10. fejezet

Nemzeti kiberhadviselési stratégiák, végrehajtó szervezetek

Dévai Dóra

Bevezetés

Mára a nemzetállamok stratégiai versengése a kibertérben is jól láthatóvá vált. Az informatikai rendszerek sérülékenységének kihasználása nemzetbiztonsági célok érdekében több évtizedre tekint vissza. Ellenben ezen képességek stratégiai szintű kiaknázása a nemzeti érdekek és célkitűzések megvalósításáért teljesen új biztonságpolitikai paradigma. A nagyhatalmi ambíciókkal rendelkező államok számára a nagyhatalmi politika részét képezi a kibertér gazdasági, diplomáciai és katonai értelemben egyaránt, ahol a stratégiai kultúrájuknak megfelelően alakítják ki képességeiket és politikájukat. A fejezetben a stratégiaelmélet és azon belül a stratégiaikultúra-koncepció felhasználásával mutatjuk be az USA és Oroszország kibervédelmi stratégiai gondolkodását és evolúcióját.

Elméleti alapvetések

Jelen tanulmány abból a hipotézisből indul ki, hogy a kiberfegyverek megjelenésekor nem csupán egy új fegyvernemről beszélhetünk,[1] hanem egy sokkal átfogóbb jelenségről, amely a technológiai fejlődés következtében hatással van a nemzetállamok közötti kapcsolatokra és a hadviselés fejlődésére is. A kibertér így stratégiai értelmet nyer egyrészt azáltal, hogy befolyásolja a nemzetállamok hatalomérvényesítési képességét, másrészt a nemzetállamok versengenek a kibertér feletti ellenőrzés jogáért. A második hipotézisünk tehát, hogy a kibervédelmi stratégia a nemzeti stratégiai kultúra szerves része, és így a doktrinális, szakpolitikai és operatív képességek kialakítása és rendszerszintű integrálása során

[1] Kovács László: *Kiberbiztonság és stratégia*. Budapest, Dialóg Campus, 2018.

https://doi.org/10.36250/01079_10

https://orcid.org/0000-0003-1024-4474

szintén megfigyelhető a kapcsolat a társadalom alapvető értékei és a nemzetállam stratégiai viselkedése között.

A stratégiaelméleti kutatások régóta keresik azokat a tényezőket, amelyek hatást gyakorolnak a stratégiai döntésekre. Az 1970-es években a nukleáris stratégiát vizsgálva alakult ki a stratégiai kultúra fogalma. Felismerve, hogy a szovjet és amerikai stratégák is bizonyos kulturális környezetben szocializálódott gondolkodók. A szocializációs folyamat során a nukleáris stratégiával kapcsolatban kialakult alapelvek, gondolkodásmód és viselkedésminták viszonylagos állandóságra tettek szert, beépülve ezáltal a kultúrába és felülemelkedve a nukleáris politika szintjén.[2] Ez a kapcsolat nem azt jelenti, hogy az adott kultúra meghatározza a stratégiaalkotás és a hadviselés valamely jellemzőjét, hanem láthatóan befolyásolja annak minden elemét. Egyes teoretikusok szerint a stratégia nemzeti szinten a társadalomnak a katonai erő használatával kapcsolatos értékrendjét tükrözi. Míg a második szint, a katonai kultúra fejezi ki azt, hogy az adott nemzet hogyan háborúzik.[3]

Az általános stratégiaelmélet a stratégiaalkotás folyamatában az első,[4] kulcsfontosságú lépésként azonosítja a stratégiai környezet értelmezését. Ez alapvetően a biztonsági környezet értelemzése, a stratégiai szintű nemzeti lehetőségek és az ezeket veszélyeztető fenyegetések azonosítása, beleértve a stratégiai vetélytársak vagy potenciális ellenfelek képességeit.[5] A célkitűzések eléréséhez használt stratégiai módszerek sokfélék lehetnek. Tipikusan ilyen az elrettentés két alapvető változata: a megtorló vagy büntető elrettentés *(deterrence by punishment),* valamint a védelem és az ellenállóképesség növelése *(deterrence by denial).* Stratégiai módszer lehet még például a szövetségesekkel való együttműködés vagy pont ellenkezőleg, a nemzetközi jogi normák ambivalenciáinak a kihasználása *(lawfare).* A stratégiai hármas utolsó eleme az erőforrások vagy eszközök hozzárendelése az adott célkitűzésekhez.[6] Ilyen eszköz például a katonai erő, a képzés és kutatás-fejlesztés, a diplomácia stb. A stratégiai kultúra tehát

[2] Szegő László: Az Amerikai Egyesült Államok stratégiai kultúrája. *Hadtudomány,* 24. (2014), 1–2. 25–34.

[3] Thomas G. Mahnken: *United States Strategic Culture.* (H. n.), Defense Threat Reduction Agency – Comparative Strategic Cultures Curiculum, 2006.

[4] Harry R. Yarger: *Strategic Theory for the 21st Century: The Little Book on Big Strategy.* U.S. Army War College Strategic Theory. Carlisle, Army War College Carlisle Barracks, Strategic Studies Institute, 2006.

[5] Yarger (2006): i. m.; Kovács (2018): i. m. (1. lj.).

[6] Yarger (2006): i. m.

kihat a stratégiaalkotás teljes folyamatára. Így a két szemlélet szintéziséből még teljesebb képet kaphatunk egy-egy nemzet stratégiai gondolkodásáról.

