Kelemen Roland

Cyberfare State – egy hibrid állammodell 21. századi születése

Military and Intelligence CyberSecurity Research Paper
2022/1.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Jelen tanulmányban a szerző a digitalizáció államra gyakorolt jelentős hatását kívánja bemutatni. Ennek során kitér a digitalizáció pozitív hatásaira, így főként a jóléti rendszerek jelentős reformjára, illetve többek között az IoT, az okoseszközök jelentőségére. Emellett az ezekből fakadó negatívumok védelem és biztonságra gyakorolt következményeit is feltárja. Ennek során megállapítja, hogy a fentiek okán, egy új típusú államodell a cyberfare state született. E cyberfare state külön almodellje jött létre a transzatlanti térség államaiban, valamint főként az eurázsiai térség keleti országaiban.

Kulcsszavak: welfare state, warfare state, totális biztonság, cyberfare state

In this paper, the author aims to demonstrate the significant impact of digitalisation on the state. In doing so, he will highlight the positive effects of digitalisation, in particular the significant reform of welfare systems and the importance of IoT and smart devices, among others. He will also explore the implications of the negative consequences for security and defence. In doing so, he concludes that, for the above reasons, a new type of state model of cyberfare state has been born. A separate sub-model of this cyberfare state has emerged in the states of the transatlantic region and in the countries of the East Eurasian region.

Keywords: welfare state, warfare state, total security, cyberfare state

BEVEZETÉS[1]

Gregory M. Kaladijan 1996-os Journal of Children and Poverty-ben megjelent Welfare vs. Cyberfare című cikkében arra vállalkozott, hogy a welfare state (jóléti állam) reformjának szükségét felvázolja. A tanulmányban az elektronikus rendszerek szociális igazgatásban történő felhasználása mellett érvelt, melyek a már működő szociális struktúrát véleménye szerint átláthatóbbá és igazságosabbá, a rendszer működését pedig ezáltal eredményesebbé tették volna.[2]

Kaladijan a kibertér fejlődésének egy korai időszakában ismerte fel annak államigazgatást, állami alrendszereket, az állami funkciókat hatékonyabbá tevő képességét, igaz, ő csak egy területre, a szociális igazgatásra és annak hosszú ideje visszásan működő rendszerének megújítására látott benne fantáziát. Szavai azonban akkor – valószínűsíthetően a fókuszált terület társadalmi érzékenysége és a kibertér fejlődésének korai szakasza okán – lényegi változást nem eredményeztek, az általa bevezetett cyberfare fogalom sem ült át a tudományos gondolkodás mainstream vonalába. Mára viszont az államigazgatás teljes rendszere,

[1] Tanulmány véglegesítésében nyújtott segítségüket, javaslataikat köszönöm Farkas Ádámnak, Németh Richárdnak, Pongrácz Alexnek, Szépvölgyi Enikőnek és Vikman Lászlónak.

[2] Tanulmányát lásd: Gregory M. KALADIJAN: *Welfare vs Cyberfare*. In Journal of Children and Proverty, 1996/1. szám, 93-104. o.

így vagy úgy, de megjelent a kibertérben, a gazdasági szereplők tevékenysége elképzelhetetlen a virtuális tér nyújtotta lehetőségek nélkül, az emberek pedig a hétköznapjaik nagy hányadát töltik e közegben. Ez azonban nem egyszerűen a welfare state reformját eredményezte, azon lényegesen túlmutat hatásában, hiszen egy teljesen átalakult struktúrájú társadalmi-gazdasági közeget eredményezett ez a folyamat, amely az állami funkciók összességét is érintette. E folyamat alapjaiból kiforgatta a társadalmi totalitás egészét,[3] így annak minden egyes részkomplexumát: a gazdaságot, a jogot, a közigazgatást és a fegyveres védelem ágazatait[4] is.

Az „evolúció" sajátja, hogy nemcsak a welfare state jegyeit vette át, módosította és szelektálta a szereplők hatalmi igényei szerint, hanem a geopolitikai környezet átalakulásának és a technológia fejlődés jelentette biztonsági problémáknak köszönhetően egyes államok visszanyúltak a warfare state (háborús állam) jegyeihez is. Warfare state esetében ki kell emelni, hogy ez nem a jó állammal – welfare state-tel – szembenálló rossz állam, hanem olyan államfejlődési stáció(k), amely megjelent a transzatlanti térség államaiban is. Jelentősége abban fogható meg, hogy az államot ért impulzusokra, kiemelten a biztonságot érintő társadalmi vagy külső hatásokra való válaszreakcióként megjelenő állami (működési, szervezeti, funkcionális) racionalizációt, a védelmi, biztonsági aktorok centralizációját jelentette.[5] Bruce D. Porter tanulmányában az Egyesült Államok államfejlődésével kapcsolatban ki is fejtette, hogy ez az államfelfogás kellett az erős szövetségi állam létrejöttéhez, mivel a külső – vagy a polgárháborús – fenyegetettség minden esetben szükségessé tette az állam működésének átgondolását, adott esetben racionalizálását.[6] Emellett azonban nem elhallgatható, hogy ezen államfelfogás a 1945 előtti nemzetközi jogi környezetében kedvezett a nemzetközi konfliktusok eszkalálódásának, ha a jogállami kereteket nem tudták megerősíteni, illetve garantálni a békés működést.

A 21. század első évtizedeiben világossá vált, hogy a digitalizáció jelentős hatást gyakorol a társadalmakra, az államra, annak minden funkciójára. A pozitív hatások erősítik a jóléti funkciókat, emellett számos területen fejtenek ki jótékony hatást (lásd kommunikáció, okos városok stb.), mindazonáltal a negatív oldala is egy újfajta fellépést kíván az állam intézményeitől. *A digitalizáció eme kettősége pedig véleményem szerint egy korábban nem látott hibrid államodellt hozott létre, amelynek megfelelő vizsgálatához nem elegendő a korábbi fogalmak régi köntösben történő*

[3] Peschka Vilmos: *A jog sajátossága*, Budapest, Akadémia Kiadó, 1988, 33. o.

[4] Farkas Ádám: *A fegyveres védelem mint állami alrendszer és annak szabályozási sajátosságai.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.; Farkas Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2019.

[5] Lásd: James T. Sparrow: *Warfare State – World War II Americans and the Age of Big Government*. Oxford, Oxford University Press, 2011.

[6] Bruce D. Porter: *The Warfare State*. In American Heritage, 1994/4. szám (https://www.americanheritage.com/warfare-state#1); Bruce D. Porter: *War and the Rise of the State – The Military Foundations of Modern Politics.* New York, The Free Press, 1994, 7. fejezet War and the American Goverment.

átgondolása, hanem szükséges egy új fogalmi közeg megteremtése, amelynek kezdő lépése egy ehhez a folyamathoz igazodó új államodell definiálása és jegyeinek meghatározása. A szerző eme államodellt cyberfare statenek nevezi, amelynek elvi alapjait jelen tanulmányban kívánja lerakni. Ennek során a tanulmány kitér a cyberfare state kialakulására, sajátos jegyeinek bemutatására, továbbá vizsgálat tárgyává teszi annak összeegyeztethetőségét a polgári jogállami intézményekkel, vagyis azzal, hogy milyen eszközök révén tud eme cyberfare state a demokratikus működés talaján maradni.

A WELFARE SATE DIGITALIZÁCIÓJA, A TECHNOLÓGIA POZITÍV HATÁSA A 21. SZÁZAD ÁLLAMÁRA

A jóléti állam a szervezett kormányzati hatalom tudatos alkalmazását jelenti annak céljából, hogy a piaci erőhatásokat egyfajta társadalmi igazságossági és elosztási eszmény mentén módosítsák. Ezt kifejezetten három területen kívánták érvényre juttatni: (1) egyéneknek és családoknak minimális jövedelmet garantálva (munkától, munkabértől függetlenül); (2) szűkíteni a gazdaság bizonytalanságait, és ezzel elérve bizonyos társadalmi kockázatok kezelését; (3) meghatározott szolgáltatások esetében a lehető legmagasabb szintű ellátás biztosítása. Az első kettőt már korlátozottan, de a szociális állam is képes volt megvalósítani.[7] Azonban a harmadik cél ezen államodellen már túlmutatott és az egyenlő bánásmód irányába kívánta módosítani a rendszert. Ez pedig a piacgazdaság negatív hatásainak figyelem középpontjába kerülése miatt történhetett meg, hiszen szükségessé vált azok enyhítése, rendezése. Azonban, eltérően a szociális államtól, már nem a minimum garantálására törekedett, hanem az optimum irányába mozdult el a rendszer.[8]

Magának a jóléti államnak létrejöttét a fenti felismeréseken túl több tényező együttállása tette lehetővé, így kifejezetten: az általános választójog kialakulása; a politikai demokrácia kompetitív logikája; a korábbinál tagoltabb és komplexebb társadalmi rétegződés; az érdekcsoportok növekvő befolyása; valamint a szocialista államodellek jóléti ígéreteivel szembeni hatékony alternatíva állítása.[9] Ezen államodell „a demokratikus jogok kiterjesztése és kiszélesítése részeként komplex jóléti rendszereket alakított ki…"[10] Ezzel pedig több funkciót

[7] Lásd többek között: SZÉPVÖLGYI Enikő: *A dualizmuskori állami gyermekvédelem és a szegényügy összefüggései*. In Jog Állam Politika, 2020/3. szám, 101-116.; SZÉPVÖLGYI Enikő: *Gondolatok az állami gyermekvédelemről szóló törvénycikkek 120. évfordulójára.* In MEZEY Barna (szerk.): Kölcsönhatások. Európa és Magyarország a jogtörténelem sodrásában, Budapest, Gondolat Kiadó, 2021, 316-323. o.; KELEMEN Roland: *A polgári kor társadalombiztosítása - Társadalombiztosítási bíráskodás a polgári korban.* In Molnár Andrea – Széplaki László (szerk.): Tanulmányok a győri felsőbíráskodás történetéből a XIX-XX. század fordulóján, Győr, Győri Ítélőtábla, 2019, 149-174. o.

