Fehér András Tibor alezredes – Négyesi Imre ezredes:

A DIGITÁLIS VISSZAÉLÉSEK KATONAI VONATKOZÁSAI ÉS AZ OROSZ MODELL

DOI: 10.35926/HSZ.2023.5.1

ÖSSZEFOGLALÓ: *A tanulmány a digitális visszaélések vizsgálatára vázol fel egy, az eddigieknél komplexebb rendszert, mely a polgárok, az állam és a társadalom védelmi szempontjait egyszerre veszi figyelembe. Ennek során röviden bemutatja a nyomásgyakorlás paradigmaváltását, lehetővé téve, hogy egyaránt tekinthessünk katonai és nem katonai puha műveletekként ezekre a digitális visszásságokra. A dolgozat második felében, példaként, az orosz állam digitális védelmi modelljét ismerhetjük meg, annak túlzásaival és indokaival együtt, mely önmagában is hasznos és aktuális információkkal szolgálhat.*

KULCSSZAVAK: *mesterséges intelligencia, puha műveletek, digitális szuverenitás, digitális ökoszisztéma, Oroszország*

A SZERZŐKRŐL:

- *Fehér András Tibor alezredes, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Informatika Tanszékének tanársegéde (ORCID: 0000-0002-8060-9056)*
- *Dr. habil Négyesi Imre ezredes (PhD), a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar egyetemi docense, az Informatika Tanszék vezetője (ORCID: 0000-0003-1144-1912)*

BEVEZETÉS

A modern technológiákkal kapcsolatos elsődleges etikai kérdés, hogy élünk-e azokkal, avagy visszaélünk velük. Különösen kiélezett ez a helyzet katonai szempontból, mivel a technológiai újítások apokaliptikus méretű áldozathoz is vezethetnek. Az atomkorszak fenyegetése sem múlt el, de napjainkban az emberek inkább a mesterséges intelligencia (továbbiakban MI) által vezérelt autonóm fegyverektől, a „gyilkos robotoktól" félnek.

Ezzel szemben a valóság az, hogy a haladás által nyújtott lehetőségekkel egyelőre nem a katonai területen lehet leghatékonyabban visszaélni. A kívánt eredmények jóval optimálisabban elérhetők a mesterséges intelligenciához kapcsolódó technológiák[1] (továbbiakban MIKT) egyéb bevetési módjaival. Ezért a fejlődés jelen fázisában a rombolásra és az emberéletek kioltására irányuló klasszikus katonai módszerek alkalmazása mellett az erőérvényesítés más módjai kerülnek jobban előtérbe. Ezeknél a politikai vagy gazdasági hatalom birtokosai nem csupán a technológiai újításokat, hanem a társadalomtudományok eredményeit is bevetik. A legkorszerűbb szervezési, kommunikációs, pszichológiai, szociológiai, gazdasági módszerek legalább olyan fontosak, mint a *high-tech* eszközök. Ebben az összefonódási folyamatban

[1] Elsősorban az IoT (Internet of Things), a BigData, a számítógépek és hálózatok gyorsulása és tudásnövekedése.

a technológia és a több ezer éve ismert erőérvényesítő módszerek egymást segítik,[2] így teljesen új perspektívák nyílnak meg.

Alább olyan erőérvényesítési formákra koncentrálunk, melyeket a számítógépes hálózat és az MIKT tesznek lehetővé. Elsődleges célunk, hogy a digitális térben kibontakozó visszaélési lehetőségek elterjedt megközelítését komplexebbé tágítsuk. Így a témát a jogvédelmi nézőponton túl állambiztonsági és katonai szempontból is kezelhetőbbé tesszük. Ehhez a szakirodalom áttekintéséből és fogalmi keretekből[3] kiinduló dedukciót használunk. Eredményünk illusztrálására – aktualitása miatt – az orosz modellt választottuk; ennek bemutatása másodlagos célunk.

PARADIGMAVÁLTÁS A NYOMÁSGYAKORLÁSBAN ÉS A VIRTUÁLIS ERŐKÖZPONTOK MODELLJE

A technológia fejlődése és a hadtudomány mindig szorosan összefüggött. A digitalizáció kínálta lehetőségek azonban a korábbiaknál sokkal összetettebb paradigmaváltást hoztak az erőérvényesítésben. E változás összetevői közül szempontunkból most két dolog emelkedik ki. Az egyik, hogy az országhatárok jelentősége lecsökkent a különféle gazdasági és politikai célok egymásnak feszülése miatt, mivel az újdonságok alkalmazása egy erősen globalizált korszakot hozott. A másik, hogy a fizikai agresszió elkerülése a nyomásgyakorlásban a digitális tér segítségével a korábbinál sokkal hatékonyabban kivitelezhető.

Az utóbbihoz kapcsolódik a puha műveletek fogalma: ezek segítségével elérhetőek az adott célok jóval kevésbé feltűnően, és nulla vagy a hagyományoshoz képest kicsi erőszak (pl. információs, gazdasági, pszichológiai, jogi vagy egyéb módszerek) által.[4] Ezeket a hadtudományban együtt szokás értelmezni a kemény (fegyveres) katonai műveletekkel vagy azok lehetőségével. Eszerint az úgynevezett hibrid műveletekben[5] a kemény módszerek támogatására összehangoltan vetnek be puha műveleteket.

A puha módszereket azonban nem csupán egy katonai jellegű művelet részeként lehet használni, tehát ezeket katonai alkalmazásuktól különválasztva is érdemes vizsgálni. Ezt indokolja a hátországok eltűnésének folyamata is a mai információs, kiber- és gazdasági térben. Hiszen ezekben a terekben a civilek védelmi jelentősége is jócskán felértékelődik. Mindenki, aki ezekben a terekben dolgozik, a védelem humán erőforrásává válik. Ehhez járul továbbá az MI, amely az intelligencia mellett ma már az érzelmeket is jól képes azonosítani és utánozni.[6] Ezért a segítségével végrehajtott befolyásolás által bizonyos célok hosszú távon eredményesebben elérhetőek lehetnek, mint katonai műveletekkel. Az így fejlődő digitális

---

[2] Porkoláb Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? Hadtudomány, 2015/3–4., 36–48. http://real.mtak.hu/29824/1/2015_3_4_5.pdf (Letöltés időpontja: 2023. 05. 01.)

[3] Az ismert fogalmak rövid összefoglalása logikailag nem maradhatott ki, de terjedelmi okok miatt elhagytuk a szakirodalom alaposabb ismertetését, melynek kritikája eredetileg harmadlagos célunk is volt.