A kiberképességek kialakítása és integrálása az Amerikai Egyesült Államokban[7]

Az Egyesült Államok védelmi döntéshozatali és tervezőrendszerében a politikai-stratégiai szintet az elnök, a Nemzetbiztonsági Tanács, a védelmi miniszter és a Védelmi Minisztérium képviseli. A katonai-stratégiai szintet a Vezérkari Főnökök Egyesített Bizottságának (VFEB) főnöke *(Chairman of the Joint Chiefs of Staff)* és az egyesített műveleti parancsnokságok *(Unified Combatant Commands)* alkotják.

Az USA-ban a technikai fejlődés és a hadügy nagyon szorosan összefonódik. Edward Hunt amerikai történész például korabeli források alapján feltárta, hogy maga az informatikai biztonság mint diszciplína megszületése hogyan köthető a Pentagonhoz és még egy sor, a Védelmi Minisztériumhoz tartozó kutatóintézethez és vállalathoz, mint az IBM. A 1960-as években ezekben az intézményekben a komputerek sérülékenységének szisztematikus vizsgálatakor született eredmények nagyban hozzájárultak a mai sérülékenységvizsgálat *(pentesting)* szakterület kialakulásához.[8]

A hetvenes években, a számítógépek terjedésével felgyorsult a folyamat. Az 1990–91-es Öbölháború látványos sikereit követően sorra jelentek meg

[7] Az Egyesült Államok haderejében a katonai kiberműveletek (*cyberspace operations:* CO) jelenlegi fogalmi rendszerét konszolidáló 2018-as szakdoktrína, a Joint Publication 3-12 Cyberspace Operations, I-4. a következőképpen határozza meg a kiberképességet *(cyberspace capability):* „olyan eszköz vagy számítógépes program, beleértve a *software, firmware* vagy *hardware* bármilyen kombinációját, amelynek a célja, hogy valamilyen hatást érjen el a kibertérben vagy a kibertéren keresztül." Ez tehát a kiberképességek szűk, kizárólag technológiai értelmezése. Azonban, ahogy a fentiekben megfogalmaztuk, a kutatás a kiberműveletekkel kapcsolatos átfogó haderőfejlesztést vizsgálja. Ezért az amerikai hadseregben általánosan elterjedt doktrína, szervezet, kiképzés, hadfelszerelés, vezetés, állomány, infrastruktúra, szakpolitika (*doctrine, organization, training, material, leadership, personnel, facility, policy*: DOTMLPF-P) modellen keresztül értelmezem a képességeket. A doktrína szerint a kiberműveletek definíciója: „A kiberképességek alkalmazása olyan esetekben, amelyekben az elsődleges cél valamilyen feladat megvalósítása a kibertérben vagy azon keresztül." Cyberspace Operations, Joint Publication 3-12.

[8] Edward Hunt: US Government Computer Penetration Programs and the Implications for Cyberwar. *IEEE Annals of the History of Computing,* 34. (2012), 3. 4–21.

az egyes haderőnemi doktrínákban és védelmi minisztériumi iránymutatásokban az információs hadviselés, később információs műveletek gyűjtőnév alatt említett új hadviselési elvek. Végül a számítógép-hálózati műveletek (*computer network operations* – CNO) három fajtája, a támadó *(computer network offense),* védekező *(computer network defense)* és felderítő műveletek *(computer network exploitation)* először 1996-ban, az információs műveleteken belül, mint annak az egyik opcionális eleme jelentek meg.[9] Az amerikai haderőnél hagyományos, nagy fokú haderőnemi önállóság keretében a kilencvenes évek közepéig még nem szabályozták összhaderőnemi szinten a CNO vagy éppen az információs műveleti képességek kialakítását.[10]

A doktrínafejlesztésben a CNO-terminológia bevezetése után a következő központosítási kísérlet 2006-ban az első önálló nemzeti katonai kiberműveleti stratégia volt,[11] sokáig csak titkosított dokumentumként. Ez a következőképpen határozza meg a kiberteret: „olyan közeg, amely az elektronikai eszközök és az elektromágneses spektrum felhasználásával adatokat tárol, módosít és továbbít hálózatos eszközökön és fizikai rendszereken keresztül."[12] A kibertérre tehát mint önálló, védendő műveleti területre tekint, amelynek integrációja a többi műveleti közeggel és a fizikai térrel prioritás. Stratégiai célként a katonai kiberfölény *(cyberspace superiority)* kivívását jelöli meg, a tágabb nemzeti érdekek védelmét még nem említi. A központosítás a szervezet szintjén is megindult. 1998 decemberében a stratégiai szintű informatikai támadásokkal szembeni központosított védelem érdekében hozták létre az Összhaderőnemi Számítógéphálózati Védelmi Alkalmi Kötelék *(Joint Task Force – Computer Network Defence)* nevű egységet, amely kezdetben mindösszesen 24 főt számlált.[13]

[9] Az információs műveletek: „az elektronikai hadviselés, a számítógép-hálózati műveletek, a pszichológiai műveletek, a katonai megtévesztés és a műveleti biztonság integrált alkalmazása, összehangoltan bizonyos támogató és kapcsolódó képességekkel, amelyekkel befolyásolja, megzavarja, lerontja vagy korlátozza a szemben álló fél humán és automatizált döntéshozatali folyamatát, miközben megvédi a saját hasonló képességeket." (JP 3-13 2006, I-1). Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 176., 246.

[10] James Mulvelon (szerk.): *Addressing Cyber Instability.* Vienna (VA), Cyber Conflict Studies Association, 2012.

[11] The Chairman of the Joint Chefs of Staff: *National Military Strategy for Cyberspace Operations*. 2006.

[12] *National Military Strategy for Cyberspace Operations* (2006): i. m.