[8] Asa BRIGGS: *The Welfare State in Historical Perspective.* In Christopher PIERSEN – Francis G. CASTEl (szerk.): The Welfare State Reader (Second Edition), Cambridge, Polity Press, 2006, 16-17., 27. o.

[9] PONGRÁCZ Alex: *Nemzetállamok és új szabályozó hatalmak a globális erőtérben – avagy megszelídíthető-e a globalizáció?* Budapest, Dialóg Campus, 2019, 55. o.

[10] PONGRÁCZ Alex – TÉGLÁSI András: *Szociális állam, jóléti állam – Elméleti és történeti alapvetés.* In BÓDI

kívánt érvényre juttatni, így többek között a társadalom által okozott, azonosítható hátrányok enyhítését (munkanélküliség, üzemi balesetek, háborús nyugellátás, stb.), a társadalom által nehezen azonosítható, vis maior jellegű hátrányok tompítását (légszennyezés, városok pusztulása), indokolatlan társadalmi hátrányok kompenzációját (pl. szolgáltatás a hátrányos helyzetű gyermekek részére), valamint befektetést a jövő generációiba (pl. oktatás), továbbá a személyes jólét alapfeltételinek megteremtését (saját ingatlan, közművek stb.).[11] Megvalósítás eszközeként foghatók meg a társadalombiztosítás, a pénzbeli juttatások, a természetbeni juttatások, a partnerségi együttműködés kialakítása egyes szervekkel és a helyi önkormányzatok szociális tevékenységének erősítése. [12] Az eszközök szerkezetére, tartalmára eltérő megoldások születtek az államról való gondolkodás, a társadalmi tradíciók és a történelmi hagyományok nemzeti sajátosságai mentén.[13] Az érintett területek, szakpolitikák köre soha nem rögzült taxatív módon, azok folyamatos változásokat mutatnak, igazodva az adott kor aktuális kihívásaihoz is.

A 21. század társadalmi folyamatai ismét próbára teszik a jóléti rendszerek és az állam alkalmazkodóképességét. Így például a munka világában megjelenő, szolgáltatás alapú gazdaság jelentős változásokat eredményez. A World Economic Forum szerint 2015-2020 között közel 7,1 millió állás szűnt meg 15 gazdasági ágazatban.[14] Így a tudás- és készségintenzív gazdaság hátrányos társadalmi következményeinek elkerülése érdekében az államnak jelentős beruházásokat kell eszközölnie ezen csoportok oktatására, átképzésére.

A változó és fejlődő technológiák, a fokozódó globális integráció és az ezekhez való alkalmazkodás képessége, a szolgáltató szektor túlságos dominanciája és az általa szült tudásintenzív gazdaság együttesen szakadékot teremtenek társadalmakon belül, illetve ezek a tendenciák az államok között is fokozzák a polarizáltságot. Szükségszerűvé vált az államról alkotott felfogásunk újragondolása is.[15] „A szabadversenyes korszak be nem avatkozó, éjjeliőr államával szemben – amely az állami szerepvállalást a közrend és a közbiztonság fenntartására és a gazdaság működési feltételeinek biztosítására korlátozta – a jóléti állam tevékeny állam volt."[16] E

Stefánia – SCHWEITZER Gábor (szerk.): Az emberi jogok alkotmányos védelme Magyarországon, Budapest, Ludovika Egyetemi Kiadó, 2021, 299. o.

[11] Richard TITMUSS: *Universal versus Selection.* In Christopher PIERSEN – Francis G. CASTEL (szerk.): The Welfare State Reader (Second Edition), Cambridge, Polity Press, 2006, 42-43. o.

[12] BRIGGS i. m. 18. o.

[13] Gøsta ESPING-ANDERSEN: *Towards the Good Society, Once Again?* In Gøsta ESPING-ANDERSEN (szerk.): Why We Need a New Welfare State, Oxford – New York, Oxford University Press, 2002, 1. o.

[14] FERENCZ Jácint: *Az információ és a technológia kettős arca a munkajogban.* In Baranyiné Kóczy Judit – Fehér Ágota (szerk.): Pedagógusképzés, oktatás a Kárpát-medencében, társadalmi kontextusok. XXII. Apáczai-napok Tudományos Konferencia tanulmánykötet, Győr, Széchenyi István Egyetem Apáczai Csere János Kar, 2019, 322. o.

[15] Gøsta ESPING-ANDERSEN: *A Welfare State for the Twenty-first Century*. In: Christopher PIERSEN – Francis G. CASTEL (szerk.): The Welfare State Reader (Second Edition), Cambridge, Polity Press, 2006, 434., 447-448. o.

[16] SZIGETI Péter: *Társadalomkutatás – Mi végre? Politikatudomány, alkotmányjog, világrendszerelmélet*, Győr, Universitas, 2011, 262. o.

megváltozott, az államot aktív cselekvésre ösztönző környezetben kézenfekvő, hogy eme jóléti állam egyes attribútumait erősítő államfelfogás tud csak eredményesen fellépni a korszak kihívásaival szemben.

Ennek egyik úttörője volt a bevezetésben már citált Kaladijan is, aki a jóléti állam reformjának lehetőségét a digitalizációban látta. A technológia hihetetlen fejlődése a 21. század első évtizedeiben arra a szintre jutott, hogy az élet szinte minden területén megkerülhetetlen tényezővé vált. Ebből a fejlődésből is kiemelkedik a kibertér által generált lehetőségek és változások tárháza, amelynek köszönhetően Kaladijan eszménye a digitálisan hatékonyabbá, igazságosabbá tett jóléti rendszerről részint megvalósulni látszik. Ez szintén a jóléti államok sajátos államfelfogásán is alapszik, hiszen annak megteremtése a társadalom oldaláról igényt támasztott a minőségi közigazgatás kialakítására, fejlesztésére; „a közigazgatás ennek következtében megszűnt a jogszabályok puszta végrehajtója és a hatósági jogalkalmazó közigazgatás kizárólagos terepe lenni”,[17] létrehozva ezzel a szolgáltató közigazgatást. Így a technológia forradalma a jóléti állam szükségszerű átalakulását is eredményezi, tehát szintén szükségszerűen magával hozta a közigazgatás, végső soron a teljes államműködés reformját is.

Az állami intézményrendszernek fel kellett vennie a versenyt az átalakult szolgáltatóiparral, amely lehetővé tette, hogy a saját otthonainkból szinte minden elérhetővé váljon az okoseszközök használatának köszönhetően. Az e-közigazgatás fokozatos kialakításával és fejlesztésével lépett e verseny pástjára az állam, amelynek köszönhetően hatékonyabbá, naprakészebbé és nem utolsó sorban polgárbaráttá (felhasználóbaráttá) vált a rendszer.[18] Az egyes szolgáltatások könnyebben elérhetővé váltak,[19] és a legtöbb esetben az eljárások is jelentősen felgyorsultak.

Az átalakulás azonban itt nem állt meg. A kibertér megjelenése a Titmuss fentebb ismertetett állami (jóléti) funkcióknak valamennyi szegmensére hat, hatott. Így többek között kézelfoghatóan az oktatásban, kutatásokban, az egészségügyben, a szociális szférában megjelent az IoT[20] és okoseszközök,[21] a mesterséges intelligencia pedig egyre jelentősebb teret foglal el. A kibertérhez csatlakozó eszközök (az állam, a gazdaság és az egyén oldaláról), valamint a korábbi évszázadok tudásának digitalizálása óriási adatmennyiséget (big data) generálva forradalmi átalakulást hoztak a fenti

[17] PONGRÁCZ i. m. (2019) 163. o.

[18] Lásd: BUDAI Balázs: *Az e-közigazgatás fogalma, jogi és stratégiai keretei.* Budapest, Dialóg Campus, 2017.

[19] Gondoljuk itt például Magyarország tekintetében az internetes ügyfélkapu rendszerre, amelynek köszönhetően számos szolgáltatást az otthonunkból ki sem mozdulva tudunk elintézni.

[20] Korunk egyik nóvuma, konvergáló technológiája a tárgyak internete (IoT – Internet of Things), amely az információtudomány fejlődésével, a szenzorok használatának fokozódó térnyerésével (ami magával hozza az árak rapid csökkenését) egyre inkább a mindennapi életünk részévé válik mind az otthonokban, mind pedig a közszférában. Lásd: NÉMETH Richárd: *Kibertámadások gazdasági vonatkozásai a vállalati szférában.* In: DERNÓCZY-POLYÁK Adrienn (szerk.): Kutatási jelentés 1. Győr, Universitas-Győr Nonprofit Kft., 2019, 307-325. o.

[21] G. KARÁCSONY Gergely: *Okoseszközök - okos jog?* Budapest, Ludovika Egyetemi Kiadó, 2020.

területeken is. Ez az egészségügyben többek között csökkentette a diagnosztikából eredő hibákat, lehetővé tette a korábban fel nem fedezett összefüggések felismerését,[22] új módszerek kidolgozását, alkalmazását. Az oktatásban lehetővé vált, válik az okoseszközök használatával és az algoritmusok révén a személyre szabott tanulás, tudásanyag átadása.[23] A big data-nak köszönhetően a kutatások soha nem látott, országhatárokat átlépő, kontinenseket összekötő hálózatokat generálnak, felgyorsítva az innovációt.