[4] Megemlítendő, hogy az itt tárgyaltak a „közepes művelet" kategóriába tartoznak egy pontosabb, de nemzetközileg nem közismert, háromszintű felosztás szerint. Lásd Resperger István: A válságkezelés és a hibrid hadviselés. Dialóg Campus Kiadó, Budapest, 2018, 23–24. https://nbi.uni-nke.hu/document/nbi-uni-nke-hu/Resperger%20Istv%C3%A1n_A%20v%C3%A1ls%C3%A1gkezel%C3%A9s%20%C3%A9s%20a%20hibrid%20hadvisel%C3%A9s.pdf (Letöltés időpontja: 2023. 05. 01.)

[5] Kiss Álmos Péter: A hibrid hadviselés természetrajza. Honvédségi Szemle, 2019/4., 18., 25. https://honvedelem.hu/images/media/5f58be696dc30542944535.pdf (Letöltés időpontja: 2023. 05. 01.)

[6] Fehér András Tibor – Négyesi Imre: A gépi érzelmek a fegyveres erőknél és az autonóm rendszerekben. Hadtudományi Szemle, 2021/3., 163–176. https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/17457/12-feher-negyes-163-176-hsz-2021-3.pdf?sequence=1&isAllowed=y (Letöltés időpontja: 2023. 05. 01.)

tér segítségével fokozatosan egyre könnyebb befolyásolni, saját érdekek felé terelni a saját állam vagy más államok polgárait, vállalatait, hivatalait. Az erőérvényesítésnek ebben az új korszakában a hagyományos katonai módszerekkel csupán a védelem egy szűkebb, fizikai szegmensét lehet biztosítani. Ez persze az állampolgárok megvédésének továbbra is alapvetően szükséges, ám már messze nem elégséges feltétele. Ezért fontos tájékozódni az erre alkalmas módszerekről, és tájékoztatni róla minden érintettet, azaz mindenkit.

A paradigmaváltás szempontunkból legfontosabb aspektusa, hogy virtuális erőközpontokban szükséges gondolkodnunk. Virtuális erőközpont lehet egy valódi, területtel rendelkező állam digitális lenyomata, de lehet területtől független tényező is. Ide sorolható egy óriásvállalat digitális ereje, ami összemérhető az államival, vagy egy független csoport, egy kis cég, mely aszimmetrikus puha műveletekkel[7] gyakorol nyomást. Úgy véljük, hogy a hatalmi struktúra ilyetén megváltozása még nem eléggé ment át a köztudatba, pedig logikusan következik a hatalom természetéből. A digitális korszak lehetőségeinek hatalmi potenciálja ugyanis éppolyan csábító, mint a történelem sok fájó emlékét okozó hatalmi mámor. A hatalomélmény örvénye a közösségi média egyszerű véleményvezéreit éppúgy húzza magába, mint a gazdasági vagy az információs hatalom birtokosait, csak az utóbbiak az amúgy is nagy hatalmukat akarják még tovább növelni. Kérdéses, hogy a virtuális tér száguldó fejlődésében képes lesz-e ezt az emberiség megfelelően kezelni és etikai szinten kompromisszumokra jutni.

Hiszen egyelőre az erőérvényesítés etikai határait még egyszerű esetekben, egyazon kultúrán belül sem vagyunk képesek egységesen kezelni, mint például a koronavírus-járvány intézkedései kapcsán. Amikor egyes cégek nem voltak hajlandók az egészségügyi szervezetek számára átadni a járvány jobb kezeléséhez szükséges adatokat, akkor voltak, akik ezeket a vállalatokat vádolták a digitális erejükkel való visszaéléssel: *„a vállalatoknak van egy magánkormánya, amely döntéseket hoz a társadalom felett, ahelyett, hogy a demokratikus kormányok hoznák meg ezeket a döntéseket."*[8] Más szerző viszont pont az állam (a regnáló kormány) túlkapásaként és a polgárok jogának megsértéseként értékeli az állam igényét az egészségügyi adatokra.[9] A konszenzus ilyen hiánya arra utal, hogy a nyugati felfogás még nem képes megfelelően lereagálni egyszerűbb információs szélsőhelyzeteket sem, a tekintélyelvű kezelés sajnos hatékonyabb.

ÉLNI ÉS VISSZAÉLNI A DIGITÁLIS TÉRBEN

Az előzőekben leírtakra alapozva tehetjük komplexebbé a digitális visszaélések elterjedt vizsgálatát. A téma több oldalról megközelíthető: egyrészt a jogérvényesítés felől (I.), e téren inkább a gazdasági szereplők és az államok érdekei és igényei érdekesek. Másrészt a jogsérelmek felől (II.), ahol emberi jogi szempontok alapján történik a vizsgálódás. Alább először vázoljuk, hogy a szakirodalom fogalmai csupán e vizsgálati módok egyikéhez kapcsolódnak, majd a két aspektust együtt tekintjük át.

---

[7] Például egy néhány fős csoport is végezhet információs műveleteket, egy apró cég digitális ereje is lehet súlyához képest óriási, egyetlen hacker is jelenthet nagy veszélyt a kibertérben.

[8] Reed Albergotti – Drew Harwell: Apple and Google are building a virus-tracking system. Health officials say it will be practically useless. The Washington Post, 15. 05. 2020. https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus (Letöltés időpontja: 2023. 01. 28.)

[9] Federico Mantellassi: Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy. Geneva Centre for Security Policy, 16. 02. 2023. https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and (Letöltés időpontja: 2023. 03. 02.)

Szuverenitás, ökoszisztéma, tekintélyelvűség a digitális térben

A jogérvényesítés (I.) oldaláról a digitális szuverenitás *(digital sovereignty)* fogalmát használják. Egyszerűen fogalmazva: a digitális térben való cselekvési és döntési képességet értik alatta. Egy 2018-as németországi IT-csúcstalálkozó meghatározása szerint: *„Egy állam vagy szervezet digitális szuverenitása abban áll, hogy a tárolt és feldolgozott adatai felett teljes körű ellenőrzése van, illetve önállóan dönt arról, hogy ki férhet hozzá."*[10] Tehát ez a digitális szuverenitás sérül, amikor valamely tényező (ebben a térben) a saját érdekeit a többi szuverenitási igény fölé sorolja, és ezt a többiekkel *szemben* valósítja meg.

