyzet áll fent több aspektusban is. Ezek például a térségben fennálló katonai és politikai szövetségesek (USA–Dél-Korea és USA–Japán) egyesített haderejében és ütőképességében mutatkozik meg az észak-koreai rezsim elszigeteltségével szemben, továbbá a haderőre fordítható erőforrások (pl.: költségvetés) és az eszközpark modernizáltságának (értsd: fejlettségének) relációjában.

[4] Ha 2022.

[5] Kong–Lim–Kim 2019: 2.

[6] „Cyberwarfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles." Fordítás: Berzsenyi 2023: 123–124.

az attitűdöt erősítette meg a kiberképességek önálló stratégiai funkciójával kapcsolatban, hogy a kibertéri katonai egységek offenzív és defenzív oldalon történő célzott és rugalmas alkalmazhatósága, valamint adaptív és fedett jellege miatt egyfajta elrettentésen alapuló védelmet is képesek nyújtani (a nukleáris csapásmérő képesség kialakításához hasonlóan) a modern háborúkat eldöntő elektronikai hadviselés korában.[7]

Észak-Korea nemzeti kiberműveleti képességeinek feltérképezését és stratégiai célrendszerének elemzését nehezíti, hogy az állami érdekeket megvalósító, jellemzően küldetésorientált műveletszervezési elvek nyomán összeállított egységek tevékenysége összefonódik a fejlett perzisztens fenyegetések (*Advanced Persistent Threat,* a továbbiakban APT vagy fejlett perzisztens fenyegetések)[8] működésével.[9] A kutatás elsődleges célja, hogy a KNDK jelentős[10] offenzív kibertéri műveleteiről és az ezeket végrehajtó katonai egységekről publikusan elérhető szakirodalom komparatív értékelése alapján jellemezze Észak-Korea kiberképességeit, és feltárja kiberhadviselési stratégiájának lehetséges elemeit.

Módszertan és hipotézis

A kutatási probléma felvetése rávilágított arra, hogy a létező elméleti keretrendszerek nem elegendő mélységben veszik figyelembe Észak-Korea (és ezáltal az északkelet-ázsiai szubrégió) kiberbiztonsági környezetének jellemzése során a kínai infrastruktúrával való összefonódás lehetőségében rejlő biztonságpolitikai kockázatokat. Ezért a kutatás új elemzési szempontként emeli be Észak-Korea feltételezhető kiberhadviselési stratégiájának értelmezésébe az ország Kínai Népköztársasághoz kötődő geopolitikai és biztonságpolitikai helyzetének értékelését és az együttműködés különböző aspektusait. A tanulmány második része ismerteti az észak-koreai állami hátterű fejlett perzisztens fenyegetések tevékenységének aktuális trendjeit. Ezután a szerző áttekintést nyújt Észak-Korea hálózati adottságairól, kiberképességeit keretező intézményi struktúrájáról, főbb stratégiai partnereiről. Végül pedig áttekinti az észak-koreai kibertéri műveletek stratégiai célrendszeréről publikált elméleteket, és bemutatja a lehetséges kiberhadviselési stratégiai irányokat. A biztonságpolitikai módszertani megközelítést alkalmazó elemzés az alábbi kutatási kérdés (KK1) és egy hipotézis (H1) felvetését vizsgálta meg:

KK1: A nyilvánosan észak-koreai aktorok tevékenységére attribútált kibertéri műveletek stratégiai célrendszere hogyan illeszkedik az ország védelempolitikájába, és miként támogatja a phenjani rezsim nemzetközi érdekérvényesítő képességét?

[7] Berzsenyi 2023: 123–125.

[8] Az APT *(Advanced Persistent Threat)* olyan kibertámadási modell, amelyben a támadó csoport vagy kiberbűnözők rendkívül komplex eljárásokat (TTP) és fejlett támadóeszközöket alkalmaznak, továbbá hosszú időn keresztül képesek észrevétlenek maradni a célzott hálózatokban, hogy érzékeny információkat szerezzenek meg. Ezen jellemzők és a célorientált feladatmegvalósítás okán feltételezhető, hogy az APT-csoportok tevékenységét állami támogatással hajtják végre. Az APT-csoportok műveletei tehát valamely hadsereg vagy nemzetbiztonsági szervezet egységének tevékenységét fedik le, vagy állami háttértámogatással működő kiberbűnözői célok megvalósítását foglalja magában.

[9] Kong–Lim–Kim 2019.

[10] Jelentős, vagyis nagy horderejű, stratégiai vagy politikai érdekek mentén bekövetkezett incidensek.

- H1: A békeidőszaki kiberműveletek kettős védelempolitikai célja, hogy egyrészt finanszírozza a haderőfejlesztést, másrészt a stratégiai céllal alkalmazott katonai provokációkat kiegészítve gazdasági és politikai engedményeket kényszerítsen ki a nemzetközi közösségből.

Észak-Korea geostratégiai helyzetéből adódóan alkalmas a Kínai Népköztársaság nemzetközi erőkivetítési törekvéseinek támogatására az északkelet-ázsiai régióban, mert a két állam között stratégiai érdekegyezés áll fenn az USA és a szubregionális politikai-katonai szövetség gyengítése tekintetében.[11] Ezért másodlagos kutatási célkitűzés a pekingi és a phenjani vezetés között feltételezhető stratégiai együttműködés kibertéri aspektusai által generált kockázatok feltérképezése és leírása. A beazonosított összefüggések hozzájárulnak a kínai és észak-koreai állami aktivitás feltárásához kapcsolódó, kiberfenyegetés-felderítő (*cyber threat intelligence,* CTI) tevékenység által nyert információk komplexebb értékeléséhez. A fenti célkitűzés mentén a szerző további egy kutatási kérdés (KK2) és hipotézis (H2) vizsgálatát végezte el:

KK2: Milyen stratégiai adottságok és érdekek teszik lehetővé a Kínai Népköztársaság és a Koreai Népi Demokratikus Köztársaság között feltételezhető együttműködést az offenzív kibertéri műveletek kivitelezésében?

- H2: A geopolitikai sajátosságok lehetővé teszik Kína számára, hogy infrastrukturális erőforrásokat bocsásson az észak-koreai katonai kiberegységek rendelkezésre, továbbá tudásmenedzsmenttel járuljon hozzá észak-koreai személyek képességeinek fejlesztéséhez.

Az Észak-Korea nemzeti kiberképességeinek vázát nyújtó szervezeti felépítés és a fejlett perzisztens fenyegetések stratégiai célrendszerének feltérképezéséhez szekunder forrásokból származó adatok álltak rendelkezésre. Ennélfogva a kutatás témaköre több módszertani limitációt is magában hordoz. Egyfelől Észak-Korea kiberképességeinek összetételét, valamint alkalmazásának stratégiai irányát ez irányú kormányzati kommunikáció hiányában csak induktív módszertani megközelítéssel lehet meghatározni, ám ez esetenként disszidensek és más hírszerzéssel kapcsolatban álló informátorok beszámolóira támaszkodik (így a forrás objektivitása csökken, emellett szekunder forrásból származó adatgyűjtésnek minősül). Ezt kiegészítve, az Észak-Koreához köthető APT-aktivitás deduktív vizsgálata betekintést adhat a képességek alkalmazásának célrendszerébe, ám ebben az esetben sem lehet élesen elkülöníteni a kiberbűnözői tevékenységet az állami hátterű, de anyagilag (is) motivált műveletektől. Mindamellett, hogy a technikai adatokra alapozott (például *digital forensics,* IoC- vagy TTP-adatok), kvalitatív és kvantitatív módszerekkel elkészített CTI-jelentések nagyobb objektivitást kínálnak, figyelembe kell venni a támadást elszenvedő fél érdekeit. A nyilvános attribúciót végző állam (egyedi nemzeti érdekei mentén) vagy a megtámadott szervezet (a kihasznált sérülékenység miatti felelősségrevonhatóságából adódóan, illetve a keletkezett kár megtérítési kötelezettsége vagy hatósági bírság miatt) ugyancsak torzíthatja az információk pontosságát és objektivitását.[12]

[11] Bartók–Wagner 2021.
[12] Berzsenyi 2023: 19.

Az északkelet-ázsiai régió biztonságpolitikai környezetének kiberbiztonsági összefüggései

Az északkelet-ázsiai régió (Kína és Tajvan, valamint Japán és a két Korea) biztonságpolitikai környezetét folyamatos haderőfejlesztési és haditechnikai modernizációs kényszer alakítja. Ennek több kiváltó oka is van, ám euroatlanti perspektívából nézve elsődleges indikátorként a kínai haderő modernizációját tartjuk számon. Ennek hátterében az áll, hogy a pekingi vezetés az Egyesült Államok (a továbbiakban USA) térségbeli jelenlétéből[13] fakadó fenyegetettségpercepcióját csökkentette a haderőfejlesztéssel és katonai reformokkal. A Koreai-félsziget elhelyezkedése egyfajta természetes védvonalat képez (és pufferzónát ad az amerikai és a dél-koreai erők között) Kína part menti régiója számára például egy amerikai blokád esetén, ami az ország védelempolitikájának egyik alapköve. Ezáltal Észak-Korea geostratégiai helyzetéből adódóan alkalmas a Kínai Népköztársaság nemzetközi erőkivetítési törekvéseinek támogatására. A kínai haderőreform mögött álló A2/AD stratégia[14] magyarázza a megnövekedett katonai – különösen haditengerészeti – aktivitást. A regionális erőkivetítés érdekében Kína a dél-kínai-tengeri zátonyokon létesített bázisokkal, haditengerészeti jelenlétével és az erődemonstrációs hadgyakorlatok révén juttatja *de facto* érvényre igényét a vitatott státuszú területek felett. Mindez az utóbbi években többek között Vietnámot, a Fülöp-szigeteket, Malajziát, Japánt és a Koreai Köztársaságot is haderejének transzformációjára késztette, ami általában partra szálló és területvédelmi képességfejlesztést takar. Ebből következik, hogy a térség dinamikus militarizációját kiváltó második indikátor a szigetcsoportok feletti kontroll megszerzését (a tengeri erőkivetítést) jelenti. A militarizációs trendeket befolyásoló harmadik indikátorként a Tajvani-szorosban és a Koreai-félsziget körül tapasztalható katonai provokációk azonosíthatók, különösképp az észak-koreai atom- és rakétaprogram fejlődése miatti fenyegetettség okán.[15]

Ebben a biztonságpolitikai környezetben az északkelet-ázsiai régió nemzeteinek haderőfejlesztési törekvései egyaránt irányulnak a területszerzésre vagy területvédelemre alkalmas katonai képességek kialakítására,[16] valamint az információszerzéstől a csapásmérésig terjedő változatos műveleti célokat kiszolgáló offenzív és kibertámadó képességek fejlesztésére. Az utóbbi öt évben számos állam – köztük Kína és Tajvan – alakította át olyan elvek mentén kibervédelmi struktúráját, amelynek eredményeképpen adaptív ellenálló képességük részévé tették a hiteles kibertéri elrettentés[17] koncepcióját kibertámadó képességek felépítésével.[18]A kibertámadó

[13] Ideértve az állandó amerikai katonai bázisok fenntartását Japánban és Dél-Koreában, a fegyverszállítást (például a Japán részére átadott Patriot és a Dél-Koreába telepített THAAD – Terminal High Altitude Area Defense légvédelmi rendszerek), a rendszeres hadgyakorlatokat, valamint a haditengerészeti erők jelenlétét.

[14] Angolul: Anti-Access/Area Denial (A2/AD) strategy: hozzáférést gátló és területmegtagadó stratégia.

[15] Bartók–Wagner 2021.

[16] Bartók 2020: 80–101.

[17] Egy ország védelmi koncepciójában a kibertéri elrettentés olyan kibertámadó képesség kialakítását foglalja magában, amely akkora mértékben csökkenti az ellenség képességeit, hogy nem tud hatékony támadást indítani. Azonban ezzel párhuzamosan elengedhetetlen egy olyan állami kibervédelmi rendszer fenntartása, amely csak aránytalanul nagy erőforrás-befektetéssel törhető át. (Lásd Kovács 2021).

[18] Yau 2020.

képességek felépítése világviszonylatban is jellemző kiberhadviselési stratégiai koncepcióváltás eredménye, amely a kibertéri szuverenitás biztosítását célozza, hiszen a 21. század műveleti környezetében, a civil információs rendszerek (például közösségi média, civil mobilkommunikációs technológiák: 4G és 5G) és katonai komponensek ugyanolyan fajsúlyosan járulnak hozzá egy ország kibervédelmi struktúrájához.[19] Az USA és térségbeli katonai szövetségesei hadgyakorlatok megszervezésével tartják fenn az általános készültséget és reagálóképességet, amelyek kiterjednek többek között haditengerészeti és kiberműveleti területre. Például az USA és Dél-Korea 2023 áprilisában jelentette be azon szándékát, hogy kibervédelmi gyakorlatokat is tartsanak *(table top excercise)* az integrált védelmi párbeszéd *(integrated defense dialogue)* kiberműveleti együttműködési munkacsoportja (Cyber Cooperation Working Group, CCWG) keretében.[20] Ugyanezen megfontolásból Tajvan kétévente rendezi meg nemzetközi résztvevőkkel a komplex (*full scale cyber range* típusú) úgynevezett Cyber Offensive and Defensive Exercise gyakorlatát.[21] Kiemelendő, hogy Tajvan esetében napjainkra a diplomáciai célú látogatások (például Nancy Pelosi amerikai demokrata házelnök tajvani útja) is eszkalációs tényezővé váltak és kínai erődemonstrációt indukáltak, amit korábban a hadgyakorlatok, haditechnikai vagy védelmi ipari együttműködések bejelentése váltott ki.[22]

Az északkelet-ázsiai régió biztonságpolitikájának relevanciája a hadiipari igények kiszolgálásának vonatkozásában is megmutatkozik: Japán, Dél-Korea és Tajvan IKT-ipara önmagában is jelentős hatást gyakorol a globális ellátási láncokra, különösen a háború sújtotta Európa számára. Emellett egyre jelentősebb az ázsiai fegyverexport volumene az EU-tagállamok irányába,[23] ezzel párhuzamosan Észak-Korea Oroszország részére szállít katonai felszerelést, többek között lőszereket. Az észak-koreai – orosz bilaterális kapcsolat kibővülése számos fenyegetést hordoz magában, amelyek a technológiai vagy haditechnikai szegmensben is megjelentek.[24]