Azonban az állam működésének átalakulása nem állt meg a jóléti rendszerek modernizálásánál, a modern technológia alapjaiban alakította át a teljes állami működési mechanizmusokat, valamint az állam és a gazdasági szereplők, továbbá az állam és a polgárok közötti interakciókat. A modern technológia ennek köszönhetően behatolt az élet minden szintjére és azokra jelentős hatást gyakorolt, így egyebek mellett a rendészetre,[24] a közlekedésre,[25] az energiahasználatra és az önkormányzatiságra, [26] és nem utolsósorban a védelem és biztonság világára is.[27]

Ez látszólag sokkal élhetőbbé tette az emberek hétköznapjait, az állam működését pedig racionalizálta, felhasználóközpontúbbá tette. Mindemellett azonban a szolgáltatásközpontúság, az adatokhoz, a képességekhez való hozzáférés lehetősége a klasszikus welfare state egyenlőségre törekvő oldalát elmozdította egy elitista működés irányába, ahol ezen erőforrások feletti tényleges rendelkezés lehetősége teremti meg a döntéshozásnak az alapjait.[28] Tökéletes példái ennek a magántulajdonban álló okos városok, ahol az adatok szinte teljességéhez hozzáférnek az olyan nagyvállalatok, mint az Amazon Seattleben, vagy Facebookville, Zucktown esetében a Meta, de többek között ilyet tervez létrehozni a Tesla Ausztráliában Yarrabend néven.[29] Szintén az adatok

[22] Tökéletes példa erre Carolyn McGregor munkássága, aki egészségügyi informatikusként számos korábban fel nem fedezett összefüggést talált a koraszülöttek kezelésével kapcsolatban. Lásd: BŐGEL György: *A big data ökoszisztémája,* Budapest, Typotex, 2015, 22-24. o.

[23] TILESCH György – Omar HATAMLEH: *Mesterséges intelligencia – Vegyük kezünkbe a sorsunkat az MI korában.* Budapest, Librid, 2021, 65-68. o.

[24] Lásd Abishur PRAKASH: *Go. AI – A mesterséges intelligencia geopolitikája.* Budapest, Pallas Athéné Könyvkiadó, 2018, 97-108. o.

[25] Atanu BHUYAN: *Designing optimal welfare policies for intermediate publictransportation systems: A developing country perspective*. In Academia Letters.

[26] Lásd: KOVÁCS László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018, 19-118. o

[27] Példaként ebben a körben érdemes megjegyezni, hogy több szerzői is kiemelte már a digitális adatokkal történő rendelkezés biztonságra, védelemre gyakorolt hatását, illetve fake news társadalmi kohéziót romboló hatását, továbbá az erre épített dezinformációs tevékenység nemzetbiztonsági vonatkozásait. Lásd: Amaël CATTARUZZA: *A digitális adatok geopolitikája – A hatalom és konfliktusok a big data korában.* Budapest, Pallas Athéné Könyvkiadó, 2020.; KELEMEN Roland: *Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben.* In Jog Állam Politika, 2021/3. szám, 71-85. o.

[28] Lásd: ÁRVA László – PÁSZTOR Szabolcs – Victoria PYANATOVA: *A multinacionális vállalati stratégiák és a változó világkereskedelem kapcsolatáról.* In Gazdaság és Pénzügy, 2020/1. szám, 57-81. o.

[29] Vincent MOSCO: *Okosvárosok a digitális világban.* Budapest, Pallas Athéné Könyvkiadó, 2019, 137-145. o.; Lásd még: DUSEK Tamás: *Az okos városok komplex mutatószámainak egyes tartalmi és módszertani problémái.* In KOVÁCS Gábor – VÖLGYI Katalin (szerk.):

garmadája felett diszponálnak a social media vállalatok, azokat tényleges termékként kezelik. *Érdekes módon tehát a nyugati államokban a gazdaság – főként a kibertérben tevékenységet realizáló – transznacionális szereplői tömegesen férnek hozzá az egyénekhez fűződő adatokhoz,*[30] *míg az alkotmányos struktúrájukban kialakított korlátoknak és fékeknek köszönhetően az államok számára ezeknek az elérhetősége erősen korlátozva van. Látni fogjuk ezzel szemben a keleti autoriter államalakulatok maguk is végrehajtották – igaz sajátos módon – az államaik digitális (jóléti) reformját, addig viszont az adatok lehető legteljesebb köre felett kívánnak rendelkezni.*

A WARFARE STATE DIGITALIZÁCIÓJA – A KIBERTÉRBEN REALITÁSSÁ VÁLT TOTÁLIS BIZTONSÁGI KIHÍVÁSOK

A keleti államok, főként Kínai és Oroszország jelentős mértékben kiaknázzák a technológiai újításokból fakadó biztonsági képességeket. Ennek eklatáns példája az okos város nyújtotta jóléti lehetőségekbe burkolt totális megfigyelés és adatgyűjtés lehetősége. Ilyen rendszert kiépítését kezdte meg Kína a 2010-es évek elejétől. *Megdöbbentő módon a világban jelenleg futó körülbelül ezer okos város-projekt közel fele Kínához köthető.* Ennek központi eleme a Citizen Cloud, „ez egy felhőalapú platform, és egyben mobil alkalmazás is, amely egyesíti a kormányzati szolgáltatások legnagyobb részét, és megkönnyíti a városlakók számára az ezekhez való hozzáférést, ide számítva az egészségügyi nyilvántartásokat, a jogosítványkérelmeket és -megújításokat, és más közösségi programokat is… a Huawei… gyártmányai teszik lehetővé az autósok számára a szabad parkolóhelyek megtalálását… A rendszer nagyon megkönnyíti a betegek és a kórházak számára a releváns nyilvántartások elérését…”[31] *A kiépülő rendszer tökéletes példája lehet az előző fejezetben elérni kívánt állami működésnek, vagyis az olyan szolgáltató államnak, amely képes jóléti intézményeit átemelni a digitális környezetbe, sőt fokozni is képes ezáltal azokat. Azonban ott van egy hatalmas „de” a mondat végén, hiszen e rendszerek révén nem csupán erre képes Kína, hanem az emberek nyomon követésére, osztályozására és adataik tényleges birtoklására is.*[32]

Szingapúr is hasonló példát mutat Okos Nemzet projektjével, amely felhasználásával „kezdetektől fogva tervezeték… egy centralizált műveleti

Üzleti vállalkozások, makro- és mikrokörnyezetük gazdálkodási és menedzsment sajátosságai" c. kutatás tanulmányai. Győr, Széchenyi István Egyetem Kautz Gyula Gazdaságtudományi Kar, 2018, 1-3. o.

[30] Ezen vállalatok az adatokhoz való hozzáférést követően nem kizárólag felhasználják ezeket az információkat, hanem kereskedelmi és politikai célokra áruba bocsátják, ezzel is erősítve az adatok geopolitikai jelentőségét. Lásd: ENGEL Péter: *A Bundeskartellamt Facebook-döntése – az adatgyűjtés versenyjogi kockázatai.* In Verseny Tükör, 2019/1. szám, 70-76. o.; GELLÉN Klára: *Tisztességtelen kereskedelmi gyakorlatok az online térben – fókuszban a közösségi média*. In In Medias Res, 2020/1. szám, 127-140. o.; FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei.* In SmartLaw Research Group Working Paper, 2021/1. szám, 1-13. o.

[31] MOSCO i. m. 111-112. o.

[32] KOLLÁR Csaba: *Kína és a társadalmi kredit rendszere.* In Hadtudomány, 2020/2. szám, 79-97. o.

központ létrehozását, a polgárokról és a látogatókról összegyűjtendő nagy mennyiségű adat kezelésére…" ez pedig lehetővé teszi „… az átfogó megfigyelést és az egyének magatartásának szigorú szabályozását…"[33] A megvalósítás hivatalos céljai között szerepel a betegségek terjedésének a gyorsabb feltérképezése vagy a terrorista támadásokra való gyorsabb reagálás lehetősége. Megvalósításán fúzióban dolgoznak az állami intézmények és a magánszféra vállalatai, akárcsak Kína esetében. A rendszerek kialakításában és az üzemeltetésében történő közreműködésért cserébe a kormányzat „megosztja az adatokat a gazdaságfejlesztés és a kereskedelmi sikerek ösztönzése céljából"[34]. Két szereplő, vagyis az állam és a technológiai vállalatok együttesen érdekeltté válnak a status quo fenntartásában, hiszen egyfelől totális felügyelet alá helyezték az egyéneket, másfelől a gazdasági fejlődés folyamatos fenntartását teszik lehetővé az állami megrendelések, harmadsorban a meglévő adatok birtokában a gazdasági szféra is meg tudja hozni a szükséges intézkedéseket, stratégiát a profit folyamatos növelése érdekében. Mit nyer ezzel a felhasználó? Javuló közszolgáltatásokat a szabadságáért cserében, de lényegében a választás lehetősége egy másodpercig sincs biztosítva a részükre. Ilyen város kialakítását tűzte ki célul az Egyesült Arab Emirátus Dubaj esetében, de ezt látjuk Rio de Janeiro-ban, Malajzia és Fülöp-szigetek jelentősebb városaiban, valamint India is meghirdette ezen programját All India City Challenge néven, amelynek alakításába azonban a helyi közösségek aktívan bele kívánnak szólni.

A rendszert a saját internet létrehozása és annak totális felügyelete tette teljessé, mint a kínai Aranypajzs rendszer, vagy az orosz internet,[35] ezzel ezen államalakulatok képesek szinte totális ellenőrzés alatt tartani saját polgáraikat, hiszen minden olyan tartalmat képesek blokkolni, amely az államhatalom szempontjából nem kívánatos. Ezen megoldás az okos város-projektekhez hasonlóan szintén követőkre talált. Irán közvetlenül kínai know-how felhasználásával kíván „halal"[36] internetet kiépíteni, amelyet Zambia is követ a kritikus tartalmak blokkolása területén. Emellett a kormányellenes, kormánykritikus hangok blokkolása is bevett gyakorlattá vált a social media felületeken, ezt alkalmazza Kuba, Nigéria, Kolumbia, Banglades, Szenegál, illetve a teljes internet elérhetőségét megakadályozva a Kongói Köztársaság, Csád, Örményország, vagy Mianmar.[37]

Az elmúlt években az is világossá vált, hogy az államok a technológia újdonságait legalább ilyen, aktív módon használják más államokkal szemben is. A hibrid konfliktusok

[33] MOSCO i. m. 109. o.