Az ilyen szuverenitás egy megfelelő digitális ökoszisztéma *(digital ecosystem)* kialakítása által valósítható meg. A kifejezés jelentése, hogy aki valós gazdasági tényező, annak szükséges a digitális világban történő megjelenését is úgy szerveznie, hogy az egy elosztott, alkalmazkodó, önszerveződő, mérhető és fenntartható társadalmi-technikai rendszerként működjön.[11] Az ilyen rendszerek versenyben vannak, vagyis a többiekkel szemben előnybe jutottak azok a vállalatok – a piac „farkastörvényei" szerint –, amelyek idejében felismerték, hogy digitális potenciáljukat rendszerként szervezzék meg. Az állami rendszerek e tekintetben csupán követni tudják a piaci erőket, így evidens, hogy átveszik az ott kialakított módszereket. Sajnos Európának el kell ismernie lemaradását más államokhoz képest a digitális ökoszisztémájának tekintetében,[12] és hazánk sem élenjáró ebben, habár a probléma felszámolása folyamatban van.[13]

Rátérve a jogsérülés (II.) oldalára: ezt a kérdést a digitális tekintélyelvűség *(digital authoritarianism)* kifejezéssel közelítik – elsősorban amerikai jogvédők. Van, aki ez alatt kifejezetten a *„tekintélyelvű kormányzás fokozására vagy lehetővé tételére szolgáló technológiákat"*[14] érti, de inkább arra alkalmazzák, hogy egyes országok különféle antidemokratikus gyakorlatokat építenek ki digitális technológiák segítségével. Ez a megközelítés az állam biztonsága szempontjából abban a felismerésben válik érdekessé, hogy minden kutató igen baljósnak tartja saját (nyugati) országára nézve is egy másik állam belső (önnön polgárai ellen elkövetett) digitális visszaéléseit. A helyzet ugyanis erősen ironikus, hiszen azokat a nyugati világban kifejlesztett digitális technológiákat, melyeket az emberi szabadság virtuális kiterjesztéseként ünnepeltettek megalkotóik, a világ más részein épp az egyéni szabadság ellen használják fel és fejlesztik tovább. Így meghaladhatják a demokráciák képességeit, amelyek épp lényegük (nyitottságuk) miatt könnyebben sebezhetőek a digitális térben.[15] Ehhez adódik hozzá, hogy a túlságosan egymástól függő gazdasági és pénzügyi rendszerek és ellátási láncok nehezítik az ilyen országok elleni nemzetközi szankciókat vagy

[10] Digital Sovereignty in the Context of Platform-Based Ecosystems. The Digital Sovereignty Focus Group of the Innovative Digitisation of the Economy Platform. Bundesministerium für Wirtschaft und Energie, 2019, 6. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digital-sovereignty-in-the-context-of-platform-based-ecosystems.pdf?__blob=publicationFile&v=7 (Letöltés időpontja: 2023. 03. 02.)

[11] Nemzeti Digitalizációs Stratégia 2022–2030. Miniszterelnöki Kabinetiroda, Budapest, 2022. 12. 05., 14. https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf (Letöltés időpontja: 2023. 03. 02.)

[12] Digital Sovereignty in the Context of Platform-Based Ecosystems…: i. m.

[13] A 2022-es helyzet alapos, önkritikus és előremutató elemzését lásd a Nemzeti Digitalizációs Stratégiában.

[14] Justin Sherman: India's Digital Path: Leaning Democratic or Authoritarian? Just Security, 04. 02. 2019. https://www.justsecurity.org/62464/indias-digital-path-leaning-democratic-authoritarian/ (Letöltés időpontja: 2022. 11. 19.)

[15] Lásd a Power3.0 blogot (https://www.power3point0.org/about/), amely ennek a jelenségnek a dokumentálásával foglalkozik.

egyéb puha műveleteket. Ezek alapján reális veszély lehet, hogy egy államban zajló belső folyamatok akár át is formálhatják a fennálló labilis globális hatalmi egyensúlyt, mégpedig a demokráciák kárára.

A digitális visszaélés irányai az erőközpontmodell alapján

A II. megközelítés szakirodalma alapján a digitális visszaélés három iránya bontakozik ki:

1. állami szervek használhatják belföldön társadalmi csoportok és saját polgáraik ellen;
2. átadják (exportálják) külföldre, és ott az idegen állam az előzőekben megfogalmazottak szerint alkalmazza, ezáltal ráadásul erősödik a kötelék is ezek között az államok között;
3. állami szervek vetik be külföldön a másik állam polgárai, csoportjai, vállalatai ellen, ezeken keresztül támadva a másik államot.

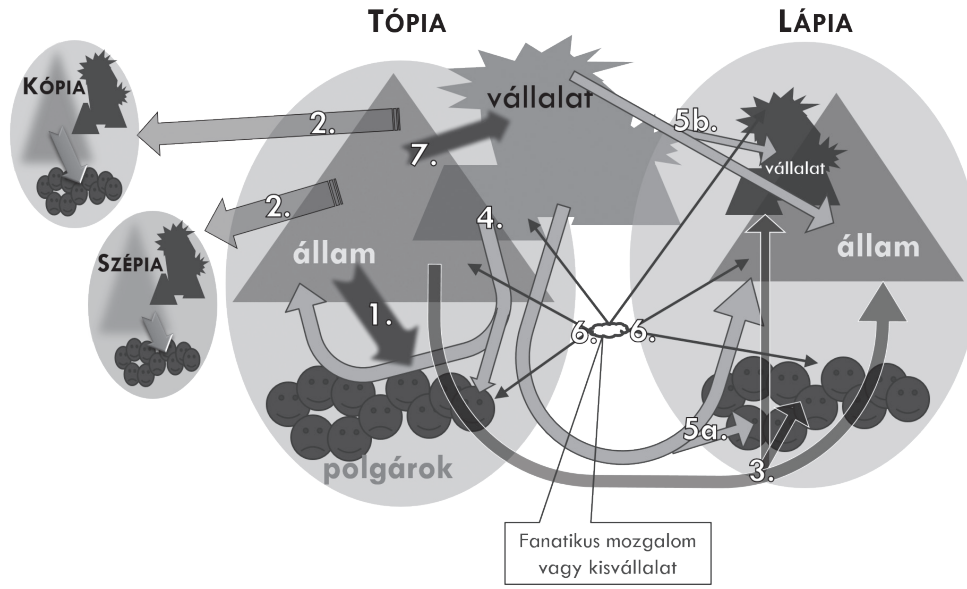
Ez a megközelítés azonban a „térugrás" módszertani hibáját követi el, mivel a virtuális tér hatásainak vizsgálatához a fizikai térben marad, és az állami erőközpontokból indul ki. Az egyik tanulmány[16] túlmegy ezen egy lépéssel, és negyedikként a vállalati szféra által használt vagy dotált technológiai visszaélést is említi – például rivális érdekcsoportok ellen –, ami szerinte demokratikus országok belügyeként kezelhető. Véleményünk szerint azonban ennek a nem állami aspektusnak precízebb kibontása szükséges, amit a korábban részletezett virtuális erőközpontok alapján tehetünk meg, amivel a „térugrási" hibát is elkerüljük. Figyelembe kell venni, hogy a „belföld" és a „külföld" térbeli keretei itt már nem mindig értelmezhetők, sőt a nemzetközi szervezetek is kihasználhatók. Így a digitális visszaélések a következő irányokkal egészülnek ki:

4. erős vállalati erők „belföldön" vetik be, mozgalmakat dotálva vagy közvetlenül;
5. erős vállalati erők „külföldön" az adott ország sajátosságainak megfelelően vetik be;
6. független kis csoportok vetik be, általában aszimmetrikus műveletként;
7. állami szervek saját vagy globális vállalat(ok) ellen vetik be;
8. (+ a nemzetközi szervezeteken keresztül gyakorolt nyomás lehetősége).

