

978-9934-564-90-1

# OROSZORSZÁG STRATÉGIÁJA A CYBERTÉRBEN

Kiadja a  
NATO Stratégiai Kommunikációs  
Kiválósági Központ



**CCDCOE**  
NATO COOPERATIVE  
CYBER DEFENCE  
CENTRE OF EXCELLENCE



# Tartalomjegyzék

Bevezetés.....	6
Oroszország "információs konfrontációja" .....	7
A .....	"kiber "7orosz felfogása
Az "információ" védelme: kognitív és .....	technikai7
Nemzetbiztonsági érdekek és stratégiai célkitűzések .....	10
Oroszország fenyegetettségének .....	megítélése11
Stratégiai .....	elrettetés12
Az információs tér biztosítása - "digitális szuverenitás.....	14
Állami szereplők és meghatalmazottak .....	19
Tevékenységek a kibertérben.....	25
Következmények és .....	célkitűzések34
Következtetés és ajánlások.....	36
Végjegyzetek.....	40



# BEVEZETÉS

Az Oroszországot a "kiber" homályos fogalmával összekötő szalagcímek a nyugati közvélemény és a döntéshozók mindennapi kenyerévé váltak. A NotPetya által okozott károktól vagy az Ukrajna és Grúzia elleni támadásoktól kezdve az amerikai és európai választásokon végrehajtott orosz hacker- és kiszivárogtatási műveletekig Oroszország támadó műveletei állandó fenyegetést jelentenek. Oroszország egyre fontosabb eszközként használja a kiberműveleteket más katonai és nem katonai eszközökkel együtt a stratégiai célok elérésére, amit Oroszország a folyamatban lévő "információs konfrontációnak" tekint.

Másrészt az elmúlt években Oroszország megpróbálta lezárni és biztosítani saját digitális információs terét. A Kreml jogi és technikai eszközök kombinációjával igyekszik mind a digitális infrastruktúra, mind a tartalom felett ellenőrzést gyakorolni, amely törekvések célja a globális internethálózattól való függetlenség biztosítása és ezáltal az információs biztonságuk növelése.

Oroszország a kibertérben folytatott tevékenységeket az "információs konfrontáció" átfogó keretrendszerének részhalmozának tekinti, amely az államok közötti kapcsolatok orosz értelmezéséből származik, és pontosabban a nagyhatalmak közötti, a világban való befolyásért folytatott küzdelem egyik részhalmozása. Az orosz gondolkodók szerint az információs konfrontáció állandó és folyamatos, és ebben a konfrontációban bármilyen eszköz felhasználható a fölény megszerzésére. A kibertérben folytatott tevékenységek az információs környezetben folytatott hadviselés számos eszköze közül az egyik, beleértve a pszichológiai műveleteket, az elektronikus hadviselést (EW) és a kinetikus akciókat. A gyakorlatban

a kibertér egyaránt felhasználható az infrastruktúra elleni fizikai támadásokra, valamint a kognitív



támadások, például dezinformáció. Az "információs konfrontáció" súlypontja azonban az emberek tudatában és az események érzékelésében rejlik, mind belföldön, mind nemzetközi szinten.

Ez a jelentés a kibertér szerepét igyekszik tisztázni az orosz stratégiai gondolkodásban.

Elemzi a kiberműveleteket, mint az orosz "információs konfrontáció" egy részhalmazát, és megvizsgálja, hogyan valósul meg ez a filozófia a gyakorlatban. A jelentés megvizsgálja mind az offenzív intézkedéseket, mint például az információs háborúban való részvételt, mind a defenzív intézkedéseket, mint például Oroszország erőfeszítéseit saját információs terének külföldi befolyástól való biztosítására.

Végezetül a jelentés számos szakpolitikai ajánlást fogalmaz meg

a NATO stratégiai kommunikációjára vonatkozóan Oroszország kibertérben folytatott offenzív tevékenységeinek kezelésére.



# OROSZORSZÁG "INFORMÁCIÓ KONFRONTÁCIÓ"

"ellenakcióra" utal.

## A "Cyber" orosz felfogása

Az "információs konfrontáció" orosz koncepciója és a kibertér ebben betöltött szerepe olyan stratégiai politikai dokumentumokban körvonalazódik, mint a Nemzetbiztonsági stratégia (2015), a Külpolitikai koncepció (2016), az Információbiztonsági doktrína (2016), a Katonai doktrína (2014), a Fegyveres erők információs térben folytatott tevékenységéről szóló koncepcionális nézetek (2016), valamint orosz katonai gondolkodók munkái és kiadványai.

Orosz szempontból a kiberhadviselés vagy annak orosz megfelelője, az "információs technológiai hadviselés" <sup>1</sup> csak egy része az **"információs konfrontáció"** (*informatsionnoe protivoborstvo*) átfogó koncepciójának. Az orosz védelmi minisztérium az információs konfrontációt a nemzeti érdekek és eszmék összecsapásaként írja le, ahol a fölényt az ellenfél információs infrastruktúrájának célba vételével igyekeznek elérni, miközben a saját objektumokat megvédik a hasonló befolyástól. <sup>2</sup> Az *informatsionnoe protivoborstvo* kifejezés angolra való fordítása nehéznek bizonyult, és gyakran helytelenül "információs hadviselés"-nek<sup>3</sup> (*informacionnaja vojna*) fordították, annak ellenére, hogy a *protivoborstvo* "ellenharcra", "ellenintézkedésre" vagy



a "háborúskodás" helyett. <sup>4</sup> Ez a dokumentum az "információs konfrontáció" kifejezést használja az ellenséges orosz információs tevékenységekkel kapcsolatos vitákban kialakult státusza miatt:

A konfrontáció jelentős pszichológiai hatáskört foglal magában, amelynek során a szereplő megpróbálja befolyásolni az információs forrásokat (az információs rendszerekben lévő dokumentumokat), valamint az ellenfél katonai állományának és a lakosság egészének tudatát. <sup>5</sup> Végső soron a kiberműveletek (vagy információtechnikai eszközök) egyike azon számos módszernek, amelyeket az információs konfrontációban a fölény megszerzésére használnak. Oroszország, és különösen Putyin orosz elnök rezsimje az információs konfrontációt a nagyhatalmak, politikai és gazdasági rendszerek és civilizációk közötti állandó geopolitikai zéróösszegű versenynek tekinti. <sup>6</sup>

kiberműveletekre. Az orosz dokumentumok továbbá nem használják a "kiberbiztonság" kifejezést, hanem inkább az "információbiztonságra" hivatkoznak. Ez a kifejezés eltér a

## Az "információ" védelme: Kognitív és Technikai

A nyilvánosan elérhető orosz doktrínák és politikai dokumentumok nem tesznek kifejezett utalást a



” Oroszország az információs teret nagyon is geopolitikai szempontból értelmezi, és a hazai információs tér a területi államhatárok folytatását jelenti, amelyet a külföldi behatolások miatt folyamatosan megsértettnek tekintenek.<sup>13</sup>

az "információbiztonság" (vagy röviden: infosec) nyugati fogalmát, mivel nemcsak a kritikus digitális hálózatok védelmét foglalja magában, hanem a társadalom kognitív integritását is.<sup>7</sup> Több oka is van annak, hogy az orosz katonai gondolkodók miért alkalmazzák a "kiber" kifejezést, amikor a nyugati fenyegetésekről és tevékenységekről beszélnek, de vonakodnak összekapcsolni a kifejezést Oroszország saját képességeivel és tevékenységeivel. Egyes szerzők szerint ez a tudatos választás a szovjet korszakbeli "kibernetika" körüli negatív konnotációkkal, valamint az "információbiztonság" kifejezésnek az orosz belpolitikában betöltött jelentőségével függ össze<sup>8</sup>.

Az operatív környezet tárgyalása során Oroszország az "**információs tér**" (*informacionnoe prostranstvo*) vagy "**információs szféra**" (*informacionnaya sfera*) kifejezést használja, amely szintén átfogóbb, mint a nyugati "kibertér" vagy "kibertér" fogalma. A 2016-os orosz információbiztonsági doktrína az **információs szférát** a következőképpen határozza meg:

"az információk, az információmatizációs objektumok, az információs

rendszerek kombinációja".



és weboldalak az internet információs és távközlési hálózatán belül [...], a kommunikációs hálózatok, az információs technológiák, az információ létrehozásában és feldolgozásában, a fenti technológiák fejlesztésében és használatában, valamint az információbiztonság biztosításában részt vevő szervezetek, valamint a szférában a társadalmi kapcsolatokat szabályozó mechanizmusok összessége".<sup>9</sup>

Az **információs tér** az információ formálására, átalakítására és tárolására irányuló tevékenységekre utal, valamint "az *egyéni és nyilvános tudatosság, az információs infrastruktúra és maga az információ befolyásolására*"<sup>10</sup>.

Ofer Fridman szerint Oroszország a kibertér fogalmát a hardver, a szoftver, az infrastruktúra és a

tartalom metszéspontjaként értelmezi<sup>11</sup>. Ebben a keretben az **információs technológiai** réteg magában foglalja a hardvert, a szoftvert és az infrastruktúrát, míg az **információs pszichológiai** réteg a hardvert, a szoftvert és a tartalmat. Függetlenül az alkalmazott eszközöktől - technológiai (például a digitális infrastruktúra tönkretétele)



vagy pszichológiai (egy üzenet manipulálása a közösségi médiában) - a kibertérben végzett tevékenységek az információs térben kifejtett hatásuk szempontjából értendők.<sup>12</sup> Fontos, hogy Oroszország az információs teret nagyon is geopolitikai szempontból fogja fel, és a hazai információs tér a **területi államhatárok folytatását** jelenti, amelyet a külföldi behatolások által folyamatosan megsértettnek tekintenek.<sup>13</sup>

A NATO-doktrína a kibertér műveleti területként értelmezi, és az **információs környezet** részének tekinti. Ez a környezet *"[...] magából az információból, valamint az információt fogadó, feldolgozó és továbbító egyénekből, szervezetekből és rendszerekből áll"*. Az e környezeten keresztül feldolgozott információk képezik a kognitív folyamatok alapját, amelyek befolyásolják az egyéni döntéshozatalt, majd a viselkedést. Ezek a folyamatok három dimenzióban - fizikai, virtuális és kognitív - játszódnak le, és a kibertér mindhárom dimenziót magában foglalja. Ebben a tekintetben a NATO információs környezetre vonatkozó koncepciója nem sokban különbözik az orosz felfogástól az "információs tér" és a kibertér ezen belül betöltött szerepéről.

Hasonlóképpen, az **"információs fegyverek"** orosz fogalma (amely a nyugati szóhasználatban gyakorlatilag nem létezik) nem csak digitális intézkedéseket foglal magában.<sup>14</sup> Bár az Orosz Fegyveres Erők homályosan úgy definiálja őket, mint *"információs technológiák, eszközök és módszerek, amelyeket a következőkre használnak*

*információs háborút vívni"*, a gyakorlatban a fogalom a tevékenységek széles körét foglalja magában (gyakran az emberi elmére gyakorolt hatásra helyezve a hangsúlyt); ide tartozik a dezinformáció terjesztése, az elektronikus hadviselés, a navigációs támogatás degradálása, a pszichológiai nyomásgyakorlás és az ellenfél számítógépes képességeinek megsemmisítése.<sup>15</sup>

Az államközi konfliktusok nyugati szemléletével ellentétben, amely a nemzetközi szerződésekből és szokásjogból (különösen az ENSZ Alapokmányában és a genfi egyezményekben) körvonalazott nemzetközi jogrendre épül, amely egyértelmű különbséget tesz háború és béke között, Oroszország "információs konfrontációja" állandó és folyamatos. Ezt a nézetet Oroszország arra használja ki, hogy a fegyveres konfliktus küszöbénél alacsonyabb szintű tevékenységeket folytasson, lehetővé téve számára, hogy kiszámíthatatlan maradjon, és stratégiai célokat kövessen, amelyek nem okoznak kinevetést. <sup>16</sup> A nyugati demokráciák egyik legfontosabb célja a szabad, stabil és nyitott internet fenntartása, ahol az alapvető jogok és szabadságok biztosítottak. Ebben a tekintetben az "információbiztonság" az adatok és rendszerek védelmét jelenti, de nem jelenti az e rendszerek felhasználói által kifejtett attitűdök és meggyőződések ellenőrzését. Ugyanakkor a nyugati demokráciákban a nyitottság és a szólásszabadság elvét az információs és kibertámadások kihasználhatják. Oroszország ezt a nyitottságot igyekszik kihasználni,



hogy "információs fölényre"  
tegyen szert, függetlenül attól,  
hogy hagyományos konfliktusban  
áll-e ellenfeleivel vagy sem.



# NEMZETBIZTONSÁGI ÉRDEKEK ÉS STRATÉGIAI CÉLOK



Research Agency, egy államilag támogatott vállalat, amelynek célja a közönség befolyásolása belföldön és külföldön egyaránt. Ezek az események segítettek Oroszországnak kifejleszteni azokat a tájékoztatási kampányképességeket, amelyek



megkönnyítették a Krím 2014-es annektálását23.



## Oroszország fenyegetése Percepció

Oroszországnak, mint hatalmas, jelentős természeti erőforrásokkal, de kevés természetes határral rendelkező országnak többször is mozgósítania kellett társadalmát a külföldi agressziókkal szemben. Ez hozzájárult ahhoz a mélységes bizonytalanságérzethez, amely szerint Oroszország biztonságát a határain túl, a vélt "befolyási övezetében" gyakorolt ellenőrzéssel lehet a legjobban garantálni.<sup>24</sup> Oroszország így hajlamos volt arra, hogy biztonságát zéróösszegű módon határozza meg, ami a klasszikus biztonsági dilemmát testesíti meg, miszerint akkor vannak biztonságban, ha ellenfeleik bizonytalannak érzik magukat. A Szovjetunió bukása után sok nyugati úgy vélte, hogy a kapcsolatok Oroszországgal újraindulnak. A Nyugattal szembeni orosz szkepticizmus azonban az 1990-es években tovább erősödött, ami nagyrészt a piacgazdaságra való rosszul kezelt átmenet során érzett súlyos gazdasági sokknak, valamint a Szovjetunió felbomlása utáni új, egységesítő nemzeti identitás hiányának volt köszönhető.

