Végh Ferenc ny. vezérezredes:

NEMZETKÖZI SZAKIRODALMI SZEMLE

A SZERZŐRŐL:
Dr. Végh Ferenc ny. vezérezredes (PhD), a Magyar Honvédség korábbi parancsnoka, vezérkari főnöke, nyugalmazott nagykövet (ORCID: 0000-0003-1688-6574; MTMT: 10087268)

VALÓS VESZÉLY: ATOMERŐMŰVEK A HÁBORÚBAN

A CIKK SZERZŐJÉRŐL: Henry D. Sokolski a Nonproliferation Policy Education Center washingtoni székhelyű nonprofit szervezet ügyvezető igazgatója. A szervezetet 1994-ben alapították azzal a céllal, hogy elősegítse a stratégiai fegyverek elterjedésével kapcsolatos tájékoztatást a politikai döntéshozók, a tudósok és a média körében. Posztgraduális szintű órákat tart a nukleáris politikáról Washingtonban, emellett a nukleáris biztonsági tanulmányok főmunkatársa a Kaliforniai Egyetemen.

FORRÁS: Henry D. Sokolski: Present Danger: Nuclear Power Plants In War. The US Army War College Quarterly: Parameters, 2022/4. (18. 11. 2022.), 5–13. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3183&context=parameters (Letöltés időpontja: 2022. 11. 02.)

A szerző szerint azt követően, hogy Oroszország elfoglalta az ukrajnai zaporizzsjai atomerőművet, az Amerikai Egyesült Államoknak módosítania kell katonai tervezését és politikáját annak érdekében, hogy kezelni tudja azt a helyzetet, amikor ellenséges katonai erők nagy, működő atomerőműveket vesznek célba, elfoglalják azokat, valamint fegyveres erőket telepítenek területükre. Világossá kell tennie álláspontját, hogy az ilyen erőműveket esetleg célpontnak tekinti-e. Ez az első olyan cikk, amely ezeket az aggályokat elemzi. Összehasonlítja Oroszország támadásait a közel-keleti kutatóreaktorok és a nem működő atomerőművek ellen, és tisztázza, milyen új katonai intézkedésekre és politikára lesz szükség a nagy és működő atomerőművek elleni hadműveletek esetén.

Zaporizzsja atomerőműve a jelen állás szerint hideg leállás üzemmódban van. Az erőmű és katonai sérülékenysége azonban téma lett a világsajtóban. 2022 nyarának elején az online jelentések fényképeket mutattak az erőmű megsérült transzformátoráról, amely kritikus fontosságú az erőmű legfontosabb reaktorhűtő és biztonsági rendszereinek folyamatos áramellátásához. Augusztusban és szeptemberben a hírek részletezték, hogyan vágták el az erőmű külső fővezetékeit, amelyeket azért építettek, hogy a reaktorokat szükség esetén kívülről elláthassák árammal. Egyes napokon az erőmű hat reaktora közül néhány működött, más napokon egyik sem. Az erőmű dízel üzemanyaggal működő vészhelyzeti elektromos generátorainak életképessége a legfontosabb téma volt.

E történetek mindegyike felvetette egy katonai eszközökkel létrehozott „Fukusima" lehetőségét: csapások az erőmű vagy az azt tápláló távvezetékek ellen, amelyek megszakíthatják a reaktorok hűtőfolyadék-szivattyúinak és biztonsági berendezéseinek működtetéséhez szükséges áramot, majd a nukleáris folyamat ellenőrizetlenné válása hatalmas radiológiai sugárzást eredményezhet Ukrajnában és szomszédjainál.

Ami még mindig hiányzik, az a Pentagon értékelése arról, hogy mindez mit jelent katonai szempontból. A közeli barátok tippeket adtak. A japánok biztonsági erők állomásoztatását szorgalmazzák minden japán atomerőműnél, javasolják rakétavédelmi rendszerek esetleges telepítését is (ahogyan azt Fehéroroszország 2019 óta teszi atomerőművénél). Szöul 2022-ben hadgyakorlatokat tervezett az amerikai erőkkel, ahol többek között robbanóanyagok telepítését és felrobbanását is imitálták egy vagy több dél-koreai reaktornál. Az ukrán elnök azzal vádolta Oroszországot, hogy Zaporizzsját egy előretolt, lassan égő, sugárzást szétterítő „nukleáris fegyverré" változtatta. Eközben a brit alsóház védelmi különbizottságának elnöke ragaszkodott ahhoz, hogy ha Oroszország szándékosan csap le Zaporizzsjára és ezáltal káros radioaktivitás éri Lengyelországot vagy Romániát, akkor az kiváltja a NATO 5. cikkelyében foglaltakat. Moldova, Románia és Ukrajna már cselekedett is, amikor mindhárom országban felkészültek jódtabletták kiosztására, ha Zaporizzsja atomerőművéből radioaktív sugárzás szabadul ki, hogy csökkentsék a pajzsmirigyrák kialakulásának esélyét.

Milyen következtetéseket vont le ezekből a Pentagon? Eddig nem sokat. A Védelmi Minisztérium szóvivője pusztán a zaporizzsjai erőmű elleni orosz katonai támadások veszélyességét és „felelőtlenségét" állapította meg. Elvárható lett volna azonban, hogy hivatkozzon azokra az értékelésekre, amelyeket a minisztérium az iráni, iraki, izraeli és szíriai reaktorok ellen végrehajtott több mint 13 katonai támadást követően készített. Lehetséges azonban, hogy a minisztérium nem végzett ilyen értékeléseket. Ha léteznének ilyen értékelések, az segítene tisztázni, miben különböznek a zaporizzsjai támadások a Közel-Keleten elkövetett támadásoktól, és mit jelentenek ezek a különbségek.

Ez utóbbi kérdésre a rövid válasz bőven elegendő. Először is, a közel-keleti támadások egyike sem irányult működő reaktorok ellen. A zaporizzsjai erőmű viszont a háború előtt több atomenergiát termelt, mint bármely más európai erőmű. Oroszország Zaporizzsja elleni támadásával valóságossá vált az esetleges jelentős radiológiai kibocsátás veszélye; a korábbi közel-keleti támadásoknál nem volt ilyen helyzet. Másodszor, a Zaporizzsja elleni támadásokkal ellentétben a közel-keleti reaktorok elleni csapások egyikét sem hajtották végre nagy hatótávolságú precíziós drónokkal vagy rakétákkal, hanem bombázó-repülőgépekkel vagy pontatlan Scud rakétákkal.

A közel-keleti csapások ráadásul a teljes atomerőmű megsemmisítésére irányultak, nem egyes alrendszereire. Zaporizzsjánál nem ez történt. Különböző időpontokban és külön-külön is csapás érte az erőmű transzformátorát, kiiktatták a négy bejövő távvezetéket, és csapás érte a kiégett fűtőelemek tárolóját is. Mindegyik támadás félelmeket keltett. Ezzel szemben a közel-keleti reaktorok elleni korábbi támadások vagy totálisak, vagy viszonylag ártalmatlan céltévesztések voltak.

Harmadszor, a megtámadott közel-keleti erőművek egyikét sem foglalta el és nem üzemeltette a támadó fél. Zaporizzsját viszont az oroszok nemcsak elfoglalták és átvállalták annak működtetését, hanem tüzelőállásként is használták, károsították a berendezéseket, befolyásolták, hogy mennyi áramhoz juthatnak az ukránok. Oroszország azzal is fenyegetőzött, hogy az erőmű elektromos termelését Oroszország felé, illetve keletre és délre fekvő orosz kézben lévő területetekre irányítja.

Negyedszer, a közel-keleti üzemek egyike sem volt nagyvárosi területek közelében. A háború előtt Zaporizzsjában és környékén közel 1,7 millió lakos volt, de sok százezren élnek még ma is itt. A radiológiai sugárzás veszélyére tekintettel evakuálták a lakosságot. Ennyi lakos egyidejű megmozdulása azonban az ukránok és az oroszok számára is megnehezítette a helyi katonai műveleteket. Ennél is fontosabb az, hogy a reaktor által esetleg kibocsátott radioaktivitás több irányba is terjedhet. Ha a szél nyugat felől fújna (ami a leggyakoribb),

akkor Oroszország szenvedne; ha kelet felé, akkor Ukrajna és a NATO-tag Románia; ha észak felé, akkor Lengyelország és esetleg más NATO-tagállamok; délen pedig Törökország, egy másik NATO-tagállam. Egy nyári időszakban történő észak-koreai támadás a dél-koreai reaktorok ellen több radioaktivitást eredményezne Japán felett, mint Dél-Korea felett. Télen ennek a fordítottja történne. E megfontolások egyike sem volt tényező a korábbi közel-keleti támadásokban.

Végül, és ehhez kapcsolódóan, a megcélzott közel-keleti reaktorok egyike sem volt olyan államokban vagy azok szomszédságában, amelyeket az Amerikai Egyesült Államoknak szerződés alapján meg kellene védenie. Washingtonnak nincs szerződéses biztonsági garanciája a Közel-Kelet egyetlen államára, még Izraelre sem. Ugyanakkor a garanciák megvannak a NATO számára Európában, Japánban és Dél-Koreában. A legtöbb tagállam nagy reaktort üzemeltet. Így van ez Japánban, Dél-Koreában, de Tajvan is üzemeltet atomerőműveket. A kínai, az orosz és az észak-koreai hatóságok szerint ezek az erőművek célpontok lehetnek. Dél-Korea, Japán, Moldova, Románia és Tajvan már védekezési intézkedéseket fontolgat.