Szemléltetésül a 8. oldalon látható 1. ábrán két elképzelt állam segítségével mutatjuk be az állami és a nem állami virtuális erőközpontok digitális visszaéléseinek lehetséges irányait (típusait).

Látható, hogy Tópia exportálja a technológiákat (2), beveti saját polgárai ellen (1), és Lápia ellen is alkalmazza (3) mind polgárain keresztül, mind közvetlenebb módokon a másik állam vagy annak vállalatai ellen. A vállalati erő Lápia állami hivatalai ellen akár annak polgárain (5a.) vagy vállalatain (5b.) keresztül is követhet el digitális visszaélést, továbbá „saját" állama és a tópiai polgárok ellen is (4). Jelöltük még a (fanatikus) független mozgalmak, illetve agresszív kisvállalatok aszimmetrikus műveleteit (6), valamint az állam vállalatokra gyakorolt nyomását (7). Az áttekinthetőség érdekében el kellett hagynunk mindezek ellenirányait (természetesen a valós helyzet vektorai minden erőközponttól mind felé mutathatnak). Az irányokra az arab számokkal hivatkozunk.

[16] Erol Yayboke – Sam Brannen: Promote and Build: A Strategic Approach to Digital Authoritarianism. Center for Strategic and International Studies (CSIS), 10. 2020., 2. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201015_Yayboke_Brannen_PromoteAndBuild_Brief.pdf (Letöltés időpontja: 2022. 11. 18.)



1. ábra *A digitális visszaélések főbb irányai (Szerkesztették a szerzők)*

AZ OROSZ MODELL ELEMZÉSE

Példaként a fenti irányokra az orosz digitális visszaélési modell néhány fontos jellemzőjét vázoljuk, mely – a kínai modell mellett – a digitális tekintélyelvűség szakirodalmának egyik fő kutatási területe. A kínai és az orosz modellek közötti egyezés, hogy egyik sem a nyugati liberális demokrácia elvei szerint használja a digitális lehetőségeket, és mindkettő exportálja az elért eredményeket (2-es irány). (Robert Morgus a posztszovjet országokon kívül a világ 26 országát említi.[17]) Az eltérés azonban jelentős. Míg a kínai egy impozáns, de költséges technológia, mely egy totális kontroll irányába fejleszt, addig az orosz modell inkább azokra a területekre koncentrál, amelyek olcsóbban biztosítanak digitáliskontroll- és befolyásolási lehetőségeket.[18]

Az orosz állami mesterséges intelligencia helyzete

A puha technológiák jövője, az MIKT lenne a legjobb az orosz modell bemutatására, ám itt csak az MI helyzetének vázolására van hely. Putyin elnök 2017-ben kijelentette, hogy az lesz a világ ura, aki az MI-szférában átveszi a vezetést,[19] ugyanakkor azt is mondta, hogy jobb

[17] Robert Morgus: The Spread of Russia's Digital Authoritarianism. Artificial Intelligence, China, Russia, and the Global Order. Air University Press, 2019, 95. https://www.jstor.org/stable/resrep19585.17 (Letöltés időpontja: 2023. 03. 17.)

[18] Chris Meserole – Alina Polyakova: Exporting Digital Authoritarianism – The Russian and Chinese Models. Brookings, 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf (Letöltés időpontja: 2022. 11. 18.)

[19] Radina Gigova: Who Vladimir Putin thinks will rule the world. CNN, 02. 09. 2017. https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html (Letöltés időpontja: 2022. 11. 22.)

lenne megakadályozni, hogy valaki rátegye a kezét ennek monopóliumára. Az utóbbit elérni – a drága világelsőség helyett – a modellbe illik: ehhez elég például a vezető szerep megszerzése[20] az UNESCO MI Etikai Bizottságában.

A technológiai hátrányt azonban nem lehet csupán politikai súllyal kompenzálni, ezért az oroszok már igen régen próbálnak a világpiacon MI-termékekkel is megjelenni.[21] A világelsőségtől távol vannak, de számos eredményről olvashatunk.[22] Bár folyamatosan emelkedik a szféra támogatása, még messze elmaradnak a kínai MI szintjétől. Kevés a kimagasló teljesítményű MI-alkalmazás (bár akad[23]), és úgy tűnik, tudományos áttörésekre nincs erejük. Ám az orosz digitális visszaélési modellhez ez is megfelel. Ezt mutatják a belföldi (1-es irány) példák a Navalnij ellenzéki képviselő pártján tüntetők azonosításától a hadkötelességet elkerülők begyűjtéséig.[24] A modell tehát működik az orosz fővárosnak és Szentpétervárnak a kínainál jóval kisebb IoT-kamerás lefedettsége mellett is.[25] Sőt felzárkózóban van olyan újabb alkalmazások által, mint a 2023 februárjában bemutatott Oculus,[26] mely az MI segítségével keresi meg a neten a törvénybe ütköző tartalmakat vagy titkosításokat.

A harci alkalmazásokban nem ez a helyzet. Nyugati elemzők szerint az ukrán invázióban olyan kézenfekvő területeken sem látható az MI használatának látványos eredménye, mint a puha (pl. információs) műveletek és a katonai döntések támogatása.[27] Kérdéses továbbá, hogy az MI technológiai fejlesztések jelenleg tervezett rohamos ütemét képesek lesznek-e tartani a beszerzéseket sújtó szankciók és az agyelszívás mellett. Szkeptikusok a kutatók azzal kapcsolatban is, hogy a háború ellenére sikerül-e biztosítani a korábbi óriási állami forrásokat, illetve jól felhasználni azokat, hiszen a nagy fejlesztések eredményességét sem az államilag támogatott vállalatok, sem pedig az akadémiai kutatások nem képesek szerintük garantálni – ezért olyan kevés a szabadalmak száma.[28] A szkepszis ellenére azonban sikeresen

[20] Az Oroszországi Föderáció UNESCO Bizottsága keretében hozták létre a Mesterséges Intelligencia Etikai Bizottságát tanácsadó testületként 2020-ban. Konstantin Emelin: Artificial Intelligence Is Under Control. UNESCO, 10. 04. 2020. http://unesco.ru/en/news/ai-committee (Letöltés időpontja: 2023. 03. 29.)