A Nyugattal szembeni bizalmatlanságot jól példázza Oroszország azon véleménye, hogy a NATO volt szovjet államokkal való bővítése agressziót jelent az általa követelt "befolyási övezet" felé. Oroszország a Nyugatot külföldi beavatkozással is vádolja, mert állítólag színes forradalmakat szít.<sup>25</sup> Igor Panarin volt KGB-tiszt úgy érvelt, hogy a Nyugat információs eszközeinek használata a 20. században az oroszokat saját országuk elpusztításához vezette, először az orosz cárok 1917-es bukásával, majd a Szovjetunió 1991-es összeomlásával.<sup>26</sup>

Emellett a Közel-Keleten és Észak-Afrikában végigsöprő 2011-es arab tavaszi forradalmak is beleillenek az oroszok



az ellenséges rezsimek megbuktatására tett következetes nyugati kísérletek narratívája, elsősorban információs eszközökkel. <sup>27</sup> Ezt a fenyegetés-felfogást emelte ki a 2016-os Információbiztonsági doktrína, amely kimondja, hogy:

*"Egyes államok hírszerző szolgálatai egyre gyakrabban használnak információs és pszichológiai eszközöket azzal a céllal, hogy destabilizálják a világ különböző régióinak belső politikai és társadalmi helyzetét, aláássák a szuverenitást és megsértsék más államok területi integritását. Vallási, etnikai, emberi jogi és egyéb szervezetek, valamint mint különálló embercsoportok, részt vesznek ezekben a tevékenységekben, és az információs technológiákat széles körben használják e célból".<sup>28</sup>*

A Kreml folyamatos offenzív álláspontja azt feltételezi, hogy a nagyhatalmak között rendszerszintű, folyamatos küzdelem folyik, ezért meg kell védenie magát a Nyugat következetes befolyásolási műveleteivel szemben. Ezt a megközelítést a 2000-es nemzetbiztonsági koncepcióban vázolták fel, amely szerint a

háborúk és fegyveres konfliktusok megelőzése érdekében Oroszországnak a nem katonai eszközöket kell előnyben részesítenie, és "az információs szférában jelentkező rivalizálás fenyegetésével szembeni ellenintézkedéseket" kell folytatnia. <sup>29</sup> Fontos az ő felfogásukban, hogy Oroszország saját fellépését védekezőnek érzékelik, a cél a potenciális konfliktusok és megtorlások megelőzése, illetve azok eskalációjának megfékezése azáltal, hogy a Nyugat fegyveres konfliktusküszöb alatt marad. <sup>30</sup>





Az információs eszközök együttesen működhetnek, mivel az orosz katonai gondolkodók szerint azáltal, hogy nem csak a vezetést és a katonaságot, hanem a lakosság teljes tömegtudata, stratégiai hatások érhetők el.<sup>35</sup>

## Stratégiai Elrettentés

Az információs technológia jelentősége az információs konfrontációban az orosz "stratégiai elrettentés" koncepciójából ered. Ez azon a felismerésen alapul, hogy a nukleáris fegyverek nem képesek kellőképpen elrettenteni a modern biztonsági fenyegetések teljes spektrumát,<sup>31</sup> ezért a stratégiai elrettentés nemcsak nukleáris és hagyományos katonai erőt foglal magában, hanem egy sor nem katonai eszközt is, például ideológiai, politikai, diplomáciai, gazdasági és - központi jelentőségű - információs és digitális intézkedéseket.<sup>32</sup> Fontos tehát megérteni, hogy a stratégiai elrettentés - elnevezése ellenére - nem csupán a nyugati értelemben vett elrettentésről szól, hanem a stratégiai célok elérésének átfogó megközelítése.<sup>33</sup> Oroszország felismerte, hogy az USA-val való katonai paritásra való törekvés költséges, és a Szovjetunió sorsára és a mai Oroszország gazdasági stagnálására való tekintettel el kell kerülni.<sup>34</sup>

Ezért a Kreml még békeidőben is szívesen használja ki a stratégiai kihívók sebezhetőségét. Az olyan közelmúltbeli erőfeszítések, mint a Krím annektálása, vagy a 2016-os amerikai választásokba való beavatkozás, megerősítették a

Oroszország számára az információs fegyverek hatékonysága a stratégiai célok elérésében anélkül, hogy a katonai konfrontáció vörös vonalait kiváltaná. Ez lehet az egyik fő oka annak, hogy az infrastruktúrát fizikailag befolyásoló kibertámadásokkal visszafogottabban bánnak, mivel azok drámaibb válaszlépéseket válthatnak ki, és így nehezebbé válik az eskaláció ellenőrzése.

Az információs konfrontáció általános célja a **stratégiai hatások** elérése és az **ellenféllel szembeni fölény megszerzése**, akár katonai, akár nem katonai eszközökkel történik. E célból a kiberműveletek alapvető szerepet játszhatnak a hagyományos erő ellensúlyozásában, mivel a kritikus polgári infrastruktúra, például az energia, a közlekedés és a C2 (Command and Control) képességek megbénítása drámaian gyengítheti az ellenfél hadrafoghatóságát. Az információs eszközök együtt is működhetnek, mivel az orosz katonai gondolkodók szerint stratégiai hatások érhetők el azzal, ha nem csak a vezetést és a katonaságot, hanem a lakosság teljes tömegtudatát célozzák meg.<sup>35</sup> Ez az orosz stratégiai gondolkodásmód operacionalizálja saját információs terük védelmét a kódok, jogi ellenőrzések és felügyeleti intézkedések



kiterjedt hálójá révén,  
amelyet a következő  
szakaszban vizsgálunk  
meg.







nem állami szereplők is részt vettek ilyen akciókban, beleértve az FSB-t (Szövetségi Biztonsági Szolgálat) és az Éjszakai Farkasokat. Ráadásul a *maskirovka* már nem kizárólag katonai célpontokra korlátozódik, hanem a polgári lakosságra is kiterjed. <sup>41</sup>



# AZ INFORMÁCIÓS TÉR BIZTOSÍTÁSA - "DIGITÁLIS SZUVERENITÁS"

2019 októberében lépett hatályba az "Oroszország szuverén internetéről" szóló törvény, amely gyakorlatilag lehetővé teszi a kormány számára, hogy saját belátása szerint lekapcsolja a globális internetet. Ennek érdekében a Kreml célja, hogy 2024-re az orosz internetforgalomnak csak 10%-át irányítsák külföldi szervereken keresztül.<sup>42</sup> A Kreml a biztonsága szempontjából alapvető fontosságúnak tekinti a hazai információs tér feletti ellenőrzést - a információs tér veszélyeztetése az állami szuverenitást fenyegető veszélyként érzékelhető. Ez a szakasz a "digitális szuverenitás" koncepciójának megvalósulását vizsgálja az orosz belföldi információs tér biztosítása érdekében hozott intézkedések feltárásán keresztül.

**A digitális szuverenitás** (*tsifrovoi suverenitet*) ebben az összefüggésben elsősorban politikai fogalomként használatos, és úgy értelmezhető, mint egy kormány azon joga és képessége, hogy saját információs terében meghatározza sorsát.<sup>43</sup> Igor Aszmanov orosz informatikai szakértő a digitális szuverenitást két részre osztja: **elektronikus szuverenitás**, amely magában foglalja a rosszindulatú szoftverektől és rosszindulatú kiberszereplőktől védett, robusztus internetes infrastruktúrát; és **információs szuverenitás**, az információk önálló ellenőrzése és az információs támadásokkal szembeni ellenállás. Az ideális állapot tehát autonóm hardverekből és szoftverekből, internetes infrastruktúrából, alárendelt tömegmédiából, egységesítő ideológiából és erős jogrendszerből állna.<sup>44</sup> A digitális szuverenitás lényeges eleme az **orosz internet** (RuNet).

- az internet orosz nyelvű, viszonylag zárt szegmense, amely népszerű

keresőmotorokból és olyan közösségi oldalakból áll, mint a Yandex, a Vkontakte és az Odnoklassniki. Bár látszólag



ártalmatlan, ez a rendszer lehetővé tette Oroszország számára, hogy elérje és befolyásolja a szomszédos országok orosz ajkú kisebbségeit, kiterjesztve Oroszország befolyási övezetét a digitális környezetben.<sup>45</sup> Az elmúlt években a RuNet alternatív online környezetből olyan térré kezdett átalakulni, ahol a Kreml aktívan elnyomja a nemkívánatos információkat - ez a törekvés a 2016-os információbiztonsági doktrínában is szerepel.<sup>46</sup> Érdekes módon, Oroszország növekvő érdeke az orosz internet leválasztásában semmissé teheti a RuNet bizonyos előnyeit, mivel korlátozza a képességüket, hogy ezeken a platformokon keresztül a határaikon kívül is ellenőrzést gyakoroljanak.

Az orosz védelmi és biztonsági elit 2012 után ismerte el az internet mint

biztonsági fenyegetés jelentőségét, amikor a politikai ellenzék széles körben használta az internetet a mozgósításhoz, először a hamis Duma-választás, majd Putyin újraválasztása ellen.<sup>47</sup> Számos lépést tettek a "digitális" koncepció megvalósítása érdekében.



szuverenitás", nevezetesen Oroszország saját nemzeti internetes szegmensének létrehozása, amely önellátóvá és függetlenné tenné Oroszországot a határain kívüli fejleményektől, ezáltal biztosítva a belső és külső fenyegetésekkel szembeni védelmet.

A zárt hálózat jelentős előnyöket biztosítana Oroszország számára az információs konfrontáció különböző fázisaiban. Oroszország nyerne a társadalmi rugalmasság és helyreállítás, a parancsnokság integritása és a mozgósítás idején mutatott általános teljesítménye tekintetében. A rendszer emellett elrettentő, tagadó hatást is kiváltana, amely a várható hiábavalóság miatt eltántorítaná az ellenfelet az ellenséges lépések megtételétől. 48 Az információs térben Oroszország és ellenfelei közötti konfliktus így igen aszimmetrikus jelleget nyerne, mivel a nyílt hálózatokon belül működő államok jelentősen korlátozott működési környezettel szembesülnének, míg Oroszország zárt hálózati nemzetként viszonylag szabadon működhetne. 49

Juha Kukkola számos olyan intézkedéscsomagot (vagy alrendszert) vázol fel, amelyek segítenek Oroszországnak "államosítani" hazai információs infrastruktúráját, például:<sup>50</sup>

1. **Tudományos - ipari alapok:** az orosz gyártású hardver és szoftver fejlesztése, valamint a biztonsági szolgálatok és a hadsereg ellátása.
2. **Állami hitelesítés és titkosítás:** erőfeszítések az adatok

az Oroszországon belüli adatforgalmat a biztonsági szolgálatok és a hadsereg számára, valamint az adatok védelmét a külföldi kizsákmányolással szemben.

3. **Feketelista és tartalomkezelés:** weboldalak eltávolítása és korlátozása.
4. **Céltott megfigyelőrendszerek és tömeges adatforgalom lokalizálása és visszatartása:** az internetszolgáltatók (ISP-k) végzik, az állam által elrendeltek szerint. A rendszer erősen centralizált, és a célok a kémelhárítás, a bűnüldözés és a politikai ellenőrzés.
5. **A létfontosságú információs infrastruktúrák (CII) védelmére irányuló erőfeszítések kiterjedt jogi rendszer révén:** a CII állami tulajdonlásán vagy ellenőrzésén, valamint a magánszereplők védelmére vonatkozó jogi kötelezettségeken alapulnak. Ez magában foglalja a legfelső szintű tartománynévkiadók (DNS), útválasztási regiszterek és az Internet Exchange Points (IXP) biztonsági mentéseit. Lehetővé teszi a nemzeti szegmens működését és a globális hálózatról való leválasztását.
6. **Információs-technológiai és információs-pszichológiai ellenintézkedések:** az államilag



ellenőrzött vagy ahhoz  
kapcsolódó  
hírszolgálatok, valamint  
az oktatási, hazafias és  
vallási intézmények  
irányítása.



” Számos lépést tettek a "digitális szuverenitás" koncepciójának megvalósítása érdekében, nevezetesen Oroszország saját nemzeti internetes szegmensének létrehozása érdekében, amely önellátóvá és függetlenné teszi Oroszországot a határain kívüli fejleményektől, így biztosítva a belső és külső fenyegetésekkel szembeni védelmet.

például a biztonsági szolgálatok és a hadsereg kibernetikai képességein keresztül. Ellenőrzi a hazai információs környezetet, és külföldön nyílt és rejtett kémkedést, valamint befolyásolási és kibernűveleteket folytat, hogy megakadályozza a lehetséges fenyegetések kialakulását.

követését, nem csak a

7. **Visszajelzés, nyomon követés, ellenőrzés és irányítás:** olyan alrendszer, amely valós idejű elemzést és reakciókat biztosít minden információs fenyegetésre.

A hazai információbiztonságot olyan rendszerek támogatják, mint a SORM és a GosSOPKA, valamint a nyilvános távközlési hálózat központi irányítására szolgáló rendszer (jelenleg fejlesztés alatt áll).

A **SORM (System of Operative-Search Measures)** egy szovjet korszakból származó megfigyelési technológia, amelyet a kormány 1998-ban kezdett el adaptálni a kialakulóban lévő digitális területre.<sup>51</sup> A SORM lehetővé teszi a telefon- és internetforgalom nyomon



metaadatok szintjén, hanem a tartalom és az adatforgalom szintjén is. Az internet- és egyéb távközlési szolgáltatók kötelesek szondákat telepíteni a hálózatukba, amelyek összekötik őket a Szövetségi Biztonsági Szolgálattal (FSB). A rendszer legújabb generációja (SORM-3) mély csomagvizsgáló képességekkel rendelkezik.<sup>52</sup> Más orosz biztonsági szolgálatok is kérhetnek hozzáférést a SORM-hoz: Noha nincs közvetlen bizonyíték a SORM külföldi használatára, kivéve néhány volt szovjet országot, természetesen érinti az Oroszországba utazó külföldi állampolgárokat.

### **A nyilvános távközlési hálózat**

#### **központosított irányítási rendszere**

jelenleg fejlesztés alatt áll, és azt a Rádiófrekvenciás Szolgálat a nyilvános távközlési hálózatok felügyeleti és irányítási központjából (TsMUSSOP) fogja irányítani. Előírja, hogy

az internetszolgáltatók (ISP-k) kötelesek bizonyos berendezéseket telepíteni a hálózatukba, amelyek képesek a forgalmat figyelni és szűrni, szükség esetén pedig teljesen blokkolni. Ez elméletileg elválasztaná az internet orosz szegmensét a globális hálózattól.<sup>53</sup>



### ***Az információs teret és a CII-t szabályozó jogszabályok***

Ezeket a technikai intézkedéseket kemény **jogi szabályozás** kíséri. Ez a rendszer kettős, hiszen egyrészt a kritikus információs infrastruktúra védelmét államosító törvényeket, másrészt az internetes tartalom és adatáramlás ellenőrzésére irányuló törvényeket egyesíti.