[13] U.S. Government Accountability Office: *Defense Department Cyber Efforts: DoD Faces Challenge in its Cyber Activities.* Report GAO-11-75. Washington D.C., 2011. július 25. 18.; Jeffrey L.

A következő fordulópont 2011-ben történt, amikor is az Obama-adminisztráció a kibervédelmi stratégia teljes körű megújításához fogott. Ne felejtsük el, hogy ekkorra túl voltunk néhány stratégiai jelentőségű eseményen a globális kibertérben, úgymint a 2007-es Észtország elleni informatikai támadás, a 2008-as grúz–orosz háború alatt indított kiberműveletek vagy 2010-ben az Egyesült Államokkal is kapcsolatba hozott Stuxnet. A Fehér Ház kidolgozta az USA első Nemzetközi Kiberstratégiáját, amelyben deklarálták, hogy a kibertérben az amerikai érdekeket akár fegyveres erővel is megvédik. Ugyanakkor a demokrata kormányzatokra jellemzően a diplomáciai eszközök és a szövetségesi együttműködés jelentősége nagymértékben felértékelődött. A Külügyminisztériumban kialakították a Kiberkoordinátori Irodát *(Office of the Coordinator for Cyber Issues),* és az USA, felvállalva a nemzetközi vezető szerepet, minden eddiginél nagyobb arányú kampányt indított a nemzetközi multilaterális diplomáciai fórumokon.

Szükség is volt a nemzetközi környezet megnyugtatására, mert a katonai kiberképességek kialakításában és alkalmazásában is léptékváltás történt. 2009 júniusában létrehozták az első Kiberparancsnokságot (*U.S. Cybercommand:* USCYBERCOM) mint Egyesített Alparancsnokságot *(Subordinate Unified Command).* Továbbá, az egyes haderőnemeknek 2010-re szintén meg kellett szervezniük a saját kiberparancsnokságukat. 2011-ben megújították a Védelmi Minisztérium Kibertérműveleti Stratégiáját, ezúttal nyilvánosságra hozva egy kivonatot. Először jelent meg az elrettentés koncepciója a kibervédelemmel kapcsolatban. Stratégiai célkitűzésként hangsúlyos az összkormányzati fellépés is. 2011-ben a Kongresszus jóváhagyta a nemzetközi támadó kiberműveleteket. Az USA ezzel egyértelműen deklarálta, hogy stratégiai szintű katonai kiberképességeket fejleszt annak érdekében, hogy megőrizze stratégiai dominanciáját, és megvédje az amerikai nemzeti érdekeket a kibertérben.

2013-ban újabb fordulópont jött. Bár először csak minősített dokumentumként, de megjelent az első összhaderőnemi kiberműveleti doktrína (JP3-12 Cyberspace Operations). Az összhaderőnemi kiberműveleti tervezés és végrehajtás eljárásrendjét megalkották, a szerep- és felelősségi köröket meghatározták, a hatásköröket kijelölték. Szervezetileg is előrelépés volt a Kiberműveleti Erők

Caton: *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*. U.S. Army War College, 2015.

(*Cyber Mission Forces:* CMF) koncepciójának kialakítása[14] és a Kiberparancsnokság, a haderőnemek[15] és a stratégiai szintű Összhaderőnemi Műveleti Parancsnokságok *(Unified Combattant Commands)* közötti együttműködés rendszere. Kitűzték a Kiberparancsnokságon belül 6500 fővel felállítandó kiberműveleti erők kiképzésének menetrendjét és a csapatok feladatrendszerét, beleértve a nemzeti védelmi célokat.

A 2015-re megújult védelmi minisztériumi kiberstratégia összefoglalja a fenti változásokat. Ezen kívül minden eddiginél részletesebben fejti ki egy komplex elrettentés koncepcióját, amely egy átfogó megközelítés jegyében magába foglalja mind a büntető, mind a „megtagadó" elrettentés számos eszközét. Az elrettentés komplex megközelítésének szintén fontos eleme az attribúció, a támadó kilétének azonosítása, amelynek érdekében a stratégia tovább erősíti a hírszerzés, a felderítés és a korai előrejelzés képességét. A stratégiában a kiberképességek fejlesztésében kiemelt stratégiai cél a kutatás-fejlesztés.[16]

2018-ra bontakozott ki az amerikai stratégiai gondolkodásban a kiberképességek kialakításával, integrációjával és alkalmazásával kapcsolatos rendszerszintű látásmód. 2018. május 4-én a Kiberparancsnokság tizedik egyesített műveleti parancsnoksággá való átszervezése megtörtént. A kiberműveleti erők elérték a teljes műveleti képességüket. Még ugyanebben az évben megjelent a kiberműveleti doktrína újabb kiadása. 2018-ra tehát kialakult a kiberképesség stratégiai szintű szervezetének alapvető struktúrája.

A következőkben az újonnan létrehozott kiberműveleti erők[17] tevékenységét tekintjük át. A CMF a haderőnemek legkiemelkedőbb tehetségeiből összeállított elit egységek, de nem tagozódnak be a haderőnemi hadosztályokba. Amint az *1. táblázat* mutatja, felosztásuk a feladatkör és a parancsnokság alapján történik.

Az úgynevezett National Mission Teams sokrétű feladatkörrel rendelkeznek, ők azok, akik elsősorban részt vesznek a Védelmi Minisztérium és a haderő védelmén túli nemzetvédelmi feladatokban. Egyfajta előretolt állásban gyakran a Védelmi Minisztérium információs hálózatain kívül eső, globális ellenséges *(red space)* vagy semleges hálózatokon *(grey space)* végeznek feladatokat a stratégiai jelentőségű fenyegetések felderítése és elhárítása (korai figyelmeztetés, támadó

[14] National Security Archive: *Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force.* George Washington University, 2019. május 3.