Szakértői feltételezések szerint az orosz technológiai támogatásnak jelentős szerepe volt abban, hogy Észak-Korea 2023 novemberében sikeresen pályára állította első műholdját, ami hozzájárul az ország (katonai) felderítő képességének minőségi növekedéséhez. Az euroatlanti közösségnek fel kell készülnie az orosz – észak-koreai katonai és gazdasági együttműködés jelentette fenyegetésre – akár a kibertérből érkező fenyegetésekre is –, és ki kell dolgozni a kockázatcsökkentő szakpolitikai lépéseket.[25] Meglátásom szerint ezen szakpolitika kidolgozásában szerepe lehet a kínai érdekek felhasználásának (akár Oroszországgal szemben), mivel Észak-Korea korábban kizárólagosan a kínai kereskedelem és geopolitika védőernyőjének hatókörébe tartozott, ennek exkluzivitására (és Kína számára a profitabilitására) konkurenciát

[19] Kovács 2021: 119–137.
[20] US Department of Defense 2023.
[21] 2021-ben energiaipart érő támadást szimuláltak 33 ország, köztük az USA csapatának részvételével. Bővebben Taiwan National Computer Emergency Response Team 2022.
[22] Bartók 2022.
[23] Például Észtország, Törökország, Lengyelország, Finnország és Norvégia együtt 18 db K9-es önjáró lövegre adott megrendelést a dél-koreai Hanwha részére, míg az első 24 db K9-esből és 10 db K2-es harckocsiból álló szállítmány már 2022 decemberében megérkezett Lengyelországba. Bővebben McLeary–Hudson 2022.
[24] Geigenberger 2023.
[25] Cha–Lim 2024.

jelent az oroszországi fegyverexport és a potenciális technológiai együttműködés. Kulcsfontosságú tehát, hogy a NATO-tagországok és a velük partner ázsiai nemzetek a digitális államigazgatási rendszereiket felépítő adatvagyon és infrastruktúra integritását garantálni tudják az APT-vel és más kiberbűnözői aktorokkal szemben (amelyek akár lehetnek észak-koreai hátterűek),[26] továbbá az ezekre támaszkodó ipari irányítási rendszerek, gazdasági társaságok és folyamatok, valamint a csúcstechnológiákat érintő kutatóhálózatok rezilienciáját is szavatolják.[27]

Az észak-koreai kibertéri műveletek aktualitás trendjei

Észak-Korea nemzeti kiberműveleti képességei folyamatos fejlődésen mentek keresztül a hírhedt Sony Pictures Entertainment (2014) rendszereit ért erődemonstráció, a Banglades Bank kompromittációja (2016) és a WannaCry 2.0 zsarolóvírus (2017) terjesztése óta elmúlt években. Az észak-koreai kibertéri aktivitást vizsgáló elemzők jellemzően a pénzügyi és az egészségügyi szektor vertikumába tartozó célpontok elleni műveletek szofisztikáltságában (az alkalmazott technikák komplexitása, kifinomultsága) és volumennövekedésében azonosították be a képességfejlődés indikátorait. Erre példa a kriptovaluta-szolgáltatásokat kompromittáló AppleJeus kampányok (2018-tól)[28] és a kórházi rendszerek adatait titkosító MAUI zsarolóvírus, amelyet 2021 májusától kezdtek terjeszteni.[29]

Ezen incidensek kapcsán arra lehet következtetni, hogy az anyagi motiváció maradt a legmeghatározóbb faktor az állami hátterű, fejlett perzisztens fenyegetések és klasztereik tevékenységében.[30] Ezt a trendmegfigyelést támasztja alá a kriptovalutákkal való visszaélések, a fintech vállalkozások (pénzügyi technológia) és pénzügyi intézmények körébe tartozó célpontok incidensszámának éves változása alapján a Mandiant 2023-ban publikált, éves áttekintést adó kiberfenyegetettség-felderítési (CTI) jelentése az észak-koreai APT-tevékenységéről.[31] Az elemzők az anyagilag motivált incidensek domináns növekedését mutatták ki a 2020–2023 közötti időszakban, amire a Covid–19 okozta világjárvány is jelentős hatással lehetett. Azért, hogy megakadályozza a járvány kitörését az országon belül, a rezsim lezárta határait, és teljesen elvágta magát a külkereskedelemtől. A szöuli Korea Trade-Investment Promotion Agency szerint Észak-Korea Kínával folytatott kereskedelmi forgalma 2020-ban 80,7%-kal esett vissza.[32] Egyrészt, a Mandiant kutatóinak állaspontja szerint, a járvány miatti kínai határlezárás azért növelhette az anyagilag motivált célpontok

[26] Krasznay 2022: 29–46.
[27] Krasznay 2020: 83–97.
[28] US Cybersecurity and Infrastructure Security Agency 2021.
[29] US Cybersecurity and Infrastructure Security Agency 2022.
[30] Értsd: észak-koreai APT-csoportok és feladat-orientált tevékenységeik p APT38 – Cryptocore (Mandiant: UNC1069), AppleJeus-aktivitás (Mandiant: UNC1720), TraderTraitor (Mandiant: UNC4899) stb.
[31] Az elemzés a Mandiant CTI szolgáltatása révén összegyűjtött információk alapján készült. Forrásai közt említi a vállalat incidenskezelésből származó *(intrusion response)* saját adatgyűjtését, kormányzati közleményeket és tájékoztatókat, valamint az OSINT-eszközök felhasználásával kinyert és észak-koreai disszidensek által átadott hírforrásokat.
[32] Shim 2021.

volumenét, mert blokkolta az országba telepített külföldi műveleti egységek személyi állományát abban, hogy hozzáférjenek az észak-koreai erőforrásokhoz, finanszírozáshoz.[33] Megjegyzendő, hogy Észak-Korea korábban is határain kívülről hajtotta végre kibertéri műveleteit, számos esetben a Kínai Népköztársaság (a továbbiakban Kína) területéről. Ennek elsősorban infrastrukturális és geopolitikai okai vannak, amit a tanulmány egy későbbi fejezetében mutat be. Emellett esetenként a műveleteket végrehajtó személyek is külföldön tartózkodtak vendégmunkásként, amit jelentősen megkönnyít – például az anyanyelvhasználat miatt – a kínai–koreai etnikai kisebbség jelenléte Kína északi tartományaiban (Liaoning és Csilin).[34] Ezenfelül a távmunkavégzés térnyerésével párhuzamosan megjelent a globális piacon az „illegális" észak-koreai munkaerő, akiket tudatosan vagy tudtukon kívül alkalmaztak vállalatok az IT-szektorban. Az észak-koreai távmunka megjelenése az IT területén a kiberkémkedés, a számítógép-hálózatok felderítésének és a szankciós politika megkerülésének (illegális finanszírozás) kockázatát hordozza magában.[35]

A pénzügyi szektor leggyakoribb célponttá válásával párhuzamosan nőtt a kibertámadó képességek stratégiai beágyazottsága a Kim-rezsim biztonságpolitikai felfogásába. Ez egyrészt egybevág a világviszonylatban is jellemző célpontkiválasztási trendekkel, másrészt viszont praktikus okokra is visszavezethető Észak-Korea elszigeteltnek mondható nemzetközi helyzetében. A biztonságpolitikai megközelítést is alkalmazó szakirodalom az észak-koreai kibertéri műveletek egyik mérvadó stratégiai céljaként tekint az ország nukleáris és haderőfejlesztési programjának finanszírozására. Ez abban mutatkozik meg, hogy a kriptovaluták és az elektronikus pénzeszközök alkalmasak az ENSZ szankciós rezsimje által érintett termékek és nyersanyagok ellentételezésére is. A korábbi években több forrás is megerősítette, hogy a phenjani rezsim a katonai erő fenntartásához és fejlesztéséhez szükséges anyagi erőforrásokat többek között a kibertér által lehetővé tett illegális finanszírozással vagy kriptovaluták ellopásával fedezte. Például a Pentagon (az USA Védelmi Minisztériuma) az észak-koreai kibermőveletek tervezéséért és végrehajtásáért felelős Központi Felderítő Irodát (RGB) terror- és illegális műveleteket végrehajtó állami szervként tartja számon. Az USA bilaterális alapon több alkalommal is szankcionálta az RGB-t a szervezethez kötődő vállalkozásokon keresztül: 2010-ben fegyverkereskedelem, majd pénzmosás miatt, ezt követően 2015-ben a Sony Pictures-t ért incidens miatt.[36]

Ezt az összefüggést támasztja alá a Chainalysis (blokkláncelemző vállalat) felmérése is, amelynek számításai alapján a 2021-ben okozott kár mintegy 429 millió dollár értékű kriptovaluta volt, ami 2022-ben ennek négyszeresére, megközelítőleg 1,7 milliárd dollárnak megfelelő értékre emelkedett. Az elemzőcég a 2022-ben bekövetkezett globális kárérték (3,8 milliárd dollár) 44%-ának bekövetkezését köti észak-koreai hátterű kriptovalutákkal való visszaélésekhez.[37] Ezzel párhuzamosan Phenjan 2022-ben hajtotta végre eddigi legnagyobb volumenű rakétafegyverzet-kísérletét, amely a CSIS kutatóintézet adatbázisa alapján legalább 70 hordozóeszközteszt

[33] Barnhart et al. 2023.
[34] Kong–Lim–Kim 2019: 2–6.
[35] US. Department of Treasury 2022.
[36] Ha–Maxwell 2018: 4.
[37] Chainalysis Team 2023.

végrehajtását jelentette, ami a korábbi átlagos éves mennyiség négyszerese.[38] Phenjan számos indítóplatformot és eltérő hatótávolságú eszközt tesztelt, ennek kapcsán kiemelhető, hogy a hiperszonikus sebesség elérése és az önállóan célra vezethető (MIRV) visszatérő fejek (a rakéta harci része) alkalmazása egyaránt elképzelhető fejlesztési irány lehet a ballisztikusrakéta-eszközök tekintetében. Ezenkívül a nemzetközi megfigyelések szerint legalább 6 alkalommal teszteltek olyan robotrepülőgépeket *(cruise missile),* amelyek egyes típusai nukleáris robbanófejek[39] hordozására is alkalmassá tehetők.[40] A robotrepülőgépek ezen alternatív fejlesztési irányának kialakítását egyaránt kiválthatta a hegyi-karabahi fegyveres konfliktusban és az ukrajnai háborúban alkalmazott drónok és robotrepülőgépek taktikai hatásának eredményessége, ami komoly kihívást jelent a kiber-, az elektronikai és a légvédelem számára. Az észak-koreai fegyverzetkísérletek növekedésének és fenntarthatóbb finanszírozhatóságának további nemzetközi relevanciája, hogy az ukrán fronton (az iráni és török gyártmányú eszközök mellett) a későbbiekben észak-koreai irányított fegyvertípusok is feltűnhetnek, akárcsak a gázai övezeben, mivel az észak-koreai fél a múltban is adott el fegyvereket palesztin szélsőségeseknek.[41]

Mérvadó trend továbbá, hogy az észak-koreai hátterű aktorok (például: APT37, APT38, APT43 és egyéb kibertéri egységek)[42] célpontkiválasztásában, alkalmazott eljárásaiban és eszközeiben (például rosszindulatú kódjaiban) egyre nagyobb átfedések mutathatók ki. A Mandiant álláspontja szerint ez a jelenség az egyedi TTP-k (vagyis taktika, technikák és eljárások) egymás közti megosztására, továbbá műveletszervezési újításra utalhat. Ez alapján feltételezhető az APT-tevékenységhez kapcsolható észak-koreai hírszerző vagy katonai intézmények szervezeti és strukturális átalakítása (lásd *Kiberképességek adaptációja az észak-koreai hadviselési kultúrába* című fejezet). Egy ilyen típusú átalakítás alátámasztja, hogy miért bővülhetett az észak-koreai APT-csoportok támadói profilja a pénzügyi szektorbeli célpontokkal. Emiatt a Mandiant kutatói ugyanerre a jelenségre vezetik vissza a blokklánc *(blockchain)* és fintech vertikumot célzó támadások dinamikus növekedését.

Phenjan egy összehangolt célpontkiválasztáson és közösen felhasználható eszközrendszeren alapuló képességfejlesztéssel nemcsak racionalizálhatja az offenzív kibertéri tevékenységét és még nehezebben átláthatóvá teheti nemzeti kibertéri környezetét *(cyber threat landscape),* hanem a működésbeli átfedésekkel megnehezítheti az attribúciós kísérleteket is.[43] Mindemellett, amennyiben a 3CX Desktop App (kommunikációs szolgáltatásokat nyújtó szoftver) 2023. tavaszi kompromittálása kapcsán beigazolódik, hogy az UNC4736 azonosítóval ellátott tevékenység valóban észak-koreai hátterű művelet, úgy ez lesz az első úgynevezett kaszkádszerű hatással bíró hálózati behatolás, amely során észak-koreai aktorok kormányzati intézmények beszállítói láncát kompromittálták.[44] A Mandiant incidens kivizsgálására felkért szakértői a kezdeti behatolási

[38] Missile Defense Project 2023.
[39] Amennyiben sikeres lesz az észak-koreai miniatürizálási fejlesztés. Ez a képesség megléte még vitatott a szakemberek körében.
[40] Kertész 2023.
[41] Ramani 2023.
[42] Például az egyes esetekben gyűjtőfogalomként is használt csoportok, mint a Lazarus vagy az Andariel.
[43] Barnhart et al. 2023.
[44] Johnson et al. 2023.

vektort a Trading Technologies által biztosított X_Trader szoftvercsomag manipulált telepítőjére vezették vissza (amelyben Windows- és Mac-verziók egyaránt érintettek voltak). Az UNC4736 trójai típusú módszerrel érte el a legitim függőségnek álcázott *(legitimate dependency)* két rosszindulatú DLL-modul futtatását (SIGFLIP és DAVESHELL) és a Veiledsignal rosszindulatú program és moduljainak telepítését *(multi-stage modular backdoor),* amelyek egy többlépcsős folyamat során hátsó kaput nyitottak az érintett hálózatokba. A Veiledsignal backdoor két DLL-modulja a Chrome, a Firefox és az Edge webböngészők kommunikációjába történő folyamatbefecskendezést *(process injection module)* és a C2 kiszolgálóval való kommunikációt tette lehetővé (*command-and-control:* C&C modul).[45]