Az információs tér feletti teljes ellenőrzés biztosítása érdekében az orosz kormány olyan törvények egész sorát fogadta el, amelyek gyakorlatilag államosítják a KII védelmét. Ezek a jogszabályok az energiát és a közlekedést szabályozó korábbi vészhelyzetekre vonatkozó rendeletekből nőttek ki.<sup>54</sup>

Egy 2012-es politika<sup>55</sup> határozottan meghatározta a CII-t, és bevezette a **GosSOPKA** (kormányzati rendszer a számítógépes támadások felderítésére, megelőzésére és hatásainak megszüntetésére) nemzeti kiberbiztonsági rendszert. A GosSOPKA-t úgy tervezték, hogy egyetlen, folyamatosan felügyelt peremmel rendelkező rendszer "pajzsa" alatt "pajzsolja" az összes kormányzati információs erőforrást. Ez a pajzs kiterjedne az összes erőforrásra és kritikus infrastruktúrára, így ezek mindegyike megosztaná a kibertámadásokkal kapcsolatos információkat egy központi hivattal, amely megállapítaná, hogyan történt a támadás, és biztonsági ajánlásokat osztana szét a rendszer többi része között.

<sup>56</sup>

infrastruktúrákról szóló törvényt, amely pontosítja az FSB ellenőrzését a rendszer felett, és megerősíti a GosSOPKA végleges koncepcionális formáját, valamint a



a hálózat összes komponensének meg kell osztania vele az adatokat. <sup>57</sup> Összefoglalva, "a "jelentős objektumok" védelmére egy olyan vertikális, hierarchikus és központosított rendszert építenek ki, amelynek lehetősége van arra, hogy a nemzet valamennyi stratégiai ágazatát bekapcsolja az FSB által működtetett kiberbiztonsági rendszerbe "<sup>58</sup>.

2012 óta számos fontos törvényt fogadtak el, amelyek célja a hazai információs tér szabályozása és a cenzúra bevezetése. Említésre méltó az úgynevezett Jarovaja-törvény, egy 2016-ban elfogadott törvénycsomag, amely a terrorizmus elleni küzdelem ürügyén arra kötelezi az internetszolgáltatókat, hogy a Kreml számára hozzáférést biztosítsanak a felhasználók személyes adataihoz<sup>59</sup>. A törvény emellett szigorítja a gyűlöletbeszéd, a szélsőségeség büntetését, és nevezetesen kriminalizálja a zavargásokban való részvételt. Az alábbiakban a Svéd Orosz Tanulmányok Központja által összeállított további kulcsfontosságú törvényeket ismertetjük. <sup>60</sup>

2012

**Internet feketelista, 139-FZ / 2012-07- 28:**

Ez a törvény egy központi feketelistát indított el, amelyet a RozKonnadzor (a távközlési, információs technológiák és tömegkommunikáció területén működő Szövetségi Felügyeleti Szolgálat) felügyel, és amely bírósági végzés nélkül is érvényesíthető. A listán jelenleg 100 000 IP-cím szerepel.

**Külföldi ügynökökről szóló törvény, 190-FZ / 2012-11-21:**

Az Oroszországon kívülről működő és politikai tevékenységet folytató nem kormányzati szervezeteknek külföldi ügynökként kell regisztráltatniuk magukat, ami növeli a kormány vizsgálati jogkörét.



**2013**

**Ügyészségi internetblokkolás, 398-FZ / 2013-12-28:** Felhatalmazza a főügyészséget, hogy tárgyalás nélkül blokkolja a jogszabályokkal ellentétesnek ítélt weboldalakat.

**2014**

**Történelmi elbeszélések terjesztése, 128-FZ / 2014-05-05:** A Szovjetunió második világháborúban betöltött szerepéről szóló "hamis információk" miatt akár öt évig terjedő börtönbüntetést ír elő. Az országos televíziós hálózatok ezeket a narratívákat arra használják, hogy a lakosságot a Kreml külpolitikai céljainak támogatására mozgósítsák. 2016-ban egy orosz állampolgár 200 000 rubeles bírságot fizetett, amiért azt posztolta, hogy a Szovjetunió együttműködött a náciakkal Lengyelország 1939-es lerohanásában.

**Törvény a bloggerekéről, 97-FZ / 2014-05-05:** A napi 3000-nél több látogatót számláló bloggereknek regisztrálniuk kell magukat a hatóságoknál, és felelősséggel tartoznak a harmadik felek által a tartalmukhoz fűzött megjegyzésekért.

**Törvény az adatok lokalizálásáról, 242-FZ / 2014-07-21:** Előírja, hogy az orosz állampolgárokról gyűjtött adatokat 2020-ig az Orosz Föderációban kell lokalizálni, és a hatóságokat tájékoztatni kell azok hollétéről.

**A Wi-Fi telefonszám biztosításáról szóló törvény, a kormányrendelet sz. 758 / 2014-07-31:** A nyilvános Wi-Fi felhasználóinak meg kell adniuk telefonszámukat. Mivel a sim-kártya megvásárlásához útlevél szükséges, ez a törvény gyakorlatilag lehetetlenné teszi a névtelen internetezést.

**A médiavállalatok külföldi tulajdonlása, 305-FZ / 2014-05-02:** Megtiltja a külföldi befektetőknek, hogy 20%-nál nagyobb részesedéssel rendelkezzenek az Oroszországban működő médiavállalatokban.

**2016**

**"Jarovaja" törvénycsomag, 374-FZ és 375-FZ / 2016-07-06:** az ITC szolgáltatókat kötelezi a tartalom és a kapcsolódó metaadatok tárolására, valamint a hatóságok számára bírósági végzés nélkül történő átadására; a titkosított adatokat használó online szolgáltatásokhoz (pl. üzenetküldés, e-mail, közösségi hálózatok) az FSZB hozzáférhet.

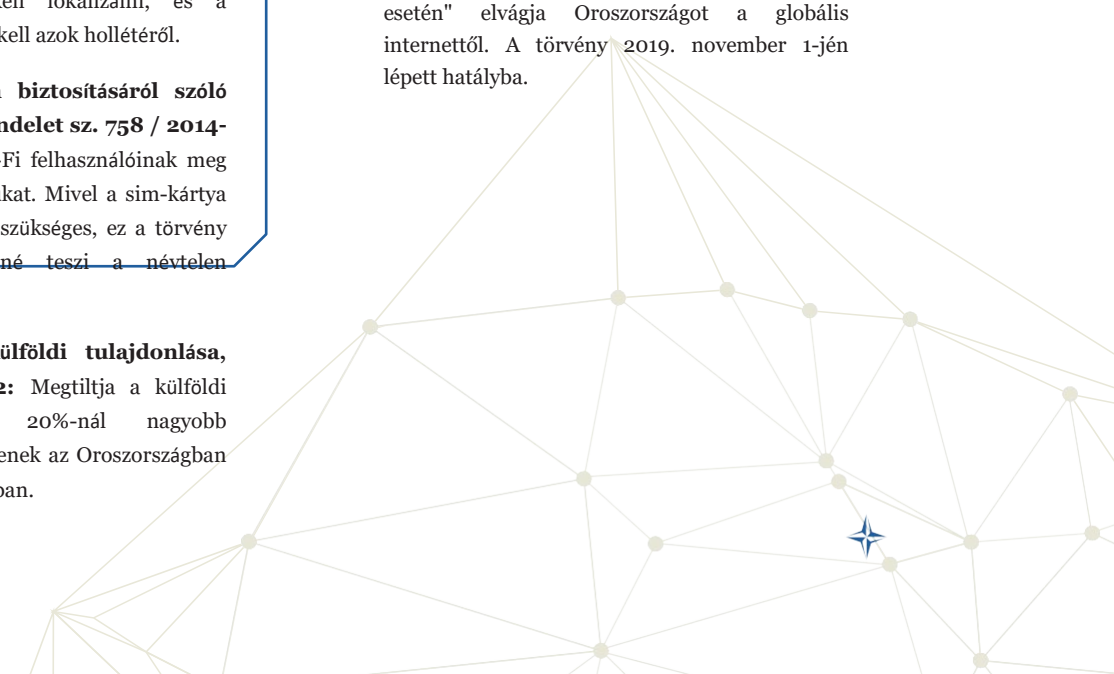
**2017**

**Az üzenetküldő szolgáltatásokat szabályozó jogszabály, 241-FZ / 2017-07-29:** előírja, hogy az üzenetküldő szolgáltatásokkal, köztük a WhatsApp-tal rendelkező internetszolgáltatóknak hat hónapig meg kell menteniük az üzeneteket és képeket, és át kell adniuk a hatóságoknak a dekódoló kulcsokat.

**Törvény a VPN betiltásáról, 276-FZ / 2017-07-29:** betiltja a proxy-szolgáltatásokat és a VPN-eket.

**2019**

**Szuverén internettörvény, 90-FZ / 05-01-2019:** olyan szoftverek telepítését írja elő, amelyek képesek szűrni, átírányítani és nyomon követni az online forgalmat, és lehetővé teszik a Rozkmondzor számára, hogy "vézhelyzet esetén" elvágja Oroszországot a globális internettől. A törvény 2019. november 1-jén lépett hatályba.





# ÁLLAMI SZEREPLŐK ÉS MEGHATALMAZOTTAK

Az információs konfrontációban Oroszország tevékenységét támogató szereplők között egyaránt megtalálhatók állami szereplők - jelentős szerepet kapnak az orosz hírszerző ügynökségek - és proxyk<sup>61</sup>. A nyilvánosan elérhető információk nem szolgálnak részletekkel az orosz hatalmi struktúrák szervezettségéről és döntéshozatali folyamatáról. Egyes nyugati kutatók azonban azt állítják, hogy a szovjet idők hierarchikus hatalmi vertikumával ellentétben az ma decentralizáltabb. A Kreml hajlamos széles kereteket szabni a megvalósítandó céloknak, és elvárja, hogy az alárendeltek dolgozzák ki és valósítsák meg a politikát. Így az alárendeltek felhatalmazást kapnak a kitűzött célok elérésére a vezetés szándéka, a helyszíni körülmények és a szereplő ebből következő megítélése alapján.<sup>62</sup> Ez a szakasz a Kreml kibertérben folytatott tevékenységeinek szereplőit és funkcióit vizsgálja.

Az orosz hírszerző ügynökségeknek három fő jellemzője van. Először is, a legfőbb prioritásuk a rezsim biztosítása - megelőző akciók révén belföldön és külföldön egyaránt. Másodsor, **versengő hírszerzéssel** foglalkoznak, harcolnak az erőforrásokért és a Kreml kegyeiért. Harmadsor, nem csupán a döntéshozatal, hanem a közvetlen cselekvés eszközének is tekintik magukat.<sup>63</sup>

**Az FSZB** (Szövetségi Biztonsági Szolgálat) a legerősebb különleges szolgálatnak számít, amelyet nagyrészt a KGB (Szovjetunió Állambiztonsági Bizottsága) utódjának tekintenek. Eredetileg belföldre összpontosított tevékenysége ellenére egyre inkább külföldön is tevékenykedik. A szolgálat felelős a kémelhárításért és a hírszerzésért, beleértve a kibertérben történő hírszerzést is. Az FSZB fontos szereplője Oroszország belföldi információs terének biztosításának is, és együttműködik olyan szövetségi ügynökségekkel, mint például a Roszkomnadzor (Szövetségi Szolgálat a

Kommunikáció, információtechnológia és tömegmédiá), Minsifri (az Orosz Föderáció Digitális Fejlesztési, Kommunikációs és Tömegkommunikációs Minisztériuma) és mások.<sup>64</sup> Az FSZB például lehallgatási és az orosz adatforgalom felügyeletére jogosult egy olyan megfigyelőrendszeren keresztül, amelyben minden oroszországi internetszolgáltató köteles részt venni.<sup>65</sup>

A nyugati hírszerző közösségek az FSZB-t a **Turla APT** (advanced persistent threat), más néven *Snake*, *Uroburos* és *Venomous Bear* kémtevékenységével hozták kapcsolatba. Programozásának minősége lényegesen kifinomultabb, infrastruktúrája összetettebb, mint más, állítólagosan Oroszországhoz kötődő támadóké, célpontjai pedig gondosabban válogatottak és hosszú távú értékkel bírnak.<sup>66</sup> A *Turla* vélhetően az egyik legrégebben ismert kiberkémkedő csoport, az Agent.btz féregtől kezdve, amelyet az amerikai hadseregben fedeztek fel.



◆◆◆◆◆◆◆◆◆ 7

hálózatokat 2008-ban, egészen a közelmúltbeli kémkedési kampányokig, amelyek műholdas internetkapcsolatokat térítették el, hogy elrejtse a parancsnoki és irányító szervereket, és csendben iráni hackerek szervereit vették igénybe, hogy a kémkedésükre támaszkodhassanak.<sup>67</sup>

**A GRU vagy GU** (az Orosz Föderáció Fegyveres Erői Főparancsnokságának Főigazgatósága) egy katonai külső hírszerző ügynökség. A korábbi, 2007-ben Észtország és 2008-ban Grúzia elleni kibernézetek során az FSZB "háttérembere" volt, a GRU azonban egyre láthatóbbá vált a támadó kibernézetekben. A nyugati hírszerző ügynökségek a közelmúlt legjelentősebb támadásait ennek az ügynökségnek tulajdonítják.<sup>68</sup> Noha nehéz megítélni, hogy a GRU vezető szerepet vállalt-e más különleges szolgálatok között a kibertérben végrehajtott műveletekben, tevékenységüket szélesebb körben fedezték fel és részletesen leírták a nyilvánosan elérhető információkban.

A GRU rendelkezik olyan képességekkel, amelyek hatékonyan felhasználhatók az információs konfrontáció információs-technikai és információs-pszichológiai dimenzióiban egyaránt. A 85. Különleges Szolgálati Központ (26165-ös egység), amely hagyományosan a jelhírszerzésért és a kriptográfiáért felelős, valamint a Speciális Technológiák Fő Központja (74455-ös egység) a számítógépes műveletekért felelős. A 74455-ös egység ismert a 2016-os amerikai elnökválasztás során végrehajtott hackelési és kiszivárogtatási műveletekről, a *NotPetya*

és más, az ukrán infrastruktúrát támadó rosszindulatú programok létrehozásáról,



és a műszaki dimenziót képviseli. A 72. Különleges Szolgálati Központ (54777-es egység), a GRU pszichológiai hadviselési apparátusának magja, legalább 2014 óta szorosán együttműködik a "technikai" egységekkel, és a kibertámadásokat digitális információs műveletekkel egészíti ki, proxykon és fedőszervezeteken keresztül.<sup>69</sup>

**A 26165-ös egység a gyanú szerint az APT28** (más néven *Fancy Bear, Pawn Storm, Sofacy, Strontium*) tevékenysége mögött áll. Ez volt az egyik legaktívabb APT-csoport, amely világszerte rendkívül kifinomult eszközöket használt műveleteihez, különösen a Kreml ellenfelei ellen. Bár a csoport tevékenységét a biztonsági cégek 2004 óta azonosítják, ezeket a támadásokat csak 2014 óta tulajdonítják nyilvánosan.<sup>70</sup> Kiderült, hogy a csoport felelős a

2014-es ukrajnai és a 2016-os amerikai választásokba való beavatkozásért, a német parlament (Bundestag) elleni 2015-ös támadásokért, a francia TV5Monde televízió elleni támadásért (az eredetileg az Iszlám Államhoz köthető *Cyber Caliphate* hackercsoportnak álcázva), a Vegyifegyver-tilalmi Szervezet (OPCW) elleni támadási kísérletért, a 2018-as pjongcsangi téli olimpiai játékokért és még sok másért. Mind az amerikai különleges ügyész Mueller vádiratai<sup>71</sup>, mind az uniós tisztviselők<sup>72</sup> az APT28-at a GRU 26165-ös egységeként azonosítják.