[15] Szárazföldi erő, légierő, haditengerészet, tengerészgyalogság.

[16] Department of Defence: *The DoD Cyber Strategy.* 2015.

[17] Az elnevezés a szerző fordítása.

műveletek stb.) érdekében.[18] Jól ismerik a kibertérben ellenséges tevékenységet végző szereplőket, és így a válaszlépéseket célra szabottan tervezik meg.[19]

1. táblázat: A kibererők feladatkör szerinti felosztása

Csapat típusa	Feladatkör
13 nemzeti kiberműveleti csapat(National Mission Teams)	Nemzeti szintű védelmi és támadó képességek
27 harci kiberműveleti csapat (Combat Mission Teams)	Az Egyesített Műveleti Parancsnokságok támogatása
18 nemzeti kibervédelmi csapat (National Cyber Protection Teams [CPTs])	A Védelmi Minisztérium információs hálózatainak a védelme
24 haderőnemi kibervédelmi csapat (Service CPTs)	A Védelmi Minisztérium információs hálózatainak a védelme
Egyesített védelmi minisztériumi információs hálózati kibervédelmi csapatok (DODIN CPTs)	A Védelmi Minisztérium információs hálózatainak a védelme
26 műveleti parancsnoksági kibervédelmi csapat (Combatant Command CPTs)	Az Egyesített Műveleti Parancsnokságok támogatása

Forrás: A JP3-12 alapján a szerző szerkesztése

A Védelmi Minisztérium információs hálózatainak védelméért a haderőnemek felelősek a saját használatukban lévő szegmensekben. Feladataik közé tartozik a hálózat konfigurálása, üzemeltetése és védelme. Jelentős előrelépés volt, amikor 2017-ben a Védelmi Minisztérium utasítása alapján a haderőnemi kiberparancsnokságok állandó tervező sejteket hoztak létre az egyesített műveleti parancsnokságokon belül.

A 2010-es évek végére megteremtették a kiberműveletek új osztályozási rendszerét is. A 2018-as kiberműveleti doktrína a műveletek célkitűzése vagy szándéka, valamint a műveleti környezet alapján három fő küldetési *(mission)* kategóriába osztja fel a kiberműveleteket: a Védelmi Minisztérium információs hálózatain végzett műveletek[20] *(DODIN operations);* kibertéri védelmi

[18] Mark Pomerleau: Here's How DoD Organizes Its Cyber Warriors. *C4ISRNet,* 2017. július 25.

[19] *Cyberspace Operations* (2018): i. m. I-9.

[20] A DODIN-műveletek magukba foglalják a már meglévő DOD-kibertér konfigurálását, üzemeltetését, kibővítését, informatikai biztonságát (CIA-követelmények). Ezek a tevékenységek tehát a hálózatra és annak sérülékenységeire fókuszálnak annak érdekében, hogy proaktív módon felkészüljenek a kibertérből érkező lehetséges fenyegetésekre.

műveletek (*defensive cyberspace operations:* DCO); és támadó kibertéri műveletek (*offensive cyberspace operations:* OCO).[21]

A stratégiai szintű Kiberparancsnoksággal párhuzamosan a négy fő haderőnem önállóan, a saját kötelékében alakította ki a kiberképességeit. A 6500 fős létszám tehát csak a közvetlenül a CYBERCOM-nak alárendelt erőket jelenti. A haderőnemek kötelékébe tartozó hadműveleti és harcászati szintű alakulatok ezenfelül szintén többezres létszámot tesznek ki.

2018 mérföldkő a hadsereg nemzeti kibervédelemben betöltött szerepének szempontjából is. Az ebben az évben kiadott nemzeti kiberbiztonsági stratégia kodifikálja a támadó kiberműveleteket a fegyveres konfliktusokon kívül is. Stratégiai célként az elrettentésre helyezi a hangsúlyt. Szintén ebben az évben a védelmi tervezés költségvetési aspektusának csúcsát jelentő nemzeti védelmi törvény *(National Defence Authorization Act)* stratégiai iránymutatásként jóváhagyta az úgynevezett „előretolt védelem" *(defend forward)* és az „állandó jelenlét" *(persistent engagement)* műveleti koncepcióját. Az előbbi felhatalmazást ad a Kiberparancsnokságnak a rosszindulatú kibertámadások megszakítására azok kiindulópontjában, tehát akár más országok területén is, beleértve a háborús küszöb alatti tevékenységet is, például a befolyásoló műveleteket. Az állandó jelenlét, tulajdonképpen a már meglévő gyakorlatot szentesítve, jóváhagyja az USA területén kívüli informatikai hálózatokban történő állandó jellegű felderítést és megfigyelést, valamint megelőző csapást is.[22] A politikai szintű stratégiai iránymutatások alapján tehát a hadsereg feladata nemcsak a katonai értelemben vett kibertér védelme, de már nem is csak a nemzeti kibertér védelme, hanem fokozatosan kiterjed a nemzeti érdekek globális kibertérben történő állandó, a fegyveres konfliktusokon kívüli védelmére is.

Az eddigiek alapján láthattuk, hogy az USA esetében a stratégiai kultúra miként befolyásolja a kiberhadviselési stratégia fejlődését. A katonai erő és a politika kapcsolata tekintetében az amerikai társadalomban, a nyugati társadalmakhoz hasonlóan, a háború a béke ellentéte, és nem a politika más eszközökkel történő folytatásának minősül. A hadsereg tevékenysége békeidőben és a hazai lakosság tekintetében szigorúan korlátozott. A rendelkezésre álló nagy mennyiségű erőforrás, az azonnali intézkedést és eredményeket elváró

[21] Caton (2015): i. m. 50.