Mit tegyen a Pentagon, ha valamit tennie kell? – teszi fel a kérdést a cikk írója, amire választ is ad. Mérje fel a háború katonai, elrettentő és biztonsági vonatkozásait ott, ahol atomerőművek működnek, azaz Európában, a Közel-Keleten és Ázsiában. Ezeknek a hadszíntereknek mindegyike amerikai katonai bázisoknak ad otthont.

Ha a térség reaktorait támadás éri, mennyire lehetnek sebezhetők az amerikai csapatok az esetleges sugárzással szemben? Milyen aktív vagy passzív védekezési intézkedések lennének hasznosak számukra? Mit tegyenek az amerikai csapatok, ha egy állam, amelynek biztonságát az Amerikai Egyesült Államok garantálja, segítséget kér, miután valamelyik reaktorát eltalálták, vagy ha polgárait sugárzás éri, miután csapást mértek a szomszédos ország atomerőművére? Milyen segítséget kell a Pentagonnak felajánlania, ha van egyáltalán ilyen segítség? A Pentagonnak készen kell-e arra állnia, hogy felajánlja az ilyen támadások után esetlegesen elveszett áram vészhelyzeti pótlását? Háborúban vagy békeidőben a Pentagonnak lég- és rakétavédelmet, hírszerzést vagy elsősegélynyújtói segítséget kellene nyújtania a baráti nemzetek atomerőműveinek védelmében? Milyen formákat ölthet ez a segítségnyújtás? Milyen ellentámadások tekinthetők arányosnak a szövetséges atomerőművek elleni csapásokkal szemben? A Pentagon válaszai országonként eltérők lehetnek.

Ezeknek a kérdéseknek az általános következtetéseit a szerző szerint azonban be kell iktatni a jövőbeli nukleáris állapot felülvizsgálatába, és a Pentagon védelmi iránymutatásainak részét kell képezniük. A megvalósítás azonban nehéz lehet. Jelenleg nincs olyan hivatal, amely az ilyen elemzések elvégzéséért felelős. A regionális parancsnokságok nem érzik magukat felelősnek e feladatok elvállalásában, hacsak nem kényszerítik őket. A Pentagon Nukleáris Elrettentési Politika Hivatala a Nyílt Felügyelet Védelmi Protokollban, a Beszerzési Hivatal (Nukleáris, Vegyi és Biológiai) államtitkár-helyettesének hivatala és a Védelmi Minisztérium stratégiai ügyekért felelős helyettes államtitkárának hivatala mind megfelelő helyek ezeknek az ügyeknek a befogadására, de eddig egyik sem vette át ezt a feladatot.

A Kongresszus utasíthatja e szervezetek vagy személyek bármelyikét, hogy vállaljon vezető szerepet a szükséges atomerőmű-elemzések elkészítésében. A Pentagonnak aktívabban kellene foglalkoznia az Amerikai Egyesült Államok nukleáris exportengedély-kérelmeinek felülvizsgálatával, tekintettel arra, hogy az ilyen erőművek mennyire lehetnek sebezhetők a katonai támadásokkal szemben. A Pentagon már most is vezető szerepet tölt be a lehetséges jövőbeli háborús övezetek helyének meghatározásában. Ez a követelmény aligha új kérdés, hiszen már az 1978-as nukleáris proliferáció elleni törvény is megköveteli, amely elvárja a Védelmi Minisztériumtól, hogy kommentálja az Amerikai Egyesült Államok polgári nukleáris exportjának nemzetbiztonsági vonatkozásait.

A Védelmi Minisztériumnak felül kell vizsgálnia és meg kell erősítenie az atomerőművek háborús célkijelölésre vonatkozó jelenlegi útmutatását. India, Irán, Izrael, Pakisztán, Törökország és az Amerikai Egyesült Államok kivételével a világ összes nemzete ratifikálta a genfi egyezmény 1977. évi I. jegyzőkönyvét. Ennek III. fejezete határozottan elutasítja a villamosenergia-termelő nukleáris erőművek megcélzását. Oroszország 2019-ben kilépett az egyezményből. Washington 1977-ben aláírta a jegyzőkönyvet, jelezve, hogy szándékában áll ratifikálni – de ezt soha nem tette meg.

A katonai erők aligha akarnak majd egy atomreaktor közelében lévő régiókban tevékenykedni, vagy felszabadítani azokat, ha a csapás után sugárzás éri a környékét. Washington el akarja ítélni Moszkvát a zaporizzsjai üzem elleni támadások miatt. Ugyanakkor a Pentagon 2016. évi haditörvény-kézikönyve lehetővé teszi az amerikai katonai parancsnokok számára, hogy célba vegyenek atomerőműveket, ha ezt „fontosnak" tartják. Hasznos lenne, ha a Pentagon legalább annyira egyértelművé tenné az atomerőművek megtámadásával szembeni elveket, mint amennyire a jegyzőkönyvben szerepel. Érdemes lenne még tisztázni, hogy a villamosenergia-termelő nukleáris állomásoknak magukban kell-e foglalniuk a kapcsolódó nukleáris létesítményeket, például újrafeldolgozó üzemeket, a kiégett fűtőelemek tárolóhelyeit stb.

Egy másik megoldásra váró kérdés az, hogy mi legyen az Amerikai Egyesült Államok politikája a nagy kutatóreaktorok elleni támadásokkal kapcsolatban. Ezt úgy lehetne megoldani, hogy felkérik a Pentagont a haditörvény-kézikönyv átdolgozására. Logikus lenne, ha a Kongresszus az ilyen reaktorok célként történő kijelölését a főparancsnokra bízná. A Zaporizzsjánál történtek után a polgári atomerőműveket „előre telepített" nukleáris fegyvereknek kell tekinteni, amelyek rombolása esetén potenciálisan hatalmas mennyiségű sugárzás terjedhet szét több ezer négyzetkilométeren, így egy reaktor megtámadása több mint hadszintéri vagy harcászati kérdés – állapítja meg írása végén a szerző.

MENNYIRE HATÉKONYAK KATONAI SZEMPONTBÓL OROSZORSZÁG KIBERMŰVELETEI UKRAJNÁBAN?

A CIKK SZERZŐJÉRŐL: Jon Bateman a Harvard Egyetem jogi karán és a Johns Hopkins Egyetemen szerzett diplomát. Jelenleg a Carnegie Alapítvány a Nemzetközi Békéért munkatársa, de dolgozott az amerikai Egyesített Vezérkar elnökének asszisztenseként és szövegírójaként, illetve a hadügyminisztérium kiberstratégiai szakértőjeként és a Védelmi Hírszerző Ügynökség elemzőjeként. Cikkei számos neves folyóiratban megjelentek, de televízióban és rádióban is gyakran kikérik a véleményét.

FORRÁS: Jon Bateman: Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Carnegie Endowment for International Peace, 16. 12. 2022., 5–31. https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf (Letöltés időpontja: 2023. 03. 26.)

Jon Bateman tanulmányának első része – az alábbiakban ennek a bemutatását olvashatjuk – betekintést nyújt Oroszország Ukrajnában végrehajtott kiberműveleteinek hatékonyságába. Bevezetőjében megállapítja, hogy mióta Oroszország 2022. február 24-én megtámadta Ukrajnát, a legtöbb nyugati kommentátor lekicsinyli a támadó kiberműveletek szerepét Moszkva tágabb háborús erőfeszítéseiben. Elemzők az orosz kiberműveleteket szórványosnak, egyszerűnek, rosszul megtervezettnek, rosszul integráltnak nevezték, és végső soron

alig hatékonynak a fegyverek okozta halálesetekhez és pusztításokhoz képest. A szakértők különböző magyarázatokat kínálnak arra vonatkozóan, hogyan és miért akadtak el az orosz kiberműveletek Ukrajnában, de a legtöbben egyetértenek az alapvető katonai kérdésben: a kiberműveletek nem mozdították elő jelentősen Moszkva műveleti céljainak megvalósulását.

Nem mindenki osztja ezt a nézetet. A prominens másként gondolkodók között van néhány nyugati kormányzati tisztviselő, akik úgy vélik, hogy a külső elemzők alábecsülték Oroszország háborús kiber erőfeszítéseit Ukrajna ellen. Szerintük az orosz kiberműveletek nagy léptékűek, katonailag hatékonyak a kulcsfontosságú pillanatokban, valamint összhangban állnak Moszkva katonai céljaival, vagyis az ukrán kormány, a fegyveres erők és a polgári lakosság megzavarásával és megfélemlítésével.

Az ilyen nézeteltérések részben töredékes, egymásnak ellentmondó és folyamatosan változó információkból fakadnak. Erre példa, hogy február 24-én az orosz katonai hírszerzés megzavarta a Viasat műholdas kommunikációs hálózatát. A feltörés óriási érdeklődést váltott ki az időzítése (egy órával az orosz csapatok határátlépése előtt) és egyértelmű katonai célja (az ukrán kommunikáció zavarása) miatt. A Viasat meghekkelésének végső katonai hatása azonban homályos és vitatott maradt. Viktor Zsora, a legkiválóbb ukrán kiberszakértő kezdetben azt mondta, hogy ez *„igazán hatalmas kommunikációs veszteséget okozott a háború legelején”*, amit széles körben úgy értelmeztek, hogy az kifejezetten katonai kommunikációt jelent. Ez a ténybeli zűrzavar hozzájárult a Viasat feltörésének homlokegyenest ellentétes szakértői értékeléséhez. Dmitri Alperovitch a háború történetének *„stratégiailag talán leghatékonyabb kiberműveletének”* nevezte, míg James Lewis szerint *„végső soron nem biztosított katonai előnyt Oroszországnak”*.