A **CyberBerkut** egy másik, a GRU-hoz köthető hacktivista stílusú csoport, amely Oroszország és Ukrajna konfliktusának kezdete óta aktív. A csoport kisajátította a korábbi



” A GRU rendelkezik olyan képességekkel, amelyek hatékonyan felhasználhatók az információs konfrontáció információs-technikai és információs-pszichológiai dimenzióiban.

Viktor Janukovics ukrán elnök különleges rendőri erőinek neve (az ukrán *berkut* szó az aranysasra utal) és logója, és az ukrainai orosz befolyásolási törekvésekhez igazodik. Az ukrán belső ellenzéki csoportként való azonosságát azonban nagymértékben megkérdőjelezzük,<sup>73</sup> és újabb vizsgálatok szerint a csoport a GRU APT28-as csoportjával koordinálja tevékenységét.<sup>74</sup> A csoport technikai és pszichológiai támadásokat egyaránt alkalmaz, és részt vett kiberkémkedésben, információs műveletekben és bomlasztó számítógépes hálózati behatolásokban, beleértve a DDoS (Distributed denial of service) támadásokat Ukrajna, a NATO és a német kormány honlapjai ellen.<sup>75</sup> A csoport elsősorban az ukrán kormány lejáratására irányuló kísérletekre összpontosít, és részt vett az ukrán elnökválasztás 2014-es szabotázi kísérletében.<sup>76</sup>

**A 74455-ös egység** gyaníthatóan a *Sandworm* csoport (más néven *Telebots*, *Voodoo Bear* és *Iron Viking*) tevékenysége mögött áll. A csoportot a kibernetikai

biztonsági iparág, mint a legpusztítóbb kibertámadásokért felelős.<sup>77</sup> A 2020. október 19-i amerikai vádiratban a GRU hackereit olyan számítógépes támadásokkal vádolták, amelyek "a világ eddigi legpusztítóbb rosszindulatú szoftvereit használták, többek között: *KillDisk* és *Industroyer*, amelyek egyenként áramkimaradásokat okoztak Ukrajnában (2015-ben és 2016-ban); *NotPetya*, amely csak a vádiratban azonosított három áldozatnak közel 1 milliárd dollárnyi kárt okozott; és *Olympic Destroyer*, amely a 2018-as pjongcsangi téli olimpiai játékok támogatására használt számítógépek ezreit hozta működésképtelenné."<sup>78</sup>

**Az SVR** (Külföldi Hírszerző Szolgálat) a két külső hírszerző ügynökség egyike (a másik a GRU), és fő feladata a humán és stratégiai hírszerzési tevékenység. A GRU-val ellentétben, amely nemcsak kémkedésre, hanem szabotázsra és információs műveletekre is használja a kibertérben, az SVR főként hagyományos kémkedési céllal lop információkat, olyan titkokat keresve, amelyek segíthetnek a Kremlnek megérteni a politikusok és döntéshozók terveit és indítékait<sup>79</sup>.





A kiberbűnözők alkalmazásának két oka lehet: egyrészt hihető tagadhatóságot biztosít, mivel nem egyértelmű a kapcsolatuk a kormánnyal, másrészt költséghatékony, mivel a hackereket csak akkor lehet támadásra hívni, amikor szükség van rájuk, és a hazafias hackerek gyakran ingyen dolgoznak.

A biztonsági közösség az SVR-t az **APT29** (*Cozy Bear/The Dukes*) tevékenységéhez kapcsolta<sup>80</sup>. Ez egy rendkívül kifinomult hackercsoport, amely folyamatosan fejlődő eszközökkel és nagy képességű operátorokkal rendelkezik. A csoport támadási infrastruktúrája összetett és költséges. A csoport hajlamos arra, hogy törvényes online szolgáltatásokat használjon ki akcióihoz, így a hamisan jóindulatú álca miatt kevésbé felderíthetővé válnak.<sup>81</sup> Az APT29-et összefüggésbe hozták a 2016-os amerikai választásokba való beavatkozással, az amerikai állami ügynökségek, think thanks és civil szervezetek, holland és norvég kormányzati intézmények elleni kémkedési műveletekkel 2017-ben, valamint mindannyiunk COVID vakcina elleni adatokkal az Egyesült Államokban, az Egyesült Királyságban és Kanadában. Az APT29 állhat az egyik legnagyobb, 2020-ban az amerikai szövetségi kormányzat, biztonsági szolgálatok és kritikus infrastruktúrák ellen irányuló kiberkémkedési akció mögött is, amelyet "SolarWinds hack"-nek neveztek el (nevét arról a cégről kapta, amelynek szoftverét

kompromittálták),<sup>82</sup> míg más szakértők hasonlóságokat észleltek a *Turla* APT által használt kódokkal.<sup>83</sup>

Az elmúlt évekig az információ a konfrontációt úgy tekintették, mint egy funkciót



a hírszerző  
szolgálatok, ezért a  
fegyveres erők  
fellépése a  
kiberműveletek és az  
elektronikus  
hadviselés közötti  
átfedések területeire  
korlátozódott. A  
média azonban  
beszámolt arról, hogy  
az orosz fegyveres  
erőkben "információs  
csapatokat" hoztak  
létre, amelyek célja az  
információs  
műveletek  
végrehajtása.<sup>84</sup> 2013-  
ban a Kreml  
bejelentette egy  
kiberegység  
létrehozását is a  
hadseregen belül,<sup>85</sup>  
amely a  
legkülönbözőbb  
szakembereket  
foglalja magában,  
köztük programozókat,  
matematikusokat,  
kriptográfusokat,  
valamint elektronikus  
hadviselési és  
kommunikációs  
szakértőket.<sup>86</sup> Az orosz  
fegyveres erőkön  
belüli  
kiberképességek  
helyzetéről azonban  
csak korlátozottan  
állnak rendelkezésre  
nyilvánosan elérhető  
információk

Az állammal kapcsolatban álló titkos  
szereplők vagy úgynevezett "proxyk"  
magukban foglalják az oligarchákat,  
vállalkozásokat, nonprofit szervezeteket,  
az orosz ortodox egyházat, a médiát,  
civilket, bandákat, a kormány által  
szervezett nem kormányzati  
szervezeteket és bűnszervezeteket.  
Számos szereplő annak ellenére, hogy  
független módon működik, hogy részeseül



pénzügyi támogatás és útmutatás a Elnöki adminisztráció.<sup>87</sup>

Fontos szereplő a "**hazafias hackerek**", akik hivatalosan nem részei az államgépezetnek, de az államhoz való kötődésük alapján akár önállóan, akár az állam által irányítva cselekedhetnek. A számítástechnikai és matematikai háttérrel rendelkező személyeket célzottan megcélozzák és hackertevékenységre csábítják.<sup>88</sup>

E csoportok mellett vannak **kiberbűnözők is**, akiket vagy a hírszerző szolgálatok fizetnek, vagy ha hajlandók képességeiket az állam szolgálatába állítani, akkor börtönbüntetésüket jelentősen csökkentik.<sup>89</sup> Az orosz hírszerző szolgálatok által a bűnöző hackerek felhasználására példa a Yahoo hackelése. Az FSZB bűnözőket használt fel (akiknek az akciói több százmillió eurós veszteséget okoztak a nyugati vállalatoknak és pénzintézeteknek) a Yahoo feltörésére, és ezzel a történelem egyik legjelentősebb adatbetörését követte el.<sup>90</sup>

A kiberbűnözők alkalmazásának két oka lehet: egyrészt **hihető tagadhatóságot** biztosít, mivel nem egyértelmű a kapcsolatuk a kormánnyal, másrészt **költséghatékony**, mivel a hackereket csak akkor lehet támadásra hívni, amikor szükség van rájuk, és a hazafias hackerek gyakran ingyen dolgoznak.

Az **Internet Research Agency (IRA)**, más néven a szentpétervári trollgyár egy magánszervezet, amely a Kreml szeszélye szerint működik. Alkalmazottai, megosztva

anyagspecifikus részlegekbe, hozzájárulnak a cikkek megvitatásához, utasítások alapján kommentálnak a közösségi médiában, és saját infografikákat és élő videókat készítenek a népszerű blogszolgáltatások számára, hogy elősegítsék a Kreml narratíváit vagy támadják ellenfeleiket.<sup>91</sup> Az IRA tevékenysége 2013 vége óta (az ukrajnai konfliktus eszkalálódása óta) tulajdonítható, és aktívan részt vesznek a Kreml-barát narratívák népszerűsítésében és ellenfeleinek támadásában Oroszországban és külföldön, valamint a polarizáció növelésén dolgoznak a közösségi médián keresztül a 2016-os és a 2020-as amerikai elnökválasztások nyomán is. Bár az IRA aktív szerepet vállalt a közönség manipulálásában és a társadalmi feszültségek fokozásában az Egyesült Államokban, szerepét és hatékonyságát nem szabad túlértékelni. Thomas Rid szerint az amerikai választások bebizonyították az IRA és az orosz titkosszolgálatok hackerei közötti jól bevált munkamegosztást. Az orosz hírszerző szolgálatok végzik hacker- és szivárogtató műveleteiket, miközben a "zajos és olcsó éket verő, a közösségi médián keresztül történő ékverést" kiszervezik harmadik fél szolgáltatóknak. Az IRA "inkább egy spammelő call centerhez, mint egy szigorú hírszerző ügynökséghez hasonlított, korlátozott operatív biztonsággal, nagyon korlátozott jelenléttel a célterületen, és az orosz hírszerzéssel való ismert operatív koordináció nélkül".<sup>92</sup> Lehet, hogy nem az IRA az egyetlen olyan cég, amely Oroszország biztonsági érdekeinek támogatására dolgozik, mivel több olyan

magáncég is van a piacon, amely hasonló szolgáltatásokat kínál a közösségi média manipulációjára<sup>93</sup>.





# Oroszország különleges szolgálatai részt vesznek a kiberműveletekben

## Service Group Targets



### GRU/GU

A fegyveres erők vezérkarának főigazgatósága

### APT28

(Fancy Bear, Pawn Storm, Sofacy, Strontium)

### CyberBerkut

### Cyberkalifátus

### SandWorm

- Ukrajna (választások, kritikus infrastruktúra) 2014 óta
- Németország (parlament) 2015
- USA (választások) 2016, időközi választások 2018
- Franciaország (média) 2015, (választások) 2017
- Montenegró (kormány) 2016 - 2017
- WADA/sportági szervezetek 2014 - 2018
- OPCW 2018
- Téli olimpiai játékok 2018
- Grúzia (parlament, média) 2019



### FSB

Szövetségi Biztonsági Szolgálat

### Turla APT

(Kígyó, Urobuross, Vízibogár, Mérgező medve)

- az Egyesült Államok kormánya 1990 óta
- Ukrajna 2014 óta
- 35 ország (iráni hackerként fellépő) 2019
- Németország (energia- és vízszolgáltatók) 2020



### SVR

Külföldi Hírszerző Szolgálat

### APT29

(Cozy Bear, Office Monkeys, Duke, CozyDuke, CozyCar)

- USA (kormányzat, katonaság) 2014 - 2015
- USA (választások, agytrösztök, civil szervezetek) 2016
- Norvégia (kormány) 2017
- Hollandia (kormány) 2017
- Anti - COVID vakcinakutatás az Egyesült Királyságban, az USA-ban és a CAN 2020-ban





” Egyetlen ország sem használta kiberképességeit olyan rosszindulatúan és felelőtlenül fegyverként, mint Oroszország, amely kis taktikai előnyök megszerzése és dühkitörések kielégítése érdekében akaratlanul soha nem látott károkat okoz. <sup>94</sup>

## TEVÉKENYSÉGEK A KIBERTÉRBEN

Oroszország a kibertérben való fellépéshez számos olyan eszközzel rendelkezik, amelyek mind **információs-technikai**, mind **információs-pszichológiai jellegűek**, és állami szereplőket, valamint megbízottakat is igénybe vesznek. Mindegyik eszköz azonban más-más célnak felel meg a legjobban, amely az információgyűjtéstől a döntéshozatal befolyásolásán át a kinetikus műveletek kiegészítéséig terjed. Fontos különbséget tenni a hazai közönségnek szánt és a külföldi országokat és az ottani különböző csoportokat célzó fellépések között is.

Oroszország egyedülálló a kortárs kiberhatalmak között a technikai és pszichológiai számítógépes hálózati műveletek elválaszthatatlanságának koncepciója tekintetében, amely a kritikus infrastruktúrára irányuló támadó kiberműveletektől kezdve a hamis közösségi médiaszemélyiségek használatáig terjed, hogy olyan üzeneteket terjesszen, amelyek Oroszország külpolitikai vagy katonai céljait

támogatják. <sup>95</sup> Oroszország minden más országnál jobban törekszik kognitív hatások elérésére a kiberműveletek végrehajtása során. <sup>96</sup>



A legtöbb taktika a háború és a béke közötti szürke zónában zajló "információs konfrontáció" befolyásolására irányul. Ez a szakasz az orosz offenzív kiberműveletek eseteinek vizsgálatán keresztül elemzi, hogyan valósul meg ez a megközelítés a gyakorlatban.

### ***Ukrajna***

Az ukrajnai konfliktus a mai napig az információs konfrontáció legösszetettebb példája, amely az orosz eszközök és módszerek bemutatója. Ukrajna a 2013-as Majdan-forradalom óta katonai konfliktusban áll Oroszországgal. Ezt gyorsan követte a Krím Oroszország általi 2014-es annektálása és a kelet-ukrajnai hadviselés. E folyamatban lévő konfliktus keretében Ukrajna alapvető tesztelési terepként szolgált Oroszország számos kiberképessége számára.