[22] 115th Congress (2017–2018): H.R.2810 – National Defense Authorization Act for Fiscal Year. 2018; Greg Myre: ‚Persistent Engagement': The Phrase Driving A More Assertive U.S. Spy Agency. *National Public Radio,* 2019. augusztus 26.

és általában nem hosszú időre előre tekintő társadalom a döntő csaták lehetőségének keresését és a teljes erőkifejtést várja el, ami direkt stratégiai elgondolásokhoz vezet.[23] Az elrettentés tekintetében például a teoretikusok egy része éppen ezért túlfegyverkezést javasol *(overkill),* vagyis a katonai képességek jól látható maximalizálása az elrettentés részét képezi. A számbeli fölény mellett a katonai képességek és az erő meghatározója a technológiai fejlettség szintje. Ebből adódóan a felmerülő problémák megoldása során előszeretettel használják az innovatív technológiai megoldásokat.[24]

A kiberképességek kialakítása és integrálása Oroszországban

Ahogyan látni fogjuk, Oroszországban a hadelméletben a kiberképességek elemzése elválaszthatatlan az információs hadviseléstől. Jelenlegi állapotát a cári időkig visszanyúló, ciklikus megújuláson átesett fejlesztések csúcspontjának tekinthetjük. Az 1970-es évek felgyorsult számítástechnikai fejlődésére reagálva az 1980-as évekre a Szovjetunióban kidolgozták a katonai technikai forradalom elméletét, vagyis hogy a technológia hogyan fogja megváltoztatni a hadviselést. Olyan hadviselési formát vizionáltak rádióelektronikai hadviselés néven, amelyben nem szükséges az ellenfelet kinetikus csapásokkal legyőzni, hanem a kommunikációs és vezetési-irányítási, felderítő, megfigyelő, kommunikációs és informatikai képességek zavarására, lehallgatására vagy elpusztítására kell törekedni.[25] Azonban, míg az USA-ban a technológiai innováció játssza a legfontosabb szerepet a haderőfejlesztésben, addig Oroszországban – részben a korlátozott mértékben rendelkezésre álló anyagi források, részben pedig a hatalom eszközeinek teljesen más koncepcionális megközelítése miatt – a technológiai és a kognitív szféra sohasem vált el egymástól.

A kilencvenes években Oroszországra is nagy hatással volt az amerikai információs hadviselési képességek fejlesztése, és arra késztette, hogy kialakítsa saját koncepcióját ezen a téren. Az amerikai helyzethez hasonlóan ez az útkeresés időszaka volt.[26] Az információs háború kifejezésből a háború szót többféleképpen

[23] Szegő (2014): i. m. 30.

[24] Szegő (2014): i. m. 30–31.

[25] Dimitry Adamsky: *Cross-Domain Coercion. The Current Russian Art of Strategy*. Paris, The Institut Français des Relations Internationales, 2015. november.

[26] Az orosz stratégák természetesen felhasználták a saját tapasztalataikat is. Tanultak például az 1994–1996 között lezajlott első csecsen háborúból is, ahol a csecsenek rendkívül jól kihasználták

is lefordították oroszra: *informacionnaja vojna, informacionnaja borba* vagy *informacionnoje protyivoborsztvo.* Az elsőt inkább a média, míg a *protyivoborsztvo* kifejezést, amely küzdelmet, ellentevékenységet vagy konfliktust is jelenthet, illetve a *borba* kifejezést inkább a hadsereg használja.[27]

Első alkalommal a 2000-es nemzeti biztonsági koncepció osztotta az információs hadviselést két alcsoportra: technikai és pszichológiai információs képességekre. A technikai információs képességek alatt a következőket értették: a hírszerzés technikai formáit, az információvédelmet, a szupermagas elektromágneses frekvenciájú fegyvereket, az ultraszonikus fegyvereket, a rádióelektronikai ellentevékenységet, az elektromágnesesimpulzus-alapú fegyvereket, valamint az informatikai hardvert és szoftvert. A pszichológiai információs képességekhez sorolták a tömegtájékoztatást, a nem halálos fegyvereket, a pszichotróp szereket és egyéb kemikáliákat.[28] Egy másik beszámoló 2003-ból szintén a pszichológiai információs képességek között említi a dezinformációt, *maszkirovkát,* a kriptológiát és a *szteganográfiát.*[29]

A technológiai pillér a katonai technikai forradalom 1970-es évekbeli koncepciójáig nyúlik vissza. Mivel az információs hadviselés az ellenfél döntéshozatali folyamatára igyekszik hatást gyakorolni, az „aktív intézkedések" *(aktyivnije meroprijatyija)*, a *reflexív kontroll* és a *maszkirovka* kézenfekvő stratégiai módszernek bizonyul a pszichológiai információs hadviseléshez. Legfőbb eszközeik a megtévesztés, a dezinformáció, a propaganda, az álca, a rejtőzködés és a tagadás. Céljuk a célcsoport valóságészlelésének és azon keresztül a döntéshozatalának a befolyásolása olyan módon, amely az orosz érdekeket szolgálja. Ez tehát egy, a kognitív szférában történő hadviselés.[30] A célcsoport lehet a saját lakosság is.[31] Az orosz stratégiai gondolkodásban az „információs tér" *(informacionnoje prosztransztvo)* mindig is megbonthatatlan egységként kezelte a technikai

a modern információs környezet és a média által nyújtott lehetőségeket. Ezenkívül különösen nagy hatással voltak az orosz elit gondolkodására a színes forradalmak és az arab tavasz eseményei.