Az elemzők különböznek abban, hogy hol húzzák meg a választóvonalat a siker és a kudarc között, állapítja meg a tanulmány szerzője. Az egyik oldalon a kiberszkeptikusok állnak, akik gyakran hangsúlyozzák, hogy az orosz hekkerek képtelenek megbénítani az ukrán döntéshozatalt és a kritikus infrastruktúrát. A másik oldalon olyan kiberpártiak állnak, akik hajlamosak kiemelni az orosz kinetikai és a kiberműveletek közötti koordináció jeleit – akármilyen jelentéktelenek is az eredmények.

Módszertani kérdések

A vita előmozdítása érdekében a tanulmány két kategóriába sorolja az Ukrajnát érintő orosz kiberműveleteket, amelyek mindegyike katonai koncepciók alapján történik.

Az első kategóriába tartoznak a számítógépes „tüzek”. Az Amerikai Egyesült Államok katonai doktrínája a tüzet úgy határozza meg, mint *„rendelkezésre álló fegyverek és egyéb rendszerek felhasználása egy célpontra gyakorolt specifikus hatás létrehozására”*. Ezek célja tehát adatok vagy rendszerek megzavarása, megsemmisítése vagy manipulálása. A kiberszakértők ezeket néha „hatásműveleteknek” vagy „zavaró és pusztító kibertámadásoknak” nevezik. Itt a *kibertüzek* kifejezés célja a katonai kontextus előtérbe kerülése és a kinetikus tüzekkel történő összehasonlítása.

A kinetikus csapásokkal való nyilvánvaló analógia miatt a bomlasztó vagy pusztító kibertámadásokat gyakran úgy tekintik, mint a katonai műveletek segítése a kibererők részéről. A kiberműveleteknek azonban más, háborús hasznuk is van. Az Egyesült Államok doktrínája szerint például a tűz csak egyike a hét úgynevezett közös funkciónak – a katonai feladatoknak, amelyek *„a közös hadviselés minden szintjén közösek”*. A többi a vezetés és irányítás, az információ, a hírszerzés, a mozgás és a manőver, az erők védelme és a fenntartha-

tóság. Bár ezek mindegyike alkalmazható a kibertérben, ez a cikk a hírszerzésre – különösen az adatgyűjtésre – összpontosít mint a második fő érdeklődési kategóriára.

Oroszország kiberműveleteinek és azoknak az ukrajnai háborúra gyakorolt hatásának felmérése nem egyszerű feladat. Az elemzőknek az ukrán kormánytól, a szövetséges kormányoktól, a kiberbiztonsági cégektől és az újságíróktól származó jelentésekre kell támaszkodniuk. Ám ezeknek a forrásoknak mindegyike csak részleges ismeretekkel rendelkezik az orosz kiberműveletekről, amelyek közül sok rejtve marad. Kevés adat áll rendelkezésünkre például arról, hogy az orosz kiberkampányok hogyan befolyásolhatták az ukrán morált – hozzájárulva annak gyengítéséhez vagy alternatívaként az invázió elleni visszhang gerjesztéséhez. Ráadásul a kiberakció látható hatásai nem mindig jelzik az elkövető valódi szándékait. Például egy telekommunikációs hálózat kibermegszakítása célzott erőfeszítés lehet az ukrán parancsnokság és irányítás zavarására egy kulcsfontosságú művelet előtt, vagy része lehet az ukrán lakosság elszigetelésére és megsértésére irányuló szélesebb körű kísérleteknek.

A cikk megválaszol néhány kérdést azáltal, hogy az orosz kiberműveletek tényleges, nem tervezett hatásaira összpontosít. Feltételezi, hogy sok felderítetlen orosz kiberművelet történik, de ezek nem nagyságrendekkel hatékonyabbak, mint az ismert műveletek.

Egy másik kihívás az, hogy politikai vagy kereskedelmi megfontolások elkerülhetetlenül meghatározzák, hogy mit, mikor és hogyan osztanak meg az orosz kiberműveletekről. Az ukrán kormánynak például stratégiai kényszere, hogy viszonylag optimista képet nyújtson a háborúról, hogy a nyugati partnerek továbbra is támogassák, az ukrán nép pedig fenntartsa a morálját. Kijev ezért vonakodott teljes mértékben nyilvánosságra hozni a veszteségeket; ugyanez igaz a kiberincidensekre is. Az ukrán tisztviselők időnként hihetetlen kijelentéseket tettek kibersikerekről. Eközben a nyugati technológiai vállalatok piaci ösztönzést kapnak arra, hogy Ukrajnának nyújtott saját kiberbiztonsági támogatásukat rendkívül sikeresnek és stratégiailag nélkülözhetetlennek mutassák be.

A tanulmány több módon is megpróbálja enyhíteni a forrásokkal kapcsolatos előítéleteket. Először is, több független forrásból származó megerősítést keres, miközben kiemeli, ha a különböző források adatai ellentmondanak egymásnak, vagy közvetlenül nem hasonlíthatók össze. Másodszor, az írás nagyobb súlyt helyez az egyértelmű tényszerű jelentésekre (például az ismert támadások leírására), mint a források analitikus jellemzésére (például azokra az állításokra, amelyek szerint az orosz kiberműveleteket összehangolják a kinetikus műveletekkel). Harmadszor, a cikk átlátható a forrásokat illetően, hogy az olvasók levonhassák saját következtetéseiket.

A világ kormányai alig várják, hogy a levont tanulságokat beépítsék a katonai kiberstratégiák, költségvetések, doktrínák és tervek folyamatos frissítésébe. Az elemzőknek a jelenleg lehetséges legjobb értékeléseket kell elkészíteniük, miközben elismerik az információs hiányosságokat és az idő múlásával történő újraértékelés szükségességét. A tanulmány megkísérel betekintést nyújtani a töredékes, egymásnak ellentmondó és változó adatok észszerű értelmezésébe.

Kibertüzek

Az oroszországi kibertüzek Ukrajnában többféleképpen kategorizálhatók. Katonai jelentőségük megértése érdekében ez a rész a kibertüzeket a megcélzott ukrán rendszerek típusa szerint csoportosítja – és ezáltal az orosz erők számára lehetséges előnyök –, nem pedig

műszaki jellemzők szerint. (Az alacsony szintű zavarok, mint például a webroncsolások és a túlterheléses támadások általában kizártak.) Később ez a rész értékeli a kiber- és a kinetikus tüzek közötti koordináció szintjét, valamint a halmozott hatások lehetőségét.

Kibertámadás a katonai felszerelések, fegyverzet és technika ellen

Moszkva leginkább érthető katonai feladata Ukrajnában az ukrán harci erő visszaszorítása és leküzdése, ennek ellenére nincs olyan nyilvánosan ismert eset, hogy orosz kiberszereplők közvetlenül megzavarták volna a katonai eszközöket a műveleti területen. Ukrajna a háborút nagyrészt a szovjet korszak katonai fegyverzetére, technikájára támaszkodva kezdte. A háború előrehaladtával Ukrajna külföldről nagy mennyiségű modern fegyvert és felszerelést szerzett be. Az Amerikai Egyesült Államok kormánya régóta aggódik amiatt, hogy az amerikai katonai harceszközök háborús kibertámadásoknak lehetnek kitéve Oroszország vagy mások részéről.

Kijev és beszállítói, illetve szövetségesei megpróbálhatják eltüntetni a katonai eszközök kiberzavarásának bizonyítékait. Bár a kutatók és az újságírók igyekeznek ilyen eseteket dokumentálni, egyelőre a források nem találtak bizonyítékot az ukrán katonai harceszközök elleni sikeres kibertámadásokra.

Kibertámadás a kommunikációs hálózatok ellen

Bár az ukrán katonai hardvereket nem érintette közvetlenül egyetlen ismert orosz kiberművelet sem, az ukrán hadsereg, a kormány és a polgári lakosság által használt kommunikációs rendszerek számos kibertámadást szenvedtek el. A legfigyelemreméltóbb epizód mindösszesze egy órával az invázió előtt történt, amikor az Oroszországi Föderáció Fegyveres Erői Vezérkarának Főigazgatóságán – közismert nevén GRU – dolgozó hekkerek követték el az úgynevezett Viasat-feltörést. A Viasat egy amerikai cég, amely a KA-SAT nevű kommunikációs műhold tulajdonosa. Nagykereskedelmi műholdas széles sávú szolgáltatásokat nyújt a végfelhasználóknak, míg a Skylogic nevű olaszországi cég üzemelteti és támogatja a földi infrastruktúrát. A Viasat szerint orosz hekkerek *„részleges megszakítást”* tudtak okozni a Skylogic hálózatának *„egyetlen fogyasztóorientált elosztójában”*, a Toowayben, amely széles sávú szolgáltatást nyújt az európai ügyfelek számára.

A Viasat a feltörést *„sokoldalúnak és szándékosnak”* minősítette. Ezzel egyidejűleg végrehajtottak egy *„földi alapú hálózati behatolást, hogy távoli hozzáférést kapjanak a KA-SAT hálózat megbízható felügyeleti szegmenséhez”*. Az oroszok elérték a hálózat érzékeny részét, majd natív szoftverrel *„pusztító parancsokat”* adtak ki *„nagyszámú lakossági modemnek egyidejűleg”*. Ezek a parancsok *„felülírták a modemek flash memóriájában lévő kulcsfontosságú adatokat, így a modemek nem fértek hozzá a hálózathoz, de nem lettek véglegesen használhatatlanok”*.