Észak-Korea kibervédelmi és digitális ökoszisztémája

Noha Észak-Korea relatív elmaradottságát és szegénységét a múltban gyakran szemléltették ritkás közvilágítást kiemelő éjszakai műholdfelvételekkel és az elektromos hálózat megbízhatatlanságáról szóló hírekkel, napjainkra a belföldi telefónia és egyéb hálózati szolgáltatások lefedettsége kielégítő mértékű. Az ország első (2G) mobilhálózatának telepítése 2002-ben indult el, de 2004-ben hirtelen leállították a projektet, egy hónappal azután, hogy Rjongcshonban robbanás történt egy vasútállomáson. A detonáció a város nagy részét lerombolta, és állítólag több ezer ember életét követelte. Az eset további nemzetbiztonsági relevanciája azonban az volt, hogy a vonat, amelyen Kim Dzsongil utazott, órákkal korábban haladt át a rjongcshoni állomáson. Emiatt az a híresztelés terjedt el, hogy a detonáció egy mobiltelefon használatával indított merényletkísérlet volt, és az észak-koreai hatóságok eszerint jártak el (egyebek mellett a mobiltelefonok használatát is betiltották).[46]

Észak-Korea napjainkban is működő két celluláris hálózatának egyikét, a Koryolink nevű belföldi mobilhálózatot az Orascom Telecom Media & Technology (OTMT) és a koreai Korea Posts and Telecommunications Co. (KPTC) kezdte el kiépíteni 2008 decemberében.[47] A Koryolink 2011-re stabil 3G-szolgáltatást nyújtott, amelynek lefedettsége kiterjedt Phenjanra, 15 nagyvárosra, több mint 100 kisvárosra, valamint néhány autópályára és vasútvonalra. Az ország egészéhez mérten ekkor 14%-os volt a területi lefedettség, amivel a lakossági részarány meghaladta a 90%-ot, 1,7 millióra becsülhető előfizetői bázissal.[48] A Kryolink profitmegosztása miatti 2015-ös viták következtében egy másik, „riválisˮ 3G adatátvitelt kínáló szolgáltatót hoztak létre, a Kangsongot, amely már kizárólagos kormányzati tulajdonban van, és teljes celluláris hálózati lefedést kínál Észak-Korea vidéki területein is.[49] Napjainkban is ez a két 3G-szolgáltatás működik a KNDK-ban, többek közt műholdfelvételek által igazoltan.

[45] Symantec Threat Hunter Team 2023.
[46] Williams 2019.
[47] A Koryolink szolgáltatást 75%-ban egy egyiptomi származású vállalkozó, Naguib Sawiris birtokolja az Orascomon keresztül, amely többségi tulajdonosa a kivitelező Cheo Technology vállalkozásnak. A tulajdoni hányad fennmaradó része a koreai Postaszolgáltatási és Távközlési Minisztérium birtokában maradt, a Koryolink márka mögött álló másik vállalaton (Korea Post and Telecommunications Co.) keresztül.
[48] Montlake 2012.
[49] Williams 2015.

A 4G- (és akár 5G-) adatátvitelt lehetővé tévő infrastruktúra-fejlesztést várhatóan a Huawei vállalat fogja kivitelezni, ám a celluláris technológiai generációváltás megkezdésének céldátuma még kétséges (habár ezzel kapcsolatos kutatási projektekről a Kim Irszen Egyetem már közzétett tudományos publikációkat). Feltételezhető, hogy a 2G- és 3G- infrastruktúra kiépítéséhez hasonlóan Észak-Korea ez esetben is a más szolgáltatók hálózatfejlesztése során piacra kerülő használt eszközöket építi be rendszerébe.[50]

A Koryolink máig a világ egyik legjobban kontrollált rendszerének tekinthető. Az észak-koreai előfizetők részére csak belföldi hívásokat és helyben hosztolt adatszolgáltatást tesz lehetővé (ami tulajdonképpen az erősen cenzúrázott és megfigyelt észak-koreai intranet kialakítását jelentette). A külföldi (előfizetők diplomaták és turisták) ellenben nem kezdeményezhetnek belföldi hívásokat, és kizárólag a globális internetes tartalmakhoz férhetnek hozzá, az észak-koreai intranethez nem. Ezeken felül a társadalom szűk, privilegizált rétege számára egy elkülönített hálózati szabály áll rendelkezésre, amely kivételként azonosítja az állam által kiadott, hazai titkosító algoritmussal ellátott mobiltelefonokat, így azokról lehetséges a külföldi hívások lebonyolítása (és elméletben mentesülnek a normának számító belföldi lehallgatás alól). Ezen kiadott mobileszközök száma a legutóbbi nyilvános forrás szerint körülbelül ezerfős kvótát jelentett (2008 körül), ami megegyezik a phenjani legfelső vezetés becsült létszámával.

A Koryolink felügyeleti és megfigyelési megoldásainak kialakításához, a celluláris környezet 2008-as kialakításától kezdve, kínai technológiai vállalatokat vontak be szakértőként. A Huaweit bízták meg a hálózati eszközök beszerzésével és annak kialakításával, hogy a titkosítási rendszer nem okoz-e instabilitást a hálózat működésében, míg a Panda International Information Technology Co. dolgozott a rendszer szoftveroldali kialakításán. A Koryolink belbiztonsági célú, törvényes lehallgatási kapacitásáról (*legal interception gateway,* LIG) ugyancsak 2008-as, a Huawei által készített tervdokumentumok adatai állnak rendelkezésre: így az infrastruktúra kezdetben legfeljebb 7 terabájtos tárolókapacitás mellett, 1200–2500 célpontot támogathatott, és egyidejűleg legfeljebb 240–300 telefonhívás és 250–300 adatmunkamenet megfigyelésére lehetett képes.

A kivitelezési tervek második fejlesztési szakaszában, 10 terabájtos adattároló kapacitással 5000 célpontra és további 300 telefonos és adatátviteli munkamenetre növelték volna az egyidejűleg történő megfigyelés hatókörét. A megfigyelőközpont a kivitelezés első és második szakaszában akár 180–200 felhasználót is támogathatott, amelyből 60–80 operátor egyidejűleg kapcsolódhatott be a hálózati forgalomba. Az akkori technológiai standardoknak megfelelően az adatmegfigyelő rendszer a HTTP (weboldalak), FTP (fájlok fel- és letöltése), SMTP, POP3 és IMAP4 (e-mail) protokollokat támogatta.[51]

Az észak-koreai belföldi mobiltelefon-szolgáltatás kiépítésével és a kommunikációs csatornák megfigyelőrendszerének kialakításával párhuzamosan a phenjani vezetés megkezdte az illegálisan és legálisan behozott kínai mobiltelefonok (és a későbbiekben

[50] Williams 2023b.
[51] Williams 2019.

az okostelefonok) eszközfelügyeletének állami megvalósítását. Erre egyfelől azért volt szükség, mert az országba csempészett kínai mobiltelefonok lehetővé tették a határ menti területeken (ahol elérhető a kínai mobiltelefonos hálózat) élő emberek számára, hogy beszélhessenek a Kínában vagy Dél-Koreában élő rokonokkal, barátokkal. Ez a felügyelet nélküli kommunikációs csatorna olyan kockázatokat teremtett, amelyek megkönnyítik a nemzetbiztonsági szempontból értékes információk kiszivárgását vagy a csempészhálózatok észrevétlen, hatékony fenntartását. Számos Dél-Koreában élő disszidens úgy lép kapcsolatba a hozzátartozóival Észak-Koreában, hogy ezeket az illegális mobiltelefonokat eljuttatja az országba közvetítőkön vagy csempészeken keresztül.

Az illegális mobiltelefonok használata elleni kormányzati fellépés módszeréről nincs publikusan elérhető, hiteles információ,[52] azonban a legálisan birtokolt (regisztrált) kínai mobiltelefonokat kompenzáció nélkül elkobozták a kétezres évek elején, és saját eszközök fejlesztésébe (ezek számos beépített felügyeleti megoldást tartalmaznak) és államilag kontrollált elosztásába kezdtek, immár a társadalom szélesebb körében.[53] A 2020-as pandémiát megelőzően az állami híradások (KCNA News) rendszeresen számoltak be a hazai okostelefonok, SIM-kártyák kifejlesztésével és a phenjani publikus wifihálózat (a Mirae) területi lefedettségének kiterjesztésével kapcsolatos technológiai sikerekről.[54]

A globális internethez legálisan a társadalom szűkebb rétegei, például az ország főbb egyetemeinek informatikai karán tanuló hallgatók, egyes nagyvállalatok és kormányzati szervezetek munkatársai férhetnek hozzá kutatási vagy kereskedelmi céllal, a phenjani vezetés politikai és kulturális narratívájától eltérő információknak való kitettség miatt. A telekommunikációért felelős észak-koreai Postaszolgáltatási és Távközlési Minisztérium (Ministry of Post and Telecommunications, 체신성) felügyeli a hálózati kommunikációs csatornákat (így a globálisan is elérhető internetet) és hajtja végre a tartalomszűrést, vagyis a „nyílt" internet cenzúrázását.

A globális internetszolgáltatás elérhetősége területileg is korlátozott, hivatalosan (értsd: az állam által legálisan biztosítva) Phenjanból és a kereskedelmi és gazdasági érdekeltség miatt a különleges státuszú zónákból (például az ipari termelőközpont, Keszong vagy a kikötőváros, Raszon) hozzáférhető.[55] Észak-Korea világhálóhoz történő hozzáférését kezdetben kizárólag legnagyobb stratégiai partnere és szövetségese, a Kínai Népköztársaság garantálta a Star Joint Venture Co. nevű hálózat- és internetszolgáltatón keresztül. A vállalat mintegy 1024 IP-címet tartott fenn a 175.45.176.0 és 175.45.179.255 közötti tartományban az észak-koreai megrendelő részére, amelyeket többek közt az ország hivatalos hírportáljai (KCNA, Rodong Sinmun) is használnak.[56]

[52] A műholdas lehallgatást megakadályozó zavaró rendszer kiépítéséhez a KPTC egy 11,4 millió euró értékű elektronikai gyártó- és tesztberendezéseket tartalmazó listát adott át az Orascomnak, 6 db Rohde & Schwarz FSP40 spektrumanalizátor, valamint 3 db Rohde & Schwarz FSQ26 jelanalizátor beszerzését igényelhették. A következő években azonban több jelentés is említést tesz arról, hogy a német gyártmányú mobiltelefon-érzékelő berendezések segítségével az Állambiztonsági Minisztérium a határ menti területeken kínai mobiltelefonokat használó észak-koreaiakat fogott el. Bővebben Williams 2019.

[53] Kim 2014: 7–9.

[54] Williams 2023b.

[55] Williams 2014.

[56] Noland 2009: 62–74; Williams 2011.

Észak-Korea 2010-től a Korea Post and Telecommunications Co. (KPTC) vállalaton keresztül 256, szintén kínai IP-címet használhat a China Unicom (vagy United Network Communications Group) nemzetközi nagyvállalat szolgáltatása révén, amelyek a 210.52.109.0 és 210.52.109.255 hálózati azonosítók közé esnek.[57] A két szolgáltatótól való függés magas kitettséget eredményezett a hálózati hozzáférést megszakító, túlterhelő vagy ellehetetlenítő módszereknek, amire konkrét példát hozott 2014-ben a Sony Pictures-t ért észak-koreai támadásra reagáló amerikai válaszcsapás.[58] Az internetszolgáltatás diverzifikációját Észak-Korea 2017 októberére tudta megvalósítani, amikor Oroszországgal kötött megállapodást arról, hogy a TransTeleCom vállalat biztosít hozzáférést a világhálóhoz.[59] Az egyezség híre még jobban megterhelte a 2017-es interkontinentális ballisztikusrakéta-kísérletek (ICBM) miatt egyre súlyosbodó KNDK–USA viszonyt, ezért az amerikai fél kibertámadást indított a frissen felállított infrastruktúra ellen, ami ideiglenesen a hozzáférés teljes megszűnéséhez vezetett.[60]

Kiberképességek adaptációja az észak-koreai hadviselési kultúrába

Általánosságban elmondható, hogy az észak-koreai hadviselési kultúra ötvözi az irreguláris hadviselés sajátosságait és az aszimmetrikus képességeket, ez utóbbi egyik sarokköve a stratégiai elrettentést biztosító nukleáris triád kifejlesztésére való törekvés. Külföldre irányuló – főleg Japán és a Koreai Köztársaság (a továbbiakban Dél-Korea) elleni – műveleteit mélységi szinten hajtotta végre, amelyek jellemző formái a rajtaütések és a kommandós támadások voltak (például a dél-koreai elnöki palota, a Kék Ház elleni 1968-as rajtaütés), titkosszolgálati műveletek (köztük japán állampolgárok elrablása az 1970-es és 80-as évek fordulóján)[61] és orvtámadások, szabotőr akciók, valamint bombatámadások és merényletek.[62]

Az 1991-es Öbölháború, az 1999-es koszovói háború és a 2003-as iraki háború tapasztalatai rávilágítottak az információs fölény jelentőségére, és egyre sürgetőbbé tették a modernebb, hálózatba kapcsolt harceszközök által lehetővé váló, C4ISR-en alapuló vezetés-irányítás kialakítását, megváltoztatva a hadviselési feltételeket és kultúrát.[63]

A KNDK kibervédelmi stratégiájának megvalósítása szempontjából meghatározó, hogy Kim Dzsongil vezetése alatt 1996-ig végbementek a Koreai Néphadsereg (Korean People's Army, KPA) vezetés-irányítási struktúráját hálózatosító reformok, emellett (nagyjából 2002–2010 között) létrehoztak egy egyedül észak-koreai

[57] Jun–LaFoy–Sohn 2015: 53 és az APNIC adatbázisa alapján: https://wq.apnic.net/static/search.html
[58] Először fordult elő, hogy az USA nyilvánosan attribútálta egy államhoz az APT-tevékenységet, és nyíltan felvállalta a megtorló intézkedést. Az USA kiberművelete 2014. december 22–23. között 9 órán át tette elérhetetlenné Észak-Koreában a teljes internethálózatot, és szolgáltatáskiesést okozott az elektromos infrastruktúrában. Bővebben NATO CCDCOE [é. n.].
[59] Williams 2017.
[60] Wagstaff–Auchard–Kiselyova 2017; DeYoung–Nakashima–Rauhala 2017.
[61] Kato 2017.
[62] Csoma 2006: 25–31.
[63] Tóth 2022.