[27] Timothy L. Thomas: Russian Views on Information-Based Warfare. *Air Power Journal,* Special Edition, 1996.

[28] Timothy L. Thomas: *Comparing US, Russian, and Chinese Information Operations Concepts*. Foreign Military Studies Office, Fort Leavenworth, 2004b.

[29] Thomas (2004a): i. m.

[30] Timothy L. Thomas: Russia's Reflexive Control and the Military. *Journal of Slavic Military Studies,* 17. (2004b), 2.; Mark Galeotti: *Active Measures: Russia's Covert Geopolitical Operations.* Marshall Center, 2019. június.

[31] Vö. az USA jogrendje (Title 10 US Code 2241) tiltja a Honvédelmi Minisztérium számára a hazai propagandatevékenységet.

és a kognitív elemeket. A kibertér *(kiberprosztansztvo)* kifejezést először csak a nyugati szövegek fordításakor vagy az amerikai kibercsapásokkal kapcsolatosan használták. Ez az elmúlt öt-tíz évben kezdett megváltozni, és az orosz stratégiai diskurzusban megjelent a vita más országok koncepciójának átvételéről.[32]

Az orosz fenyegetettségpercepció az információs térben a politikai rendszer biztonságát veszélyeztető fenyegetésekre helyezi a hangsúlyt. A 2000-es nemzeti biztonsági koncepció[33] kifejti, hogy Oroszország folyamatos küzdelemben áll a nyugati hatalmakkal, akik titkosszolgálati eszközökkel szünet nélkül azon munkálkodnak, hogy befolyásolással a politikai rendszer ellen hangolják a közvéleményt. Az információs térben folytatott küzdelem olyannyira felértékelődött, hogy akár a stratégiai győzelem eszköze is lehet, és így az orosz stratégiai elrettentés részét képezi.[34]

A 2010-es évekre érett be az a fordulat az orosz politikai és katonai gondolkodásban, amely során – a nyugati katonai technikai képességfejlesztéshez képesti lemaradást ellensúlyozandó – egy indirekt stratégián alapuló, a katonai és a nem katonai eszközöket (politikai, hírszerzési, diplomáciai, információs, gazdasági stb.) vegyítő stratégiát vezettek be.[35] 2013. március 24-én Valerij Geraszimov hadseregtábornok a Hadtudományi Akadémia plenáris ülésén mondta el híres beszédét az ezen elveket összegző új generációs hadviselésről.[36] A 2008-as orosz–grúz háborút követően átfogó modernizáció indult meg, amelyben kiemelt szerepet kap az információs képességek fejlesztése. Nem véletlen, hogy az információs háború új, átfogó definíciója is ekkor jelent meg a stratégiai dokumentumokban. 2011-ben az Oroszországi Föderáció fegyveres erejének információs térbeli tevékenységének koncepciója így fogalmaz:

> „Az információs háború *(informacionnaja vojna)* egy, az információs térben két vagy több állam között történő konfrontáció, amelynek a célja az információs rendszerekben, folyamatokban és erőforrásokban történő károkozás, a politikai, gazdasági és társadalmi rendszerek gyengítése érdekében, a népesség masszív pszichológiai manipulációja az állam és a társa-

[32] Timothy L. Thomas: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 2014.

[33] A nemzeti biztonsági koncepció 2009-től nemzeti biztonsági stratégia.

[34] M. A. Garejev: Sztratyegicseszkoje szderzsivanyije. Problemi i resenyija. *Krasznaja Zvezda,* No. 183., 2008. február 8.

[35] Timothy L. Thomas: *Russia. Military Strategy.* Fort Leavenworth, Foreign Military Studies Office, 2015; Valerij Geraszimov: Cennoszty Nauki v Predvigyinyiji. *Vojenno-Promislennyij Kurjer Online,* 2013. február 27.

[36] Geraszimov (2013): i. m.

> dalom destabilizálása érdekében, valamint kényszerítő eszköz, hogy az állam az ellenfél számára kedvező döntéseket hozzon."[37]

Az információs tevékenységet folytató szervezetek rendszere és működése sokkal kevésbé ismert, mint az USA esetében. A Szövetséges Biztonsági Szolgálat (*Fegyeralnaja szluzsba bezopasznosztyi Rosszijszkoj Fegyeraciji* – FSZB), az Állambiztonsági Bizottság (*Komityet goszudarsztvennoj bezopasznosztyi* – KGB) utódszervezete főként a belbiztonságért felel, beleértve az infokommunikációs rendszerek biztonságát. Nyugati szakértők az FSB-hez kötik például a Turla Advanced Persistent Threat- (APT-) csoportot.[38] A katonai hírszerző szolgálat, az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnöksége (*Glavnoje razvegyivatyelnoje upravlenyije* – GRU) az FSB-vel közösen hajtotta végre, többek között, a 2007-es észtországi és a 2008-as Grúzia elleni informatikai támadást, a 2016-os amerikai félidős választások alatti kampányt vagy a NotPetya-műveletet. Egységei rendelkeznek az információs műveletek technikai és pszichológiai eszköztárával. Egy-egy tevékenységre specializálódnak, mint például a *malware*-fejlesztés, a szivárogtatás vagy a propaganda. A 85. Különleges Szolgálati Központ (az úgynevezett 26165-ös egység) például rádióelektronikai felderítést és kriptológiai tevékenységet folytat, de ezt hozzák összefüggésbe az APT28-as csoporttal is, amely ismert Fancy Bear, Pawn Storm, Sofacy, Strontium néven is. Egy másik ismertté vált alakulat, a Különleges Technológiai Főközpont (az úgynevezett 74455-ös egység) kiberműveleteket végez, példának okáért a 2016-os amerikai kampányt vagy az ukrajnai infrastruktúra elleni támadásokat.[39] A harmadik nagyobb szervezet, amelyet gyakran hoznak kapcsolatba az információs térben történő tevékenységekkel, az Oroszországi Föderáció külföldre irányuló polgári hírszerző szervezete, a Szluzsba vnyesnyej razvedki Rosszijszkoj Federaciji (SZVR), amelyet APT29 vagy Cozy Bear hackercsoportként azonosítottak. Ezt teszik felelőssé például a Covid–19-vakcinákkal vagy a SolarWindsszel kapcsolatos kémkedésért is. Mindkét szervezet létszáma titkos, de orosz források szerint a GRU személyi állománya többszöröse a polgári hírszerző szolgálatának. A GRU-val ellentétben, amely szabotázs-, kiber- és információs műveleteket is végrehajt, az SZVR inkább hagyományos