Az incidensnek széles körű hatása volt, megszakadt az internetszolgáltatás „több ezer Ukrajnában tartózkodó ügyfél és több tízezer egyéb vezetékes széles sávú ügyfél számára Európa-szerte” – írja a Viasat. Egyes berendezéseket gyorsan helyreállítottak, míg más modemek offline állapotban maradtak. Noha a Viasat-kapcsolat megszakításának nagy része Ukrajnán kívül történt, Moszkva elsődleges célja kétségtelenül az ukrán kommunikáció akadályozása volt, miközben az orosz csapatok átlépték a határt, és rakéták csapódtak be országszerte. A hekkelés végső katonai hatásáról azonban továbbra is vita folyik.

A helyszíni források azonban más képet festettek a katonai kommunikáció akkori állapotáról. Több ukrán szárazföldi parancsnok, aki részt vett Kijev kezdeti védelmében, azt

mondta, hogy Oroszország a háború nyitó napjaiban és heteiben *„teljes mértékben zavarta az ukránok kommunikációs és műholdas hálózatait”*. Ez hatékonyan akadályozta az ukrán drónok bevetését, elzárta a normál hírszerzési csatornákat, valamint a tiszteket *„a frontvonalbeli katonákkal való kapcsolat nélkül”* hagyta. Ezek a jelentések zavarásra hivatkoztak, nem hekkelésre, és nem említették konkrétan a Viasatot. Oroszország mindkét módszert összehangoltan alkalmazta inváziója során, és ezeknek lehetnek egymást kiegészítő hatásai, amelyeket az ukrán csapatok a harc hevében nem tudtak megkülönböztetni. A helyszíni tanulmányok megerősítették, hogy Oroszország zavarása meglehetősen hatékony volt a Kijev elleni támadás során, legalábbis kezdetben, annak ellenére, hogy némileg hatással volt az orosz erők kommunikációjára is.

A Viasat feltörésének nagy horderejű híre elfedi azt a tényt, hogy egy másik nagy ukrán internetszolgáltató, a Triolan egyidejűleg kibertámadás áldozata lett. Erről az eseményről keveset tudni. A Triolant március 9-én ismét feltörték, és a támadók állítólag a gyári beállítások visszaállítására kényszerítették a *„hálózat kulcscsomópontjait”*. Mindkét incidens jelentős, egy-két napig tartó szolgáltatási zavarokhoz vezetett. Később márciusban, az állami tulajdonban lévő Ukrtelecom – az ország legnagyobb földi távközlési szolgáltatója – elszenvedte azt, amit Oroszország *„masszív ellenséges kibertámadásként”* jellemez. A kibertámadás és a korrekciós intézkedések eredménye 85%-os kapcsolatvesztés volt, bár a szolgáltatás másnapra nagyrészt helyreállt. Kijev közölte, hogy a katonai műveleteket ez nem érintette.

Összességében Ukrajna távközlési hálózatai – bár a háború előtti alapállapotokhoz képest némileg leépültek – rendkívül rugalmasnak bizonyultak. A kulcsfontosságú strukturális tényezők közé tartozik a vállalati tulajdon és a műszaki architektúra decentralizációja, a mérnökök agilitása, az iparág háborús együttműködési készsége, a korábbi kiberbiztonsági befektetések és a kiegészítő műholdas hálózatok – mint például a Starlink – elérhetősége.

Kibertámadás más számítógépes hálózatok ellen

A kommunikációs hálózatokon túl az orosz kibertüzek számos egyéb kormányzati és kereskedelmi hálózatot is célba vettek Ukrajnában. A legfigyelemreméltóbb incidensek azok a kibertámadások, amelyek adatokat törölnek, és ezáltal működésképtelenné teszik a rendszereket. Moszkva számos ilyen támadást hajtott végre, különösen a háború kezdetén.

Június végén a Microsoft *„nyolc különböző rosszindulatú programot – néhány törlőt és a pusztító kártevők más formáit – észlelt 48 különböző ukrán ügynökséggel és vállalattal szemben”*. Az ukrán kormány is hasonló számról számolt be: a háború első négy hónapjában ötvenhat kiberművelet befolyásolta az ukrán rendszerek elérhetőségét.

Bár a kibertámadásokat nehéz észszerűen számszerűsíteni és hasonló módon összehasonlítani, ezek a számok bármilyen történelmi mércével mérve rendkívül magasnak tűnnek. Ez arra utal, hogy Oroszország példátlan pusztító kibertámadás-sorozatot hajtott végre Ukrajna ellen – ez talán a valaha végrehajtott legnagyobb támadássorozat, és valószínűleg több, mint amennyit Moszkva valaha is végrehajtott a teljes korábbi történetében.

Az ukrajnai orosz kibertüzek figyelemre méltó mértékét jelzi a telepített kártevő szoftverek nagy száma. Oroszország nyolc-tíz ilyen egyedi szoftvercsaládot használt a háború első néhány hónapjában. Egyedül február 24-én *„több pusztító kártevőt telepített sikeresen, mint amennyit a világ többi kiberhatalma összesen alkalmaz egy adott évben”*.

Moszkva minden intézkedés mellett rendkívüli erőfeszítéseket tett és technikai erőforrásokat fektetett be, hogy háborús kibertüzeket realizáljon olyan célpontok ellen, mint az ukrán kormány, az informatikai, energetikai és pénzügyi szervezetek. Ezek hatásáról azonban kevés

nyilvános információ áll rendelkezésre. Moszkva Ukrajnában pusztító kibertüzei nemcsak a nagy számok miatt voltak figyelemre méltók, hanem a háború kezdetén bekövetkezett masszív koncentrációjuk és az azt követő meredek visszaesésük miatt is.

Összességében huszonkét szervezet szembesült pusztító orosz kibertámadásokkal a háború első hetében. Az ezt követő öt hétben azonban a Microsoft átlagosan csak körülbelül három támadást észlelt hetente. Április közepére ez az arány heti egy támadásra csökkent, ez a szint június végéig tartott. A Microsoft augusztusban és szeptemberben kevés tevékenységet észlelt, amit októberben egy kis kiugrás követett. A civileket érintő kiberműveletekről nyilvános információkat gyűjtő CyberPeace Institute is a pusztító támadások nagy halmazáról számolt be az első hetekben. Áprilistól októberig nem dokumentált támadást.

A Microsoft eredményeinek magas szintű jellemzése alapján valószínűsíthető, hogy a korai támadás némileg hozzájárult Ukrajna kezdeti sokkjához és zavarodottságához közvetlenül az invázió után. Amilyen mértékben Ukrajna észszerű lépéseket tett ezekkel a támadásokkal szemben – például a kritikus rendszerek alapvető adatainak biztonsági mentését –, nehéz belátni, hogy az orosz kibertüzek miként viszik közelebb Moszkvát katonai céljainak eléréséhez.

Kibertámadás az ipari vezérlőrendszerek ellen

Bár a legtöbb orosz kibertűz digitális hálózatokat céloz meg, néhányan megpróbálták manipulálni vagy károsítani az ipari vezérlőrendszerek által működtetett fizikai infrastruktúrát. A mai napig azonban nincs bizonyíték arra, hogy az ilyen irányú erőfeszítések sikerrel jártak.

Április 8-án a GRU hírhedt 74455-ös egysége meg akarta szakítani az áramellátást egy meg nem nevezett ukrán régióban, amikor rosszindulatú programokat telepített egy kompromittált közműhálózatba. Az új kártevőt úgy tervezték, hogy telepítést követően megnehezítse a szolgáltatás visszaállítását. Ezúttal azonban Ukrajna nemzeti számítógépes segélyhívó csoportja és a szlovákiai székhelyű ESET kiberbiztonsági cég észlelte és állította meg a folyamatban lévő támadást.

A hatalmi infrastruktúrát ért orosz kinetikus csapások súlyos problémákat okoztak az egész országban a háború teljes időtartama alatt. Az időszakos áramkimaradások ukránok százezreit vagy millióit érintették, és órákig vagy akár hetekig tartottak. Az ukrán hadseregre gyakorolt hatás nem ismert, de a polgári szenvedések a kezelhetőtől a súlyosig terjedtek.

A kiber- és kinetikus támadások koordinálása

Az elemzők között nincs egyetértés abban, hogy az oroszok a háború kezdeti szakasza után összehangolták-e kibertámadásaikat a kinetikus támadásaikkal az egységes katonai célok elérése érdekében. Ezek a támadások jelentős előtervezést és operatív koordinációt igényeltek volna. A kiber- és a kinetikus tüzek koordinációja többféle formát ölthet. Kezdetben a Microsoft úgy értékelte, hogy *„az orosz hadsereg számos alkalommal párosította kibertámadásait a hagyományos fegyverekkel, amelyek ugyanazokat a célpontokat célozták meg”*. A vállalat szerint Oroszország időnként *„kibertámadásokat alkalmaz a számítógépes hálózatok letiltására egy célpontnál, mielőtt szárazföldi csapatokkal, illetve légi- vagy rakétatámadásokkal lerohanná azt”*. Amennyiben valóban összehangolták a fizikai támadásokkal, akkor vagy nem érték el a kívánt hatást, vagy kiberfelderítési műveleteknek szánták őket.