Oroszország krími művelete során az EW, a kiberműveletek közötti koordináció



és az információs műveleteket a kinetikus tevékenységek támogatására használták. Például 2014-ben az ukrán telefonszolgáltató, az UKRTelecom azt állította, hogy a Krímben tartózkodó orosz csapatok megbabrálták a kritikus fontosságú optikai kábeleket, és megszakították a félsziget és az anyaország közötti kapcsolatot (vezetékes, mobil- és internetszolgáltatások).<sup>97</sup> Az ukrán parlament tagjainak mobiltelefonjait megzavarták, az ukrán kormány honlapját pedig lekapcsolták. Március 8-án DDoS-támadások érték az Ukrán Nemzetbiztonsági és Védelmi Tanácsot és az Ukrinform ukrán állami hírügynökséget. Március 16-án, a Krím annektálásáról szóló népszavazás napján a NATO honlapjait a GRU-hoz kötődő "CyberBerkut" hacktivistacsoport támadta meg.<sup>98</sup>

Az "információs konfrontáció" technikai és pszichológiai eszközeit ötvöző, jelentős példa volt az ukrain elnökválasztás célba vétele 2014 májusában.

A választások az Oroszországgal fennálló konfliktus nyomán zajlottak, és az oroszbarát Viktor Janukovics elnök lemondása és az országból való elmenekülése után felállított új ukrán kormány lejáratását célozták. Három nappal a 2014. májusi elnökválasztás előtt támadást indítottak a Központi Választási Bizottság (CEC) hálózata ellen. A támadás hatástalanította a szavazatszámolás valós idejű megjelenítését, és azzal tetőzött, hogy a támadók nyilatkozatot tettek közzé a CEC weboldalán, amelyben egy szélsőjobb oldali jelölt elnökválasztási győzelmét állították. A tényleges szavazatszámolás megjelenítése 40 perccel a végső bejelentés előtt helyreállt az ukrán televízióban, ugyanakkor a CEC hamis győzelmet állító, manipulált képét azonnal levetítették az orosz tévécsatornákon, ami az orosz hackerek és az orosz média közötti koordinációra utal.<sup>99</sup> Bár ennek a támadásnak nem voltak hosszú távú hatásai, ez is példa arra, hogy számos orosz művelet célja egyszerűen a zavarás, az instabilitás és a félelem elszítása.



## Az ukrán villamosenergia-hálózat és infrastruktúra megzavarása

Ukrajna is áldozatul esett a villamosenergia-infrastruktúrája ellen irányuló zavaró kibertámadásoknak, amelyek 2015-ben és 2016-ban a lakosság nagy része számára áramkimaradásokat okoztak. Biztonsági kutatók szerint ezek voltak az első olyan esetek a történelemben, amikor a kibertámadók jelentős áramkimaradást okoztak; emellett "a világ eddigi legpusztítóbb rosszindulatú szoftvereit használták".<sup>100</sup> 2015 decemberében regionális elektromos hálózatokat támadtak meg, ami két-hat órás áramkimaradást eredményezett, ami 200 000-230 000 embert érintett.<sup>101</sup> Hasonló incidensre került sor 2016-ban<sup>102</sup>, amikor a támadók rövid időre lekapcsolták az áramot Kijev lakosságának egyötödében, és a vasúti rendszereket is érintették. Mindkét incidens több fázisban zajlott, kezdve a spear phishinggel és a hitelesítő adatok begyűjtésével, a hálózatok feltérképezésével, az adatok kiszivárgásához szükséges eszközök létrehozásával, a vezérlőrendszerek távoli elfoglalásával, végül pedig a rosszindulatú szoftverek telepítésével.<sup>103</sup> Az energetikai infrastruktúra elleni hasonló támadásokat regisztráltak a

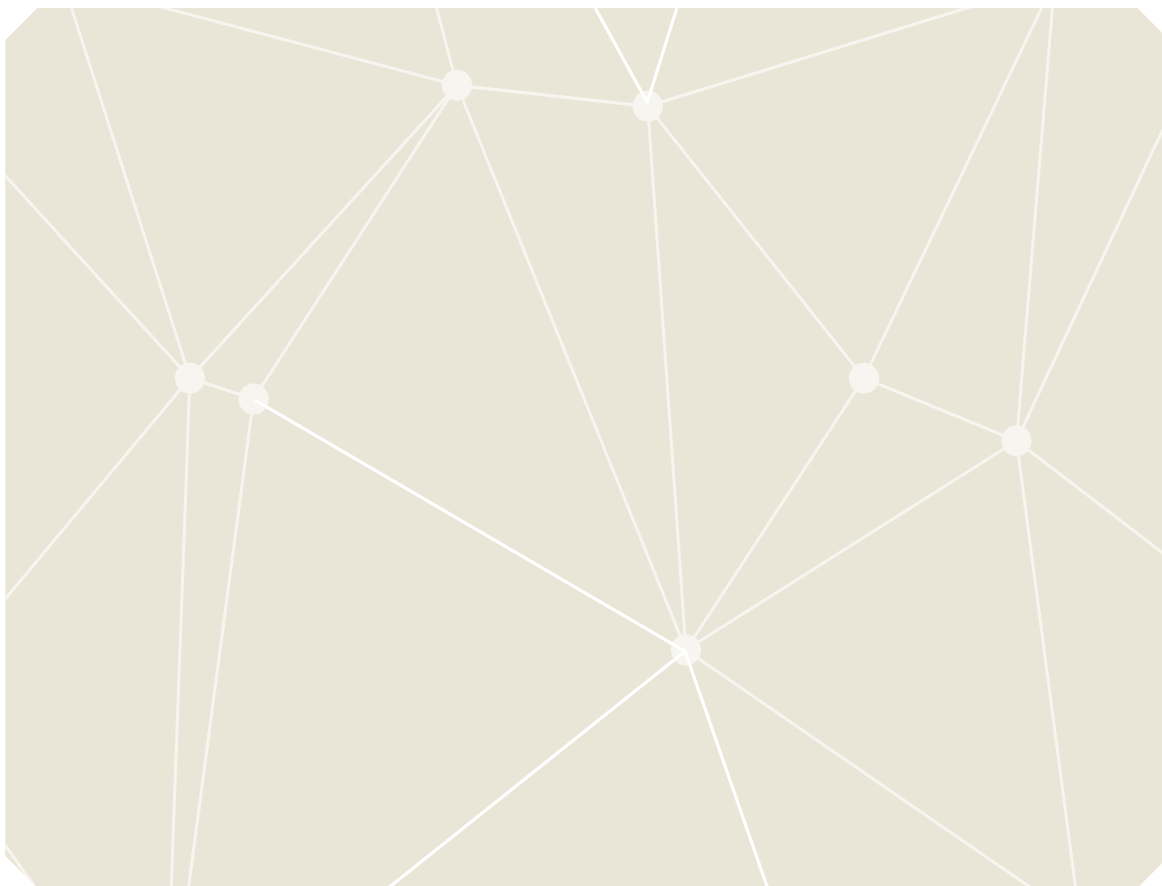




**Georgia**

Oroszországnak hosszú konfliktustörténete van Grúziával, különösen a 2008. augusztusi háborúval, amely után Grúzia elveszítette területének körülbelül egyötöde felett az ellenőrzést. Grúzia az egyik első példa arra, hogy katonai műveleteket és kiber-információs támadásokat együttesen alkalmaztak.<sup>107</sup>





### **Választási beavatkozás**

Amint fentebb említettük, az információs konfrontáció egyik stratégiai célja, hogy a politikai döntéshozatalt és a lakosság érzelmeit célba véve fölénybe kerüljön a vélt ellenféllel szemben. A választások különösen sebezhetőek, mivel lehetőséget nyújtanak a külső szereplők számára nemcsak arra, hogy támogassanak egy számukra kedvező jelöltet, hanem arra is, hogy kétségeket ébresszenek a választások tisztességes és szabad lebonyolításával kapcsolatban, megkérdőjelezzék az ország stabilitását, és általában véve aláássák a demokratikus folyamatokba vetett bizalmat.

Az orosz beavatkozást több országban is azonosították a választásokba. A 2016-os amerikai elnökválasztásba való beavatkozás a legjobban dokumentált eset, amely jól mutatja, hogy Oroszország mind az info-technikai, mind az info-pszichológiai eszközök felhasználásával *dolgozik*. Ez a beavatkozás az amerikai választási infrastruktúrát ért támadásokat, az amerikai választási infrastruktúra megszerzését, és ezt követően a

kiszivárgott, a Demokratikus Kongresszusi Kampánybizottság (DCCC) és a Demokratikus Nemzeti Bizottság (DNC) adatai, beleértve a párt jelöltjének, Hillary Clintonnak az e-mailjeit, valamint az IRA és az Oroszországhoz kapcsolódó média által folytatott kiterjedt információs kampány<sup>112</sup> Azonban a célzott információs és kiberműveletek





utalt erre. A pletykát gyorsan cáfolták, és több médiaforrás is bebizonyította, hogy ezek a dokumentumok hamisítványok.





egy évvel korábbi amerikai elnökválasztás során a DNC hacker-akcióban.

### Montenegró NATO-csatlakozásának megcélzása

kampányt, a fenyegetőzéseket

A kiberműveleteket nagyobb kampányok részeként használták fel a NATO bővítési folyamatának akadályozására, amelyet a Kreml agresszívnek és fenyegetőnek tart. Ez történt Montenegró esetében is, amikor 2016 végén a NATO-val folytatott csatlakozási tárgyalások utolsó fázisában volt. Oroszország a támadás több formáját is vállalta: Montenegró az orosz média által folytatott információs



a bortermelésre és más termékekre vonatkozó embargók, a 2016. októberi parlamenti választások során elkövetett *államcsínykísérlet, valamint az orosz különleges szolgálatoknak tulajdonítható kibertámadások (ATP28 vagy Fancy Bear).* Ebben az időszakban Montenegróban jelentősen megnőtt a kibertámadások száma (azonban nem mindegyik tulajdonítható Oroszországnak), amelyek főként állami intézményeket és médiumokat céloztak. A 2013-as mindössze 22 ilyen incidensről 2017-ben mindössze kilenc hónap alatt közel 400-at regisztráltak.<sup>115</sup>





APT28-nak tulajdonították. <sup>118</sup>

**Befolyásolási kampányok: "Szellemíró"  
és "Másodlagos infekció"**

ki magukat,

A "Ghostwriter" nevű csoport 2017 márciusa óta a Nyugat-ellenes narratívák felerősítésére összpontosít Lengyelországban, Lettországban és Litvániában. Kampányukkal kapcsolatban több különálló incidenst is azonosítottak. Hamisított hivatalos dokumentumokat használtak, kormányzati és diplomáciai levelezésnek adták ki magukat, hamis narratívákat terjesztettek, és hírportálokat használtak fel legitimnek tűnő cikkek terjesztésére. Legalább 14 nem hiteles személyazonosság, akik helyieknek adták



újságírók és elemzők hoztak létre vagy felerősítette a hamisított tartalmat.<sup>119</sup>

A "Ghostwriter" időzítése egybeesik a NATO-csapatoknak a Baltikumba és Lengyelországba való megérkezésével a megerősített előretolt jelenlét (eFP) részeként. Az érkező csapatokat az orosz médiában és a közösségi médiában intenzív dezinformációs kampányok célpontjává tették.<sup>120</sup> A

"Ghostwriter" tevékenysége nem korlátozódott a hamis online személyiségek/robotok/médiumok létrehozására az online üzenetek felerősítése érdekében (ezt a módszert főként az Internet Research Agency ügynökei használják), e tevékenységek olyan technikai eszközöket is magukban foglaltak, mint pl.





A manipuláció hasonló módszereit (hamisított dokumentumok, megszemélyesítés, az információk botok/hamis személyiségek által történő felerősítése a közösségi és online médiában) azonosították a "Másodlagos infekció" elnevezésű, több célpontot érintő kampányban.

mint a weboldalak kompromittálása és a hivatalos e-mailek meghamisítása.

A biztonsági cégek nem tulajdonították a "szellemiró" tevékenységét egyetlen szereplőnek sem, azonban jelezték, hogy az Oroszország biztonsági érdekeit szolgálja, "elsősorban az amerikai és NATO-csapatokkal szembeni bizalmatlanság szítására törekszik Európában azáltal, hogy jelenlétüket agresszívnek és veszélyesnek állítja be a helyi lakosság számára, és aláássa a NATO-tagok közötti katonai kapcsolatokat"<sup>121</sup>.

Bár a két művelet között nincs bizonyított kapcsolat vagy koordináció, a manipuláció hasonló módszerei (hamisított dokumentumok, megszemélyesítés, a

a közösségi és online médiában botok/hamis személyiségek által nyújtott információk) a "Secondary Infekcion" elnevezésű, több célcsoportot érintő kampányban azonosították. A Graphica elemzése egy 6 éves információs műveletet fedezett fel, amely Európa és Észak-Amerika országait célozta meg hamis történetekkel és hamisított dokumentumokkal. Az elemzés legalább 2500 tartalmat fedezett fel hét nyelven, 300 online platformon, amelyeket a Kreml kritikusan és elnökjelöltek ellen használtak az Egyesült Államokban, Franciaországban, Németországban, Svédországban és más országokban. Az információs támadások középpontjában Ukrajna állt, azonban aktívak voltak az amerikai (2016) és a francia (2017) választásokon, valamint a WADA (Nemzetközi Doppingellenes Ügynökség) ellen is.<sup>122</sup>