[21] A digitális visszaélésre alkalmas MI-technológiákat már 10 éve is exportálták nyugatra. Lásd Andrei Soldatov – Irina Borogan: 5 Russian-Made Surveillance Technologies Used in the West. Wired, 10. 05. 2013. https://www.wired.com/2013/05/russian-surveillance-technologies (Letöltés időpontja: 2023. 03. 17.)

[22] Artificial intelligence and autonomy in Russia. Center for Naval Analyses, 08. 09. 2022. https://www.cna.org/our-media/newsletters/ai-and-autonomy-in-russia (Letöltés időpontja: 2023. 01. 18.)

[23] Robo-C2. Promobot. https://promo-bot.ai/robots/robo-c/ (Letöltés időpontja: 2023. 03. 17.)

[24] Андрей Захаров: Злость, страх и силуэты. Мэрия Москвы раскрыла, какие алгоритмы распознают людей по лицам. BBC News Русская служба, 25. 08. 2022. https://www.bbc.com/russian/features-62658404 (Letöltés időpontja: 2022. 11. 27.)

[25] Moszkvában 213 ezer körül van a számuk, Szentpéterváron ezer főre 12,7 felderítőeszköz jut. Number of surveillance cameras installed in Moscow and Saint Petersburg in Russia from 2021 to 2022. Statista. https://www.statista.com/statistics/1156026/surveillance-cameras-density-moscow-st-petersburg (Letöltés időpontja: 2022. 11. 27.)

[26] В РФ запущена система автоматического поиска запрещенного контента „Окулус". Interfax, 13. 02. 2023. https://www.interfax.ru/russia/885877 (Letöltés időpontja: 2023. 03. 12.)

[27] Samuel Bendett: Russia's Artificial Intelligence Boom May Not Survive the War. Defense One, 15. 04. 2022. https://www.defenseone.com/ideas/2022/04/russias-artificial-intelligence-boom-may-not-survive-war/365743 (Letöltés időpontja: 2022. 11. 19.)

[28] Samuel Bendett: Russia's AI Quest Is State-Driven – Even More than China's. Can It Work? Defense One, 25. 11. 2019. https://www.defenseone.com/ideas/2019/11/russias-ai-quest-state-driven-even-more-chinas-can-it-work/161519 (Letöltés időpontja: 2022. 11. 19.)

alkalmazzák az MI-t például KUB–BLA felderítő harci drónokban.[29] Tehát az orosz MI egyelőre nem jelentős, de nem is lebecsülendő.

Az orosz intranet

A digitális tekintélyelvűség szakirodalmában aránytalan hangsúlyt kap az internet lekapcsolására irányuló törekvés, így kénytelenek vagyunk alaposabban kitérni rá, mivel ezt a beállítást félrevezetőnek tartjuk. Tény, hogy 2021-ben egy időre lekapcsolták a Runet orosz hálózatot,[30] és már 2019-től folynak erre irányuló, hivatalosan elismert tesztek.[31] Ez a törekvés éveken át csak erőlködés volt: például ha valamit tiltottak, akkor más sem működött.[32] Mára azonban egyre több oldal vagy szolgáltatás tiltása sikeres, tehát a korábbinál nehezebb megkerülni az orosz állami akaratot mind törvényileg, mind technikailag.

Ám véleményünk szerint helytelen ezek alapján az ország digitális leválasztására koncentrálni. Sokkal logikusabbnak tűnnek az olyan megfogalmazások, melyek szerint a vezetés az ország digitális szuverenitását egy orosz intranet megvalósításában látja, melyben az ország a világháló egészéhez csak a felügyelt átjárókon keresztül kapcsolódik. Szemléletesebb a digitális vasfüggöny[33] elnevezés, melynek üzemeltetése nem okoz gazdasági sokkot. Érdekesség, hogy a „lekapcsolásból" adódó gazdasági károk szakirodalma igen ellentmondásos (talán része lett az információs műveleteknek). Becslések szerint egy 2022-es internetleállás kára egy nap alatt 442 millió dollár volt,[34] más forrás szerint összesen 861 millió dollárt vesztett az orosz állam a leállítások miatt 2022 első három hónapjában.[35] Annyi biztos, hogy hivatalos nyilatkozatok szerint nincs meg az ország internet nélkül.[36] Tehát valószínűsíthető, hogy kerülik az ilyen áldozatos védelmet.

---

[29] Donatas Palavenis: The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War. Air Land Sea Space Application (ALSSA) Center, 01. 10. 2022, 3. https://www.alsa.mil/Portals/9/Documents/articles/221001_ALSA_Article_Donatas_Palavenis.pdf (Letöltés időpontja: 2023. 03. 29.)

[30] В России протестировали работу Рунета при отключении от глобальной Сети. РБК, 21. 07. 2021. https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739 (Letöltés időpontja: 2022. 11. 26.)

[31] Российский рунет выдержал первые испытания. Pravda.ru, 23. 12. 2019. https://www.pravda.ru/news/politics/1461663-runet (Letöltés időpontja: 2022. 11. 26.)

[32] Például a Twitter tiltásának egyik próbája az egész internetet lelassította. Lásd Russia Slows down Twitter over „Banned Content". BBC News, 10. 03. 2021. https://www.bbc.com/news/world-europe-56344304 (Letöltés időpontja: 2022. 11. 19.)

[33] Más neveken „szilíciumfüggöny", „internetes vasfüggöny". Lásd Janus Rose: Russia's Digital Iron Curtain Is Starting To Take Shape. Vice, 17. 03. 2022. https://www.vice.com/en/article/5dg4kb/russias-digital-iron-curtain-is-starting-to-take-shape (Letöltés időpontja: 2022. 11. 26.)

[34] Elina Sinkkonen – Jussi Lassila: Digital Authoritarianism and Technological Cooperation in Sino-Russian Relations: Common Goals and Diverging Standpoints. In: Sarah Kirchberger et al. (eds): Russia-China Relations: Emerging Alliance or Eternal Rivals? Global Power Shift Cham: Springer International Publishing, 169. https://link.springer.com/content/pdf/10.1007/978-3-030-97012-3_9?pdf=chapter%20toc (Letöltés időpontja: 2023. 05. 02.)

[35] Jason Lalljee: Russia's economy already lost $860 million this year because the government keeps shutting down the internet. Business Insider, 19. 03. 2022. https://www.businessinsider.com/russia-internet-censorship-cost-economy-putin-ukraine-sanctions-twitter-2022-3 (Letöltés időpontja: 2023. 03. 22.) Megjegyzendő, hogy a forrás a NetBlocks nevű angol csoportra hivatkozik, ám a csoport weboldalán a cikkek megjelenése körül nem található ilyen kalkuláció. A túlzó számot mégis több portál átvette.