2022. július 1-jén volt egy eset, amikor az orosz kinetikai és kibertüzek állítólag ugyanarra a célpontra irányultak. Aznap a DTEK nevű ukrán áramszolgáltató közölte, hogy Oroszország sikertelenül kísérelt meg kibertámadást a vállalat ellen, hogy *„destabilizálja az áramtermelő és -elosztó vállalatok technológiai folyamatait”*. Az orosz XakNet hekkercsoport – amely félhivatalos kapcsolatban áll Moszkvával – vállalta a felelősséget. Ezzel egy időben az orosz

erők tüzérségi és rakétatámadásokat hajtottak végre a DTEK Dnyipropetrovszk megyei Krivij Rih mellett lévő Krivorizka hőerőműve ellen. Az ukrán energiainfrastruktúra elleni orosz kinetikus támadások a háború rutinjellemzői voltak.

Az orosz katonai hírszerzés ilyen kibertámadásainak ismétlődő időbeli, ágazati és földrajzi összekapcsolása a megfelelő katonai kinetikus támadásokkal a műveletek közös halmazát jelzi, prioritásokat, és erős közvetett bizonyítékot szolgáltat arra vonatkozóan, hogy az erőfeszítések összehangoltak. Figyelemre méltó, hogy Oroszország októberben – egy hosszú csendes időszak után – újraindította pusztító kibertámadásait, miközben jelentősen növelte rakéta- és dróncsapásainak számát. Ez bizonyos magas szintű összehangolást tükrözhet, még akkor is, ha a szoros taktikai koordináció nem bizonyított.

Az integrált kiber- és kinetikus támadások hatékonysága

Oroszország valószínűleg elért bizonyos célt egyes kiber- és kinetikus tüzekkel, elsősorban azok laza összehangolása révén. Fontos még egyszer megkérdezni, hogy ez milyen katonai hasznot hozott. Ezeknek az összehangolt tüzeknek a katonai jelentőségét Oroszország hadműveleti terveivel összefüggésben kell értékelni. Valószínűleg félelmet és pánikot akartak kelteni azáltal, hogy polgári célpontokat támadtak Dnyipróban, megteremtve a pszichológiai feltételeket a város tervezett ostromához.

Egy kibertámadás hatása a kifinomultságától is függ. Az orosz kibererők forgatókönyve szerint a rakéta megsebesítette, de nem ölte meg az ukrán áldozatokat, majd a kibertámadás sokáig késleltette a sürgősségi egészségügyi ellátást. Ez elég volt ahhoz, hogy halált okozzon.

Kumulatív hatások

Oroszországnak az a képessége, hogy koordinálja a kiber- és a kinetikus támadásokat – bár fontos, de – nem feltétlenül meghatározó. Az ilyen támadásoknak akkor is lehetnek katonai hatásai, ha rosszul vagy lazán koordinálják őket. A kinetikus műveletekkel nem igazán koordinált kibertámadásoknak is lehetnek kumulatív hatásai Ukrajnában.

Az egyes kiberműveletek harci kárainak felmérésére szolgáló megoldások még kiforratlanok – a kumulatív hatás megértése még nehezebb. Az egyik megközelítés a kiber- és a kinetikus támadások összhatásait hasonlítja össze a rendelkezésre álló mennyiségi és minőségi mérőszámok alapján. Ezt két egymást kiegészítő szempontból lehet megtenni. A kibertámadások felfoghatók a kinetikus támadások közvetlen megfelelőiként, de úgy is, mint egyedi jellemzőik alapján megkülönböztetett funkciók.

A háború első négy hónapjában Oroszország 3654 rakétacsapást hajtott végre, de az ukrán és a Microsofttól származó adatok szerint csak mintegy 50 hatásos kibertámadást. Jogos azt feltételezni, hogy átlagosan egy rakétacsapás nagyobb katonai előnyökkel járt Oroszország számára, mint egy pusztító kibertámadás. El lehet képzelni lehetséges ellenpéldákat – például egy olyan kibertámadást, amely megbénítja az ukrán vasúti szállítmányokat, és ezáltal késlelteti a kritikus készletek szállítását a vitatott frontra –, de erre nincs bizonyíték.

Következtetés

Összességében elmondható, hogy a kibertámadások nem növelték érdemben Oroszország kinetikus tűzerejét, és nem töltöttek be olyan különleges funkciókat, amelyeket a kinetikus fegyverek nem tudtak volna. Sok orosz kibertámadás ugyanazokat a kategóriájú ukrán rendszereket célozta meg, amelyeket kinetikus fegyverekkel is támadtak – például kommunikációs, elektromos áram és közlekedési infrastruktúra –, ahelyett, hogy olyan célpontok ellen irányultak volna, amelyek ellen a kinetikus fegyverek kevésbé alkalmasak. Szinte az

összes célkategória esetében a kinetikus támadások nagyságrendekkel több kárt okoztak. Bár a kibertámadások bizonyos körülmények között egyedülálló előnyöket kínálnak, ezek az előnyök nem valósultak meg Oroszország Ukrajna elleni műveleteiben. Hasonlóképpen, az orosz kibertámadások nem értek el semmilyen rendszerszintű hatást, és vitathatatlanul kevésbé költséghatékonyak – vagy legalábbis a kinetikus támadásoknál kisebb a műveleti hatásuk.

Hírszerzési lehetőség

A kommentátorok a kibertámadásokra összpontosítanak, és sokkal kevesebb figyelmet szenteltek annak, hogy a kiberfelderítés mennyire és hogyan támogatja az orosz háborús erőfeszítéseket. A kiberműveletek *„nem háborúkat nyernek, hanem kémkedést, megtévesztést, felforgatást és propagandatörekvéseket támogatnak”*. Ez a kettősség figyelmen kívül hagyja azt a tényt, hogy a háború alatti kémkedés az egyik félnek valóban segíthet a győzelem elérésében.

Az ukrán nemzeti kiberbiztonsági ügynökség jelentése szerint ellenséges hekkerek 242 információgyűjtési műveletet hajtottak végre a háború első négy hónapjában. Összehasonlításképpen az ügynökség mindössze 56 olyan kiberműveletet (vagyis kibertámadást) számolt össze, amelyek befolyásolták az ukrán rendszerek elérhetőségét. Az biztos, hogy a kiberműveleteket nehéz értelmesen számszerűsíteni és pontosan jellemezni. Ugyanez az ukrán kormánydokumentum még több kiberműveletet (498) sorolt fel kétértelmű kategóriákban – mint például behatolás, behatolási kísérlet vagy rosszindulatú kód –, amelyek nem utalnak egyértelmű elkövetői szándékra vagy műveleti eredményre.

A békeidő és a szürke zóna körülményeiből tudjuk, hogy a kiberműveletek hatékony kémeszközök lehetnek. Segíthetik Moszkva nagyobb háborús erőfeszítéseit a stratégiai tervezésben, a célpontok kiválasztásában, a megszállási tevékenységekben, a befolyásolási műveletekben és a tárgyalások támogatásában. A szerző az írása további részében részletesen kifejti a hírszerzés fontosságát ezeken a területeken.

Következtetés

Valószínűleg a hírszerzés és nem a támadások állnak Oroszország ukrajnai kiberműveleteinek középpontjában, ennek ellenére ez is kevés katonai hasznot hozott. Ami még alapvetőbb, Oroszország átfogó megközelítése a háborúhoz – a hadászati tervezéstől a megszállt területek elfoglalásáig – azt sugallja, hogy a kulcsfontosságú katonai döntéseket nem egy szigorú, minden forrásból származó hírszerzési folyamat vezérli.

Moszkva intézményi korlátai ellenére a háború előrehaladtával még mindig érhet el áttörést a kiberhírszerzés terén. Elképzelhető, hogy az orosz hekkerek valós idejű földrajzi helymeghatározási adatokat szerezhetnek, amelyek lehetővé teszik merénylet elkövetését Zelenszkij elnök ellen, vagy az ukrán erők – és különösen a nagy értékű nyugati fegyverek – elleni időben történő és pontos csapásmérést. Esetleg hozzáférhetnek olyan titkos és érzékeny adatokhoz – például Ukrajna harci veszteségei, a politikai és a katonai vezetők közötti széthúzások, információk Kijev elképzeléseiről és szándékairól az esetleges béketárgyalásokról –, amelyek nyilvánosságra hozása az ukrán és a nyugati közvélemény számára előnyben részesítheti Moszkvát. Az orosz titkosszolgálati információgyűjtés ezért jelenti a legnagyobb folyamatos kiberkockázatot Ukrajna számára – zárja sorait a tanulmány szerzője.

AZ ŰRTÁMOGATÁS NÖVEKVŐ SZEREPÉRŐL A FEGYVERNEMI CSAPATOK, ALEGYSÉGEK ÉS HADERŐNEMEK HARCTEVÉKENYSÉGÉBEN

A CIKK SZERZŐJÉRŐL: Ivanov Vlagyimir Leontyjevics vezérezredes 1992-től 1996-ig az Oroszországi Föderáció katonai űrerőinek parancsnoka, a hadtudományok doktora, professzor. E tanulmányában az űrerők növekvő szerepéről és az ezzel kapcsolatos teendőkről ír.