[34] MOSCO i. m. 110. o.

[35] GOSZTONYI Gergely: *Special Models of Internet and Content Regulation on China and Russia.* In ELTE Law Journal, 2021/2. szám, 87-99. o.

[36] A halal fogalom az iszlám vallásban fontos értéket képvisel, jelentése megengedett vagy tiszta. Az iszlám jog szerint minden tevékenység megfelel a halal-nak, amely megengedett és az előírásoknak, dogmáknak megfelel. Ennek felhasználásával kontrollált internetes információ áramlást nevezhetjük halal internetnek. Lásd: *Iran creates „Halal Internet" to control online information.* In RSF – Reporters without Borders. 2016. szeptember (https://rsf.org/en/news/iran-creates-halal-internet-control-online-information).

[37] GOSZTONYI i. m. 97-98. o.

eszközparkjába beemelt kibertéri műveletek rendkívül széles tárházát adják a szembenálló állam egyes rendszereinek támadására. Folyamatos fenyegetést jelentenek a dezinformációs kampányok, amelyek érdemben az államalakulatok mindegyikével szemben alkalmazhatóak. Az oroszok folyamatos dezinformációs tevékenysége figyelhető meg az elmúlt évtizedben. Ennek során beavatkoztak a 2016-os amerikai elnökválasztásba, akár álhírek terjesztésével, akár a szembenálló jelöltekkel kapcsolatos kompromitáló információk kiszivárogtatásával, vagy a social media platformokon keresztül megfelelően időzített hírcsomagokat juttattak el felhasználókhoz.[38] A francia sárgamellényes tüntetés időszakában hamis híreket terjesztettek német, spanyol, holland, lengyel, svéd és olasz nyelven. Az RT orosz állami hírcsatorna néhány riportere részt vett a tüntetéseken, és úgy ábrázolta a helyzetet, mintha Párizs háborús övezet volna. A dezinformációs kampányból nem maradhatott ki a hagyományos média munkatársainak lejáratása sem, őket korruptnak, megbízhatatlannak, a kormánnyal mindenben összejátszónak mutatták be.[39] A legyártott és azonosított száz álhírt, több mint 4,1 millióan osztották meg és 105 millióan tekintették meg.[40] De mindkét állam rendkívül erős dezinformációs kampányt folytatott a Covid-19 járvánnyal és nyugati vakcinák hatékonyságával kapcsolatban, ezzel is nehezítve a térség járvány elleni védekezését.[41] Jelenleg zajló orosz–ukrán háború is élesen rávilágit erre a problémakörre. A háború szinte, vagy inkább láttatni kívánt szinte minden pillanatát követni tudjuk a social media felületein.[42] Ennek célja mindkét oldalról, hogy a hadviselő felek megfelelően tudják tálalni érdekeiket saját, illetve a világ más társadalmai irányába, vagyis mindkét oldal él a dezinformáció eszközével.[43] Földi László biztonságpolitikus ezt a következőképpen foglalta össze: „Nagyon álságos ez a helyzet, a közvéleményt afelé tolják, hogy tendenciózusan döntsünk, miközben gyakorlatilag kihúzzák a lábunk alól azt a lehetőséget, hogy objektívek maradjunk… megjegyezve, hogy az egyik fél amerikai, a másik fél pedig orosz propagandáról beszél, miközben valójában mindkét hatalomnak

[38] Lina ROSENSTEDT: *Improving Cooperation with Social Media Companies to Counter Electoral Interference.* In Hybrid Coe Paper, 2021/5. szám, 5. o.

[39] Jarmo MAKELA: *Countering Disinformation: News Media and Legal Resilience.* In Hybrid CoE Paper. 2019/1. szám, 10-13. o.

[40] *Yellow Vests Flooded by Fake News – Over 100M Views of Disinformation on Facebook. Avaaz Report.* 15.03.2019. (https://avaazimages.avaaz.org/Report%20Yellow%20Vests%20FINAL.pdf).

[41] Ben DUBOW – Edward LUCAS – Jake MORRIS: *Jabbed in the Back: Mapping Russian and Chinese Information Operations During Covid-19.* The Center for European Polidy Analysis (CEPA), 2020.

[42] PATÓ Viktória Lila: *A háború hatása a közösségi médiára.* In Nemzeti Közszolgálati Egyetem Európai Stratégia Kutatóintézet (https://eustrat.uni-nke.hu/hirek/2022/03/01/a-haboru-hatasa-a-kozossegi-mediara).

[43] HUSZÁK Dániel: *Példátlan információs háború zajlik Ukrajna körül – Elképesztő mennyiségű hazugság ömlik a világra.* In Portfolio (https://www.portfolio.hu/global/20220226/peldatlan-informacios-haboru-zajlik-ukrajna-korul-elkepeszto-mennyisegu-hazugsag-omlik-a-vilagra-529377).

megvannak a maga eszközei a befolyásolásra."[44]

Legalább ilyen jelentős a különböző intenzitású kibertámadások elkövetése akár civil, gazdasági célpontok ellen,[45] akár állami intézmények rovására. Ezek közül legismertebb a 2007-es Észtországot és a 2008-as Grúziát ért támadás,[46] azonban ezenfelül számos kisebb volumenű szcenáriót tudunk feljegyezni az elmúlt évtizedből. Ilyennek tekinthetjük a Észak-Koreához köthető WannaCry zsarolóvírus támadást is, amely jelentős károkat okozott több államnak, gazdasági szereplőnek.[47] Szintén megfigyelhető ennek az eszköznek az alkalmazása a jelenleg zajló orosz-ukrán háborúban is, amikor az orosz haderő legalább annyira aktív a kibertérben, mint a hagyományos hadviselés területén.[48] *Ezzel kapcsolatban érdemes leszögezni, hogy a kibertér nem hozott létre önmagában új konfliktuskategóriákat, nem eredményezett a korábbitól ismeretlen hadviselési metódusokat, hanem ez valójában a hadiviselés korábbi eszköztárának a fejlesztését jelentette: a hatékonyság és az erő sokszorozását, műveleti képességek fokozását.*[49] Az orosz–ukrán konfliktus korábbi szcenáriói is visszatükrözik ezt. A West Point-i katonai szakértők szerint az oroszok szinte példa nélküli módon egymást kiegészítve, kombinálva alkalmazzák a kiberhadviselés, az elektronikus hadviselés és az információ műveletek eszközparkját.[50] Ahogy ezt Kiss Álmos Péter kifejtette: „az oroszok egyáltalán nem osztják fel az információs teret. Nincs különálló kibertér, nem tesznek

[44] Holló Bettina: *Földi László a háborúról: Állásfoglalásra késztetnek, de az igazság magjától is eltántoríthatnak.* In Index (https://index.hu/belfold/2022/03/06/haboru-ukrajna-alhirek-biztonsagpolitika-foldi-laszlo-demko-attila/).

[45] „A 2020-as évben pusztító útjára indult Covid-19 járvány az informatikai biztonság területén is kifejtette hatását – globális szinten jelentősen megnövekedett a kibertámadások száma. A Kaspersky felmérése szerint „az Európai Unióban az internetet használó számítógépek 13,7 százalékán tapasztaltak legalább egy böngészőalapú, rosszindulatú programtámadást", (és a támadások számát tekintve) „az első tíz között találjuk Magyarországot is.". Nagyságrendileg ugyan az otthoni gépek vannak leginkább kitéve kémkedésnek, adatlopásoknak, rongálásnak és egyéb támadásoknak, de céges környezetben a statisztikák nem kevésbé lesújtóak. Az amerikai CSI egy korábbi felmérése szerint a válaszadók 85%-a észlelt már számítógépes betörési kísérleteket az adott naptári évben, sőt, 64% esetében ez anyagi veszteséget is jelentett." – Németh Richárd: *A kibertérből érkező fenyegetések elleni védekezés vállalati környezetben.* In GIKOF Journal, 2021, 48. o.

[46] Kelemen Roland – Pataki Márta: *A kibertámadások nemzetközi jogi értékelése.* In Katonai Jogi és Hadijogi Szemle, 2015/1. szám, 53-90. o.

[47] *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. Department of Justice, 2018. szeptember 6. (https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and).

[48] Joe Tidy: *Ukraine crisis: 'Wiper' discovered in latest cyber-attacks*. In BBC News, 2022. 02. 24. (https://www.bbc.com/news/technology-60500618).

[49] Sascha-Dominik Bachmann – Hakan Gunneriusson: *Hybrid Wars: The 21st Century's New Threats to Global Peace and Security.* In South African Journal of Military Studies, 2015/1. szám, 82. o.