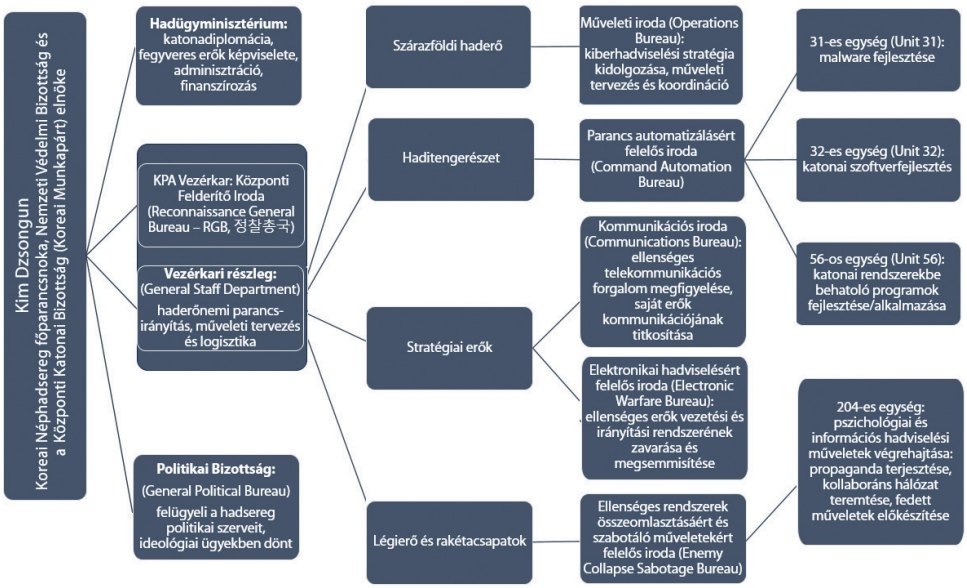
területről hozzáférhető internetstruktúrát, a Kvangmjongot (광명망, light network).[64] Az ország ezenkívül rendelkezik még három önálló kormányzati, katonai és nemzetbiztonsági intranethálózattal. A Bangpe (방패, „pajzsok", katonai célú), a Gumbjol (금별, „arany csillag") és a Bulgungom (붉은검, „vörös kardok") nevű hálózatok biztosíthatják a hadsereg irányítási láncának folytonosságát és más létfontosságú ellátórendszerek folyamatos üzemeltetését támadás esetén.[65] Ezzel párhuzamosan, Kim Dzsongil vezetése alatt, a phenjani védelempolitika felismerte, hogy az USA és szövetségesei hálózatosított haderejének aszimmetrikus erőfölénye mellett a folyamatosan fejlődő információs társadalmak sérülékenyek és kitettek a kibertérből érkező bomlasztó műveleteknek.

E gondolkodásmód kialakítására hatást gyakorolt a KNDK térségbeli szövetségese, a Kínai Népköztársaság. Kína a „korlátok nélküli hadviselés" elméleti keretrendszerének 1999-es publikálása nyomán emelte be saját hadviselési kultúrájába az információs társadalmak sérülékenységét.[66] Ezek alapján a phenjani rezsim logikus fejlődési utat járt be az információs műveletek alkalmazásával és vele együtt az elektronikai hadviselés és kibertámadó képességek beemelésével Észak-Korea érdekérvényesítő eszköztárába, amivel az ellenséges nemzetek belső politikai-társadalmi kohéziójának megbontására törekszik. Az észak-koreai katonai vezetési struktúrában a kiberműveleteket végrehajtó katonai egységek nagyrészt két csoportra oszlanak. Az egyik a Koreai Néphadsereg vezérkari részlege (Korean People's Army General Staff Department, KPA GSD), a másik a fentiekben is említett Központi Felderítő Iroda. A következőkben ezen szervezetek funkcióját mutatjuk be az észak-koreai haderőn belül.

Kim Dzsongil vezetése alatt, a 2000-es évek elején, a hadseregen belül kialakított elektronikai és informatikai képességek elsődleges funkciójaként a vezetés-tervezés-irányítás folyamatát biztosító rendszerek védelmét határozták meg (a KNDK-ban parancsautomatizáció biztosításának nevezték). Ezen védelmi fókuszú koncepció kibővítéséről a Koreai Néphadsereg publikálta 2005-ben Kim Dzsongil elektronikai hadviseléssel elérhető hatásokról tartott *(Electronic Warfare Referrence Guide)* közvetlen beszédét, amelyben a vezető kulcsfontosságú, művelettámogató és tartalék erőként jellemezte a kibertérben műveleteket végrehajtó egységeket. Kim ezáltal stratégiai szinten prioritásba helyezte a kiberképességek kiépítését. A haderőbe történő adaptáció strukturális alapjait a 2009–2010-es reformok teremtették meg, először haderőnemi kereteken belül.

Észak-Korea valószínűsíthető információs hadviselési stratégiai koncepcióját egy 2003-ban Dél-Koreába menekült disszidens – Kim Heungkvang, aki a Hamheung Egyetem informatikai karának professzora volt – segítségével tárták fel, a 2009–2010-es reformot követően megismert szervezeti struktúra alapján. A haderőnemekhez tartozó egységek információs és elektronikai műveletek tervezésére és végrehajtására voltak képesek, felépítésüket az 1. ábra szemlélteti.

[64] North Korean Internet: List of Internal Kwangmyong Websites. 2021. Bővebben: https://github.com/Alyzana/kwang-myong-addresses/blob/master/sites-en
[65] Jun–LaFoy–Sohn 2015.
[66] Bartók 2018.



1. ábra: Észak-Korea kiberhadviselési műveletekért felelős katonai struktúrájának ismert részlete

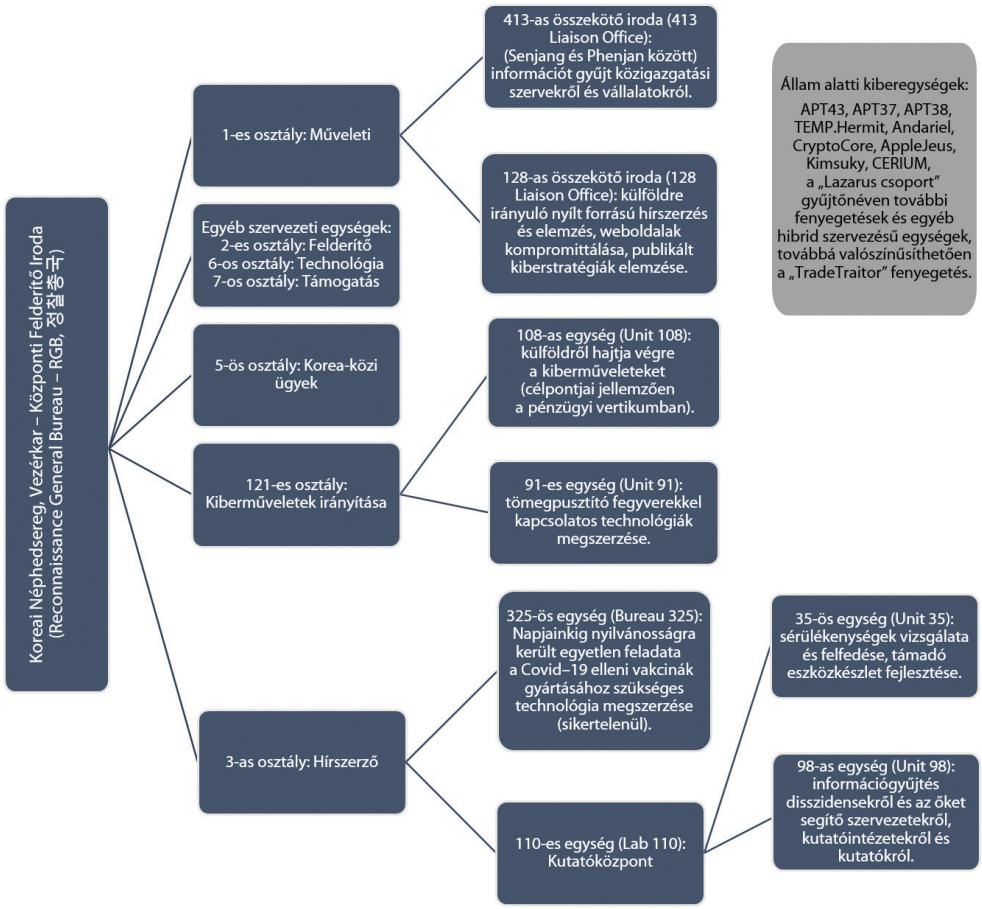
Forrás: a szerző szerkesztése a dél-koreai védelmi minisztérium 2018-ban kiadott védelmi fehér könyve[67] *és* Kong–Lim–Kim *2019 elemzése*[68] *alapján*

A haderőnemi szervezeten belüli kiber- és elektronikai műveleti egységek irányítását az összhaderőnemi erőkifejtés jegyében a vezérkar (General Staff Department, GSD) koordinálja. Tevékenységüket békeidőszakban (értsd: provokációs célú) a konvencionális műveletek támogatására korlátozták.

Ezt a feltételezést támasztja alá, hogy a Koreai Néphadsereg elektronikai műveleti egységei a 2010-es Jonphjong-szigetet érő bombázást megelőzően sikeresen zavarták egy dél-koreai AN/TPQ–37 radar működését.[69]

A Koreai Néphadsereg vezérkarának felderítő részlegén, az úgynevezett Központi Felderítő Irodán belül alakították ki a komplex(ebb) kiberműveleti képességet. Az RGB ismert szervezetrendszere, amelyet a 2. ábra mutat be, az önálló kiberműveletek megtervezését és végrehajtását támogatja, többek között belföldi és külföldi (összekötő irodák) telepítésű egységek révén, amelyeket az állam alatti kiberegységek tevékenysége egészít ki.

[67] ROK Ministry of National Defense 2018: 28.
[68] Kong–Lim–Kim 2019: 4.
[69] Jun–LaFoy–Sohn 2015: 37.



2. ábra: Az észak-koreai Központi Felderítő Iroda (RGB) szervezeti struktúrájának ismert részlete
Forrás: a szerző szerkesztése KONG–LIM–KIM *(2019)*[70] *és a CSIS tanulmányainak*[71] *információi alapján*

Az észak-koreai államigazgatási szervezetrendszeren belül az RGB jelentős autonómiát élvező szervként látja el feladatkörét, és közvetlen beszámolási kötelezettsége van Észak-Korea legmagasabb politikai döntéshozó szerve, a Koreai Munkapárt Politikai Bizottsága felé.[72] Szervezeti struktúráját tekintve a felderítő tevékenységi körök 6 főbb divízió (a 2. ábrán osztály) hatásköre alá vannak delegálva: műveleti, felderítő, hírszerző, Korea-közi ügyek, technológiai és támogató osztályok, amelyek tevékenysége főként

[70] KONG–LIM–KIM 2019: 4.
[71] JUN–LAFOY–SOHN 2015: 39–44.
[72] HA–MAXWELL 2018: 4.

japán, dél-koreai és amerikai műveletekre koncentrálódik.[73] Kim Heungkvang kiberbiztonsági területen dolgozó észak-koreai disszidens[74] beszámolója alapján ezen divíziókon kívül helyezkedik el a 121-es osztály műveleti területe. A megközelítőleg 500 fős egységet dél-koreai kutatásokban és védelmi dokumentumokban gyakran nevezik elektronikus felderítési vagy kiberhadviselés-irányító osztálynak (Bureau 121, Cyber Warfare Guidance Bureau vagy Electronic Reconaissance Bureau),[75] mert a kompetenciájába olyan műveletek tartoznak, mint a pénzügyi rendszerek elleni offenzív tevékenység; hírszerzési vagy technológiai (általában katonai fejlesztések) adatok kinyerése akár számítógépes rendszerekbe való behatolás által; sérülékenységek feltárása és támadóeszközök fejlesztése.[76]

Kim Dzsongun 2011-es hatalomra kerülése után közvetlenül a Koreai Munkapárt Belügyi Bizottsága (KKP State Affairs Commission) alá rendelték a kibertérben operáló egységeket (3. ábra). A testület Kim elnökletével működik, így az átszervezés jól mutatja az új vezető hatalom koncentrációját és bizalmasai körének törekvését a békeidőbeli információs műveletek feletti kizárólagos befolyás megszerzésére (a haderő legfelsőbb vezetői körével szemben).[77] Kim Dzsongun vezetése alatt 2012-re megduplázták az RGB és a GSD személyi állományát, így dél-koreai hírszerzési források szerint körülbelül 3000-ről megközelítőleg 6000 főre emelkedett a létszámuk, miközben a szervezetek feladatrendszerét és képességeit is bővítették, ezáltal nyilvánvalóvá vált, hogy az észak-koreai aszimmetrikus hadviselési keretrendszeren belül a kiberképességek önállóan is megjelentek műveleti szinten, nem csak harci támogató feladatkörben.[78] (Ezt igazolja az észak-koreai vezetőt lejárató film miatt 2014-ben politikai okokból indított, erődemonstrációs célú kibertámadás a Sony vállalat ellen.) A dél-koreai védelmi minisztérium kalkulációja alapján 2018-ra a kibertéri műveletek végrehajtására szakosodott állomány megközelítőleg 6800 fős lehetett.[79] Az állomány várható növekedésének kalkulációja kapcsán korlátozott információk állnak rendelkezésre. Az észak-koreai oktatásban már az alapszintű képzés alatt megkezdődik a matematika iránt fogékony hallgatók kiválasztása, akik középiskolai szakirányú tanulmányaikat már elkülönített, kiváltságosnak számító csoportokban folytatják, így későbbi tanulmányaik során informatikai képzést kaphatnak. A középiskolák legjobban teljesítő tanulói jelentkezhetnek a hazai felsőfokú informatikai képzésre: a Kim Irszen Egyetemre, a Mirim Egyetemre (katonai), a Kim Csaeng Egyetemre, a phenjani Pjongszung Tudományegyetemre és a Phenjani Informatikai Egyetemre. Ezen intézmények hallgatói kiválóságai az RGB vagy a GSD állományába kerülhetnek. Emellett a Kim Csaeng Egyetemen működik egy hallgatói képességeket fejlesztő

[73] Észak-Koreában az egyes közigazgatási szervek igazgatási egységeit számokkal jelölik, amelyek között megtalálhatók irodák vagy osztályok *(bureau)*, egységek *(unit)* és összekötő irodák *(liaison office)*, ezek általában külföldi kirendeltségű feladatellátó egységek és irányítóközpontok közötti kommunikációért felelnek.