[36] A TASZSZ hírügynökség Lavrov külügyminisztert idézi. Russia won't be left without Internet, guarantees Lavrov. TASS, 17. 05. 2022. https://tass.com/politics/1452143 (Letöltés időpontja: 2022. 11. 26.)

Az a tendencia tehát, hogy a *kézben tartottság* legyen a vezérelv. Ez a digitális leválasztást csak vészhelyzetekre tartogatja, akárcsak a hibrid hadviselési szemlélet a kemény műveleteket. A kézben tartottság által a megszerzett adatok elemzése sajnos a polgárokról történő adatgyűjtésre is alkalmas, illetve újabb és újabb tartalmak, tartalomtípusok szűréséhez (1-es irány) vezetett. Az ilyen tárgyú törvények egyre több olyan weboldal és szolgáltatás ellen tesznek lehetővé jogi fellépést, melyek a hivatalos álláspontól eltérnek.[37] Sorra szankciók vagy letiltás alá kerülnek (7-es irány) azok a szolgáltatók, amelyek nem tesznek eleget a törvénynek, és nem engedélyezett hírek vagy ellenőrizetlen tartalmak lehetőségét nyújtják. Egy ideig a lakosság virtuális magánhálózatok (VPN[38]) használatával kerülte ki a megfigyelést és a korlátozást. Ám 2021-től letiltották azokat a VPN-vonalakat is, melyek üzemeltetői nem voltak hajlandók összekapcsolni szolgáltatásaikat az FGIS-adatbázissal.[39]

A visszaélések mellett szükséges rámutatni, hogy mindebben egy digitális szuverenitási igény is összecsap különféle érdekeknek a térségre kényszerítésével. Ebben a felek saját digitális erejükkel igyekeznek nyomást gyakorolni az orosz lakosokra, akiknek így valódi szabadsága nemigen marad. A szuverenitási igény nyilván a külföldi szerverektől és szolgáltatásoktól való teljes függetlenséget is célozza, mint azt például a saját, orosz biztonsági tanúsítvány bevezetésére[40] vagy a szoftverek függetlenítésére[41] irányuló törekvések példái mutatják.

A külső nyomásgyakorlás hátulütője, hogy a belső visszaéléseknél kihasználható: megideologizálhatóak a törvények, ha „ezek a külföldi ügynökök ellen" szólnak. A politikainál tanulságosabb példákat láthatunk erre a vállalati szférában, hiszen az ország ilyen nem állami szereplőkkel is évek óta harcban áll (5-ös és 6-os irány). Most pedig – az Ukrajna elleni kemény műveletekre reagálva – a vállalatok beleálltak a harci helyzetbe. Például a Meta vállalat úgy enyhítette az „erőszakos fenyegetések" szabályait, hogy az orosz megszállók halálát kívánni már nem jár büntetéssel,[42] a Microsoft pedig nem enged hozzáférést a szervereihez.[43]Az ilyen puha műveletek azonban csak a nyugati hírekben hangoznak jól, Oroszországban az állami kommunikációnak adnak muníciót. Hasonlóképp egyes cégek szankcionális kivonulása is kedvezhet az orosz vezetésnek. Például az Instagram távozása után bejelentették annak orosz alternatíváját, a Rosgramot,[44] melynek így önként adták át a piacot és ezzel együtt

[37] A Freedom House civil szervezet jelentéses példát hoz különböző visszaélésekre. Freedom on the Net 2022 – Russia. Freedom House. https://freedomhouse.org/country/russia/freedom-net/2022 (Letöltés időpontja: 2022. 11. 26.)

[38] Virtual Private Network – ehhez csatlakozva elrejthetők azok a digitális adatok, melyekkel egy szolgáltatás használója beazonosítható.

[39] Federal Government Information System – állami ellenőrzés alá vonja a VPN-identitást és -adatforgalmat is.

[40] Bill Toulas: Russia creates its own TLS certificate authority to bypass sanctions. Bleeping Computer, 10. 03. 2022. https://www.bleepingcomputer.com/news/security/russia-creates-its-own-tls-certificate-authority-to-bypass-sanctions (Letöltés időpontja: 2022. 11. 26.)

[41] Még az MS Windowst is cserélik. Lásd Thomas Claburn: Russia bans foreign software purchases for critical infrastructure. The Register, 01. 04. 2022. https://www.theregister.com/2022/04/01/russia_bans_foreign_software (Letöltés időpontja: 2023. 03. 17.)

[42] Rose: i. m.

[43] Matthew Hughes: Microsoft stops serving Windows downloads to Russian users. KnowTechie, 21. 06. 2022. https://knowtechie.com/microsoft-stops-serving-windows-downloads-to-russian-users (Letöltés időpontja: 2023. 03. 17.)

[44] Laura Howells – Laura A. Henry: Digital Authoritarianism at War: Controlling Russia's Information Space. NYU Jordan Center, 26. 04. 2022. https://jordanrussiacenter.org/news/digital-authoritarianism-at-war-controlling-russias-information-space/ (Letöltés időpontja: 2022. 11. 27.)

az informálás lehetőségét. Sokkal hatékonyabb az a módszer (pl. a Twitter, a Facebook és a BBC alkalmazta), mely az orosz közönség számára szolgáltatásából egy, a Tor böngészőn keresztül (inkognitóban) elérhető verziót készített el.[45]

Ezzel igen érdekes új mozzanatra világíthatunk rá a hibrid erőérvényesítésben: a kissé alvilági, korábban kétes ügyletekre használt *„dark web"* válik az információs műveletek hivatalos küzdőterévé. Oroszország a maga részéről pedig legalizálta a szoftverkalózkodást a Microsoft fent említett tiltása miatt. Szerintünk ehhez adódhat idővel a digitális valuták legalizálódása a nem hivatalos hibrid műveletek támogatásához, és az internetszabadság etikai paradoxonokba fulladhat.

Az orosz modell kialakulása, jellemzői és a szuverenitás esélye

A helyzetképek után kis oknyomozó történelem. Az orosz modell alapját az képezi, hogy az internet évtizedeken át tudott terjedni – nem úgy, mint Kínában. Csak 1998-ban kezdődött meg a telekommunikáció korlátozására használt technológiák számítógépes hálózatokra adaptálása.[46] Ráadásul a cégek sokáig kijátszották, illetve bojkottálták ezeket a rendelkezéseket,[47] így a korlátozások lényegében 2012-ig sikertelenek voltak. Ezért maradt az orosz polgárok digitális szabadsága sokáig egy élhetőbb szinten. A késlekedés fő oka, hogy a szovjet birodalom széthullása miatt sokáig erőtlen volt a központi szervezet, ami szükséges lett volna a technológiai fejlődés állami kontrollálásához. Ehhez járult az ellenőrzéshez szükséges apparátus múltban ragadt szemlélete, mely csak a fizikai kényszerítés terén mozgott otthonosan, és nem látta meg a digitális tér jelentőségét. Sőt úgy tűnik, máig sem képes igazán kihasználni a kiberteret.[48] Ezek az emberi okok állnak a modell mögött. A késés miatt az orosz emberek megszokták és megszerették a világháló által nyújtott szabadságot és szolgáltatásokat. Így most (az utóbbi 10 évben) sokkal több társadalmi feszültséggel jár az a folyamat, amelyben a hatalom el kívánja venni az emberektől, amit használtak és szerettek, ez kedvez az ellenséges (nyugati) akaratnak.