[50] Aar Aaron F. Brantly – Nerea M. Cal – Devlin P. Winkelstein: *Defending the Borderland - Ukrainian Military Experiences with IO, Cyber, and EW.* Army Cyber Institute at West Point, West Point, 2017 24. o.

különbséget a számítógép-hálózatokat érintő műveletek és más információszerző, információfeldolgozó és információáramlást zavaró tevékenység között. Az orosz információs hadviselés harctere tehát a teljes kognitív tartomány."[51] *Látható, hogy a kibertéri eszközpark beépült a haderő tevékenységébe legyen az akár befolyásolás, akár hírszerzés, akár támadó eszköz, amely így a békeidős összhaderőnemi felkészítésnek, majd pedig eszközparkjának immanens részét képezi. Így lehetséges az, hogy a hagyományos háborúnak is vannak – lásd orosz–ukrán – hibrid szcenáriói.*

A kibertér a fentieken túl lehetőséget biztosít a szakadár és terrorista csoportok anyagi támogatására, szervezésére, amelyek így képesek lehetnek későbbi akciókhoz kapcsolódó információszerzésre, az ilyen akciók kibertéri támogatására, az akciók kibertéri előkészítésére és adott esetben – ahogy Lewis fogalmazott[52] – a közlekedési hálózatokkal, finomítókkal, gátakkal, katonai létesítményekkel, kórházakkal, bankokkal, kormányzati intézményekkel stb. szembeni támadás lefolytatására. Nem véletlen, hogy az oroszok rendkívül sikeresek voltak az ukránok elleni hibrid konfliktus során, hiszen tökéletesen tudták alkalmazni a korábbi évtizedek tapasztalatait és kapcsolati hálóját.[53]

A kibertér és a hozzá tapadó technológiai újdonságok pozitív hozadékai mellett olyan, az államok biztonságát, biztonsági környezetét befolyásoló természettel bír, amely így számos ponton tépázza meg az 1945 utáni nemzetközi jogi rezsimet, sok esetben feloldva azt a napi politikai realitások folyamában. A kibertérben alkalmazott vagy támogatott hadászati eszközök nem újak, azonban a korábbi eszközöket a végletekig tudják fokozni, eredményesebbé és hatékonyabbá tenni. Jól bizonyítják ezt a hibrid konfliktusok, kiemelten az ISIS tényekedése, valamint 2014-től az oroszok ukrajnai tevékenysége volt az egyik mintapéldánya ennek a hadviselésnek, amelynek magasabb fokozatba kapcsolását jelenti a 2022 februárjában kirobbant nyílt háború. A korábbi szcenáriók esetében is már egyértelművé vált, hogy a technológiai újításokat alkalmazva, egyre fokozottabb mértékben kezdődött meg az ENSZ Alapokmányban lefektetett erőszak általános tilalmának eróziója. Főként annak köszönhetően, hogy a polgári és kombattáns elkülönítése a harcászat nem klasszikus terepén szinte lehetetlenné vált, így a betudhatóság korábban kiforrott és többnyire a felek által betartott szabályait nem, vagy csak nagyon nehézkesen lehet alkalmazni. Az ukrán háború rávilágított arra is, hogy a népek önrendelkezése és külső állam beavatkozásától mentes létezése is feloldódni látszik a nagyhatalmi törekvésekben, amelyeket akár későbbi nemzetközi szerződésekkel is

[51] KISS Álmos Péter: *A hibrid hadviselés természetrajza.* In Honvédségi Szemle, 2019/4. szám, 31. o.

[52] James A. LEWIS: *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,* In Center for Strategic and International Studies, 2002 (https://www.steptoe.com/images/content/4/5/v1/4586/231a.pdf).

[53] KÁNCZ Csaba: *Az orosz titkosszolgálatok és a szervezett bűnözés ijesztő kapcsolatrendszere.* In privátbankár.hu, 2021. (https://privatbankar.hu/cikkek/makro/az-orosz-titkosszolgalatok-es-a-szervezett-bunozes-ijeszto-kapcsolatrendszere.html).

megerősítenek,[54] illetve végső esetben nagyhatalmi deklarációkkal legitimálnak.[55] A háború és béke határa elmosódott az elmúlt években, a legtöbb konfliktus esetében nem tudjuk, hogy az „éppen még" vagy az „éppen már" állapotában vagyunk. Erre szintén rávilágított az orosz–ukrán válság, hiszen a tényleges harci cselekmények a felek között már jóval a 2022-es inváziót megelőzően megindultak.

Ezek összessége eredményezi a biztonság és védelem újradefiniálását, a totális biztonság irányába történő elmozdulást.[56] A nemzetközi közösség államainak egyik pólusa már megtette ezt, és ezen államalakulatok – főként a kibertér révén – már sokkal közelebb helyezkednek a warfare state államához, amely saját biztonságának szavatolását csak a hatalom révén, az erő által látja biztosítottnak.[57] Ezen államokban a haderő folyamatos erősítése mára létérdekké vált, a politikai hatalom, haderő és gazdaság hármasa egyetlen érdeket szolgál: a status quo minimum fenntartását, vagy még inkább a hatalmi szféra kiterjesztését.

A CYBERFARE STATE – A TOTÁLIS BIZTONSÁG ÉS VÉDELEM (JOG)ÁLLAMI ADAPTÁCIÓJÁNAK A LEHETŐSÉGES

A kibertér és az ahhoz kapcsolódó rendszerek ilyen rendkívül sikeres kiaknázása, felhasználása és alkalmazása, amely főként Kínában, vagy Oroszországban, Szingapúrban, illetve akár egyes aspektusokban Észak-Koreában figyelhető meg – de mint láttuk, emellett számos követő államra talált legalább részmegoldásaiban – megteremtette a cyberfare state hatalmi államon nyugvó almodelljét. Ennek keretében az állam a birtokolt erőhatalom révén ténylegesen létrehozza a saját szuverén kiberterét, azt teljes egészében birtokolja, ellenőrzi, az ettől elkülönült külső kibertérben megjelenő államok technikai, szabályozási, védelmi hiányosságait kihasználva pedig soha nem látható eredményességgel tudja befolyásolni, eszkalálni más társadalmak töréspontjait, illetve tudja megbénítani egyes alrendszereit. Mindezeket anélkül, hogy legtöbb esetben ténylegesen fegyveresen konfrontálódna a megtámadott állammal. Ezt a rendszert azért működtetik, a tevékenységet azért valósítják meg, mert a kialakult új biztonsági

[54] Lásd a minszki szerződéseket az ukrán konfliktusban. Lásd bővebben: PÓTI László: *Minszk-2 után két évvel: Hol tart a békefolyamat?* In KKI Elemzések, 2017/5. szám.

[55] *Vlagyimir Putyin elismerte a két szakadár népköztársaságot.* In hirado.hu, 2022.02.22.

[56] FARKAS Ádám: *Gondolatok a totalitás 21. századi esszenciájához.* In PONGRÁCZ Alex (szerk.): Ünnepi tanulmányok a 65 éves Cs. Kiss Lajos tiszteletére. Út vocatio scientia, Budapest, Ludovika Egyetemi Kiadó, 2021, 65-80. o.

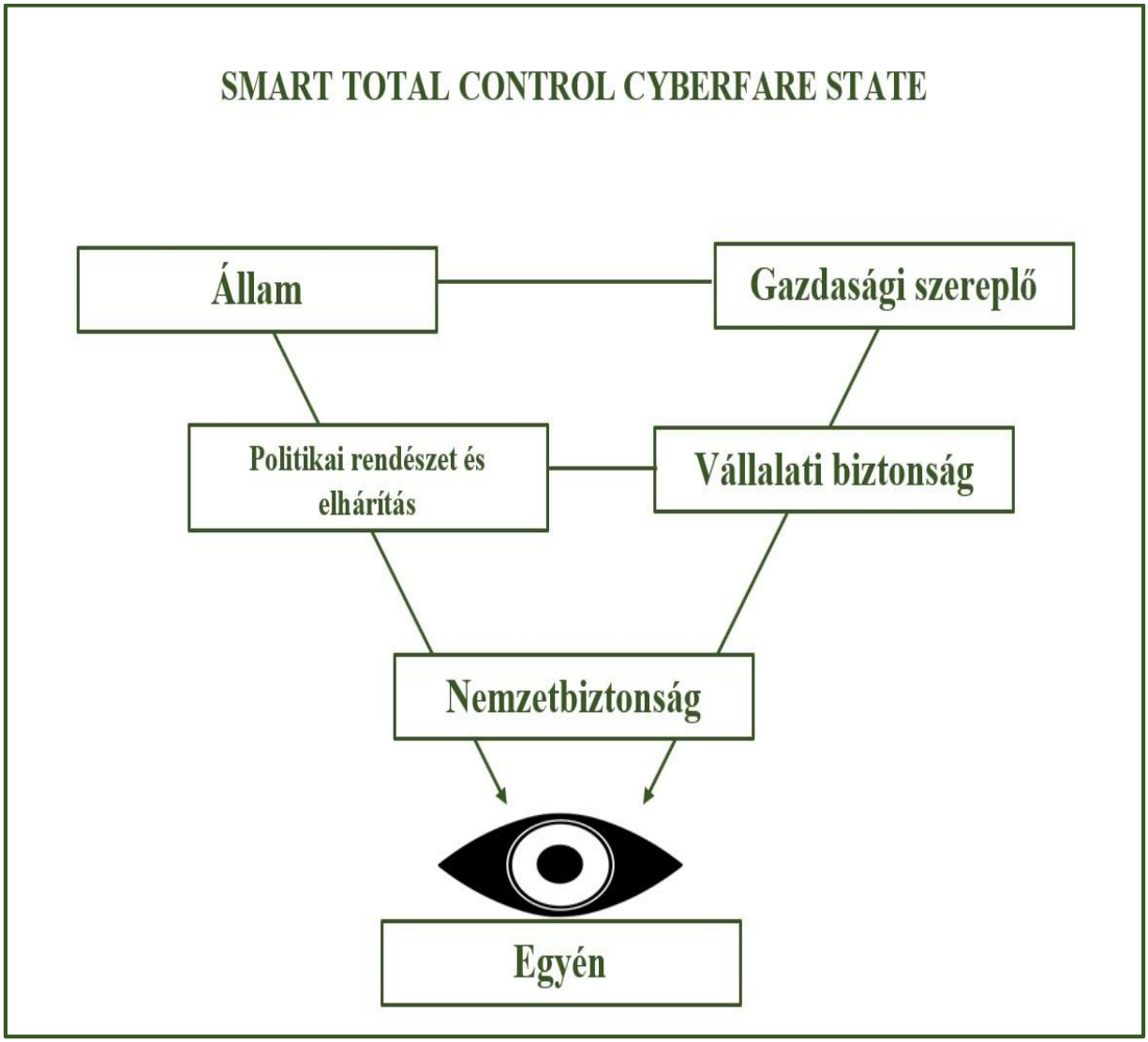
[57] Fred J. COOK: *The Warfare State.* In The Annals of the American Academy of Political and Social Scince, 1964/1. szám, 102-109. o.; Keith L. NELSON: *The Warfare State: History of Concept.* In Pacific Historical Review, 1971/2. szám, 127-143. o.; David EDGERTON: *Warfare State – Britain, 1920-1970.* Cambridge, Cambridge University Press, 2006, 59-107. o.

környezetben meglátásuk szerint a totális felügyelet és totális „erőszak-monopólium a béke és a kiszámítható rend legfőbb biztosítéka”[58]. Ennek kialakításában pedig – mint láttuk – fúzióban tevékenykednek, működnek és fejlesztenek az egyes államok és gazdasági szereplőik. Az egyén ezekben az államokban a lehető legteljesebb kontroll alatt éli hétköznapjait, lényegében kizárólag egyes részobjektumok üzemeltetője (munkája révén) és fogyasztója a rendszer által engedett és kínált szolgálatásoknak, de valódi döntéssel nem rendelkezik adatvagyona felett sem. Ebben a közegben tehát az állam hatékony működését, biztonságának szavatolását az állam és a gazdasági szereplők összefonódása, érdekközössége teremti meg, ahol e közös cél érdekében az egyént, mint a (kiber)biztonság legtörékenyebb láncszemét[59] megpróbálják kivonni, szerepét a lehető legcsekélyebb mértékűvé tenni, ennek pedig eszköze a személye feletti totális kontroll és adatai feletti állami és gazdasági rendelkezés totalitása.