[74] Kim Heungkvang az észak-koreai értelmiségek szolidaritási mozgalmának *(North Korean Intellectuals Solidarity)* alapítója, amely csoport kutatásaival és kampányaival Észak-Korea felszabadításáért és a disszidensek életkörülményeinek javításáért küzd. A csoport információit a dél-koreai Egyesítési Minisztérium és a védelmi szervek egyaránt használják a KNDK védelmi és offenzív képességeinek feltérképezésekor.

[75] Miller 2018.

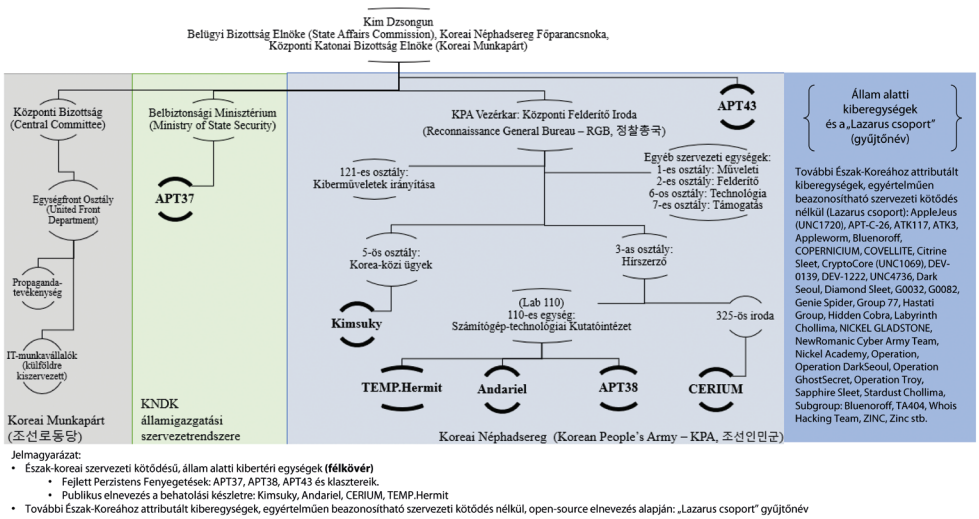
[76] Jun–LaFoy–Sohn 2015: 40–44.

[77] Kong–Lim–Kim 2019: 2–6.

[78] Gause 2015: 38.

[79] Kong–Lim–Kim 2019: 3.

központ, amelyet az észak-koreai programozói feladatokat, kutatásokat és képzéseket koordináló Koreai Számítástechnikai Központ (Korean Computer Center) tart fenn.[80] Az állomány képzése külföldön is zajlik, számottevő észak-koreai hallgatói közösség folytatja programozói és informatikai tanulmányait például India és Kína egyetemi képzésein, szoros nemzetbiztonsági felügyelet mellett.[81] Egy észak-koreai disszidens, aki korábban magas rangú tisztviselő volt, azt vallotta, hogy az ország évente 50–60 elit katonát küld külföldre, hogy informatikát tanuljanak, akik később akár offenzív területeken, kibertámadóként a Központi Felderítő Iroda vagy más irreguláris egységek személyi állományába kerülnek.[82]



3. ábra: A Koreai Népi Demokratikus Köztársaság állam alatti kiberegységeinek szervezeti kötődése

Forrás: a szerző szerkesztése a Mandiant 2023-as jelentése[83], Malpedia adatbázisa[84] és Kong–Lim–Kim 2019 elemzése[85] alapján

A phenjani rezsimhez köthető állam alatti kiberegységek (értsd: kiberbűnözői és egyéb hackercsoportok) ismert szervezeti beágyazottságát a 3. ábra mutatja be. Az Észak-Koreához köthető állam alatti fenyegető csoportok számontartása és elkülönítése nem egységes nemzetközi szinten. Az APT-k és klasztereik tevékenységét más-más kódnéven jegyzik az elemzőközpontok, továbbá a különféle fenyegető aktivitások elnevezése egy-egy kampányból ered (open-source módon például Kimsuky vagy DarkSeul), vagy csak összefoglaló jelleggel *Lazarus-csoport* néven vezeti a szakmai

[80] Jun–LaFoy–Sohn 2015: 52–53.
[81] Egy hallgatóhoz egy nemzetbiztonsági szervhez tartozó felügyelő van kirendelve.
[82] Han 2016.
[83] Barnhart et al. 2023.
[84] Malpedia 2024.
[85] Kong–Lim–Kim 2019: 4.

közösség a detektált eseteket nyilvántartásaiban.[86] Tovább nehezíti a tényleges észak-koreai „állami támogatású hackercsoportok" számának meghatározását, hogy az azonos eszközöket alkalmazó kampányokért más-más csoport vállal felelősséget nyilvánosan, így meglátásom szerint felmerül az a lehetőség, hogy azok létrehozása is eseti jellegű lehet, és a támadó személyek ugyanazok. Az egyes csoportok mögött a Központi Felderítő Iroda vagy a Koreai Néphadsereg egységeinek tagjai lehetnek, akiket *ad hoc* jelleggel válogatnak össze a különböző típusú, például kiberkémkedési kampányokra. A MITRE ATT&CK által önálló egységként jegyzett Lazarus (ID: G0032)[87] tevékenységéhez kötődnek az eddigi legjelentősebb károkat okozó támadások, feltehetőleg 2009 óta aktív az egység, azóta főleg a pénzügyi és magánszektort érintő célzott kibertámadások kötődtek hozzá. Ennélfogva tevékenységével az APT38 profilja is átfedésbe kerül, azonban jelentős, egyedül pusztító céllal indított, politikailag motivált kibertámadások is köthetők hozzá nyilvános attribúció alapján. Az APT38 és feltételezhetően a Lazarus csoport egyik ismert tagja Park Dzsinhjok, akit a Sony elleni támadásért és a WannaCry zsarolóvírus bevetéséért tett felelőssé az USA, ám nem fogták el, ezért igazságszolgáltatás elé egyelőre nem került, így az eset kiberdiplomáciai lépésként értékelhető. A Lazarus csoport további hírhedt kampánya a dél-koreai főváros villamosenergia-hálózatát érő DarkSeoul támadás és a 2011-es Ten Days of Rain nevű dél-koreai kormányzati weboldalakat és az Egyesült Államok Dél-Koreában állomásozó katonai egységének rendszerét érő túlterheléses támadássorozat (*distributed denial of service* – DDoS), amely kampány során a támadók által használt malware 10 napon keresztül elérhetetlenné tette a rendszert, majd törölve önmagát, használhatatlan állapotban hagyta a megfertőzött eszközt.[88] A Lazarusra (ID: G0032) jellemző programozási stílust, célpontkiválasztást és támadási módszereket (továbbiakban összefoglaló néven TTP, *tactics, technics and procedures*) több csoport is alkalmazta, ezért alcsoportjai, feladat-orientált műveletszervezési elvek mentén létrehozott *ad hoc* egységei vagy alternatív elnevezései is lehetnek (4. ábra).[89] A *Kimsuky csoport,*[90] amelyet először 2013-ban regisztráltak, elnevezését a célzott adathalász e-mailjeit küldő fiktív személyről, Kim Szukjangról kapta. A csoport dél-koreai kutatóintézetek és az Egyesítési Minisztérium ellen folytat kiberkémkedési tevékenységet trójai vírusok segítségével.[91] A Kimsuky által használt TTP szintén nagy hasonlóságot mutat a Korea Hydro & Nuclear Power vállalat elleni incidenssel, amely a dél-koreai atomenergia-szektort fenyegette.[92] Az APT37[93] és APT43 csoportok műveletei pedig

[86] Lásd a Malpedia adatbázisa: Malpedia 2024.
[87] MITRE ATT&CK 2023.
[88] McAffee 2011: 3.
[89] „A Lazarus Group további ismert azonosítói: Dark Seoul, Hidden Cobra, Hastati Group, Anderiel, Unit 121, Bureau 121, NewRomanic Cyber Army Team, Bluenoroff, Guardians of Peace. A csoport karakterisztikája összefüggést mutat további APT tevékenységekkel, mint pl. Group 77, Labyrinth Collima, Operation Troy, Operation GhostSecret, Operation AppleJeus, APT38, Stardust Chollima, Whois Hacking Team, Zinc, Appleworm, Nickel Academy, APTC-26, NICKEL GLADSTONE, COVELLITE." Berzsenyi 2023: 124.
[90] „A Kimsuky további ismert azonosítói: Velvet Chollima, Black Banshee, Thallium, Operation Stolen Pencil." Berzsenyi 2023: 124.
[91] Tarakanov 2013.
[92] Kong–Lim–Kim 2019: 8.
[93] Az APT37 további ismert azonosítói: Group 123, InkySquid, Operation Daybreak, Operation Erebus, Reaper Group, Reaper, Red Eyes, Ricochet Chollima, ScarCruft, Venus 121. (Berzsenyi 2023: 124).

feltehetően Észak-Korea ipari és katonai kémkedésre szakosodott offenzív tevékenységei.[94] Az Andariel (MITRE ID: G0138 és Mandiant: UNC614) elsősorban a dél-koreai kormányzati szervek, katonai szervezetek és amerikai vállalatok ellen intézett destruktív jellegű műveleteket. Az Andariel fenyegető csoport profiljába tartoznak még a pénzügyileg motivált műveletek, amelyeket kórházak (MAUI zsarolóvírus), ATM-ek, bankok és kriptovalutát forgalmazó vállalatok ellen is végrehajtott.[95]

Elméletek az észak-koreai kibertéri műveletek stratégiai koncepciójáról

Észak-Korea napjainkig nem publikált kiberképességei célrendszerére vonatkozó stratégiát. Ennek ellenére több olyan elméleti keretrendszert is megjelentettek, amelyeket a kutatók az észak-koreai kibertéri tevékenység önálló stratégiai célrendszerének leírására vagy éppen feltételezett kiberhadviselési doktrínájának feltárása érdekében alkottak meg biztonságpolitikai elemzési szempontok mentén. Az államhoz nyilvánosan attribútált kibertéri műveletek alapján három főbb stratégiai gondolkodási irány és műveleti szintű értelmezési keretrendszer különíthető el.

Az első elméleti keretrendszert Jun, LaFoy és Sohn (Center for Strategic & International Studies, CSIS kutatóközpont, 2015) dolgozta ki a KNDK hadviselési hagyományai és békeidőszakbeli provokációinak dinamikája mentén. Az elemzés kiindulópontja, hogy a Kim-rezsim évtizedek óta fegyverkísérletekkel, határkonfliktusokkal és terrorcselekményekkel igyekszik felhívni magára a nemzetközi közösség figyelmét és növelni a félsziget körüli katonai feszültséget. Ennek oka, hogy minél nagyobb a katonai eszkaláció kockázata, annál magasabb szintű diplomáciai fórumon próbálják meg rendezni a felek közti viszonyt. A rezsim által kikényszerített diplomáciai fórumon az észak-koreai fél általában gazdasági és politikai előnyöket követel az általa kiváltott feszültségek csökkentéséért cserébe.[96] Habár a kutatóintézet a későbbiekben sem mutatott ki általánosítható, közvetlen kapcsolatot a békeidőszaki provokációk politikai céljai és a kiberműveletek megindítása közt, megállapítható, hogy a phenjani vezetés érdekérvényesítő eszközként tekint a kiberképességekre, és alkalmazta azokat erődemonstrációs céllal.[97] A CSIS kutatói emiatt „háborús vagy magasabb intenzitású konfliktusos időszakra" és „békeidőbeli vagy alacsony intenzitású konfliktussal terhelt időszakra" osztották fel az Észak-Koreához köthető kibertérbeli műveleteket. A vizsgált időszakban a phenjani rezsim főként kiberhírszerzési (Kimsuky-kampányok) és bomlasztó hatást kiváltó kiberműveleteket hajtott végre az információs műveletek részeként, akár kritikusinfrastruktúra-szolgáltatók ellen is. Ez utóbbira példa a 2011-es Ten Days of Rain DDoS kampány, a 2013-as DarkSeoul művelet[98] és a 2014-es Operation KHNP (Korea Hydro and Nuclear Power), amely egy dél-koreai nukleáris erőmű műszaki leírásait

[94] Barnhart et al. 2023.
[95] MITRE ATT&CK 2022.
[96] Jun–LaFoy–Sohn 2015: 51.
[97] Cha–Lim 2024.
[98] 2013-ban a Dark Seoul elnevezésű észak-koreai csoport sikeresen kompromittálta és blokkolta három szöuli bank és három médiavállalat rendszereit. A támadók több napig zavart keltettek Dél-Korea pénzügyi szektorában, összesen több mint 800 millió dolláros kárt okozva. Bővebben Park–Park–James 2018.

és munkavállalóit érő adatszivárogtatás volt.[99] A tanulmány egyik konklúziója, hogy Észak-Korea (2009–2014 között) a békeidőszaki provokációk részeként eredményesen alkalmazta kiberképességeit, és ambícióként jelenik meg ezen számítógép-hálózati műveletek elektronikus és kiberhadviselésre alkalmas képességgé fejlesztése. Ám komoly kockázata van annak, hogy a szofisztikáltabb kiberműveletek hatásának téves felmérése miatt Phenjan átlépi a katonai *status quo*t. Emiatt a kutatók stratégiai szintű szakpolitikai lépéseket javasoltak az USA – Dél-Korea szövetség részére, amelyekkel korlátozhatják a KNDK haderejének irreguláris műveleti szabadságát a kibertérben, és növelhetik információs társadalmaik rezilienciáját.[100]

A második koncepciót megalkotó Ha és Maxwell (Foundation for Defense of Democracies, FDD, 2018) a gazdasági és politikai célokat egyaránt kiszolgáló incidenseket vizsgált meg és értékelte esetpéldaként a „*cyber enabled economic warfare*" (CEEW), vagyis „gazdasági hadviselés a kibertérben" elméleti koncepció keretrendszere mentén. Ez az elmélet a kibertéri műveletekkel elérhető illegális finanszírozás lehetőségének (például a megszerzett kriptovaluták hagyományos pénznemekké transzformálásával) és az információs társadalmak hosszú távú gazdasági kifárasztásának kombinálhatóságát emeli ki. Idesorolható a kriptovaluta- és számlapénzforgalomba beférkőző kiberbűnözői aktivitás, továbbá a FASTCash kampány, amely bankjegykiadó automatákat kompromittált Ázsia-szerte,[101] a bangladesi központi bank bankközi átutalásokat lebonyolító SWIFT rendszerének kompromittálása,[102] továbbá az APT38 tevékenységére visszavezetett WannaCry zsarolóvírusos kampány.[103] Biztonságpolitikai szempontból megközelítve a kiberműveletek célrendszerét, Észak-Koreának a rezsim fenntartásához és a katonai fejlesztések finanszírozásához szükséges támadások volumenét olyan mérték alatt kell tartania, hogy a szürkezónás tevékenysége ne hátráltassa a 2018-ban megindult politikai enyhülési folyamatot a további védelmi garanciák megadása és az ENSZ BT szankciós nyomásának enyhítése érdekében. Megjegyzendő, hogy az észak-koreai kibertéri tevékenység visszaszorítása érdekében már korábban is fellépett a nemzetközi közösség, habár csak korlátozott, diplomáciai eszközökkel. Az ENSZ BT 2006-tól tartja szankciós nyomás alatt a Központi Felderítő Irodát (RGB) és a vele együttműködő vállalkozásokat, mivel számos alkalommal kíséreltek meg tömegpusztító és csúcstechnológiás fegyverrendszerek technológiájára vonatkozó minősített adatot ellopni.[104] Ennek markáns esetpéldája a (Dél-Koreába is telepített THAAD rakétaelhárító rendszert fejlesztő) Lockheed Martin és alvállalkozóját érő

[99] 2014. december 15-től kezdődően a feltehetően észak-koreai patrióta hacktivisták „Who am I = No Nuclear Power" elnevezéssel kezdtek el a Korea Hydro & Nuclear Power (KHNP) alkalmazottairól információkat közzétenni az atomerőműre vonatkozó bizalmas műszaki dokumentumokkal együtt.