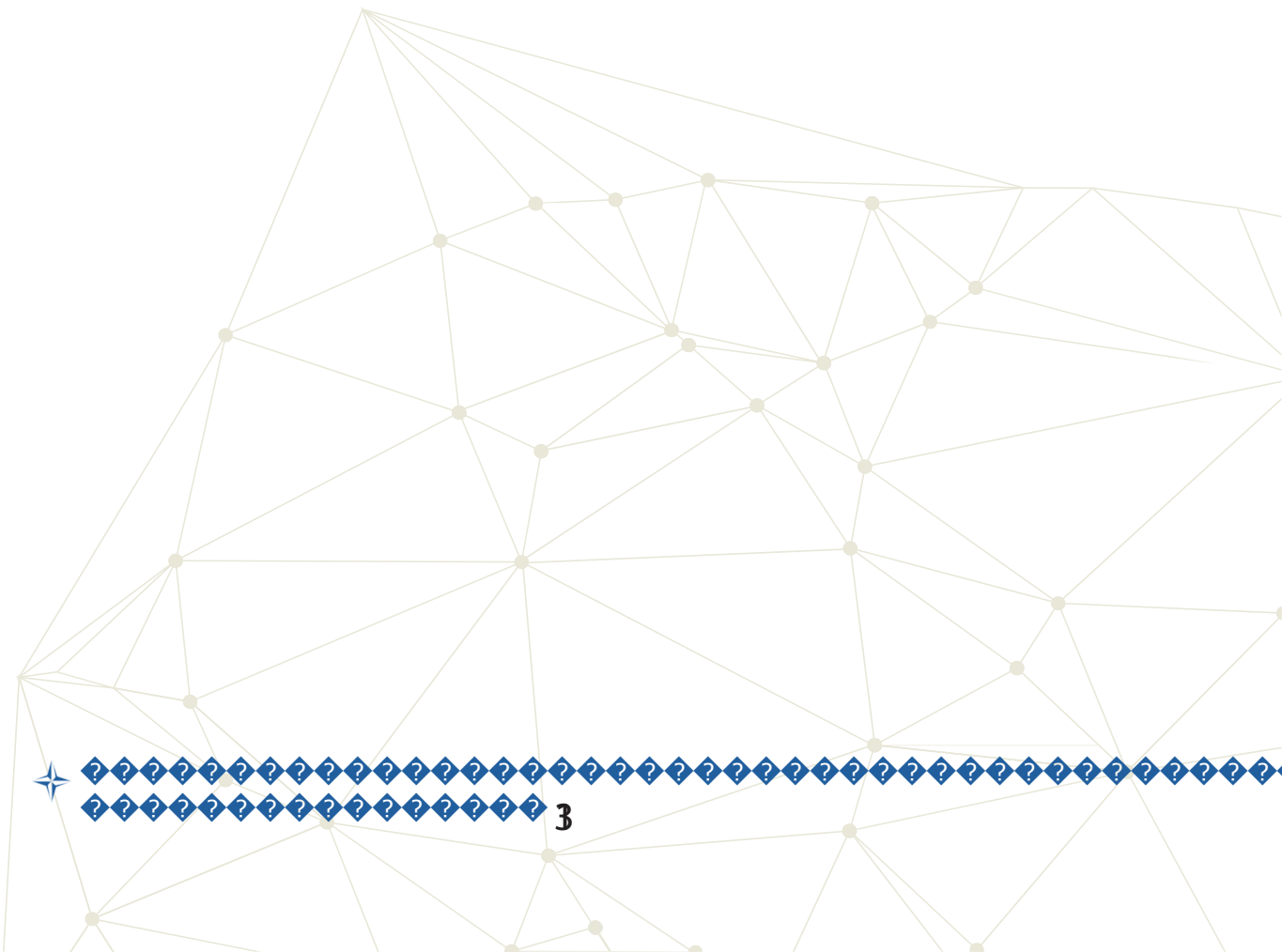
## Szellemíró hadművelet: COVID-19 miatt a NATO elhagyja a Baltikumot

2020. április 21-én egy ismert litván újságíró (15min.lt) és tényellenőrző, Vilius Petkauskas blogján álhír jelent meg. A "A NATO kivonja csapatait Litvániából" címet viselő cikket azonnal terjesztették a *TheDuran* és az *OpEdNews* marginális weboldalakon (amelyek korábban már terjesztettek NATO-ellenes narratívákat lett és litván hangzású nevekkel ellátott névtelen online személyiségek segítségével), valamint a





erotesziteseket mutatjak.



” Oroszország ügynökei nem félnek attól, hogy lebuknak, és nem haboznak újra megtámadni ugyanazt a célpontot, miután azonosították őket.

## KÖVETKEZMÉNYEK ÉS CÉLKITŰZÉSEK

tevékenységek generálására korlátozta.

Oroszország nem egy egységes kibertámadási stratégiát alkalmaz minden célpontra, hanem alkalmazkodik és kihasználja a felmerülő lehetőségeket.<sup>124 A</sup> A fent bemutatott incidensek arra utalnak, hogy a kiberműveleteket mind a hagyományos ellenfelek elleni katonai akciók (mint Grúzia és Ukrajna esetében), mind a befolyásolási tevékenységek célpontjai (mint az USA, a NATO, a balti országok, Montenegró stb. esetében), valamint az instabilitás és félelemkeltés lehetőségének felmerülésekor is felhasználják. Példaként említhetők a franciaországi kiberkalifátus akciók vagy az európai országok demokratikus folyamataiba való beavatkozás. Továbbá az orosz ügynökök nem félnek a lebukástól, és nem haboznak újra megtámadni ugyanazt a célpontot, miután azonosították őket (mint például a WADA esetében), valószínűleg azért, mert az ilyen tevékenységek eddig nem jártak következményekkel.

Oroszország elkerülte a nyílt eskalációt, és kibertevékenységét a kibernetikai



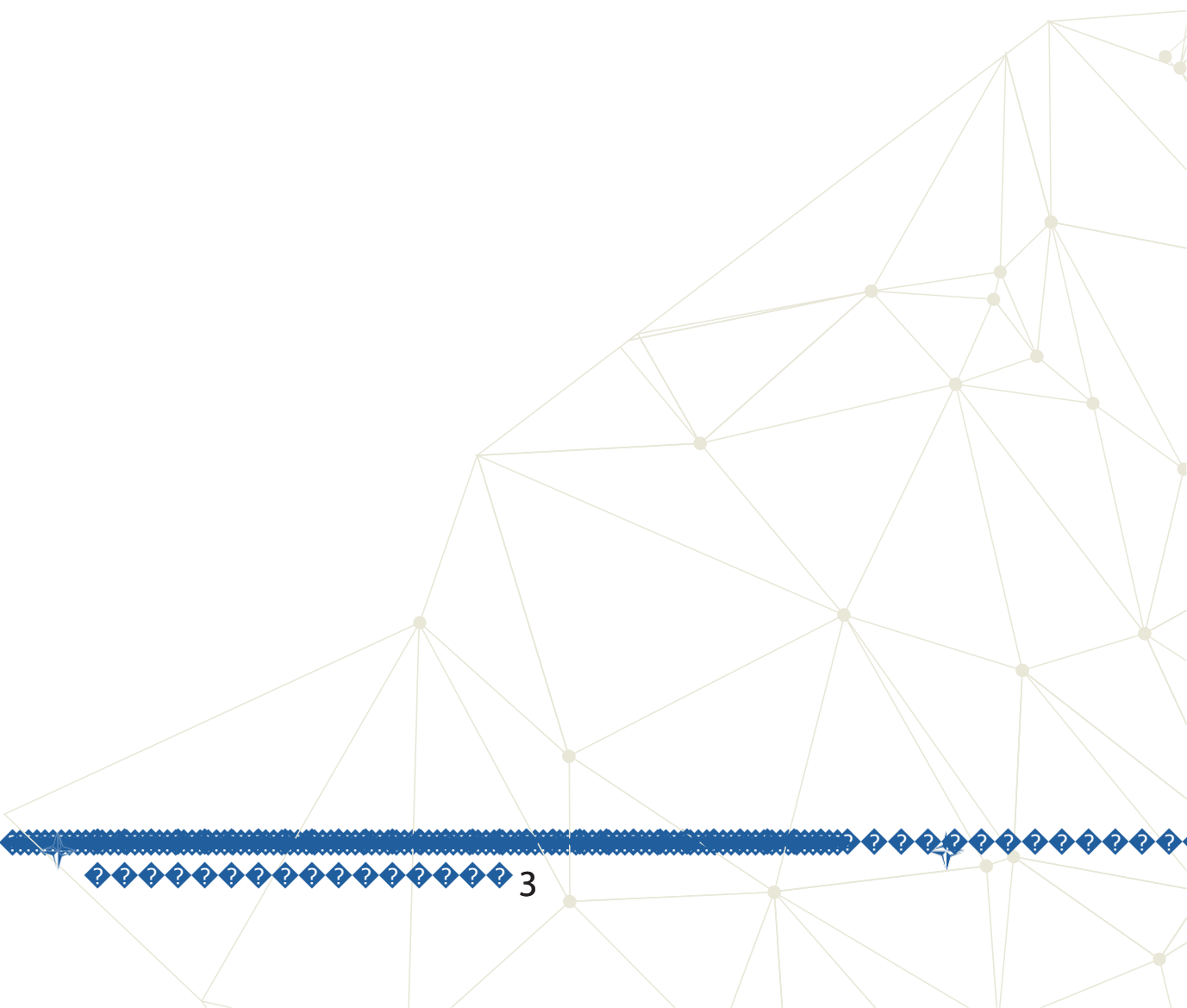
olyan hatások, amelyek jelenleg a hagyományos fegyveres választ kiváltó küszöbérték alattinak <sup>tekinthetők</sup><sup>125</sup>, legalábbis a jelenleg azonosított műveletek esetében. Ezt a támadási stílust részben lehetővé teszi (bár ez a közelmúltban változott) az a nyugati paradigma, amely a kritikus infrastruktúrák elleni pusztító támadó kiberműveletekre összpontosít, amelyek elméleti csúcspontját gyakran "kiber-Pearl Harborként" emlegetik. <sup>126</sup> Két tényező azonban megváltoztathatja Oroszország stratégiai számításait a kiberműveletekkel kapcsolatban. Az első a stratégiai elrettentési koncepcióját érinti, amelynek értelmében Oroszország úgy döntene, hogy az információs eszközök más eszközökkel együtt fokozottabban alkalmazza azokat, hogy megpróbálja a geopolitikai konfrontációt de-escalálni, vagy egy nyílt háborút Oroszország számára elfogadható feltételekkel lezárni.

<sup>127</sup> A második tényező

az orosz internetes szuverenitás állapota, amely siker esetén jelentősen csökkentené Oroszország kifelé irányuló támadási felületét, és ezáltal lehetővé tenné számára, hogy eszkalációs intézkedéseket tegyen, kisebb kockázattal szembesülve a hatékony megtorló intézkedésekkel. <sup>128</sup>

A NATO kiberfenyegetésekre való reagálási képességét befolyásoló fejlemény az attribúció problémája. Az orosz hackerek hamis zászlókat használtak, amikor az ISIS-hez kapcsolódó CyberCaliphate csoportnak adták ki magukat, hogy megtámadják a francia televíziót, az amerikai hadsereget és médiát, valamint észak-koreai hackerek kódját használták a 2018-as dél-koreai téli olimpia elleni támadás során. A hamis zászlós műveletek új szintre léptek, mivel a jelentések szerint az orosz hackerek más országok infrastruktúráját eltérítik, hogy kémkedjenek a

célpontok és rosszindulatú szoftverek célba juttatása. 2019 októberében az orosz *Turla* hackercsoport beszivárgott az *OilRig*, egy prominens iráni hackercsoport szervereire, és 35 különböző országot figyelt meg a rendszereik segítségével. Azt állítják, hogy az ilyen hamis zászlós támadások célja nemcsak a zűrzavar és a tagadhatóság megteremtése, hanem annak a narratívának a vetése, hogy a tulajdonítás nem lehetséges, ami aláássa a hírszerző ügynökségek hitelességét, amikor a kibertámadásokat a Kremlnek tulajdonítják, és aláássa az esetleges megtorló intézkedéseket.<sup>129</sup>





# KÖVETKEZTETÉS ÉS AJÁNLÁSOK

Orosz szempontból az "információs konfrontáció" állandó, és az ehhez használt eszközök között minden lehetséges eszköz megtalálható. Oroszország védelmi erőfeszítéseinek első vonalát a hazai információs tér jelenti, amelyet szigorúan ellenőriznek az adatfelügyelet és a Kreml ellenfelei ellen irányuló korlátozó jogrendszer révén. A Kreml információs-pszichológiai és információs-technikai fegyvereket vet be azzal a céllal, hogy stratégiai győzelmet érjen el hagyományos erő alkalmazása nélkül és anélkül, hogy a célországban bármilyen eszkalációs drótot kioldana. A hazai információs tér biztosítása nemcsak a társadalom pszichológiai kohéziójának védelmét teszi lehetővé a külföldi beavatkozástól, hanem a hazai tudományos és technológiai fejlesztéseket is megvédi a külföldi versenytől.

Meggyőződve arról, hogy a Nyugat folyamatosan információs háborút folytat Oroszország ellen, a támadó akciókat olyan válaszlépésekkel indokolják, amelyek állítólag azért szükségesek, hogy megakadályozzák a konfrontáció további eszkalálódását. A NATO szabad és nyitott információs környezetét és a "háborús" és "békeidő" gyakran kettéválasztott felfogását a Kreml kihasználta, így a Szövetség és tagjai már régóta várják a "kibertér" fogalmának és az információs környezethez való viszonyának aktualizálását.

A NATO-nak arra kell összpontosítania, hogy a fenyegetések teljes spektrumával szemben ellenálló képességet építsen ki, beleértve a fegyveres konfliktus küszöbénél kisebb fenyegetéseket is, mivel Oroszország számára az információs konfrontáció állandó, és nem korlátozza a békeidő és a háborús időszak közötti különbségtétel. A nyugati országok egyre inkább megértik, hogy

a kibertér az állandó konfrontáció környezete. Ez vezetett a politika és a doktrína megváltoztatásához, valamint ahhoz, hogy az amerikai kiberparancsnokság elfogadta a "tartós szerepvállalás" stratégiáját, és a francia fegyveres erők minisztériuma is hasonló megközelítést alkalmaz.<sup>130</sup> Bár jelentősek, ezek az erőfeszítések csak az információs konfrontáció technikai aspektusait kezelik. Ezt a hiányosságot kezeli a brit fegyveres erők egy speciális kibernművelati egység bevezetése, amely az információs-pszichológiai dimenzióval kapcsolatos támadó és védekező feladatokat egyaránt ellátja, de a szövetség egészére kiterjedően többet kell tenni.<sup>131</sup>

Vlagyimir Putyin elnökségének 1999-es kezdete óta nem történtek jelentős változások vagy ellentmondások az "információs konfrontációval" kapcsolatos hivatalos orosz doktrinális és koncepcionális kiadványokban. Ehelyett a doktrinális gondolkodás



a korábbiakra épült és azokat kiegészítette, egyes koncepciókat és módszereket még a szovjet időkből is átvett.<sup>132</sup> Mindazonáltal, mivel Oroszország "információs konfrontációra" irányuló képességei és módszerei folyamatosan fejlődnek, ez azt jelenti, hogy a válaszoknak adaptívnak és előremutatóknak kell lenniük.

Ez a dokumentum számos intézkedést javasol a Szövetség és tagállamai számára védelmi képességeik fokozása érdekében, kezdve azzal, hogy elismerik, hogy az oroszok a kibernetika egy tágan értelmezett, technikai és pszichológiai szempontokat egyaránt magában foglaló információs szférán belüli eszközként értelmezik:

- **StratCom funkciók integrálása, különös tekintettel a kiberműveletekre:** A szinergiák megteremtése, sőt az olyan funkciók teljes integrálása, mint a pszichológiai műveletek, a közügyek, a kiberműveletek, az elektronikus hadviselés és egyes jogi szempontok, jelentős mértékben megkönnyítené a StratCom parancsnokság számára a szinergia megteremtését. alkalmazodóképesség a békeidőben való képességbővítés céljából. A szövetségesek fontolórrá vehetik a gyorsreagálású kommunikációs csoportok létrehozását, egy olyan átfogó megközelítést, amelyet független erőforrásként lehetne létrehozni, amely a műveletek során gyorsan bevethető ellenséges információs környezetbe.
- **Az információs környezet kockázatelemzésének fokozása** az alábbiak azonosításával

mely népcsoportok és infrastruktúrák a legsebezhetőbbek a kiber- és információs támadásokkal szemben. A NATO elemzőit több előzetes kutatással és tervezéssel kell megbízni.