Ezen államok (kiber)biztonság szavatolását jelentő legjobb gyakorlat kialakítása, folyamatos nyomkövetése és szükséges korrekciója az állam és az ebben érintett gazdasági szereplők közös érdeke és együttműködésük gyümölcse, amelyben az egyén nem érdekeltként, hanem kizárólag irányított, kontrollált erőforrásként jelenik meg. Ebben a legjobb gyakorlatban a kibertérre támaszkodó technológiai újításokon nyugvó szociális, jóléti intézményeket, végső soron szolgáló közigazgatás javítását, modernizálását társítják a totális kontroll és adatok feletti totális rendelkezés lehetőségével, amelyekhez sok esetben támadó potenciál kiépítése kapcsolódik. A cyberfare state ezen hatalmi jellegű attribútumokat felmutató államait a fentiek okán smart total control cyberfare statenek nevezhetjük.

[58] Pongrácz Alex: *A politika folytatása más eszközökkel? Avagy gondolatok az állam és az erőszak kérdésköréről.* In Államtudományi Műhelytanulmányok, 2017/17. szám, 9. o.

[59] Informatikai szempontból lásd: Németh Richárd: *Kiberfenyegetettség nagyvállalati környezetben.* In Magyar Bűnüldöző, 2020/2. szám, 23-41. o.



Smart total control cyberfare state (saját szerkesztés)

Ezzel szemben a nyugati államoknak a saját cyberfare state modelljük kialakítása során teljesen más alapokról kellett, kell indulniuk. A digitalizáció jóléti reformját már megkezdték a 2000-es évek elején, és ebben, ha nem is minden területen, de látványos sikereket értek el. Az első fejezetben látható volt, hogy sikerrel alakították át a szolgáltató közigazgatást, nagy volumenű innováció jelent meg többek között az oktatás, kutatás, egészségügy területén, emellett rendkívül sikeres okos város programok[60] is futnak, de az önvezető járművekkel kapcsolatos

[60] A nyugati államok okos város projektjeiről, azok elvi alapjairól lásd bővebben: SZALAI Ádám: *Az okosváros-koncepciók kritikai földrajzi vizsgálata – elméleti háttér és lehetséges kutatási irányok.* In Tér és Társadalom, 2020/2. szám, 88-107. o.; RAB Judit – SZEMEREY Samu: *Az okos város fejlesztési modell módszertani alapjai.* Budapest, Lechner Nonprofit Kft, 2018.

projektek,[61] vagy az MI programok[62] is számos előnnyel kecsegtetnek. Azonban itt is jelentős eltéréseket lehet kimutatni a másik pólus államaihoz képest, ugyanis ebben kulcsfontosságú, sőt élenjáró szereplők voltak a technológiai óriásvállalatok, azonban – szemben például Kínával – ez nem jelentette az állam és a gazdasági szereplők fuzionális összefonódását, ellenben sok esetben jelentős érdekellentétek alakultak ki, ami adódik a piacok struktúrájából, az állam és gazdasági szereplők közötti kapitalista államfelfogás tradicionális ellentéteiből.[63] Szintén teljesen más képet mutat az egyéni adatok kezelhetősége ezen államok esetében. Sok esetben a transznacionális vállalatok gazdasági érdekeik fokozott érvényesítése érdekében a kezelt adatokkal visszaéltek, amely bár jelentős bírságot eredményezett, azonban gazdasági helyzetükben, társadalomban betöltött szerepükben ez nem jelentett változást. Itt az állam, vagy azok közössége próbál egyre szigorúbb szabályokat alkotni.[64] Másik oldalról az állam, a biztonsági környezet átalakulása miatt, próbálja a nemzetbiztonság sebezhetőségét csökkenteni és az ehhez kapcsolódó információ éhséget csillapítani. Ez pedig ellentétes a gazdasági és az egyéni szereplők érdekeivel, emellett az alkotmányosan körül határolt állami működés miatt jelentős akadályokba ütközik, melyet sok esetben hangos ellenkezés, nemzetközi bírói fórumok előtti fellépés követett.[65] ***Ebben a közegben elképzelhetetlen volna az egyén, vagy akár a gazdasági szereplők feletti felügyelet még közel hasonló szintjének a kialakítása is, mint amit Kínában láthattunk. A kontrolleszközökön túl, a kibertérhez való hozzáférés korlátozása sem képzelhető el olyan mértékben, mivel egyes államok egyenesen alapjogoként tekintenek az internethez való hozzáférésre, de más államok esetében is garanciák garmadája védi azt.***[66] Emellett ez jelentősen szembemenne gazdasági szereplők profitorientált érdekeivel is. Ezek a megállapítások a békeidős, normál működésre igazak, ezeket jelentősen

[61] Ezzel kapcsolatos jogi dilemmákat lásd bővebben: SOMKUTAS Péter – KŐHIDI Ákos: *Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó?* In In Media Res, 2017/2. szám, 232-269. o.; CSITEI Béla: *Az önvezető járművek és az Európai Unió joga.* In LÉVAYNÉ FAZEKAS Judit – KECSKÉS Gábor (szerk.): Az autonóm járművek és intelligens rendszerek jogi vonatkozásai, Győr, Universitas-Győr Nonprofit Kft, 2020, 55-73. o.

[62] KESERŰ Barna: *A mesterséges intelligencia néhány magánjogi aspektusáról.* In GLAVANITS Judit (szerk.): A gazdasági jogalkotás aktuális kérdései. Budapest, Dialóg Campus, 2019, 109-123. o.

[63] SZIGETI Péter: *Kapitalizmus és a tőkés termelési mód elmélete.* In Eszmélet, 2019, 1-59. o.; PONGRÁCZ Alex: *Az állam gazdaságpolitikai szerepvállalásának változásai.* In Pro Publico Bono, 2017/3. szám, 168-195. o.

[64] Például GDPR rendelet szabályanyaga és gyakorlata. Lásd bővebben: SEPSI Tibor: *GDPR útikalauz adatkezelőknek.* Budapest, Wolters Kluwer, 2019. Egyéb területeken is akut problémák forrása: G. KARÁCSONY Gergely: *A videójátékok adatkezelési gyakorlata: kommunikáció és profilalkotás.* In G., KARÁCSONY Gergely (szerk.): A videojátékok jogi kérdései. Győr, Széchenyi István Egyetem, 2021, 25-38. o.

[65] Lásd a svéd és brit példát: Catalin CIMPANU: *Sweden and UK's surveillance programs on trial at the European Court of Human Rights.* In ZDNet, 2019. 07. 12.

[66] GOSZTONYI Gergely: *Az internet-hozzáférés korlátozásának gyakorlata az Emberi Jogok Európai Bírósága előtt.* In In Medias Res, 2021/1. szám, 91-101. o.

transzformálná egy klasszikus államközi konfliktus, vagy belső rendet támadó szélsőséges események, amelyeket egy teljesen más felhatalmazási közegben kellene az államnak megoldania. Egy ilyen helyzet elkerülése azonban minden érdekelt számára elsődleges érdekké kezd válni.

Az elmúlt évek konfliktusai, társadalmi feszültségei világossá tették, hogy valamiféle elmozdulás szükséges a biztonság digitális terrénumának fokozása frontján is, hiszen lassan a hétköznapok részévé válnak a zsarolóvírusok, a szolgáltatás megtagadó támadások, trollok tevékenysége,[67] amelyek más államokhoz vagy sok esetben a szervezett bűnözéshez kapcsolódtak.[68] A Covid-19 járvány mellett megjelent infodemia,[69] vagy a social media platformok szűrőbuborék gyakorlata,[70] a fake news, a deepfake tartalmak már olyan irányba vitték el a véleménynyilvánítás szabadságát, ahol az egyén már sokszor nem tud különbséget tenni valós és valótlan tartalmak között. Az átlagos felhasználót jelentősen befolyásolják a véleményük, döntésük kialakítása során. Az ezekkel szembeni – jogállai keretek közötti – fellépés fontosságát mutatja, hogy az Európai Unió is szorosabb jogi keretek közé kívánja helyezni a social media platformok működését és átláthatóbbá kívánja tenni a szűrési mechanizmusokat is.

Ezek a feszültségek pedig egyértelműen kéz a kézben járnak a hagyományos tér biztonságának korróziójával is, mivel főként a külső szereplő általi szcenáriók abba az irányba is hatnak, hogy negatívan befolyásolják a közbizalmat. Ezeknek a kampányoknak a hatását erősítik, illetve létrejöttét lehetővé teszik egyik oldalról a lawfare, vagyis a joggal való rosszindulatú visszaélés[71], valamint az

[67] Jessika ARO: *Putyin trolljai – Igaz történetek az orosz infoháború frontvonalából*. Budapest, Corvina, 2021.