[100] Jun–LaFoy–Sohn 2015.

[101] A FASTCash kampány módszere, hogy távoli hozzáféréssel behatolnak a bankok pénzforgalmi Switch alkalmazásának szervereihez, és elősegítik a hamis tranzakciókat. Egy 2017-es incidens során a KNDK kiberegységei lehetővé tették, hogy több mint 30 különböző országban található ATM-ekből egyidejűleg készpénzt vegyenek fel. Egy másik, 2018-as incidens során 23 különböző országban lévő ATM-ből tudtak egyidejűleg készpénzt felvenni. Bővebben lásd US Cybersecurity and Infrastructure Security Agency 2020.

[102] A 2016. februári támadás során a támadók 951 millió dollárt akartak elrabolni, amelyből ténylegesen mintegy 81 millió dollárt sikerült átutalni az általuk megadott Fülöp-szigeteki számlaszámokra, ezzel hatalmas bevételhez juttatva a phenjani vezetést. Bővebben Hammer 2018; Rahman 2016.

[103] US Department of the Treasury 2020: 2.

[104] United Nations Security Council 2012.

sikertelen behatolási kísérlet, amelyet az USA Igazságügyi Minisztériuma a Lazarus észak-koreai APT-csoport tevékenységére attributált 2018-ban.[105] A másik konkrétabb példa, amely hathatott a kutatók elméletének kidolgozására, a 2018–2019-es évek bizalomépítő intézkedései. Kiinduló körülményként a Donald Trump elnöki ciklusa során felfokozott, ellenséges hangvételű kommunikáció tekinthető, amely mellett a 2017. szeptemberi intenzív interkontinentális rakétatesztek (ICBM) és a föld alatti nukleáris próbarobbantás olyan mértékűvé fokozták a katonai fenyegetést, hogy 2018-ra az észak-koreai fél ismételten tárgyalási pozícióba kerülhetett Dél-Koreával (2018. április, Mun–Kim-találkozó) és az amerikai legfelsőbb vezetéssel (2018. július, Szingapúr: Trump–Kim-találkozó). A 2018. áprilisi panmindzsoni nyilatkozatban a koreai felek többek között azt is vállalták, hogy a két állam kapcsolatának rendezéséig tartózkodnak a további provokatív akcióktól az összes műveleti térben, így a kibertéri műveletekben is.[106]Annak ellenére, hogy a két Korea viszonyrendszerének újbóli normalizálását célzó 2018. szeptemberi phenjani nyilatkozatban vállalt bizalomépítő kezdeményezések nem valósultak meg,[107] és az enyhülési folyamat 2019-re megrekedt, a diplomáciai párbeszéd és az addig nyert gazdasági előnyök (például a keszongi ipari park újranyitása) képesek voltak validálni a *de facto* állam[108] nemzetközi státuszát és megszilárdítani Kim belső hatalmát. Az amerikai és dél-koreai bilaterális csúcstalálkozók nyomán megvalósult a phenjani rezsim fennmaradását biztosító hosszú távú stratégiai célja: a békeidőszaki provokációkkal katonai patthelyzet kialakítása (a kínai geopolitikai érdekek védőernyője alatt) az USA és térségbeli szövetségeseinek erejével szemben, amit magas szintű diplomáciai kezdeményezések rendszere kezel.[109] Tanulmányában Ha és Maxwell megerősítette, hogy Észak-Korea az irreguláris kibertámadó képességeit a civil szféra és a pénzügyi kritikusinfrastruktúra-elemek ellen vetheti be, és amennyiben a rezsim politikai céljai nem valósulnak meg, az RGB tevékenységének növekedésére (anyagilag is motivált, de politikai és hírszerzési célú támadások) lehet számítani.[110]

2019–2020 fordulóján publikálták a harmadik koncepciót, amely a nemzetközi kutatási trendeket követve számításba vette a kibertér geopolitikai aspektusait. A NATO tallinni Kibervédelmi Kiválósági Központja (NATO CCDCOE) által közzétett elemzésben a kutatók (Kong Ji-Young, Jong In Lim, Kim Kyoung Gon) rávilágítottak arra, hogy Észak-Korea azért működik együtt más államokkal, mert ezzel nemcsak az attribúciót nehezíti, hanem egy összetett, további konfliktusokat generáló helyzet elé is állítja a megtámadott országot, amennyiben az megtorló válaszlépéseket kívánna tenni. A tanulmány a kibertér adta aszimmetriát felhasználó katonai stratégia végrehajtó szervezeteiként értelmezi a Központi Felderítő Iroda és a hadsereg vezérkara alatt elhelyezkedő kiberegységek (GSD) potenciális képességeit. Ebben a keretrendszerben a Központi Felderítő Iroda például kiberhírszerzési, befolyásoló vagy

[105] US Department of Justice 2018.
[106] Republic of Korea Ministry of Foreign Affairs 2018.
[107] Például a jongbjoni atomerőmű és a Tongchang-ri kísérleti rakétabázis bezárása. Bővebben Cheong 2018.
[108] A koreai háborút lezáró béke hiányában a nemzetközi jog alapján a KNDK-t számos ország nem ismeri el önálló államszervezetnek.
[109] Ha–Maxwell 2018: 1–2.
[110] Ha–Maxwell 2018.

zavarkeltő tevékenysége hozzájárul a katonai műveletek előkészítéséhez az információs és kibertérben. Az ismert szervezeti struktúra alapján az észak-koreai ambíciószint annak elérése lehet, hogy a GSD és az RGB kompetenciaterülete lehetővé tegye önálló offenzív kiberműveletek kivitelezését katonai vezetési rendszerek vagy kritikus információs infrastruktúra (*critical information infrastructure,* CII) elemei ellen. Ezzel párhuzamosan jelenik meg a haderőnemi kiberegységek meglepetésszerű vagy előzetes csapásmérő művelettámogató funkciója, amelyet a kutatók a *blitzkrieg* taktikához hasonlítottak.[111] A tanulmány az észak-koreai kiberhadviselési koncepció fő elemeként a minél nagyobb volumenű károkozási képesség megteremtését emelte ki – például sérülékenységek feltárása és malware-ek vagy kiberfegyverek fejlesztése által –, amit a nukleáris és rakétaprogramok mellett ugyancsak elrettentő képességként vagy megelőző csapásként alkalmazhatnak stratégiai kontextusban.[112]

Külföldről indított észak-koreai kibertámadások háttere

A bemutatott elméleteket egészíti ki a Recorded Future kiberbiztonsági vállalat 2020-ban publikált tanulmánya, amely az általuk elemzett esetpéldák technikai adatai alapján feltérképezte, hogy Észak-Korea mely államok területére visszavezethető lokációkról indított kibertámadást. Az Indiából és Kínából indított támadások esetében a támadók fizikailag is jelen voltak az országokban hivatalos tartózkodási engedéllyel rendelkező munkavállalóként és egyetemi képzésben részesülő hallgatóként vagy fedett személyként, míg a kutatócsoport által megnevezett további államok tekintetében távoli hozzáférésre utaló adatokat tártak fel. Az előbbi feltételezést erősítette meg egy disszidens is, aki korábban az észak-koreai hadseregben magas rendfokozatot töltött be, miszerint a KNDK éves szinten körülbelül 50–60 elit katonát vezényel külföldi egyetemekre informatikai képzésre, hogy tanulmányaik befejeztével a hírszerzéshez (RGB) vagy más kiberműveleteket végrehajtó egységekhez csatlakozzanak.[113] Ázsiában az érintett geolokációk Malajziára, Nepálra, Indonéziára, Thaiföldre és Banglades területére utaltak, míg Afrikában Kenya és Mozambik területe volt érintett. Új-Zéland esetében feltételezhető egy botnethálózat (magyarul zombigép- vagy zombihálózat) kialakítása, amely olyan végpontok (értsd: számítógépek és más okoseszközök) összessége, amelyek felett átvették az irányítást.[114] Napjainkra, a távmunkavégzés terjedésével párhuzamosan, ugyancsak megjelentek a magukat más nemzetiségűnek kiadó észak-koreai személyek az IT-ipar különböző szegmenseiben. Észak-Korea ezen személyeket Kínában és Oroszországban működő online munkaerő-közvetítő

[111] Kong–Lim–Kim 2019: 13.
[112] Kong–Lim–Kim 2019: 13–17.
[113] Kong–Lim–Kim 2019: 3.
[114] Recorded Future – Insikt Group 2020.

leányvállalatok segítségével juttatja munkához, bérezésük pedig hozzájárul a rezsim finanszírozásához.[115]

A Recorded Future és a korábban idézett, NATO CCDCOE által közzétett kutatói jelentések egyaránt mandzsúriai geolokációkat tártak fel az Észak-Koreához köthető APT-csoportok fő tevékenységi területeként, ahol a koreai–kínai etnikai kisebbség él. Ennek nemzetbiztonsági relevanciája, hogy megkönnyíti a koreai anyanyelvű, fedett műveletekben részt vevő személyek elhelyezését. Például a terület egyik központi városának számító Senjangból és környékéről már észleltek észak-koreai offenzív tevékenységet, emellett a geolokációs adatok alapján a Koreai-öböl mentén fekvő Dalian városának érintettsége is felmerült.[116] Dalianban található annak az észak-koreai cégnek a kirendeltsége (Chosun Expo Joint Venture), ahol a CIA által a Sony Pictures elleni és a WannaCry 2.0 zsarolóvírusos támadás egyik felelőseként megnevezett Park Dzsinhjok dolgozhatott szoftverfejlesztőként. Az amerikai hatóságok azzal vádolják Parkot, hogy az APT38 kódnevű csoport tagjaként kínai területről hajtott végre a phenjani rezsim céljait szolgáló kibertámadásokat, beleértve a 81 millió dolláros kárt okozó, bangladesi központi bankot kifosztó 2016-os incidenst.[117]

Az észak-koreai hírszerző és más nemzetbiztonsági műveletek kapcsán Japán territoriális érintettségét is feltárták. Ez valójában az ország területén élő, észak-koreai identitást valló koreai nemzetiség érdekvédelmi szervezetéhez (koreai nevén: Csongrjon) kötődik.[118] A szervezet radikális szárnya kapcsolatban áll a japán alvilági csoportokkal, továbbá támogatásához köthető a 80–90-es években elrabolt japán állampolgárok Észak-Koreába hurcolása.[119] A Csongrjon ezen radikális szárnya továbbra is hozzájárul Észak-Korea különböző illegális és titkosszolgálati aktivitásához. Például 2017-ben a japán Nemzeti Rendészeti Ügynökség arról számolt be, hogy a japán jakuzával és más nemzetközi bűnszervezetekkel kapcsolatban álló 260 személy segítette az észak-koreai támadókat abban, hogy 17 japán prefektúrában összesen 17 700 bankautomatát (ATM) kompromittálva, mintegy 16,6 millió dollárt lopjanak el.[120] Egy másik kirívó eset, amikor a japán rendőrség 2016-ban átkutatta a Csongrjon tokiói székházát (felbontva a szervezet *de facto* követségi immunitást élvező státuszát a sorozatos titkosszolgálati és pénzügyi botrányok következtében). A terhelő bizonyítékok alapján több észak-koreai személyt is letartóztattak, többek között a tokiói Korea Egyetem

[115] A Yanbian Silverstar Network Technology Co. Ltd. (ismertebb nevén China Silver Star vagy 延边银星网络科技有限公) egy csilini (Kína) székhelyű szoftverfejlesztő vállalat, amelyet az USA már 2018-ban szankcionált. A China Silver Star észak-koreai vezérigazgatója (Jong Szonghva (정성화) az oroszországi Vlagyivosztokban is létesített testvérvállalatot (Volasys Silver Star). Tehát mindkét vállalat észak-koreai irányítás alatt áll, és az amerikai kormányzat szerint IT-kiszervezési tevékenységet végeznek, amelyről jelentésében az FBI azt állítja, hogy „dollármilliókat" kerestek a phenjani rezsimnek. Bővebben lásd Williams 2023a.

[116] Kong–Lim–Kim 2019: 14.

[117] US Department of Justice 2018.

[118] Lee 2018.

[119] Kato 2017.

[120] Kyodo News 2020.