Azonosítaniuk kell, hogy milyen ellenséges üzenetküldő populációk a legérzékenyebbek, és azonosítaniuk kell az ezekhez a sebezhetőségekhez vezető alapvető problémákat. Ez segít a szövetségeseknek olyan irányelvek kialakításában, amelyek megvédik a lakosságot a külföldi befolyástól, valamint a kibertámadások során az ellenálló képesség és az egység előmozdítása.

- **Az interoperabilitás fokozása a kibertámadások elleni válságkezelési gyakorlatok növelésével, amelyek a stratégiai kommunikáció egyéb funkcióit is magukban foglalják:** Ez az elem kulcsfontosságú a NATO gondolkodásmódjának modernizálásához abban az értelemben, hogy ösztönzi a az információs támadások felismerése és annak megértése, hogy ezek hogyan valósulnak meg a kiberműveletekkel együtt.
- **Az EU és a nemzeti kormányok támogatása a digitális biztonság fokozásában, például az adatvédelem és a közösségi média jobb szabályozásának támogatása révén:** A NATO jelentős szerepet játszhat a nemzeti kormányok és az EU támogatásában a szövetségesek és partnerek közötti digitális környezet biztosításában. Ennek az erőfeszítésnek nem az információs tér

feletti ellenőrzés  
érvényesítéséről kell szólnia,  
hanem a védelmi

mechanizmusok kiépítéséről.  
annak biztosítása érdekében, hogy a magánadatok és  
a





” A NATO-nak arra kell összpontosítania, hogy a fenyegetések teljes spektrumával szemben ellenálló képességet építsen ki, beleértve a fegyveres konfliktus küszöbénél kisebb fenyegetéseket is, mivel Oroszország számára az információs konfrontáció állandó, és nem korlátozza a békeidő és a háborús időszak közötti különbségtétel.

a polgárok digitális lábnyoma ne kerüljön ellenséges kezekbe, ugyanakkor meg kell védeni az olyan alapvető demokratikus értékeket, mint a szólásszabadság.

szinten az attribúció fokozása és az ilyen támadások hatékony kommunikálása a

- **Az elrettentés megerősítése, többek között az attribúció és az olyan partnerekkel való együttműködés révén, mint az EU és a magánszektor:** A nyílt információs környezet sebezhetőségén túl, az információs konfrontációnak nincs olyan jelentős stratégiai elrettentő ereje, mint amelyet a nukleáris paritás biztosít a hagyományos értelemben. A nyugaton a beavatkozás és a kibertámadások több magas szintű incidense után tapasztalt tétlenség az ellenfelek körében az alacsony költség/magas jutalom érzékelését keltette. Ezért a hiteles elrettentő erő megteremtése az információs konfrontáció területén alapvető fontosságú. Az elrettentéshez való hozzájárulás másik módja a kiber- és információs támadásokra válaszul hozott erőteljesebb politikai intézkedések meghozatala a politikai következmények fokozásával. Politikai



a nyilvánosság segít a társadalmi ellenálló képesség javításában. Az EU e tekintetben kiváló partnere a NATO-nak, mivel új szankciórendszert fogadott el kifejezetten a kibertámadásokról a vonatkozóan.

133

**Az egész kormányzatra kiterjedő megközelítés és a társadalom szélesebb körű bevonásának előmozdítása.**

Az információs környezet összetett jellege miatt a NATO-n túl számos szereplőre van szükség a hatékony védelemhez. A magánvállalkozásoknak és a civil társadalomnak szorosan együttműködnie kell a hibrid fenyegetésekkel szembeni ellenálló képesség kiépítésében. A NATO-országok integritása az

egész társadalomra kiterjedő erőfeszítés, mivel minden személy és eszme kihasználható, és az ellenfelek célja a célcsoportok attitűdjeinek és viselkedésének befolyásolása. Ezért az ajánlásokon túlmenően fontos a tájékozott és kritikus lakosság, amely immunis a dezinformációval szemben, és amelynek oka lesz arra, hogy politikai vezetőire bízva a társadalom védelmét. a kiber- és informatikai támadások esetén nem lehet alábecsülni.

■





# Végjegyzetek

- 1 A fogalmak hasonlóságának további magyarázatát lásd: Kukkola J. (2020), *Digitális Szovjetunió. Az internet orosz nemzeti szegmense mint stratégiai kulturális elképzelések által formált zárt nemzeti hálózat*, 184. o.
- 2 Orosz Föderáció. Információs konfrontáció, Fogalomtár, Orosz Védelmi Minisztérium. <http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary>; V. Veprintsev, A. Manoylo, A. Petrenko, D. Frolov. (2015). Оперции информационно-психологической войны, Горячая линия - Телеком, pp. 347-348.
- 3 Az információk hadviselést azonban gyakran használják, amikor az információk térben történő ellenfél általi agresszióra utalnak, Lauder M.A. (2019), Számítógépek által leadott lövések, 6. o.
- 4 Kukkola J., Ristolainen M., Nikkarila J-P (2017). *Játék Változó: A kibertér strukturális átalakulása*, 119. o.
- 5 V. Veprintsev, A. Manoylo, A. Petrenko, D. Frolov. (2015). Оперции информационно-психологической войны, Горячая линия - Телеком, pp. 347-348.
- 6 Kukkola J., *Digitális Szovjetunió*. 107. o.
- 7 Orosz Föderáció. (2016). Az Orosz Föderáció információbiztonsági doktrínája, Külügyminisztérium. az Orosz Föderáció; J. Kukkola, M. Ristolainen, J-P. Nikkarila, Game Changer, 10. o. & N. Popescu, S. Secrieru. (2018). *Hacks, leaks and disruptions - Russian cyber strategies*, EUISS, pp. 17.
- 8 J. Kukkola, *Digitális Szovjetunió*.
- 9 Orosz Föderáció. (2016). Az Orosz Föderáció információbiztonsági doktrínája, az Orosz Föderáció Külügyminisztériuma.
- 10 Orosz Föderáció (2011). Konceptcionális nézetek az Orosz Föderáció fegyveres erőinek az információk térben folytatott tevékenységéről, Orosz Védelmi Minisztérium.
- 11 O.Fridman előadása az *IISS webináriumnán "Oroszország kiberhasználata" címmel Kényszer*", 2020. december 3.
- 12 O.Fridman előadása az *IISS webináriumnán "Oroszország kiberhasználata" címmel Kényszer*", 2020. december 3.
- 13 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, 11-12. o.; Kukkola J., Ristolainen M., Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', *Journal of Information Warfare*, Vol. 17, No. 2 (2018), 83-100.
- 14 Giles K. (2016), *Handbook of Russian Information Warfare*, p. 10.; K. Giles és W. Hagestad II. (2013). Egy közös nyelv által megosztva: Kiberdefiníciók kínai, orosz és angol nyelven, NATO CCDCOE.
- 15 Orosz Föderáció. (2011). Konceptcionális nézetek a Az Orosz Föderáció fegyveres erőinek tevékenysége az információk térben; Mshvidobadze K. (2011). *The Battlefield On Your Laptop*, RFE. & Giles és Hagestad II, *Divided by a common language*.
- 16 U.S. Cyber Command. (2018). Kibertéri fölény elérése és fenntartása: Az amerikai kiberparancsnokság parancsnoki jövőképe, pp. 2-10.
- 17 Olsen J., Creveld M. (2011). *Az operatív művészet fejlődése: Napóleontól napjainkig*. Oxford University Press, pp. 88-89.
- 18 Lambeth B. (1993). A sivatagi vihar és annak jelentése: *The View from Moscow*, RAND, 73. o.
- 19 Thomas T., *Az információalapú hadviselés orosz nézetei*, p. 30.
- 20 Giles K. (2016). Oroszország "új" eszközei a Nyugattal való szembenézéshez: *Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, 28-29. o.; Popescu N., Secrieru. S. (2018). *Hacks, leaks and disruptions - Russian cyber strategies*, EUISS, pp. 5, 15-16.; Blank S. *Cyber War and Information War a la Russe*, p. 84.; Soldatov A. *With its cyber troops the Russian military has become political*, Raam op Rusland. Oroszország, 2018. október 31.
- 21 lasiello E. (2017). *Oroszország javuló információk műveletei: Form Georgia to Crimea*, Army War College, 52-54. o.
- 22 Giles K. (2016), *Russia's 'New' Tools for Confronting the West*, 29. o.
- 23 Giles K.(2016), *Russia's 'New' Tools for Confronting the West*, pp. 29-31.; Soldatov A. *With its cyber troops the Russian military has become political*.
- 24 Giles K. (2019). *Moszkvai szabályok: What Drives Russia to Confront the West*, Chatham House, Brookings Institution, pp. 35-38.
- 25 A "színes forradalmak" kifejezést a volt Szovjetunió országaiban az autokratikus rendszerek megdöntésére irányuló, nem erőszakos tüntetésekre használják, mint például a grúz rózsás forradalom (2003), az ukrán narancsos forradalom (2004) és a kirgizisztáni tulipános forradalom (2005). Egyes források a "színes forradalmak" kifejezést az ázsiai és balkáni hasonló tiltakozó megmozdulásokra is használják.
- 26 Fridman O., *The Russian perspective on Information Warfare*, Defence Strategic Communications, Vol 2, 2017, pp. 75-76.
- 27 Giles K., *Handbook of Russian Information Warfare (Az orosz információk hadviselés kézikönyve)*, 41. o.
- 28 Orosz Föderáció (2016), *Az Orosz Föderáció információbiztonsági doktrínája*
- 29 Blank S., *Cyber War and Information War a la Russe*, 84. o.; Orosz Föderáció (2000). *Az Orosz Föderáció nemzetbiztonsági koncepciója*



- Orosz Föderáció, Az Orosz Föderáció  
Külügyminisztériuma.
- 30 Fink Loukianova A. (2017). [A stratégiai elrettentés fejlődő orosz koncepciója: Risks and Responses](#), Arms Control Association; Id: Kofman M., Fink A., Edmonds J. [Russian Strategy for Escalation Management: Evolution of Key Concepts](#). 2020. április, CNA
- 31 Bruusgaard V. (2016). Russian Strategic Deterrence, Global Politics and Strategy, pp. 9-10.; Fink Loukianova A. (2017). [A stratégiai elrettentés fejlődő orosz koncepciója: Risks and Responses](#), Arms Control Association;
- 32 Lauder M.A. (2019), Gunshots by computers, 16. o.; Meakins J. (2018). (Digitális) tagadásban élni: Russia's Approach to Cyber Deterrence, European Leadership Network, 7. o.
- 33 Bruusgaard V., Russian Strategic Deterrence, pp. 14-19.; Forsström P (2019). Venäjän sotilasstrategia muutoksessa: Tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen, National Defence University, p. 183.
- 34 J. Kukkola, M. Ristolainen, J-P. Nikkarila, Game Changer, 21., 23. o.
- 35 Giles K., Handbook of Russian Information Warfare, pp. 16-18.
- 36 Kincaid C. (2014.04.09.), How Putin Uses KGB-style "Active Measures", Accuracy in Media; Jaitner M, Mattsson P. (2015), Russian Information Warfare of 2014, NATO CCD COE, 39. o.
- 37 Egyesült Államok Külügyminisztériuma. (1981). Szovjet "Aktív Intézkedések": Hamisítás, dezinformáció, politikai műveletek.
- 38 Rasmussen R. C. (2015). "Cutting Through the Fog: Az orosz STRATCOM Ukrajnában". Center for International Maritime Security.
- 39 Thomas T. (1996). Russian Views of Information-Based Warfare, Airpower Journal, pp. 31-32.
- 40 Keating K. (1981). Maskirovka: The Soviet System of Camouflage, U.S. Army Russian Institute, 4. o.; Beaumont R. (1982). Maskirovka: Soviet Camouflage Concealment and Deception, The Texas Engineering Experiment Station, pp. 1-3.; Lauder M.A, Gunshots by computers, p. 45.
- 41 Lauder M.A., Számítógépek által leadott lövések, 45. o.
- 42 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, pp. 5, 93.
- 43 Kukkola J., Ristolainen M, Nikkarila J-P, Game Changer, 11-12. o. & Pynnöniemi K. Kari M., Russia's New Information Security Doctrine (Oroszország új információbiztonsági doktrínája).
- 44 Kukkola J., Ristolainen M, Nikkarila J-P, Game Changer, p. 11.; Barandiy M. (2018). Ideológia és információs támadások: How the Kremlin Builds its Informational Sovereignty; Ashmanov I. (2013). Информационный суверенитет России: новая реальность. Россия навсегда;
- 45 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, pp. vii, 12. o.
- 46 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, p. 13.
- 47 Kukkola J. Digitális Szovjetunió. 321. o.
- 48 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, xiii, 20. o.; Lavikainen J, Pynnöniemi K. és Saari S, Voiman Venäjä, Puolustusministeriö 66. o.; Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, vii. o.; Kukkola J. Digital Soviet Union.
- 49 Kukkola J., Ristolainen M, Nikkarila J-P., Game Changer, p. xi.
- 50 Kukkola J. Digital Soviet Union; Kukkola J. [The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry](#), pp.16 - 21; in: Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCD COE, 2021.
- 51 Polyakova A és Meserole C. (2019). A digitális tekintélyelvűség exportálása: az orosz és a kínai modell. Brookings Institution.
- 52 Cimpanu C, [Some of Russia's surveillance tech leaked data for more than a year](#), ZDNet 30 Aug 2019;; J A Lewis, [Reference Note on Russian Communications Surveillance](#), Center for Strategic and International Studies, 2014. április 18.
- 53 Kukkola J. Digitális Szovjetunió, 351. o.
- 54 Kukkola J. Digitális Szovjetunió, 328. o.
- 55 Az Orosz Föderáció lakossága biztonságának, valamint a kritikus és potenciálisan veszélyes objektumok természeti fenyegetésekkel, ember okozta és terrorista cselekményekkel szembeni védelmének biztosításával kapcsolatos állami politika alapelvei a 2020-ig terjedő időszakra vonatkozóan.
- 56 Turovskij D. [Moszkva kibervédelme: Hogyan tervezi az orosz kormány megvédeni az országot a közelgő kiberháborútól](#). Meduza, 2017. július 19.
- 57 Kukkola J. Digitális Szovjetunió, 349. o.
- 58 Kukkola J. Digitális Szovjetunió, 346. o.
- 59 Polyakova A és Meserole C. (2019). A digitális tekintélyelvűség exportálása: az orosz és a kínai modell. Brookings Institution.
- 60 "RUNET: A tekintélyelvű internet növekedése," svéd Center for Russian Studies (2018), 3-29. o., 10. sz.
- 61 Ez a jelentés az "állami szereplők" alatt a kormányzati intézményeket és az alárendelt struktúrákat (pl. hírszerző ügynökségek) érti. A "meghatalmazottak" kifejezéssel minden olyan nem kormányzati szereplőt jelölünk, amely közvetlenül vagy közvetve az államtól kap feladatokat, vagy az állam érdekeinek megfelelően dolgozik.
- 62 Galeotti M.. (2016). "Putin's Hydra: Inside Russia's Intelligence Services", ECFR, 12-13. o. & Lauder M.A., Gunshots by computers, 40-43. o.
- 63 Galeotti M., Putyin hydra, 4-8. o.
- 64 Az orosz információs tér biztosításában részt vevő intézményekről bővebben lásd. J. Kukkola (2020), Digitális Szovjetunió.