[37] The Russian Ministry of Defense: *Russian Federation Armed Forces' Information Space Activities Concept*. Moszkva, 2011.

[38] Janne Hakala – Jazlyn Melnychuk: *Russia's strategy in cyberspace.* Riga, NATO Strategic Communications Center of Excellence, 2021.

[39] Hakala–Melnychuk (2021): i. m.

hírszerző tevékenységet folytat.[40] A „klasszikus" hírszerző szervezetek mellett számos egyéb, homályos hátterű szervezet is folytat tevékenységeket az információs térben. Ilyenek például az úgynevezett katonai tudományos cégek *(naucsnyije kompanyiji),* a félkatonai hazafias hackercsoportok, mint a CyberBerkut, a különböző bűnözői csoportok vagy a hírhedtté vált, szentpétervári trollfarm, az Internetkutató Ügynökség *(Agentsztvo Internet-Isszledovanyij),* amely egy, a Kremlhez szorosan köthető magánvállalat.

Összességében elmondható, hogy az orosz stratégiai gondolkodásban az információs konfrontáció megközelítése holisztikus, ötvözi a digitális-technológiai megoldásokat a kognitív pszichológiai eszközökkel. Egységesen használható stratégiai eszköznek tekinti a katonai és a nem katonai, a kinetikus és a nem kinetikus megoldásokat, illetve az állami és nem állami szereplőket. Továbbá, nem választja el élesen a háború és a béke állapotát, a lakosságot a fegyveres erőktől vagy a hazai és a nemzetközi népességet mint célközönséget. Előszeretettel választja a megtévesztés, rejtés és álcázás módszereit, és így a stratégiai célokhoz jellemzően titkosszolgálati vagy zavaros hátterű végrehajtó szervezeteket rendel.

Esettanulmány

Az elmúlt időszak egyik legjelentősebb informatikai ellátási láncot ért eseménye a SolarWinds Orion hálózatkezelő szoftverén keresztül több ezer számítógép-hálózaton elhelyezett kémprogram volt. Az úgynevezett Sunburst rosszindulatú programot használó műveletet 2020 decemberében fedezték fel, de szakértők szerint egészen 2019 októberéig nyúlik vissza. Több száz amerikai szervezet érintett az adatlopásban, köztük egy tucat kormányhivatal, mint például a Pénzügyminisztérium, a Pentagon, a Belbiztonsági Minisztérium és azon belül a szövetségi számítógép-hálózatok biztonságáért felelős ügynökség (*Cybersecurity and Infrastructure Security Agency* – CISA), de érintett a Microsoft, az Intel és a Cisco is.[41]

Az eset a célpontok, a kompromittált adat mennyisége és a támadás jellege miatt különösen érzékeny nemzetbiztonsági szempontból, illetve még nem lehet

[40] Hakala–Melnychuk (2021): i. m.

[41] Justin Katz: Cyber Exec: 50 Orgs 'Genuinely Impacted' by Solarwinds Hack. *FCW,* 2020. december 21.

biztosan tudni, hogy csak kémkedésre használták-e, vagy további károkozásra alkalmas mechanizmusokat is bejuttattak az elkövetők.

További kérdéseket vet fel a hatékony és jogszerű válaszlépés. A hálózatok működését akadályozó vagy az informatikai rendszereket romboló beavatkozások esetén a nemzetközi jog felhatalmazást ad a károkozás megszüntetésére irányuló és azokkal arányos ellenlépésekre.[42] Ugyanakkor önmagában a kémkedést a nemzetállamok hallgatólagos megegyezése alapján nem bünteti a nemzetközi jog. A nemzetállamok a saját hatáskörükben foganatosíthatnak diplomáciai vagy büntetőjogi lépéseket. 2016 óta az USA élen jár a gazdasági és pénzügyi szankciók alkalmazásában a jelentős kibertámadások elkövetőivel szemben.

A korábbi esetekhez hasonlóan ebben az esetben is komplex, „látható és nem látható" lépésekből álló válaszadás történt. 2021 áprilisában Joseph Biden átfogó elnöki rendeletben megnevezte az SVR APT29 csoportját mint a SolarWinds-kémkedésikampány elkövetőjét, és újabb pénzügyi szankciókat vetett ki Oroszország káros nemzetközi tevékenysége ellen, beleértve a kiberteret. Ezen kívül kiutasítottak 10 orosz diplomatát.[43]

A SolarWinds-kampányt az amerikai kiberhadviselési stratégia kontextusában is kiértékelték. Szakértők rámutattak, hogy ez nem az előretolt védelem és az állandó jelenlét koncepciójának kudarcát jelenti, hanem arra hívja fel a figyelmet, hogy ez a két műveleti koncepció és az offenzív kiberműveleti képesség önmagában nem nyújt elégséges elrettentő erőt. Sokkal nagyobb hangsúlyt kell fektetni a kormányzati és a magánszektor informatikai védelmének szabályozására.[44]

Irodalomjegyzék

115th Congress (2017-2018): H.R.2810 – National Defense Authorization Act for Fiscal Year 2018. Online: www.congress.gov/bill/115th-congress/house-bill/2810/text

Adamsky, Dimitry: *Cross-Domain Coercion. The Current Russian Art of Strategy.* Paris, The Institut Français des Relations Internationales, 2015. november. Online: www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

[42] Michael M. Schmitt (szerk.): *Tallin Manual 2.0.* Cambridge, Cambridge University Press, 2017.