A már idézett művek alapján négy egyéb tényezőt is kiemelünk. A *kommunikációs függőségből* (1) kifolyólag az orosz gazdaság erősen ráépült a nyílt internetre, hiszen részévé vált a multinacionális gazdaságnak. A *gazdaság erőtlensége* (2) miatt az ország az elmúlt években nemcsak az MI-hez kapcsolódó technológiákban nem volt képes még önállóvá válni, hanem saját „Szilícium-völgyük" vagy operációs rendszerük sincs – hiába próbál erőn felül részt venni a modern technológiák terjesztésében és saját termékek fejlesztésében. Ez a *gazdasági függőség* (3) magával hozta, hogy a működésbiztonság érdekében érdemesebb volt teljes, kiforrott technológiákat megvenni külföldről. Ezt próbálja a Nyugat a jelen konfliktusban a szankciók révén kiaknázni. De emiatt okoz gondot a nagyon modern eszközök és a jóval lassabban fejlődő orosz rendszerek *inkompatibilitása*[49] (4) is. Érdemes lenne ezeket a tényezőket saját régiónk szempontjából is megvizsgálni.

---

[45] Luke Harding: Twitter launches privacy-protected site on dark web to bypass Russia's block. The Guardian, 10. 03. 2022. https://www.theguardian.com/technology/2022/mar/09/twitter-tor-version-russia-block (Letöltés időpontja: 2022. 11. 18.)

[46] 2000-től kezdődött a korlátozások törvényi megalapozása. Lásd Meserole–Polyakova: i. m. 2.

[47] Sinkkonen–Lassila: i. m. 170.

[48] Mivel központi kiberparancsnokság sincs. Lásd Soldatov–Borogan: i. m. 30.

[49] Sinkkonen–Lassila: i. m. 169. Megjegyzendő, hogy erre a kínai beszállítókra való áttérés sem megoldás, az más illesztési problémákat vetne fel.

ÖSSZEFOGLALÁS ÉS KÖVETKEZTETÉSEK

Az előzőekben leírtak alapján megállapítható, hogy a digitális visszaélések orosz modellje működőképes. Bár a teljes digitális szuverenitás kialakításához kevés, mégis világszerte keresettek a megoldásai. A példa rávilágít a tanulmány azon megállapítására, hogy a puha módszerek nem csupán a katonai hibrid műveletek részeiként értelmezendők. Mint rámutattunk, az érintett terek civil dolgozói is a védelem humán erőforrásává válnak. Ezért vezettük be a virtuális erőközpontok modelljét, melyek nyomásgyakorlási vektorainak elemzésével megragadhatóvá próbáltuk tenni azt a bonyolult erőérvényesítési mátrixot, melynek minden ország – így hazánk is – részese. Így lehetett vázolni a digitális visszaélések többszempontú vizsgálatának módszerét, melyben személyiségjogi szempontok együtt kezelendők az állam és a társadalom érdekeivel. (A vállalati szféra szempontjainak kibontására nem volt mód, csupán felvetettük a puha és a közepes műveletek nem állami vektorait.)

Ezzel a megközelítéssel lehet esély arra, hogy a digitális szuverenitás elérhessen egy elégséges nívót az egyéni, a csoport-, a vállalati, a társadalmi és az állami szintek mindegyikén. Ehhez nyilván minden szintnek és tényezőnek kompromisszumokkal kell hozzájárulnia. Sőt megegyezésre kell jutni például olyan álláspontok tekintetében is, hogy hol vannak az erőérvényesítés etikai határai – nem úgy, mint a bemutatott pandémiás eset kapcsán. Szükséges lenne a globális biológiai ökoszisztémához hasonlóan a globális digitális ökoszisztémát is élhetővé tenni, bár erre jelen pillanatban kevés az esély, hiszen mint láthattuk, inkább a *dark web* emelkedik hivatalos küzdőtérré.

Végül a most folyó háborúhoz vezető újabb tényezőre is akadunk a leírtakat továbbgondolva. Régóta világosak az orosz célok, melyek felé tavalyig puha módszerekkel haladtak, sokunk az ilyenfajta erőérvényesítés folytatására számított. *A vezetésnek azonban szembesülnie kellett a puha műveleteik csődjével.* Hiszen mint láthattuk, az orosz cégek a világpiacon eltörpülnek, és nagyon lemaradtak a közösségi média terén, vagyis csekély az információformáló vagy gazdasági nyomásgyakorló erejük. Még országon belül sem sikerült teljesen a felügyelt intranet megvalósítása, így a saját lakosság véleményformálása sem volt a kívánt mértékű, nemhogy a világ közvéleményéé. A puha műveletek e csődjét nem okként említjük, csupán tényezőként, mely arra figyelmeztet, hogy a kemény műveletek kora nem ért véget a hibrid háborúk korában sem.

FELHASZNÁLT IRODALOM

- Albergotti, Reed – Harwell, Drew: *Apple and Google are building a virus-tracking system. Health officials say it will be practically useless.* The Washington Post, 15. 05. 2020. https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus
- Artificial intelligence and autonomy in Russia. Center for Naval Analyses, 08. 09. 2022. https://www.cna.org/our-media/newsletters/ai-and-autonomy-in-russia
- Bendett, Samuel: *Russia's AI Quest Is State-Driven – Even More than China's. Can It Work?* Defense One, 25. 11. 2019. https://www.defenseone.com/ideas/2019/11/russias-ai-quest-state-driven-even-more-chinas-can-it-work/161519
- Bendett, Samuel: *Russia's Artificial Intelligence Boom May Not Survive the War.* Defense One, 15. 04. 2022. https://www.defenseone.com/ideas/2022/04/russias-artificial-intelligence-boom-may-not-survive-war/365743
- Claburn, Thomas: *Russia bans foreign software purchases for critical infrastructure.* The Register, 01. 04. 2022. https://www.theregister.com/2022/04/01/russia_bans_foreign_software