- 65 Väliisluureamet, International Security and Estonia, 54. o.; Connell M, Vogler S., Russia's Approach to Cyber Warfare, p. 7.; Galeotti M. (2016), Putyin hidra, 2. o.; Defense Intelligence Agency (2017). Russia Military Power: Building a Military to Support Great Power Aspirations (Oroszország katonai ereje: A nagyhatalmi törekvéseket támogató hadsereg építése), 72. o.
- 66 Väliisluureamet, International Security and Estonia, pp. 48-49.; Paganini P.(2017). [A Snake APT csoport offenzívára készül a magasan jegyzett Mac-felhasználók ellen](#), Security Affairs, 2017. május 5.
- 67 Greenberg A. [A SolarWinds hackerek megosztották a trükköket a Hírheft orosz kémcsoport](#). Wired. január 11, 2021
- 68 Lilly.B, Cheravitch J., The Past, Present and Future of Russia's Cyber Strategy and Forces, in: 12th International Conference on Cyber Conflict, NATO CCDCOE Publications, 2020., pp. 139-141.
- 69 Lilly.B, Cheravitch J. The Past, Present and Future of Russia's Cyber Strategy and Forces (Oroszország kiberstratégiájának és erőinek múltja, jelene és jövője), pp. 142-146. o.
- 70 Rid. T. (2020) Aktív intézkedések: A dezinformáció és a politikai hadviselés titkos története. Profile Books, 364-365. o.
- 71 Garret M. Graff, [Indicting 12 Russian Hackers Could Be Mueller's Biggest Move Yet](#), Wired, 2018. július 13. <https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear/>
- 72 [A TANÁCS \(EU\) 2020/1536 végrehajtási rendelete](#), 2020. október 22.
- 73 Jövőbeli rekorder. (2015). A Cyber Berkut a DDoS mutatóanyagokból a kibertámadási eszközök szállítójává lépett elő; E. Kovács. (2014). Három NATO-weboldalt tettek tönkre a Cyber Berkut ukrán hackerei, Softpedia.; J. Haines. (2015). Russia's Use of Disinformation in the Ukraine Conflict, FPRI.
- 74 Maurer T. (2015). Cyber Proxies and the Crisis in Ukraine, CCDCOE, 85. o. & A. Greenberg. (2017). 'Everything We Know About Russia's Election-Hacking', Wired.
- 75 Védelmi Hírszerző Ügynökség, Oroszország katonai ereje, 39-40. o.
- 76 Maurer T, Cyber Proxies and the Crisis in Ukraine, 81. o.
- 77 Greenberg A. [US Indicts Sandworm, Oroszország legpusztítóbb kiberháborús egysége](#) Wired, 2020. október 19.
- 78 Az Egyesült Államok Igazságügyi Minisztériumának [sajtóközleménye](#), október 19, 2020
- 79 Nakashima E. és Timberg C. [Russian government hackers are behind a broad spionage campaign that has compromised U.S. agencies, including Treasury and Commerce](#), The Washington Post, 2020. december 14., december 14.
- 80 Väliisluureamet, Nemzetközi biztonság és Észtország, 56. o.
- 81 Weedon J. (2015). Túl a kiberháborún: Oroszország stratégiai kiberkémkedés és információs műveletek alkalmazása Ukrajnában, CCDCOE, 69-70. o., magyarul: "A "kiberháború": Oroszország stratégiai kiberkémkedése és információs műveletei Ukrajnában".
- 82 Nakashima E. és Timberg C. [Orosz kormányzati hackerek állnak egy széles körű kémkedési kampány mögött, amely veszélyeztette az amerikai ügynökségeket, köztük a pénzügyminisztériumot és a](#)



- Kereskedelem, The Washington Post, 2020. december 14., december 14.
- 83 Greenberg A. [A SolarWinds hackerek megszították a trükköket a Hírhedt orosz kémcsoport.](#) Wired. Január 11., 2021.
- 84 Connell, Vogler, Russia's Approach to Cyber Warfare, 7-8. oldal.
- 85 Connell, Vogler, Russia's Approach to Cyber Warfare, pp. 7-8.; Soldatov A. és Borogan I., Russia's Approach to Cyber: Hacks, Leaks and Disruptions: Russian Cyber Strategies.2018, 17. o.
- 86 Beckhusen R.. [Az orosz hadsereg saját kibercsapatokat hoz létre, a háború unalmas.](#) 2015. május 28.
- 87 Lauder M.A. (2019), Gunshots by computers, 43. o.; Pernik P. (2018), Hacking for influence, 9. o.
- 88 Maurer T. (2018). Kibersoldosok: The State, Hackers, and Power, pp. 94-95.
- 89 Connell, Vogler, Russia's Approach to Cyber Warfare, pp. 10-11. & Väilsluureamet. (2019). "A nemzetközi biztonság és Észtország", pp. 50-53.
- 90 Maurer T., Hinck G., Oroszország kiberstratégiája.
- 91 Chen A., [The Agency](#), The New York Times Magazine, 2015. június 2.
- 92 T. Rid. Aktív mérések: A dezinformáció és a politikai hadviselés titkos története. Profile Books, 2020, 409. o.
- 93 További információért lásd: [NATO StratCom COE. A közösségi média manipulációjának fekete piaca.](#) Riga, 2018. november.
- 94 John Demers, az amerikai nemzetbiztonsági főügyész helyettes nyilatkozata a GRU-hackerek elleni vádirat kapcsán. Lásd: Az Egyesült Államok Igazságügyi Minisztériumának [sajtóközleménye](#), 2020. október 19.
- 95 Cheravitch J., Lilly B. (2021), Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its A tagok válaszolhatnak, In: Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCD COE, 45. o.
- 96 Lauder M.A. (2019), Gunshots by computers, pp. 35, 40.; Maurer T., Hinck G. (2018). Oroszország kiberstratégiája, ISPI.
- 97 Weedon J., Túl a "kiberháborún": K. Geers (szerk.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015, pp. 67-77, [https://ccdcoe.org/uploads/2018/10/Ch08\\_CyberWarinPerspective\\_Weedon.pdf](https://ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf)
- 98 Croft A, Apps P. [NATO-weboldalakat ért kibertámadás a krími feszültséggel összefüggésben](#), 2014. március 16.
- 99 Koval N., "Revolution Hacking". In K. Geers (szerk.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCDCOE Publications, Tallinn 2015. Pp. 56-58.
- 100 Az Egyesült Államok Igazságügyi Minisztériumának [sajtóközleménye](#), október 19, 2020
- 101 [Your Guide to Russia's Infrastructure Hacking Teams](#), Wired, 2017. december 7.



- 102 Zetter K., [Az ukrán elektromos hálózatot ismét feltörték](#), Motherboard Tech by Vice, 2017. január 10,
- 103 Lauder M.A., Pisztolylövészek számítógépekkel, 39. o.
- 104 S.Jewkes, O.Vukmanovic, [Feltételezett Oroszország által támogatott hackerek a balti energiahálózatokat célozzák meg](#), 2017. május 11., Reuters
- 105 E.Nakashima. [Az orosz hadsereg állt a NotPetya mögött kibertámadás Ukrajnában A CIA következtetései](#). 2018. január 12., The Washington Post
- 106 A. Greenberg. [The Untold Story of NotPetya, the MostPetya, the Most](#) [A történelem legpusztítóbb kibertámadása](#), 2018. augusztus 22., Wired.
- 107 A. Greenberg. [Az USA az orosz GRU-t hibáztatja az átfésülésért. Kibertámadások Grúziában](#), Wired, 2020. február 20.
- 108 E.Tiik, K.Kaska, L.Vihul, [Nemzetközi kiberincidensek: Jogi Considerations](#), NATO CCD COE, 2010, 69-71. o.; P.Pernik.
- A kibertámadások kezdete: Észtország esetei,
- Grúzia és Ukrajna, in: [Hacks, leaks and disruptions: Oroszország kiberstratégiái](#), EU ISS, 2018. október, 59-60. o.
- 109 Cimpanu C., [Grúzia történelmének legnagyobb kibertámadása, amelyhez a kibertámadás kapcsolódik.](#) [a feltört web hosting szolgáltatóhoz](#), 2019. október 28.; Lindsey N., [Massive Web Defacement Attack Grúziában Újra felveti az új Politikai indítatású kibertámadások miatti aggodalmak](#), november 6. 2019,
- 110 A z [USA és Nagy-Britannia Oroszországot okolja a 2019-es grúziai kibertámadásért](#) [Weboldalak](#), 2020. február 21. RFE/RL grúziai szolgálata
- 111 [Grúziát súlyos kibertámadás érte](#). 2019. október 28., BBC
- 112 További részletek az Oroszország 2016-os amerikai beavatkozásáról [elnökválasztás](#), lásd: [Jelentés az alábbiakat vizsgáló vizsgálatról Orosz beavatkozás a 2016-os elnökválasztásba](#), Amerikai Igazságügyi Minisztérium, 2019. március.
- 113 Vilmer J.B.J. [A "#Macron szívárogtat" művelet: egy utólagos boncolás](#), The Atlantic Council, 2019. június 20.
- 114 Lilly B. [Rendet teremteni a CHAOS-on keresztül: a keretrendszer a orosz kibernézetek és dezinformáció megértése a 2020-as amerikai választások idején és azon túl](#), CyberWire, november 2, 2020
- 115 D.Tomic, M. Zivanovic. [Az orosz Fancy Bear Hacks Its Way Montenegróba](#). BIRN, 2018. március 5.
- 116 O.Jonsson. [A következő front: A Nyugat-Balkán](#), in: [Hacks, szivárgások és zavarok](#): EU ISS, 2018. október, 87. o.
- 117 D.Tomic, M. Zivanovic. [Az orosz Fancy Bear Hacks Its Way Montenegróba](#). BIRN, 2018. március 5.
- 118 D.Tomic, M. Zivanovic. [Az orosz Fancy Bear Hacks Its Way Montenegróba](#). BIRN, 2018. március 5.; O.Jonsson. [A következő](#)
- 120 További információért lásd: [Orosz narratívák a NATO-ról Telepítés](#), <https://medium.com/dfrlab/russian-narratives-on-natos-deployment-616e19c3d194> **#BalticBrief**: NATO-ellenes narratívák célpontja [Enhanced Forward Presence](#)", <https://medium.com/dfrlab/balticbrief-enhanced-anti-nato-narratives-target-enhanced-forward-presence-fdf2272a8992>
- 121 [Fenyvetéskutatás: Ghostwriter' Influence Campaign: Ismeretlen szereplők kihasználják a webhelyek kompromisszumait és Hamisított tartalmak az oroszokhoz igazodó narratívák terjesztésére Biztonsági érdekek](#), FireEye, 2020. június 29.
- 122 [A "Secondary Infekcion" műveletről további részletek találhatóak.](#) itt: <https://secondaryinfekcion.org/>
- 123 [További részletekért lásd: N. Aleksejeva. A tényellenőr személyazonossága ellopták, hogy disinfót terjesszenek a NATO-ról és a COVID-19-ről, DRF Lab. április 29, 2020](#)
- 124 Pernik Piret. [Hacking for Influence - Külföldi befolyásolás Tevékenységek és kibertámadások](#). 2018. február, ICDS Észtország, p.15
- 125 Pernik, [Hacking for Influence](#), 13. o.
- 126 J. Lewis. (2017). [Harc a rossz ellenséggel, más néven a Patthelyzet a kiberbiztonságban](#), a Cipher Brief.
- 127 Ven Bruusgaard, [Russian Strategic Deterrence \(Orosz stratégiai elrettentés\)](#), 17-18. oldal.
- 128 Pernik, [Hacking for Influence](#), 13. o. & Ministère des Armées, [Éléments publics de doctrine militaire de lutte informatique \(A katonai informatikai doktrína nyilvános elemei\)](#) TÁMADÓ.
- 129 A. Greenberg. [Az orosz hackerek rövid története hamis zászlók](#). Wired, 2019. december 21,
- 130 U.S. Cyber Command. (2018). [Achieve and Maintain Kibertéri fölény: Az amerikai kibernetikai hadsereg vezetésének jövőképe](#) Command, pp. 2-10.; Taillat S. (2019). [Jelzés, győzelem, és stratégia Franciaország katonai kiberdoktrínájában](#), War on the Sziklák.
- 131 Doffman Z. [Kiberhadviselés: Army Deploys "Social Media Warfare" Division to Fight Russia](#), Forbes. 2019. augusztus.
- 132 Kukkola J. (2020): [Digitális Szovjetunió](#).
- 133 Goebel N. [Az EU szankciókkal büntetné a kibertámadókat](#). Deutsche Welle, 2019. május 17.



Elöl: A Nyugat-Balkán, in: Hacks, leaks and disruptions:  
Oroszország kiberstratégiái, EU ISS, 2018. október, 88. o.

119 További információért lásd: [Fenyegetéskutatás: Ghostwriter'](#).

[Befolyásolási kampány: Ismeretlen színészek kihasználják a honlapot](#)

[Kompromisszumok és koholt tartalmak a narratívák terjesztése érdekében](#)

[Aligned With Russian Security Interests](#), FireEye, június 29.  
2020





Készítette és közléstesi a  
**A NATO STRATÉGIAI  
KOMMUNIKÁCIÓS KIVÁLÓSÁGI  
KÖZPONTJA**

A NATO Stratégiai Kommunikációs Kiválósági Központja (NATO StratCom COE) a NATO által akkreditált többnemzeti szervezet, amely kutatásokat végez, tanulmányokat tesz közzé, és stratégiai kommunikációs képzést nyújt kormányzati és katonai személyzet számára.

Küldetésünk, hogy pozitívan járuljunk hozzá a Szövetség stratégiai kommunikációval kapcsolatos ismereteinek bővítéséhez, és elősegítsük a pontos, megfelelő és időben történő kommunikációt a tagok között, mivel a gyorsan változó információs környezetben a célok és szerepek kialakulnak és fejlődnek.

2014 óta működünk, és jelentős kutatásokat végeztünk a NATO-országok információs környezetre vonatkozó helyzetfelismerésének javítása érdekében, valamint szakértelmünkkel hozzájárultunk a gyakorlatokhoz és képzésekhez.