FORRÁS: Владимир Леонтьевич Иванов: О возрастании роли космического обеспечения боевых действий частей и подразделений видов и родов войск. Клуб военачальников Российской Федерации, 05. 10. 2022. http://kvrf.milportal.ru/o-vozrastanii-roli-kosmicheskogo-obespecheniya-boevyh-dejstvij-chastej-i-podrazdelenij-vidov-i-rodov-vojsk/ (Letöltés időpontja: 2023. 03. 28.)

A szerző írása az Oroszországi Föderáció katonai vezetőinek klubja által működtetett honlapon jelent meg. Leontyjevics nyugállományú vezérezredes megállapítja, hogy a szárazföldi erők a fegyveres erők legrégebbi haderőneme a világon, és a háborúban a győzelem végső soron ezek sikerétől függ.

A fegyveres harcnak ebben a szférájában azonban az oroszországi katonai térben rejlő lehetőségeket egyelőre rendkívül kevéssé használják ki. Széles körben tárgyalt téma az úgynevezett „űrháború" kirobbantásának és az űrrepülőgépek szándékos megsemmisítésének a veszélye, ez azonban a valóságban nem létezik a csapásmérő űrfegyverek hiánya miatt. Ugyanakkor valóban veszélyt rejt magában, hogy az amerikai fegyveres erők információs fölényt szereznek az orosz fegyveres erőkkel szemben az űrhöz kapcsolódó szárazföldi hadszíntéri műveletekben. Az információs és az űrtámogató technológiák széles körű bevezetéséről van szó az amerikai oldalon, ami átlagosan 2-4-szeresére növeli a hagyományos fegyverek alkalmazásának hatékonyságát.

Az információs és az űrtámogatás az ukrajnai különleges katonai művelet résztvevőinek akciói során

Az információs és az űrtámogatás olyan cselekvések, illetve összehangolt és egymással összefüggő intézkedések összessége, amelyek célja az űrrendszerek, komplexumok és orbitális konstellációk rendeltetésszerű (működési) felhasználása kölcsönhatásban lévő erők, valamint információs és űrtámogatási eszközök által. Az űrplatformok speciális berendezések hordozói, és az űrinformáció fogyasztói a fegyveres erők haderőnemei.

Napjainkban a következő típusú információs és világűri lehetőségeket alkalmazzák a gyakorlatban:

1. rakétaindítások észlelése, rakétatámadásra történő figyelmeztetés;
2. felderítés (megfigyelés):
   – az ellenség erőinek, eszközeinek és objektumainak felfedése és megfigyelése a megfelelő parancsnok döntése alapján;
   – az ellenség csapatainak megfigyelése és ellenőrzése az illetékes parancsnok döntése alapján;

– az adott objektumok pontos térbeli pozicionálása (földrajzi koordinátáinak meghatározása) és a megsemmisítendő objektumok célmegjelölése.

3. stratégiai kommunikáció és információ átjátszása;
4. internetalapú kommunikációs, adatátviteli és harcirányítás globális információs hálózati létrehozása különböző célú adatok továbbítására harcászati szintig bezárólag;
5. titkosított kommunikáció biztosítása az állam különleges szolgálatai számára;
6. navigációs adatok biztosítása a saját mozgó objektumok és a pontos idő jelzése a saját erők számára;
7. meteorológiai támogatás keretében a saját csapatok aktuális időjárási adatokkal történő ellátása;
8. topológiai és térképészeti adatok biztosítása különféle digitális térképek elkészítéséhez, beleértve a nagy pontosságú térképeket, a nagy hatótávolságú támadó robotrepülőgépek korrekciós területeit;
9. a nagy hatótávolságú rádióberendezések beállításának elősegítése – ez a nagy antennarendszerek és rakétavédelmi rendszerek beállítása, elsősorban az antenna optikai és sugárzási tengelyeinek összehangolására.

Az ukrajnai különleges katonai művelet során a 2–8. információs és űrtámogatási módszereket alkalmazzák.

Az ukrán haderő információs és űrtámogatása kapcsán mindenekelőtt meg kell jegyezni, hogy ennek végrehajtása során az Amerikai Egyesült Államok széles körben felhasználja az 1991-es *Sivatagi Vihar* hadművelet és a 2003-as iraki háború során szerzett tapasztalatokat. Így 1991-ben a Prince Sultan légitámaszponton (Szaúd-Arábia) megalakult az űrerők és -eszközök alkalmazását koordináló űrközpont. Jelenleg a németországi Ramstein légibázison működik az ukrán haderő információs és űrtámogatását irányító NATO-űrközpont, amely valójában amerikai, mert a Szövetségnek nincsenek sem űreszközei, sem pedig ilyeneket irányító eszköze, sem pedig a műholdakról érkező speciális információk fogadására szolgáló központjai, és a belátható jövőben sem tervezi, hogy ilyenekkel rendelkezzen.

A 2003-as iraki háború alatt a többnemzeti erők csoportosításának tájékoztatására és űrtámogatására mintegy 60 űreszköz erőforrásait használták, közülük csak öt volt katonai felderítőeszköz, a többi polgári volt, mivel a hadseregnek nem volt elegendő eszköze a problémák megoldásához közel valós időben.

Az alábbi Föld körül keringő eszközöket használják:

– az Amerikai Egyesült Államok Navstar globális navigációs rendszere (közismertebb nevén GPS);
– Elon Musk Starlink elnevezésű műholdas rendszere, amely részben az ukrán fegyveres erők érdekében a kommunikációs és adatátviteli harcirányító rendszer alapját képezi;
– polgári kereskedelmi célú műholdakból álló, különböző célokra (optikai, rádiós és elektronikus felderítésre) használt, távérzékelő műholdakból álló rendszer, amely alapvetően harcászati célú felderítést végez.

A GPS és a Starlink a felhasználóktól függetlenül működik, az adataikhoz történő hozzáféréshez speciális terminálok szükségesek.

Az amerikai Navstar (GPS) globális űrnavigációs rendszer működése többé-kevésbé ismert, ez képezi az összes nyugati nagy hatótávolságú precíziós fegyverrendszer alapját. Tehát az Irakkal folytatott háborúban először használták széles körben a Navstar információit (a tehetetlenségi navigációs rendszert egy GPS-vevővel egészítették ki, amely nagyságrenddel

növelte a pontosságot). Egyes jelentések szerint az ilyen fegyverek részesedése a 2003-as iraki háborúban 95%-os volt (összehasonlításul: az 1991-es *Sivatagi Vihar* műveletben 7%-os). Jelenleg a GPS-terminálok a harci információs és irányító rendszerek szerves részét képezik, és megtalálhatók a legtöbb importált és jelentéktelen mértékben a modernizált ukrán fegyverrendszerekben. Egy ilyen rendszer hatékonyságát az ukrajnai HIMARS rakéta-sorozatvető példáján figyelhetjük meg: a lövedékeinek körkörös szórása 7 m, ha az orosz légvédelem nem semmisíti meg. Szinte az összes pilóta nélküli repülőgép, illetve az ukrán harckocsik és páncélozott szállító harcjárművek jelentős része is fel van szerelve ilyen navigációs eszközzel.

Új elem, hogy Elon Musk amerikai műholdas széles sávú internetrendszerét, a Starlinket használják harcirányítási célokra. Ez hivatalosan nem katonai rendszer, hanem polgári globális internetes műholdrendszernek számít, amely felváltja a mobiltelefonok cellatornyait. Telefonos kommunikációt és mobilinternetet biztosít. A szerző elemzi, hogyan segíti a Starlink az ukrán fegyveres erőket.

Az ukrajnai különleges katonai művelet megkezdése után az amerikai hadsereg műholdas kommunikációval kapcsolatos problémáiról szóló töredékes adatok alapján a SpaceX bejelentette, hogy a lehető leghamarabb leszállítja a Starlink-készleteket. A sajtóközlemény nem szólt semmit a katonai felhasználásról, csak azt említette, hogy Ukrajna lakosait internettel kell ellátni. Bár addig a békés ukrán polgári lakosságnak nem volt információja kommunikációs és internetes problémákról, viszont nagyszámú üzenet jelent meg az ukrán haderő katonáitól Elon Musk számára köszönettel az internetért, ami önmagában is ékesszólóan beszél a Starlink leszállításának okairól.

Így jelent meg a Starlink Ukrajnában. A bázisállomások („átjátszók") nagy valószínűséggel Lengyelország és Románia területén találhatók, ezek elegendők ahhoz, hogy Ukrajna nagy részén széles sávú internet-hozzáférést biztosítsanak. Bizonyítékok vannak arra, hogy az ország nyugati részén egy földi átjátszót is telepítettek.

A szerző idézi a The Washington Postot: *„Ez a Pentagon által bérelt műholdrendszer immár zavartalan adatátvitelt biztosít az ukrán haderő számára, amely hírszerzési információkat kap a NATO-parancsnokságtól. Elemzés készül az orosz csapatok mozgásáról, parancsokat adnak ki, és mindezt a Starlink rendszeren keresztül juttatják el az ukrán haderő terminál-jaira, és speciális számítógépes hálózatot használnak az adatok továbbítására."*

Ostobaság lenne nem továbbítani a földfelszínt pásztázó több száz távérzékelő műholdról érkező felderítési információt (képeket) a Starlink széles sávú (azaz rendkívül informatív) internetes műholdrendszerén keresztül. Bármennyire is titkolják az Amerikai Egyesült Államok, a NATO, Elon Musk és a SpaceX képviselői, hogy a „tisztán civil" Starlink internetes rendszeren keresztül folyik az ukrán haderő hírszerzési tevékenysége, ez az információ mégis nyilvánossá vált.