Gazdaságtudományi Karának volt dékánját, Pak Dzseiszót[121] (angol átírásban: Park Jae Isao) egy kiterjedt pénzügyi csalás ügyében. Azonban a Paknál tartott házkutatás után további terhelő bizonyítékok kerültek elő a lefoglalt számítógépéről, ez alapján feltárták, hogy Pak egy egész ügynöki és informátori hálózatot finanszírozott a Kínai Népköztársaságban és a Koreai Köztársaságban. Az ügynököket személyesen (Sanghajban) vagy elektronikus úton (titkosított vagy kódolt e-mailben és privát hálózaton keresztül) utasította, hogy manipulálják a 2007-es dél-koreai elnökválasztást, hatoljanak be a tömegmédiába. (Az elnökválasztást végül I Mjongbak nyerte meg [2008–2013], aki az észak-koreai kapcsolatok bővítését elutasító, konzervatív jobboldali Szabad Korea Párt tagja.) A számítógépen talált adatok alapján Pak arra is utasította ügynökeit, hogy a 2008-as dél-koreai általános parlamenti választásokon a Phenjan felé békülékeny politikát támogató erőket segítsék, és befolyásolják a közvéleményt az I Mjongbak elleni tüntetésen való részvételre, továbbá a „felbujtás" megszervezésében szintén közreműködhettek.[122]

Összegzés és konklúzió

A kutatás központi célkitűzése az volt, hogy az északkelet-ázsiai régió biztonságpolitikai környezetének kontextusában jellemezze az észak-koreai kibertéri műveletek stratégiai célrendszerét, és elősegítse további objektív következtetések levonását az államhoz köthető fejlett perzisztens fenyegetések tevékenységével kapcsolatban. Ennek érdekében a szerző két kutatási kérdés és két hipotézis vizsgálatát végezte el.

KK1: A nyilvánosan észak-koreai aktorok tevékenységére attribútált kibertéri műveletek stratégiai célrendszere hogyan illeszkedik az ország védelempolitikájába, és miként támogatja a phenjani rezsim nemzetközi érdekérvényesítő képességét?

Amennyiben abból indulunk ki, hogy a legtöbb államhoz hasonlóan Észak-Korea kibervédelmi stratégiai célja is alapvetően az, hogy csökkentse támadható felületét, az magyarázatot adhat sajátos, belföldi hálózati kialakítására és okoseszköz-felügyeleti törekvéseire, egyúttal megmagyarázza a külföldről indított műveleteinek szükségszerűségét. Összességében elmondható, hogy Észak-Korea internet- és hálózatfüggőségét stratégiai okokból szándékosan alacsonyan tartják, mert ez elméleti síkon csökkenti az ország és a társadalom technológiai függőségéből eredő kockázati szintjét és kitettségét a kibertámadások okozta károknak. Emellett a hálózati adatforgalom, a kommunikáció felügyelete és a cenzúrázás hozzájárul ahhoz, hogy az elérhető információ ne veszélyeztesse az elnyomó politikai rezsim stabilitását. Elméleti síkon ezt két alapvetés is megerősíti, amelyek hatottak a KNDK kiberképességekkel kapcsolatos hadviselési kultúrájára. Egyrészt a folyamatosan fejlődő információs társadalmak,

[121] Pak a tokiói rendőrség nyomozása, valamint a hivatkozott *Sankei* folyóirat tényfeltárása alapján nem csak a japánban élő, észak-koreai identitást valló koreaiak érdekvédelmi szervezetéhez, a Csongrjonhoz (japánul: Chosen Soren) kötődött. Az elérhető információk alapján a Csongrjonon keresztül kapcsolatban állhatott az észak-koreai hírszerző szolgálat egyik hírhedt szervével, amely harmadik országban ügynököket és illegális finanszírozási tevékenységet irányít, az úgynevezett 225-ös Irodával. Az Iroda műveleteinek felderítése során Pak tevőleges közreműködésére vonatkozó, terhelő bizonyítékok kerültek elő.

[122] *Sankei News* 2016.

a technológiai függőség mértékével megegyezően, sérülékenyek és kitettek a kibertérből érkező, például bomlasztó célú információs műveleteknek.[123] Ebből következik, hogy elrejthető és könnyen letagadható offenzív kiberműveletek révén csökkenthető az Egyesült Államok és térségbeli szövetségeseinek aszimmetrikus erőfölénye. Másrészt azon „szürkezónás", például (dez)információs, kiberhírszerzési vagy anyagilag motivált műveletek, amelyek a jelenleg publikus észak-koreai képességek révén elérhetők, ugyan alacsonyabb eszkalációs kockázattal járnak (ami jelenleg megfelel Észak-Korea érdekérvényesítési ambíciószintjének), ám nem használhatók fel hiteles kibertéri elrettentés eléréséhez. Az a műveleti képesség (amely például cselekvési vagy információs szempontok mentén megvalósuló stratégiai autonómia[124] elérését is jelenti a kibertérben) jelentős politikai és katonai eszkalációs kockázatot von maga után (például kiberfegyver bevetése).[125] Azonban egy hálózatosított, modern haderővel szemben hiteles elrettentést jelenthet, így Észak-Koreának érdekében áll ezen képességi szint elérése.

1. táblázat: A KNDK (állami és állam alatti) kiberegységei, amelyek kiberstratégiai funkciókat látnak el

Észak-Korea kiberstratégiai céljait végrehajtó egységek			
KPA Vezérkar (General Staff Department – GSD) • Haderőnemek • Elektronikai hadviselés	**Központi Felderítő Iroda (RGB)** • 121-es Iroda (Bureau 121) • Egységek és összekötő irodák (413, 128, 108, 110, 91, 35, 98)	**Fejlett Perzisztens Fenyegetések (APT)** • APT37, APT38, APT43 és klasztereik • További állam alatti kiberegységek	**IT-szakemberek** (távmunka) • Felderítő és anyagi haszonszerzési funkció

Forrás: a szerző szerkesztése

A védelempolitikájának gyakorlati átültetése során a phenjani vezetés megfordíthatta ezt a gondolatmenetet annak érdekében, hogy felkészíthesse digitális ökoszisztémáját az USA igazolt katonai (és állam alatti) kiberképességeivel szemben. A rezsim erőforrásainak szűkössége mellett védelempolitikai megfontolásból tudatosan alacsonyan tartja a saját területén elérhető hálózati megoldások lefedettségét, és társadalmi funkció szerint szegmentálja azokat: lakossági, katonai és belbiztonsági célok mentén. A belföldi és nemzetközi felhasználók közti információáramlás ellenőrzésére alkalmazott számos módszer egyike a Koryolink belföldi celluláris hálózatán kialakított tartalom- és forgalomszűrési megoldás. A hálózati kapacitások (fizikai infrastruktúra és adatforgalom) korlátozottsága az elavult (vagy alacsonyabb minőségű, saját fejlesztésű) belföldi technológiai megoldásokkal együttesen infrastrukturális szempontból

[123] Haig 2022.

[124] „A stratégiai autonómia […] alapvetően három fajtáját különböztethetjük meg […]: döntéshozatali autonómia, cselekvési autonómia és információs autonómia. Az első a politikai akaratra és a döntéshozatali folyamatra helyezi a hangsúlyt, a második a katonai és civil képességek és a műveleti készenlét fejlesztésére, a harmadik pedig a hírszerzésre, elemzésekre és adatgyűjtésekre." Bővebben lásd Szabolcs 2020: 28.

[125] Például nulladik napi *(zero-day)* sérülékenység felhasználásával vagy a teljes ún. *cyber-kill-chain* folyamaton (Lockheed Martin által kidolgozott koncepció) végbemenő számítógép-hálózati behatolással megvalósított kiberművelet.

korlátozzák Észak-Korea kibertéri egységeinek (1. táblázat) műveleti lehetőségeit, defenzív és offenzív oldalon egyaránt. Emiatt az offenzív kiberműveleteket végrehajtó egységek külföldre telepítésével a phenjani vezetés egy hatékonyabb erőforrás-allokációt valósít meg. Ennek további hasznos vetülete, hogy egyúttal ugyanezen célországban megvalósíthatja a személyi állomány képzését és/vagy munkaerőpiacra történő belépését (amivel ugyancsak további anyagi erőforrások előteremtése is lehetséges a rezsim számára). Mindezzel párhuzamosan védelempolitikai oldalon a korlátozott infrastruktúra fenntartására (és fejlesztésére) fordított erőforrás-felhasználás összességében csökkenti Észak-Korea technológiai függőségéből eredő kockázati szintjét a regionális szomszédjai társadalmához képest.

A kutatás első hipotézisét – miszerint (H1) „a békeidőszaki kiberműveletek kettős védelempolitikai célja, hogy egyrészt finanszírozza a haderőfejlesztést, másrészt a stratégiai céllal alkalmazott katonai provokációkat kiegészítve gazdasági és politikai engedményeket kényszerítsen ki a nemzetközi közösségből" – a szakirodalom összehasonlító elemzése igazolta. Összességében a KNDK aszimmetrikus nemzetközi viszonyrendszerében a kiberműveleti képességek kialakítása és fejlesztése költséghatékonyabb a konvencionális haderő eszközparkjának fenntartási és modernizációs költségeihez képest. Ezenfelül a kinetikus műveletekhez és fegyverkísérletekhez képest az offenzív kibertéri tevékenység kevésbé hordozza magában a válaszcsapás megindításának és a konfliktus eszkalációjának kockázatát, míg az általuk kiváltható hatás ugyanúgy kiterjedhet a fizikai térre. Az észak-koreai kiberegységek és az állam által támogatott irreguláris csoportok (APT) tevékenysége könnyebben elrejthető és letagadható a kinetikus műveletekhez képest, mindemellett adaptív alkalmazkodóképességük hosszú távú, célzott és fedett tevékenységet tesz lehetővé az ellenséges rendszerekben, ezáltal hatékonyan megvalósítva többek között a hírszerzési és felderítő vagy egyéb (például: anyagi) erőforrások kinyerésére irányuló célokat.[126] A Ha és Maxwell (2018) által leírt mechanizmus lényege, hogy a rezsim hosszabb távon igyekszik békeidőszaki provokatív akcióinak (például rakétakísérletek) eszközrendszerét kibővíteni olyan kibertéri műveletekkel, amelyekkel finanszírozni tudják a rezsim és hadereje fenntartását, és egyúttal növelhetik az információs társadalmak gazdasági alrendszereinek fenyegetettségét, gyengítve az államok gazdasági erejét adó kritikus pontokat. Ezzel arra kényszerítik ellenfeleiket, hogy a konfliktus eszkalációjának elkerülése érdekében gazdasági és politikai engedményeket tegyenek a rezsimnek, ami egy jellemző észak-koreai tárgyalási technika. Ha és Maxwell előrevetítette, hogy amennyiben Észak-Korea beleegyezik a nukleáris és fegyverprogramjainak korlátozásába, akkor a gazdaságilag motivált kibertámadások (elméletükben úgynevezett kibertér által lehetővé tett gazdasági hadviselés) valószínűleg még nagyobb részét fogják képezni a békeidőszaki provokációs stratégiának az esetek számától függetlenül. A 2024-es év a phenjani nemzetközi érdekérvényesítési gyakorlat eszkalációs (konfliktust fokozó) időszakába fog tartozni az áprilisban esedékes dél-koreai és a novemberi amerikai elnökválasztás miatt, mivel ezek új alkupozíció kialakítását teszik lehetővé. Ezzel összefüggésben Észak-Korea a korábbi évekhez képest több provokatív, köztük kiberműveleti akciót fog véghez vinni ezekben a hónapokban, vagy a dél-koreai – amerikai

[126] Jun–LaFoy–Sohn 2015: 19–25; Berzsenyi 2023.

bilaterális integrált védelmi párbeszéd tervezett kibervédelmi gyakorlatára reagáló válaszlépésként időzítve.

A második kutatási kérdés (KK2) arra kereste a választ, hogy milyen hatást gyakorol az északkelet-ázsiai régió biztonságpolitikai helyzetére a Kínai Népköztársaság és a Koreai Népi Demokratikus Köztársaság feltételezhető együttműködése az offenzív kibertéri műveletek kivitelezésében. Ennek kapcsán a kutatás alátámasztotta, hogy (H2) a pekingi vezetés észak-koreai felsőoktatást és munkavállalást támogató politikája, az infrastruktúra-szolgáltatás nyújtásával kiegészülve, olyan geopolitikai helyzetet teremt, amelyben az Észak-Korea által indított műveletek egyúttal alkalmasak Kína nemzetközi erőkivetítési stratégiájának és kibertérben megvalósítható céljainak kiszolgálására a kelet-ázsiai régióban az Egyesült Államok és szövetségesei ellen. Az ebből következő kockázati tényezők:

- Mobilitás. Kína különösen ideális környezetet nyújthat fedett kibertámadó tevékenység vagy hírszerző műveletek kivitelezéséhez az ott élő kínai–koreai közösség (például nyelvhasználat, munkalehetőség) jelenléte miatt.
- Kompetenciák átadása. A Kínában képzett új szakemberek létszáma és a külföldi munkavégzés révén szerzett tudástranszfer jelenti az észak-koreai kibertámadó képességek fejlődésének egyik indikátorát. A Koreai Néphadsereg vagy az RGB kibererőinek lehetséges növekedését előrejelző kalkulációk tovább árnyalhatók, amennyiben az észak-koreai felsőoktatási intézményekben képzett szakemberek mellett a külföldi hallgatók és munkavállalók létszámát és mobilitását megfigyeljük. E tekintetben a potenciális fogadó államokat (a felsorolást lásd a Recorded Future idézett kutatásában) kiberdiplomáciai csatornákon keresztül érdekeltté kell tenni úgy, hogy az adatszolgáltatást például védelmi célú felkészülésként vagy a kiberbűnözés csökkentésére tett erőfeszítésként tematizáljuk, elkerülve a NATO és globális partneri közösségének érdekeivel való további szembehelyezkedést.
- A nemzetközi jog korlátai. Harmadik ország infrastruktúrája ellen nem lehet retorzió kockázata nélkül támadást indítani.

Ezek mentén megállapítható, hogy a Központi Felderítő Iroda (RGB) kiberegységeihez köthető fejlett perzisztens fenyegetések a szürkezónában operálva, saját céljaik megvalósítása mellett, alkalmasak Kína térségbeli kiberhatalmi céljait kiszolgáló erőfeszítéseinek támogatására, mert a kínai területről megindított műveletek nyilvános attribúciója magas politikai kockázattal jár.[127] Ezzel alátámasztható az Egyesült Államok (kiberhatalmi státuszával összefüggő) érdekérvényesítő képessége térségbeli szövetségesei előtt, és egyúttal csökkentheti a szövetségesi kohéziót.

[127] F. Yang 2022.