[68] MEZEI Kitti: *A szervezett bűnözés az interneten.* In MEZEI Kitti (szerk.): A bűnügyi tudományok és az informatika, Pécs, Budapest, Pécsi Tudományegyetem, MTA TK, 2019, 125-147. o.

[69] A fogalmat a WHO vezette be és a következőképpen határozta meg: „az infodémia egy problémával kapcsolatos túlzott információáradat, amely megnehezíti a megoldás azonosítását. Magában foglalja az egészségügyi szükséghelyzet során terjedő félretájékoztatást, dezinformációt és pletykákat. Az infodémia hátráltathatja a hatékony népegészségügyi válaszintézkedéseket, továbbá zavart és bizonytalanságot kelthet az emberek körében." Lásd: WHO: Coronavirus disease 2019 (COVID-19) Situation Report - 45. o.

[70] KOLTAY András: *A social media platformok jogi státusa a szólásszabadság nézőpontjából.* In In Media Res. 2019/1. szám, 1-56.o.

[71] A lawfare egy régóta ismert napjainkban folyamatosan szélesedő, de a hadviselési felfogásból kinövő értelmezési keret, amely a jogi normákat, vagy azok lehetséges értelmezését fordítja a szembenálló fél ellen. Lásd: PETRUSKA Ferenc – VIKMAN László: *Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából.* In Military and Intelligence CyberSecurity Research Paper, 2021/4. szám, 1-18. o.; HÓDOS László: *A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai.* In Honvédségi Szemle, 2020/4. szám, 49-64. o.; FARKAS Ádám – RESPERGER István: *Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai.* In FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020, 132-149. o.; VIKMAN László: *A műveletszervezés jogi feladatai.* In Honvédségi Szemle, 2021/2. szám, 44-56. o.

államok jogi sérülékenysége[72] is, amelynek köszönhetően „… kételyt, bizalmatlanságot szítsanak és megosszák a társadalmat."[73] Vagyis a transzatlanti térség jogállamisági garanciáit szükségszerűen figyelembe vevő nemzetbiztonsági szabályrendszere ismét a figyelem középpontjába került, ugyanis „… ha a védelmi és biztonsági funkciók szabályozása nem kellően korszerű, nem kellően konzisztens, nem kellően stabil és kiszámítható, akkor az az állammal szembeni bizalom erózióját eredményezheti"[74]. Ezzel az általános mechanizmust és az ahhoz kapcsolódó jogrendet is megkérdőjelezik. Így „… a társadalmi félelemek eszkalálódnak… Ez persze egy negatív spirált eredményez. Minél inkább teszik ezt, annál nagyobb a zűrzavar és az erőszak, és minél nagyobb a zűrzavar és az erőszak, annál kevésbé képesek az államok a helyzet kezelésére, következésképp annál több ember vonja meg a bizalmát az államtól…"[75] Vagyis a közrendbe és az azt szavatoló államba vetett bizalom elvesztése annulálná a biztonságot, ezáltal felszámolná a normál állapotot,[76] alapjaiban alakítaná át a mai ismert transzatlanti térséget.

Ezzel pedig meg is érkeztünk ahhoz az indokhoz, amiért a nyugati pólus államainak három fontos szereplője az állam, a gazdasági aktorok és az egyén az együttműködés terepére kell, hogy lépjenek. A cyberfare state a transzatlanti térségben úgy formálható, alakítható ki tehát, hogy közben mindenféleképpen szavatolni kell a jogállam alapvető szegmenseit, de mindeközben meg kell teremteni a biztonsággal való egyensúlyt. Vagyis szemben a smart total control cyberfare state-tel a totális biztonság felé való elmozdulás nem eredményezheti a szabadság felolvadását. Emellett azonban egyensúlyba kell hozni az egyéni és gazdasági érdekeket a valós biztonsági környezettel. Ugyanis a gazdasági szféra érdeke is a működőképes állami, gazdasági és társadalmi alrendszerek, amelyek nélkül elképzelhetetlen volna a kapitalista gazdálkodás megfelelő működése, a befektetések biztonságának a szavatolása. Ezt jól mutatják az ukrán-orosz háború jelenlegi gazdasági hatásai és visszásságai,

[72] Szemben a lawfare esetkörével a jogi sérülékenység a komplex biztonsági felfogáshoz illeszkedő kategória, amely a társadalmi rezíliencia egyik fontos összetevője. Lásd: Aurel SARI: *Legal Resilience in an Era of Grey Zone Conflicts and Hybrid Threats*. In Exeter Centre for International Law Working Paper 2019/1. szám; FARKAS Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

[73] Yvonne HOFSTETTER: *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Budapest, Corvina, 2020, 85. o.

[74] FARKAS Ádám: A *kortárs technológia-fejlődés és innováció viszonya a honvédelmi szabályozással.* In MTA Law Working Paper, 2021/4. szám, 4. o.

[75] SZIGETI Péter: *Vázlat a közbiztonság három dimenziójáról: világrendszer – nemzetállami szint és lokalitás.* In SZIGETI Péter: A valóság vonzásában – Jogelméleti és Jogtudományi Közlöny, Győr, ELTE-SZIF ÁJK, 2001. (https://mek.oszk.hu/04200/04241/04241.htm#16)

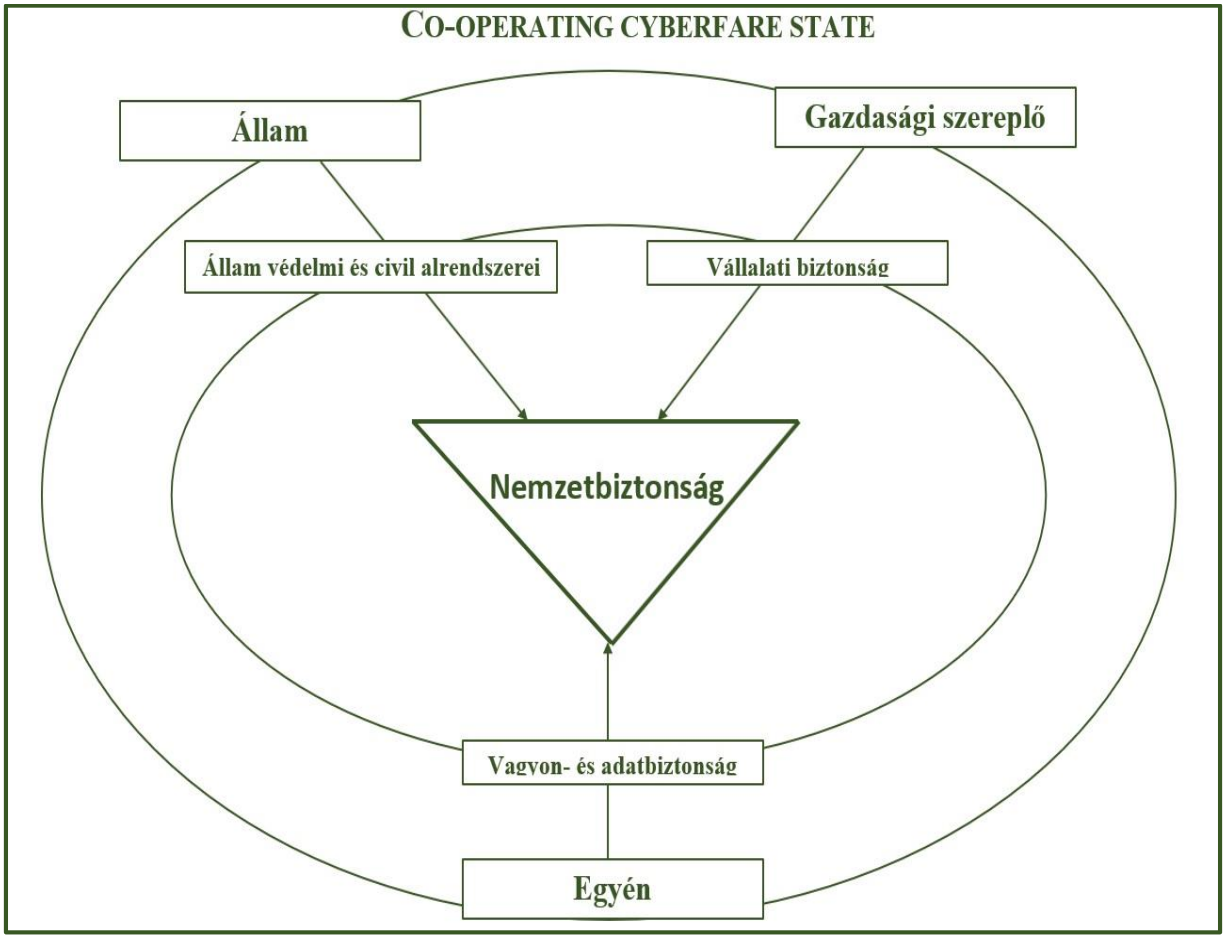
[76] A biztonság társadalmi érzetének fontosságát, normál állapotot fenntartó jellegét jól érzékelteti Márai Sándor: „A biztonság ebből az érzésből épült fel ötvenmillió ember számára: hogy a császár éjfél előtt lefekszik, s már reggel ötkor felkel és gyertyafény mellett ül, amerikai fonott nád karosszékében, íróasztalánál, s a többiek, akik felesküdtek az ő nevére, mind engedelmeskednek a szokásoknak és a törvényeknek." – MÁRAI Sándor: *A gyetyák csonkig égnek.* Budapest, Helikon Kiadó, 2008, 47.o.

továbbá a már jelzett hosszútávú hatások és törekvések (például Európa energetikai és védelmi önállósítása, mezőgazdasági hatásai stb.), de ezt erősítették a Covid-19 világjárvány gazdasági hatásai is, illetve jelentősebb terrortámadásokat követő tőzsdei reakciók is. Az egyén szempontjából az adatai integritása, a tulajdon védelme, a normális életmechanizmusok biztosítása csak működő állami intézményrendszer mellett képzelhető el. Az elmúlt években átalakult biztonsági környezet már alapjaiban támadja ezeket az alrendszereket, aminek rendkívül veszélyes fordulópontját jelenti az orosz-ukrán háború.