[43] The White House: *Fact Sheet. Imposing Costs for Harmful Foreign Activities by the Russian Government* (2019. április 15.).

[44] Robert Morgus: The SolarWinds Breach Is a Failure of U.S. Cyber Strategy. *Lawfare,* 2020. december 18.

Caton, Jeffrey L.: *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications.* U.S. Army War College, 2015.

Department of Defence, Joint Staff: *Cyberspace Operations. Joint Publication J-P 3-12.* Washington D.C., 2018.

Department of Defence, The Chairman of the Joint Chiefs of Staff: *National Military Strategy for Cyberspace Operations.* 2006. Online: www.hsdl.org/?abstract&did=35693

Department of Defence: *The DoD Cyber Strategy.* 2015.

Galeotti, Mark: *Active Measures: Russia's Covert Geopolitical Operations.* Marshall Center, 2019. június. Online: www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0

Garejev, M. A.: Sztratyegicseszkoje szderzsivanyije. Problemi i resenyija. *Krasznaja Zvezda,* No. 183., 2008. február 8.

Geraszimov, Valerij: Cennoszty Nauki v Predvigyinyiji. *Vojenno-Promislennyij Kurjer Online,* 2013. február 27. Online: https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.

Hakala, Janne – Jazlyn Melnychuk: *Russia's strategy in cyberspace.* Riga, NATO Strategic Communications Center of Excellence, 2021.

Hunt, Edward: US Government Computer Penetration Programs and the Implications for Cyberwar. *IEEE Annals of the History of Computing,* 34. (2012), 3. 4–21. Online: https://doi.ieeecomputersociety.org/10.1109/MAHC.2011.82

Katz, Justin: Cyber Exec: 50 Orgs 'Genuinely Impacted' by Solarwinds Hack. *FCW,* 2020. december 21. Online: https://fcw.com/articles/2020/12/21/sunburst-hack-fifty-orgs-russia.aspx

Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018.

Mahnken, Thomas G.: *United States Strategic Culture.* (H. n.), Defense Threat Reduction Agency – Comparative Strategic Cultures Curiculum,Comparative Strategic Cultures Curiculum, 2006. Online: https://irp.fas.org/agency/dod/dtra/us.pdf

Morgus, Robert: The SolarWinds Breach Is a Failure of U.S. Cyber Strategy. *Lawfare,* 2020. december 18. Online: www.lawfareblog.com/solarwinds-breach-failure-us-cyber-strategy

Mulvelon, James (szerk.): *Addressing Cyber Instability*. Vienna (VA), Cyber Conflict Studies Association. 2012.

Myre, Greg: ‚Persistent Engagement': The Phrase Driving A More Assertive U.S. Spy Agency. *National Public Radio,* 2019. augusztus 26. Online: www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency

National Security Archive: *Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force*. George Washington University, 2019. május 3. Online: https://nsarchive.gwu.edu/news/cyber-vault/2019-05-03/preparing-computer-network-operations-uscybercom-documents-trace-path-operational-cyber-force.

Pomerleau, Mark: Here's How DoD Organizes Its Cyber Warriors. *C4ISRNet,* 2017. július 25. Online: www.c4isrnet.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/

Schmitt, Michael. M. (szerk.): *Tallin Manual 2.0.* Cambridge University Press, 2017.

Szegő László: Az Amerikai Egyesült Államok stratégiai kultúrája. *Hadtudomány,* 24. (2014), 1–2. 25–34. Online: www.mhtt.eu/hadtudomany/2014/1_2/2014_1_2_3.pdf

The Russian Ministry of Defense: *Russian Federation Armed Forces' Information Space Activities Concept.* Moszkva, 2011. Online: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

The White House: *Fact Sheet. Imposing Costs for harmful foreign activities by the Russian Government* (2019. április 15.). Online: www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

Thomas, Timothy L.: *Russia. Military Strategy.* Fort Leavenworth, Foreign Military Studies Office, 2015.

Thomas, Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 2014. Online: https://doi.org/10.1080/13518046.2014.874845.

Thomas, Timothy L.: *Comparing US, Russian, and Chinese Information Operations Concepts*. Fort Leavenworth, Foreign Military Studies Office, 2004a.

Thomas, Timothy L.: Russian Views on Information-Based Warfare. *Air Power Journal,* Special Edition, 1996. Online: https://apps.dtic.mil/sti/pdfs/ADA529685.pdf

Thomas, Timothy L.: Russia's Reflexive Control and the Military. *Journal of Slavic Military Studies,* 17. (2004b), 2. Online: www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

U.S. Government Accountability Office: *Defense Department Cyber Efforts: DoD Faces Challenge in its Cyber Activities*. Report GAO-11-75. Washington D.C., 2011. július 25.

Yarger, Harry R.: *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. U.S. Army War College Strategic Theory. Carlisle, Army War College Carlisle Barracks, Strategic Studies Institute, 2006.