- Digital Sovereignty in the Context of Platform-Based Ecosystems. The Digital Sovereignty Focus Group of the Innovative Digitisation of the Economy Platform. Bundesministerium für Wirtschaft und Energie, 2019. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digital-sovereignty-in-the-context-of-platform-based-ecosystems.pdf?__blob=publicationFile&v=7
- Emelin, Konstantin: *Artificial Intelligence Is Under Control*. UNESCO, 10. 04. 2020. http://unesco.ru/en/news/ai-committee
- Fehér András Tibor – Négyesi Imre: *A gépi érzelmek a fegyveres erőknél és az autonóm rendszerekben.* Hadtudományi Szemle, 2021/3., 163–176. https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/17457/12-feher-negyes-163-176-hsz-2021-3.pdf?sequence=1&isAllowed=y; DOI: 10.32563/hsz.2021.3.12
- Freedom on the Net 2022 – Russia. Freedom House. https://freedomhouse.org/country/russia/freedom-net/2022
- Gigova, Radina: *Who Vladimir Putin thinks will rule the world*. CNN, 02. 09. 2017. https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html
- Harding, Luke: *Twitter launches privacy-protected site on dark web to bypass Russia's block*. The Guardian, 10. 03. 2022. https://www.theguardian.com/technology/2022/mar/09/twitter-tor-version-russia-block
- Howells, Laura – Henry, Laura A.: *Digital Authoritarianism at War: Controlling Russia's Information Space*. NYU Jordan Center, 26. 04. 2022. https://jordanrussiacenter.org/news/digital-authoritarianism-at-war-controlling-russias-information-space/
- Hughes, Matthew: *Microsoft stops serving Windows downloads to Russian users*. KnowTechie, 21. 06. 2022. https://knowtechie.com/microsoft-stops-serving-windows-downloads-to-russian-users
- Kiss Álmos Péter: *A hibrid hadviselés természetrajza*. Honvédségi Szemle, 2019/4., 17–37. https://honvedelem.hu/images/media/5f58be696dc30542944535.pdf
- Lalljee, Jason: *Russia's economy already lost $860 million this year because the government keeps shutting down the internet*. Business Insider, 19. 03. 2022. https://www.businessinsider.com/russia-internet-censorship-cost-economy-putin-ukraine-sanctions-twitter-2022-3
- Mantellassi, Federico: *Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy.* Geneva Centre for Security Policy, 16. 02. 2023. https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and
- Meserole, Chris – Polyakova, Alina: *Exporting Digital Authoritarianism – The Russian and Chinese Models*. Brookings, 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf
- Morgus, Robert: *The Spread of Russia's Digital Authoritarianism. Artificial Intelligence, China, Russia, and the Global Order.* Air University Press, 2019, 89–87. https://www.jstor.org/stable/resrep19585.17
- Nemzeti Digitalizációs Stratégia, 2022–2030. Miniszterelnöki Kabinetiroda, Budapest, 2022. 12. 05. https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf
- Number of surveillance cameras installed in Moscow and Saint Petersburg in Russia from 2021 to 2022. Statista. https://www.statista.com/statistics/1156026/surveillance-cameras-density-moscow-st-petersburg
- Palavenis, Donatas: *The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War.* Air Land Sea Space Application (ALSSA) Center, 01. 10. 2022. https://www.alsa.mil/Portals/9/Documents/articles/221001_ALSA_Article_Donatas_Palavenis.pdf
- Porkoláb Imre: *Hibrid hadviselés: új hadviselési forma, vagy régi ismerős?* Hadtudomány, 2015/3–4., 36–48. http://real.mtak.hu/29824/1/2015_3_4_5.pdf; DOI: 10.17047/HADTUD.2015.25.3-4.36
- Power3.0 blog. https://www.power3point0.org/about/

- Resperger István: *A válságkezelés és a hibrid hadviselés*. Dialóg Campus Kiadó, Budapest, 2018. https://nbi.uni-nke.hu/document/nbi-uni-nke-hu/Resperger%20Istv%C3%A1n_A%20v%C3%A1ls%C3%A1gkezel%C3%A9s%20%C3%A9s%20a%20hibrid%20hadvisel%C3%A9s.pdf
- Robo-C2. Promobot. https://promo-bot.ai/robots/robo-c/
- Rose, Janus: *Russia's Digital Iron Curtain Is Starting To Take Shape*. Vice, 17. 03. 2022. https://www.vice.com/en/article/5dg4kb/russias-digital-iron-curtain-is-starting-to-take-shape
- Russia Slows down Twitter over „Banned Content". BBC News, 10. 03. 2021. https://www.bbc.com/news/world-europe-56344304
- Russia won't be left without Internet, guarantees Lavrov. TASS, 17. 05. 2022. https://tass.com/politics/1452143
- Sherman, Justin: *India's Digital Path: Leaning Democratic or Authoritarian?* Just Security, 04. 02. 2019. https://www.justsecurity.org/62464/indias-digital-path-leaning-democratic-authoritarian/
- Sinkkonen, Elina – Lassila, Jussi: *Digital Authoritarianism and Technological Cooperation in Sino-Russian Relations: Common Goals and Diverging Standpoints.* In: Kirchberger, Sarah – Sinjen, Svenja – Wörmer, Nils (eds): Russia-China Relations: Emerging Alliance or Eternal Rivals? Global Power Shift Cham: Springer International Publishing, 165–184. https://link.springer.com/content/pdf/10.1007/978-3-030-97012-3_9?pdf=chapter%20toc; DOI: 10.1007/978-3-030-97012-3_9
- Soldatov, Andrei – Borogan, Irina: *5 Russian-Made Surveillance Technologies Used in the West*. Wired, 10. 05. 2013. https://www.wired.com/2013/05/russian-surveillance-technologies
- Toulas, Bill: *Russia creates its own TLS certificate authority to bypass sanctions*. Bleeping Computer, 10. 03. 2022. https://www.bleepingcomputer.com/news/security/russia-creates-its-own-tls-certificate-authority-to-bypass-sanctions
- Yayboke, Erol – Brannen, Sam: *Promote and Build: A Strategic Approach to Digital Authoritarianism*. Center for Strategic and International Studies (CSIS), 10. 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201015_Yayboke_Brannen_PromoteAndBuild_Brief.pdf
- В России протестировали работу Рунета при отключении от глобальной Сети. РБК, 21. 07. 2021. https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739
- В РФ запущена система автоматического поиска запрещенного контента „Окулус". Interfax, 13. 02. 2023. https://www.interfax.ru/russia/885877
- Захаров, Андрей: *Злость, страх и силуэты. Мэрия Москвы раскрыла, какие алгоритмы распознают людей по лицам.* BBC News Русская служба, 25. 08. 2022. https://www.bbc.com/russian/features-62658404
- Российский рунет выдержал первые испытания. Pravda.ru, 23. 12. 2019. https://www.pravda.ru/news/politics/1461663-runet