Következtetésként a szerző megállapítja, hogy a rendkívül informatív széles sávú Starlink internetes műholdas rendszerét az ukrajnai harcok során sikeresen használják harcirányító rendszerként és adatkommunikációra, és az harcászati szintig képes működni. A Starlink nagy stabilitást, megbízhatóságot és interoperabilitást mutatott a harci információs és vezérlőrendszerekkel az ukrán szárazföldi erők számos fegyvertípusához, főleg az importált fegyverekhez.

Az amerikai Védelmi Minisztérium mellett más amerikai és NATO-tagállami struktúrák is gyűjtenek információkat az Ukrajnában zajló eseményekről. Ez többféleképpen történik.

Mindenekelőtt távérzékelő műholdakat használnak. A Föld távérzékelését, valamint katonai űrfelderítést (megfigyelést) végeznek az optikai tartományban, valamint a látható mellett az infravörös és ultraibolya tartományban is. A távérzékelő műholdak az optikai mellett rádiós

hullámtartományban is működnek: az időjárási körülményektől függetlenül működő radarok és rádióelektronikai eszközök elősegítik a geopozicionálást, a rádióhullámokat kibocsátó eszközök helyének a meghatározását, valamint a kibocsátott rádiójelek szerkezetét, megfejthetik a továbbított információkat, meghatározhatják a sugárzó eszköz jellemzőit. A távérzékelő műholdak nem egyformák, körülbelül a felük meglehetősen egyszerű, csak a Föld felszínének felmérésére alkalmas, és csak egyharmaduk képes geopozicionálásra, ez pedig több mint 130 műhold.

Az iraki háború tapasztalatai azt mutatják, hogy az űrben telepített felderítőeszközöknek meg kell különböztetniük a fából készült harckocsimakettet és a fémréteggel bevont felfújható csalit a valóditól, ezért át kellett térni a spektrális-zónás rendszerekre, amelyek lehetővé teszik a céltárgy egyes jellemzőinek azonosítását az apró jelek elemzése alapján. Például egy földön álló repülőgép másképp néz ki az elektromágneses hullámok látható, ultraibolya, infravörös és rádiólokációs hullámtartományában. Ha egy távérzékelő műhold egyidejűleg képet készít egy tárgyról az elektromágneses spektrum több tartományában, és össze is veti azt egy olyan jellel (egy képpel az elektromágneses hullámok meghatározott tartományában), amelyet a Föld felmérését (távérzékelést) végző cég űrinformációs archívumában tárolnak, akkor a napszak, a felhőzet, a csapadék, a homokvihar, a por, a füst stb. befolyása elhanyagolható lesz. A katonai felderítő műholdak általában csak két elektromágneses (látható és rádiólokációs) hullámtartományban készítenek képeket.

Az Amerikai Egyesült Államok naponta legalább 50 különböző polgári távérzékelő műholdat használ megfigyelésre: elektrooptikai és rádiólokációs (szintetikus apertúrájú radarral), valamint rádiótechnikai felderítést végeznek. A legtöbb műhold 40–60 km szélességű területet képes megfigyelni.

A fentiekből látható, hogy az Amerikai Egyesült Államok által Ukrajna felett az űrből megszerzett információk mennyisége meglehetősen jelentős, de vajon mindez átkerül-e az ukrán fegyveres erőkhöz, és azok teljesen szuverén módon rendelkezésükre állnak? Erre határozottan nemet mondhatunk. Ennek több oka is van: technikai, szervezeti, politikai és katonai.

Minden hírszerzési információt a NATO Űrinformációs Központjába küldenek és ott dolgoznak fel, majd az illetékes vezetők döntése szerint adagolva, a Starlink hálózaton keresztül eljuttatják Ukrajnába. Vagyis ez egy meglehetősen hatékony módja az ukrán fegyveres erők katonai műveletei befolyásolásának és ellenőrzésének is.

Úgy tűnik, az amerikaiak által szolgáltatott hírszerzési információk nagy része áttekintő jellegű (a helymeghatározás pontossága a földön néhányszor 10 m). Ez bőven elég ahhoz, hogy észleljék az oroszok mozgó oszlopait, tüzelőállásban lévő tüzérségüket, és számos egyéb feladatot megoldjanak.

Az ukrán hadsereg konzultál az Amerikai Egyesült Államokkal az amerikai HIMARS alkalmazása előtt. Amikor az ukrán fegyveres erők ezeket a rendszereket használják, akkor valós időben kapott információk vezérlik őket. Az amerikai tisztségviselők nem adnak útmutatást, de vannak olyan konzultációk az amerikai és az ukrán titkosszolgálatok között, amelyek lehetővé teszik Washington számára, hogy leállítsák a HIMARS rakéták bármilyen kilövését, ha az amerikaiak elégedetlenek a kitűzött céllal.

A tanulmány az orosz űrtámogatást is taglalja. Az Oroszországi Föderáció fegyveres erői csoportosítása számára a különleges katonai művelet érdekében a következő típusú információs és űrtámogatást valósítják meg:

1. felderítés (megfigyelés):
   – az ellenség erőinek, eszközeinek, objektumainak felfedése és megfigyelése;
   – az adott objektumok pontos térbeli pozicionálása (geopozicionálás) és megsemmisítendő célok megjelölése.

2. stratégiai kommunikáció;
3. speciális kommunikáció (az állam speciális szolgáltatásai);
4. navigáció – a mozgó objektumok számára pontos helymeghatározás és a csapatok pontos idővel történő ellátása;
5. meteorológiai támogatás – a csapatok naprakész időjárási adatokkal történő ellátása;
6. A topogeodézia és térképészet a terület különféle digitális térképeinek elkészítése, beleértve a nagy pontosságú térképeket a nagy hatótávolságú cirkálórakéta-repülési korrekciójához szükséges területekről geocentrikus koordinátákban.

Nem szükséges részletesen leírni az Oroszországi Föderáció Fegyveres Erői csapatainak tevékenységéhez kapcsolódó információs és űrtámogatást. Ez alapvetően nincs másként Oroszországban és az Amerikai Egyesült Államokban. A különbség a keringő műholdak jelenlétében, összetételében, számában és ennek megfelelően a kapott információ gyakoriságában és mennyiségében van.

Oroszországban még nincs olyan műholdas rendszer, amely hasonlít Elon Musk Starlink műholdas széles sávú internetes rendszeréhez, amely az ukrán haderő érdekében részben harci vezetési és irányítási rendszert biztosít a kommunikációhoz és adatátvitelhez harcászati szintig bezárólag. Jelenleg Oroszország globális piaci részesedése növelésének fő akadálya a megfelelő műholdak hiánya és a földi infrastruktúra nem megfelelő fejlettsége.

Mint látható, a fegyveres erők amerikai információs és űrtámogatása, valamint az ukrajnai eseményekben való közvetlen részvétele megmutatta az űrnek mint a fegyveres harc szférájának növekvő szerepét.

Milyen lépéseket kell tenni annak érdekében, hogy a 21. században az orosz haderő teljes körű információs és űrtámogatást kapjon?

1. A stratégiai űrövezet operatív berendezése és az űrinfrastruktúra fenntartása (fejlesztése), amely biztosítja a katonai és a kettős felhasználású űreszközök garantált és hatékony alkalmazását.
2. Sürgősen folytatni kell az 1994–1997-ben megkezdett munkát, a hadászati irányokban a csapatok csoportosításának információs és űrtámogatását harcászati szintig, ideértve az új technikai bázist. A fő probléma nem technikai, hanem szervezési.
3. Radikálisan emelni kell az egész tisztikar „űrműveltségének" szintjét, hogy ne csak az űreszközök jelentőségét értsék meg a haderőnemek minden fajtája hatékonyságának emelésében harcászati szintig bezárólag, hanem tudják, hogyan használják magukat az űrtechnológiákat.
4. Már most legalább olyan kutatások megkezdése szükséges, amelyek a szárazföldi erők hadműveleteiben történő felhasználásra szánt űrrendszerekkel, ballisztikus formációval és műholdrendszerek összetételével szemben támasztott követelményeket határozzák meg azokon a területeken, ahol a leginkább észlelhető a lemaradás a potenciális ellenfelektől. Ugyanakkor meg kell jegyezni, hogy Oroszországban erre minden lehetőség adott.
5. A szárazföldi erőknél a jövőben el kell kezdeni az űralegységek létrehozását, kezdetben a hadosztály szintjén, mivel változik a katona harctéri megjelenése és felszerelése.
6. A háborús műholdrendszer összetételének tartalmaznia kell a csapatok tájékoztatására és űrtámogatására alkalmas civil űrrendszereket, amelyek egyfajta mobilizációs erőforrást kell hogy képezzenek.
7. A viszonylag olcsó mini- és mikroűreszközök széles körű elterjedése és ezek alapján a különböző célú műholdcsoportok kialakítása lehetővé teszi a szárazföldi erőknek, hogy saját műholdas rendszerrel rendelkezzenek. Ezeket a műholdcsoportokat az űrerők fogják irányítani (ahogyan ez most Oroszországban, az Amerikai Egyesült Államokban és a

világ többi részén történik), és az adataikat a szárazföldi csapatok űralegységei fogják a rendeltetésüknek megfelelően felhasználni.

Ennek a megközelítésnek a megvalósításával a legújabb, nagy pontosságú és csúcstechnológiás fegyverrendszereket fogják a leghatékonyabban alkalmazni. A stratégiai fegyverek esetében ezeket a problémákat már megoldották. Következnek a szárazföldi erők, zárja mondanivalóját a tanulmány szerzője.