Felhasznált irodalom

Barnhart, Michael et al. (2023): Assessed Cyber Structure and Alignments of North Korea in 2023. *Mandiant,* 2023. október 10. Online: www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023

Bartók András (2018): „Korlátok nélküli hadviselés" (超限战) – Egy kínai nézőpont a 21. század hatalmi versengéséről. *Hadtudományi Szemle,* 11(3), 338–346. Online: https://folyoirat.ludovika.hu/index.php/hsz/article/view/3995/3261

Bartók András (2020): Sárkányok és kistigrisek: Kelet-Ázsia regionális fegyverkezési versenyének általános és országspecifikus jellemzői a Kínával kapcsolatos fenyegetettségpercepciójú országok esetében 1. *Nemzet és Biztonság,* 13(4), 80–101. Online: https://doi.org/10.32576/nb.2020.4.6

Bartók András (2022): Sokan tartanak Kína tajvani inváziójától, megnéztük a forgatókönyveket. *Telex,* 2022. augusztus 25. Online: https://telex.hu/velemeny/2022/08/25/tajvan-kina-aggodalmak-szembenallo-erok-invazio-forgatokonyvek-usa-japan-tamogatas

Bartók András – Wagner Péter (2021): A kínai A2/AD és a válaszreakciók Kelet-Ázsiában (2.). *KKI Elemzések,* 2021/7, 3–18. Online: https://doi.org/10.47683/KKIElemzesek.E-2021.07

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

Cha, Victor – Lim, Andy (2024): Slow Boil: What to Expect from the DPRK in 2024. *CSIS,* 2024. január 16. Online: www.csis.org/analysis/slow-boil-what-expect-dprk-2024

Chainalysis Team (2023): 2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers. *Chainalysis,* 2023. február 1. Online: www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/

Cheong, Wa Dae (2018): *Pyongyang Joint Declaration of September 2018.* Online: www.mofa.go.kr/eng/brd/m_5476/view.do?seq=319608&srchFr=&srchTo=&srchWord

Csoma Mózes (2006): *A koreai félsziget politikai viszonyai és azok biztonságpolitikai aspektusai.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12047/ertekezes.pdf;jsessionid=D2CBB0501C9C3852B9F788A081906D14?sequence=1

DeYoung, Karen – Nakashima, Ellen – Rauhala, Emily (2017): Trump Signed Presidential Directive Ordering Actions to Pressure North Korea. *The Washington Post,* 2017. szeptember 30. Online: www.washingtonpost.com/world/national-security/trump-signed-presidential-directive

F. Yang, Fan (2022): The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective. In Levite, Ariel E. et al. (2023): *Managing U.S.-China Tensions Over Public Cyber Attribution*. Washington, D.C.: Carnegie Endowment for Inter-

national Peace. Online: https://carnegieendowment.org/files/Perkovich_et_al_Cyber_Attribution_web.pdf
Gause, Ken E. (2015): *North Korea's Provocation and Escalation Calculus: Dealing with the Kim Jong-un Regime.* Washington: CNA Analysis & Solutions. Online: https://apps.dtic.mil/sti/tr/pdf/ADA621100.pdf
Geigenberger, Laura (2023): Russian Ambassador to Pyongyang Provides Insights into Current Trade with North Korea and the Status of its Weapons Development. *Daily NK,* 2023. május 30. Online: www.dailynk.com/english/russian-ambassador-to-pyongyang-provides-insights-into-current-trade-with-north-korea-and-the-status-of-its-weapons-development/
Ha, Matthew (2022): The Evolution of Kim Jong Un's 'All-Purpose Sword'. *FDD,* 2022. október 28. Online: www.fdd.org/analysis/2022/10/28/the-evolution-of-kim-jong-uns-all-purpose-sword/
Ha, Mathew – Maxwell, David (2018): *Kim Jong Un's 'All-Purpose Sword'. North Korean Cyber-Enabled Economic Warfare.* Washington, DC: FDD Press.
Haig Zsolt (2022): Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle,* 15(2), 115–130. Online: https://doi.org/10.32563/hsz.2022.2.7
Hammer, Joshua (2018): The Billion-Dollar Bank Job. *The New York Times,* 2018. május 3. Online: www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html
Han, Sangmi (2016): North Korea sends 50 to 60 Talented Students to Study Abroad to Train as Cyber Agents. *Voice of America,* 2016. június 14. Online: www.voakorea.com/a/3375411.html
Johnson, Jeff et al. (2023): 3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible. *Mandiant,* 2023. április 20. Online: www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
Jun, Jenny – LaFoy, Scott – Sohn, Ethan (2015): *North Korea's Cyber Operations. Strategy and Responses.* Lanham: Rowman & Littlefield. Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf
Kato, Katsunobu (2017): *Abductions of Japanese Citizens by North Korea.* Tokyo: Secretariat of the Headquarters for the Abduction Issue. Online: www.mofa.go.jp/files/000433596.pdf
Kertész Bence (2023): A lopakodó tigris: Észak-Korea rakétafejlesztésének titkos rekordéve. *Biztonságpolitika.hu,* 2023. február 11. Online: https://biztonsagpolitika.hu/kiemelt/a-lopakodo-tigris-eszak-korea-raketafejlesztesenek-titkos-rekordeve
Kong, Ji-Young – Lim, Jong In – Kim, Kyoung Gon (2019): The All-Purpose Sword: North Korea's Cyber Operations and Strategies. *11th International Conference on Cyber Conflict (CyCon),* 1–20. Online: https://doi.org/10.23919/CYCON.2019.8756954
Kovács László (2021): Offenzív kiberműveletek II.: Kibererők és képességeik. *Hadmérnök,* 16(3), 119–137. Online: https://doi.org/10.32567/hm.2021.3.7
Kim, Yonho (2014): *Cell Phones in North Korea. Has North Korea Entered the Telecommunications Revolution?* Washington: US–Korea Institute at SAIS – Voice

of America. Online: https://38north.org/wp-content/uploads/2014/03/Kim-Yonho-Cell-Phones-in-North-Korea.pdf
Krasznay Csaba (2020): Kiberbiztonsági K+F+I Európában. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest: Ludovika, 83–97. Online: https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1&isAllowed=y#page=84
Krasznay Csaba (2022): Adatok és automatizáció a kiberbiztonság szemszögéből. *Századvég,* 2022/1, 29–46. Online: https://szazadvegfolyoirat.hu/wp-content/uploads/2023/09/Szazadveg_2022_01_teljes.pdf
Kyodo News (2020): Suspected Ringleader of Huge, Coordinated ATM Scam Entered N. Korea. *Kyodo News (South Korea),* 2020. április 5. Online: https://english.kyodonews.net/news/2020/04/2b45db5e313b-suspected-ringleader-of-huge-coordinated-atm-scam-entered-n-korea.html
Lee, Yaecan (2018): Japan's North Korean Diaspora. *The Diplomat,* 2018. január 5. Online: https://thediplomat.com/2018/01/japans-north-korean-diaspora/
Malpedia (2024): *Lazarus Group.* Online: https://malpedia.caad.fkie.fraunhofer.de/actor/lazarus_group
McAffee (2011): *Ten Days of Rain. Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea.* Online: www.mcafee.com/blogs/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf
McLeary, Paul – Hudson, Lee (2022): Better Call Seoul: U.S. Watches Nervously as Europe Turns to South Korea for Weapons. *Politico,* 2022. november 1. Online: www.politico.com/news/2022/11/01/europe-south-korea-weapons-00064427
Miller, Steve (2018): Where Did North Korea's Cyber Army Come From? *VOA News,* 2018. november 20. Online: www.voanews.com/a/north-korea-cyber-army/4666459.html
Missile Defense Project (2023): North Korean Missile Launches & Nuclear Tests: 1984–Present. *Missile Threat,* 2023. április 25. Online: https://missilethreat.csis.org/north-korea-missile-launches-1984-present/
MITRE ATT&CK (2022): *Andariel.* Online: https://attack.mitre.org/groups/G0138/
MITRE ATT&CK (2023): *Lazarus Group.* Online: https://attack.mitre.org/versions/v7/groups/G0032/
Montlake, Simon (2012). Pyongyang Calling For Egyptian Telecoms Tycoon Naguib Sawiris. *Forbes,* 2012. november 19. Online: www.forbes.com/sites/simonmontlake/2012/11/18/pyongyang-calling-for-egyptian-telecoms-tycoon-naguib-sawiris/
NATO CCDCOE [é. n.]: *Sony Pictures Entertainment attack (2014).* Online: https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014) Letöltés ideje: 2020. 07. 07.
Noland, Marcus (2009) Telecommunications in North Korea: Has Orascom Made the Connection? *North Korean Review,* 5(1), 62–74. Online: www.jstor.org/stable/43910262.
Park, Kyoung Jae – Park, Sung Mi – James, Joshua I. (2017): A Case Study of the 2016 Korean Cyber Command Compromise. *European Conference on Information Warfare and Security,* 315–321. Online: https://arxiv.org/pdf/1711.04500

RAHMAN, Mizanur (2016): *A Forensic View of Bangladesh Bank Reserve Heist.* University of Dhaka. Online: https://doi.org/10.13140/RG.2.2.35280.51200

RAMANI, Samuel (2023): North Korea's Covert Alliance With Iran Aligned Militias in the Middle East. *38north,* 2023. október 23. Online: www.38north.org/2023/10/north-koreas-covert-alliance-with-iran-aligned-militias-in-the-middle-east/

Recorded Future – Insikt Group (2020): *How North Korea Revolutionized the Internet as a Tool for Rogue Regimes.* Online: www.recordedfuture.com/blog/north-korea-internet-tool

Republic of Korea Ministry of Foreign Affairs (2018): *Panmunjom Declaration for Peace, Prosperity and Unification of the Korean Peninsula.* 2018. április 27. Online: www.mofa.go.kr/eng/brd/m_5478/view.do?seq=319130&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1&titleNm=

ROK Ministry of National Defense (2018): *Defence White Paper: Changes and Challenges in the Security Environment – North Korea's Military Command Structure.* 28. 2018. december 31. Online: www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201908070153390840.pdf

Sankei News (2016): 朝鮮大学校元幹部逮捕「スパイ天国・日本」狙い撃ち 北朝鮮の指示役、韓国大統領選でも暗躍 (A Korea Egyetem előző intézményvezetőjének letartóztatása, „Kémek Paradicsoma, Japán" – Az észak-koreai ügynökök a dél-koreai elnökválasztással kapcsolatban is tevékenykedtek). *Sankei News.* 2016. Online: www.sankei.com/affairs/news/160202/afr1602020050-n1.html

SHIM, Elizabeth (2021): Report: North Korea's Trade with China Declined 80% in 2020. *UPI,* 2021. február 22. Online: www.upi.com/Top_News/World-News/2021/02/22/Report-North-Koreas-trade-with-China-declined-80-in-2020/2431614020515/

Symantec Threat Hunter Team (2023). X_Trader Supply Chain Attack Affects. Critical Infrastructure Organizations in U.S. and Europe. *Symantech Enterprise Blogs,* 2023. április 21. Online: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

SZABOLCS Laura (2020): Európai stratégiai autonómia – A közös védelem alapjai és korlátjai. *Nemzet és Biztonság,* 13(3), 15–35. Online: https://doi.org/10.32576/nb.2020.3.3

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

TARAKANOV, Dmitry (2013): The „Kimsuky" Operation: A North Korean APT? *Securelist,* 2013. szeptember 11. Online: https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/

TÓTH András (2022): A Katonai Egységes Felhőalapú Eszközrendszer fogalmi rendszerének meghatározása. *Hadtudomány,* 32(4), 112–125. Online: https://doi.org/10.17047/Hadtud.2022.32.4.112

United Nations Security Council (2012): *Security Council Committee Determines Entities, Goods Subject to Measures Imposed on Democratic People's Republic of Korea by Resolution 1718 (2006).* New York, 2012. május 2. Online: www.un.org/press/en/2012/sc10633.doc.html

US Cybersecurity and Infrastructure Security Agency (2020): *Guidance on the North Korean Cyber Threat*. Online: www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a
US Cybersecurity and Infrastructure Security Agency (2021): *AppleJeus: Analysis of North Korea's Cryptocurrency Malware.* Online: www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a
US Cybersecurity and Infrastructure Security Agency. (2022): *North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector.* 2022. július 7. Online: www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a
US Department of Defense (2023): *Joint Press Statement for the 22nd Korea-U.S. Integrated Defense Dialogue.* 2023. április 12. Online: www.defense.gov/News/Releases/Release/Article/3360919/joint-press-statement-for-the-22nd-korea-us-integrated-defense-dialogue/ Hozzáférés: 2023. 05. 31.
US Department of Justice (2018): *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.* 2018. szeptember 6. Online: www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
US Department of the Treasury (2020): *Guidance on the North Korean Cyber Threat.* Online: https://ofac.treasury.gov/sanctions-programs-and-country-information/north-korea-sanctions
US Department of Treasury (2022): *Guidance on the Democratic People's Republic of Korea information technology workers.* 2022. május 16. Online: https://ofac.treasury.gov/media/923131/download?inline
Wagstaff, Jeremy – Auchard, Eric – Kiselyova, Maria (2017): Russian Firm Provides New Internet Connection to North Korea. *Reuters,* 2017. október 2. Online: www.reuters.com/article/us-nkorea-internet-idINKCN1C70D2
Williams, Martyn (2011): North Korea's Chinese IP addresses. *38 North,* 2011. június 26. Online: www.northkoreatech.org/2011/06/26/north-koreas-chinese-ip-addresses/
Williams, Martyn (2014): Internet Coming to Kaesong Industrial Zone. *38North,* 2014. február 10. Online: www.northkoreatech.org/2014/02/10/internet-coming-to-kaesong-industrial-zone/
Williams, Martyn (2015): Koryolink Faces Big Problems with Cash, Competition. *38North,* 2015. június 25. Online: www.northkoreatech.org/2015/06/25/koryolink-faces-big-problems-with-cash-competition/
Williams, Martyn (2017): Russia Provides New Internet Connection to North Korea. *38North,* 2017. október 1. Online: www.38north.org/2017/10/mwilliams100117/
Williams, Martyn (2019): North Korea's Koryolink: Built for Surveillance and Control. *38North,* 2019. július 26. Online: www.northkoreatech.org/2019/07/26/north-koreas-koryolink-built-for-surveillance-and-control/
Williams, Martyn (2023a): North Korean Programmers Used a Hosted Laptop to Freelance Online, Says FBI. *38North,* 2023. október 24. Online: www.northkoreatech.org/2023/10/24/north-korean-programmers-used-a-hosted-laptop-to-freelance-online-says-fbi/

Williams, Martyn (2023b): Is 4G on the Horizon for North Korea? *38North,* 2023. november 4. Online: www.northkoreatech.org/2023/11/04/is-4g-on-the-horizon-for-north-korea/

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