NUKLEÁRIS HÁBORÚHOZ VEZETHET-E AZ OROSZ KATONAI ÖSSZEOMLÁS?

A CIKK SZERZŐJÉRŐL: Tim Willasey-Wilsey 27 évig szolgált brit diplomataként Afrika, Latin-Amerika, Ázsia és Európa különböző országaiban. Főbb kutatási területe a geopolitika. Írásában véleményét fogalmazza meg egy esetleges orosz vereséggel kapcsolatban.

FORRÁS: Tim Willasey-Wilsey: Could a Russian Military Collapse Lead to Nuclear War? RUSI, 25. 01. 2023. https://rusi.org/explore-our-research/publications/commentary/could-russian-military-collapse-lead-nuclear-war (Letöltés időpontja: 2023. 01. 30.)

Dmitrij Medvegyev korábbi orosz elnök felvetette, hogy egy ukrajnai orosz vereség atomháborúhoz vezethet. Boris Johnson korábbi brit miniszterelnök ostobaságnak minősítette az ötletet. Mi történne tehát, ha az orosz hadsereg fellázadna vagy összeomlana?

A zendülésre vagy a hadsereg hirtelen szétesésére nincs pontos sablon. A brit hadsereg az első világháborúban a nyugati fronton a hatalmas veszteségek és a rossz életkörülmények ellenére sem lázadozott, az orosz hadsereg pedig sokkal rosszabb körülményeket viselt el a második világháború keleti frontján. A csapatok mindkét esetben hittek abban, hogy meg kell nyerni a háborút, és tudták, hogy ez nemzeti erőfeszítés, amely a társadalom minden rétegét érinti. Ezzel szemben az afgán hadsereg nem lázadozott 2021 júliusában és augusztusában – egyszerűen eltűnt, mert a katonák már nem hittek a háborúban, mivel az Amerikai Egyesült Államok a saját mélyen korrupt kormányuk háta mögött tárgyalt a tálibokkal.

Lehet, hogy még mindig vannak orosz katonák, akik elhiszik elnökük állítását arról, hogy Ukrajna náci állam, de egyre gyakrabban kell elgondolkodniuk azon, hogy miért vállalják a jelentős kockázatot és a szörnyű körülményeket. Valóban az orosz nemzetért vagy Vlagyimir Putyin politikai túléléséért? Ezenkívül a sebtében toborzott és részben kiképzett hadkötelesek hamarosan megtapasztalják azt a különbséget, amely a régi szovjetkori felszerelésük és a drónok, a precíziós tüzérségi tűz között mutatkozik. Már akadt néhány bizonyíték a zendülésközeli állapotra. A Harkiv környéki váratlan kiürítés szeptemberben a kitörés jegyeit viselte, a csapatok sietve elhagyták állásaikat, felszereléseket és személyes tárgyakat hagyva maguk után.

Nyugaton egy nagy oroszországi összeomlás okot adna az ünneplésre, a háború gyors befejezését és a konfliktus által okozott gazdasági hatások – különösen a magas energia- és élelmiszerköltségek – enyhítését ígérné. A valóságban azonban egy zendülés néhány napig nagyon jelentős kockázattal járna.

A szerző a következő forgatókönyvet tartja elképzelhetőnek: az ukrán erők hirtelen azt tapasztalnák, hogy nincs ellenállás előttük, miközben az orosz csapatok rendezetlenül

visszavonulnak. Akárcsak a brit hadsereg 1918 augusztusában, hirtelen 20 kilométert tudnak előrehaladni 20 méter helyett egy nap alatt. A gyors előrelépés próbára tenné az ukrán logisztikát, de néhány napon belül Ukrajna visszaszerezné a 2022. február 24. óta elvesztett összes területet. Ekkor súlyosbodna a helyzet. A moszkvai kormány kétségtelenül ultimátumot adna, hogy Ukrajna ne sértse meg a Donbasz február 24. előtt orosz ellenőrzés alatt állt területeit, és mindenekelőtt ne lépjen be a Krím félszigetre. Moszkva nyilvánvalóan hajlandó lenne nukleáris fegyverek bevetésére is területi integritásának védelme érdekében.

Emmanuel Macron francia elnök és Olaf Scholz német kancellár sürgős üzenetet küldene Volodimir Zelenszkij elnöknek, hogy ne lépje túl a február 24-i határt. Az Egyesült Királyság határozottabb irányvonalat követhetne, és esetleg arra ösztönözné Zelenszkijt, hogy vegye vissza a Donbaszt, de a NATO és a G7 szövetségesei közötti konzultációig tartson egy kis szünetet, mielőtt átkelne a Krím félszigetre. Joe Biden amerikai elnök valószínűleg inkább az utóbbi álláspont felé hajlana, annak tudatában, hogy a Krím sokkal érzékenyebb kérdés, hiszen az orosz fekete-tengeri flotta hazája, és hagyományosan orosz ellenőrzés alatt állt egészen addig, amíg Nyikita Hruscsov kissé szeszélyes döntése 1954-ben át nem engedte Ukrajnának – amely egyébként akkoriban a Szovjetunió része volt.

Hogyan reagálna Zelenszkij? Valószínűleg szoros határidőt adna csapatainak, hogy vegyék bírtokba mind a Donbaszt, mind a Krímet. Arra kérné Párizst és Berlint, hogy egy-két napra szüksége van hadserege előretörő lendületének megállítására, miközben hangsúlyozná a Donbasz és a Krím polgárainak védelmét a visszavonuló orosz katonák által elkövetett háborús bűnökkel szemben. Biztosítaná Oroszországot arról is, hogy nem fognak behatolni a 2014 előtti orosz területekre, ugyanakkor fenntartaná a jogot, hogy a tüzérségi tüzet viszonozza az országhatáron túlra.

Eközben Ukrajna több tízezer orosz foglyot ejtene. Megint a franciák és a németek kérvényeznék, hogy azonnal engedjék el őket, és engedjék meg, hogy hazaszökjenek. Zelenszkijnek azonban két ellentétes gondolata lenne. Először is, a foglyok között kétségtelenül lennének háborús bűnösök is. Ez azt vonná maga után, hogy Közép-Ukrajnába telepítik, és hónapok alatt hivatalosan is kivallatják őket. Volnának köztük olyan tisztek is, akik hozzáférnek az orosz képességekkel kapcsolatos fontos hírszerzési információkhoz, és néhányan hajlandók lennének disszidálni. Másodszor, a foglyok fontos alkualapot jelentenének minden jövőbeli békemegállapodásban. Van itt némi hasonlóság ahhoz, ahogy India 93 ezer pakisztáni katonát tartott vissza nyolc hónapig Kelet-Pakisztán (ma Banglades) 1971-es összeomlása után egészen a Simla-egyezmény következő évi aláírásáig.

Egy nukleáris eszköz felrobbantása a Fekete-tenger vagy Közép-Ukrajna felett mint figyelmeztetés az ukrán előrenyomulás megállítására lehetőség lenne a nehéz helyzetbe kerülő orosz vezetés számára. Moszkvában zűrzavar lenne a zendülés és annyi terület elvesztése után. Putyin kétségtelenül hibáztatná és menesztené Szergej Sojgu védelmi minisztert és Valerij Geraszimovot, de túl sok felelőssége van a háborúban ahhoz, hogy elkerülhessen bizonyos következményeket. Ez lehet az a pillanat, amikor Alekszandr Bortnyikov (az FSZB igazgatója) vagy Nyikolaj Patrusev (az FSZB korábbi igazgatója) Putyin kiszorítására törne. Nagy a valószínűsége annak, hogy bármely új vezető ugyanabból az ex-KGB-istállóból származna, mint Putyin, és ugyanolyan vagy még inkább héja, vagyis háborúpárti lenne.

Medvegyevnek igaza van abban, hogy egyetlen atomfegyverrel rendelkező ország sem veszítette el a nemzeti túlélés háborúját. Ez új terület lenne az egész világ számára, és nagy kockázattal járna, továbbá a moszkvai hatalmi harc kérdéseket vetne fel az orosz atomarzenál feletti parancsnoki jogkörrel kapcsolatban. Egy volt magas rangú brit védelmi tisztviselő szavaival élve: *„A lázadás meghatározásánál fogva tönkretenné a parancsnoki*

lánc megbízhatóságát." Egy új nacionalista vezető pedig eközben Moszkvában azzal érvelhetne, hogy a NATO-országok tették lehetővé Ukrajna sikerét, ezért célpontnak kell tekinteni őket.

A szerző véleménye szerint ezek egyike sem érv amellett, hogy ne szorítsuk ki Oroszországot Ukrajnából, de mindez arra készteti a nyugati vezetőket, hogy teljes világossággal közöljék szándékaikat Moszkvával. Alapvető fontosságú lenne biztosítani az orosz kormányt és népet, hogy a 2014 előtti területi integritásuk nincs veszélyben. A cikkíró hipotézise szerint az is fontos lenne, hogy minden nyugati szövetséges egyetértsen abban, hogy a Krím továbbra is Ukrajnához tartozik, de az orosz fekete-tengeri flotta Oroszország tulajdona marad mindaddig, amíg nem tanúsít ellenállást a Krím Ukrajna általi visszafoglalását követően. A flotta további állomásoztatásának kérdései pedig egy későbbi békekonferencia témái lennének.