Az állam-gazdaság-társadalom kölcsönhatásos fungálására előnyként építő almodellt együttműködő vagy co-operating cyberfare state-nek nevezhetjük, ahol az együttműködés kiindulópontja szintén a jóléti, szociális digitalizáció. Ennek során a felek között olyan multidiszciplináris megközelítésen nyugvó legjobb gyakorlatot kell kialakítani, amely a jogállami garanciák mellett, a biztonság hatékonyságát is előtérbe helyezi. Ennek a legjobb gyakorlatnak magába kell foglalnia az állami szereplők, ezen belül a civil és katonai karakterű szervek[77] tapasztalásait, elvárásait, elméleti megközelítéseit, továbbá a gazdasági szereplők ugyanezen aspektusait, valamint a kutatói, innovációs oldalról nem kizárólag a műszaki tudományok képviselőit, hanem a társadalomtudományok (jogász, szociológus, közgazdász) és a hadtudomány művelőit is be kell vonni a munkába.[78]

[77] Katonai karakterű szervek fogalmáról lásd bővebben: FARKAS Ádám: *A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben.* In Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata, 2012/elektronikus szám, 3-6. o.

[78] FARKAS Ádám: *A multidiszciplinaritás helye, szerepe a védelem és biztonság szabályozásának és szervezésének komplex kutatásaiban.* In Közjogi Szemle 2021/4. szám, 22-28. o.; FARKAS Ádám: *A történelmi tapasztalat és a tudomány helye, szerepe a 21. századi védelmi és biztonsági gondolkodásban.* In Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/1. szám.



Co-operating cyberfare state modellje (saját szerkesztés)

Deklarációk, policyk, stratégia alkotás vonalán számos ilyen együttműködés megvalósulását vetítették előre, amelyek közül több már a megvalósítás pályájára is lépett. Ilyennek tekinthető az egyes kiberbiztonsági stratégiák,[79] a NATO reziliencia programjai,[80] egyes államok kibervédelmi képességeinek kialakítása.[81] Az olyan

[79] VIKMAN László: *Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán.* In SmartLaw Research Group Workin Paper 2022/1. szám.

[80] Lásd: MOLNÁR Ferenc: A *reziliencia kérdése és a NATO.* In Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok, 2021/15. szám; FARKAS Ádám – SPITZER Jenő: *Az információs korszak és az állami reziliencia egyes kérdései.* In Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok, 2021/18. szám; KESZELY László: *Hibrid hadviselés és nemzeti ellenálló képesség (resilience), avagy átfogó megközelítés újratöltve.* In Katonai Jogi és Hadijogi Szemle, 2018/1. szám, 29-62. o.; VIKMAN László: *A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra,* In Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14. szám.

[81] FARKAS Ádám: *Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán.* In Military and Intelligence CyberSecurity Research Paper, 2021/1. szám; VIKMAN László: *A német kiberbiztonsági szisztéma áttekintése: Szervezeti keretek, különös tekintettel a nemzetbiztonsági*

össztársadalmi problémákat orvosló programok azonban, mint amilyenek például az Európai Unió többször meghirdetett a dezinformációval szembeni média tudatos nevelése több év elteltével is csak a deklarációk szintjén létezik.[82] E területen érdemi elmozdulást jelenthet az új digitális szolgáltatókkal kapcsolatos jogalkotás,[83] illetve az állami hozzáállás változása.[84] Az egyén szintjéig ható, ténylegesen megvalósuló programokkal azonban nem igazán találkozhatunk, talán azért, mert eddig igazán akuttá a probléma nem alakult, káros hatásai viszont jelentős számban most is megfigyelhetőek.[85]

A jogállami keretek között működő cyberfare state esetében, a 21. század biztonsági környezetében nem hagyható figyelmen kívül az egyén szerepe sem; nem véletlen, hogy a konkuráló államok mindent megtesznek annak érdekében, hogy az egyént, az egyéni döntés szabadságát kikapcsolják, hiszen a rendszer szempontjából a legjelentősebb biztonsági kockázatot továbbra is az emberek, az egyének jelentik. Ebből adódóan a co-operating almodell államaink jogállami keretek közötti válaszokat kell találniuk erre a kérdésre is, jelenleg azonban az látszik, hogy nem igazán tudnak mit kezdeni az egyéni szereplők tömegével, nem igazán tudják a helyüket definiálni a biztonsági környezetben, annak ellenére – ahogy a lenti ábrán látszik is –, hogy mind az állam, mind pedig a gazdasági szereplők alrendszereiben aktívan közreműködnek.

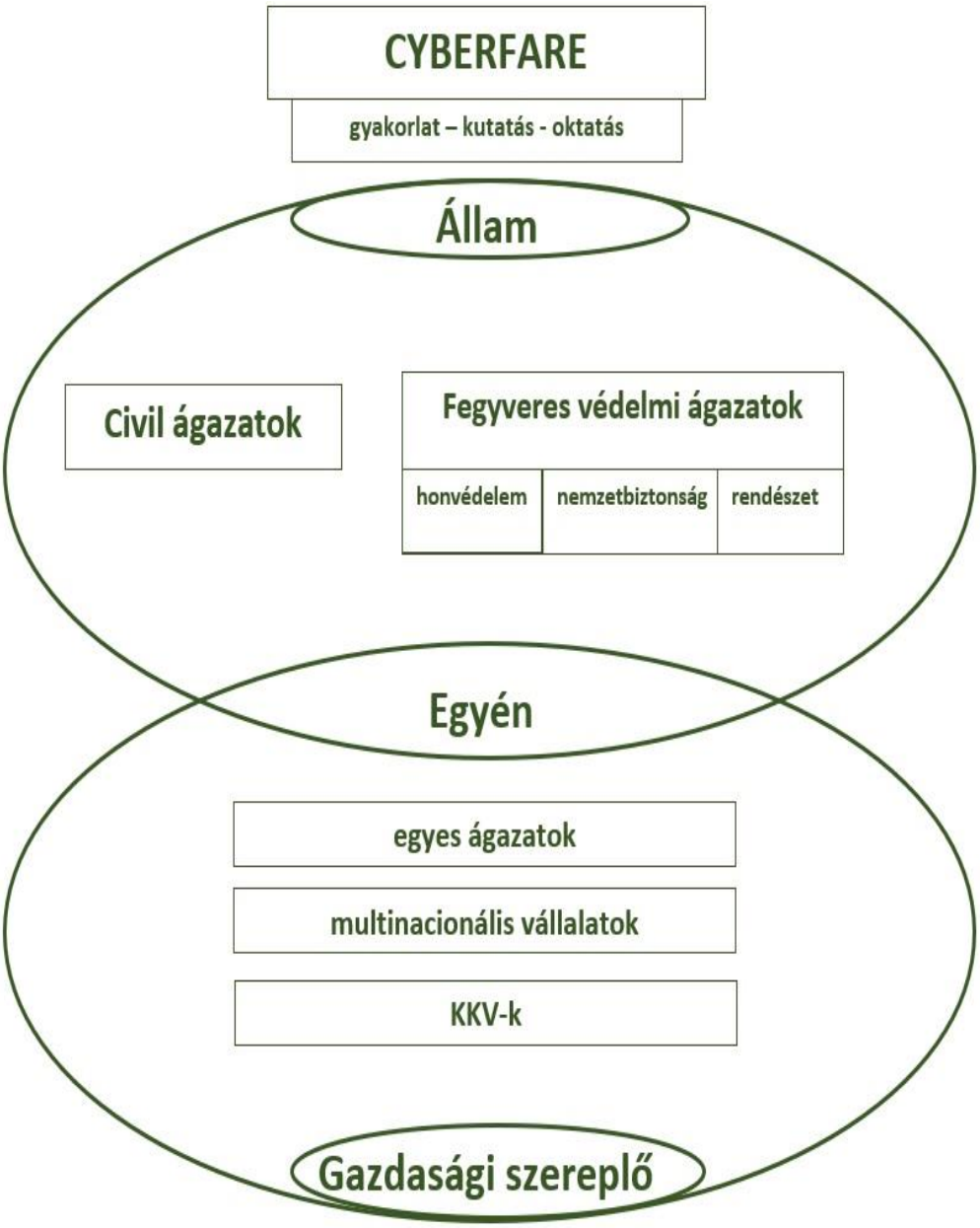
szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. In Military and Intelligence CyberSecurity Research Paper, 2021/2. szám.

[82] Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Brüsszel, 2018.12.15., Join(2018)36. Final; Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. Brüsszel, 2020.12.3. COM(2020) 790 Final.

[83] Az Európai Bizottság javaslat Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, Brüsszel, 2020.12.15., 2020/0361(COD).

[84] Gosztonyi Gergely: *Az internetes tartalomszabályozással kapcsolatos új gondolkodási irányok az Amerikai Egyesült Államokban.* In Miskolci Jogi Szemle, 2021/4. szám, 40-54. o.

[85] Mary Aiken: *Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést?* Budapest, Harmat – Új Ember, 2020.; Douglas Murray: *A tömegek tébolya – Áldozatok a politikai korrektség oltárán?* Budapest, Alexandra, 2020.



Az egyén relevanciája kibertérben a co-operation cyberfare state esetében (saját szerkesztés)

Az egyének munkaerőként és fogyasztóként is aktív szereplők, akik mindkét szerepükben potenciális veszélyforrások az állami és gazdasági rendszerekre, és természetesen ugyanekkora mértékben a saját adatvagyonukra vagy hagyományos tulajdonukra. Így szükségszerű volna meghaladni azt a felfogást, hogy az egyéni felelősség szintjére engedjük ezeknek a problémáknak a megoldását, amelyben még magára is hagyjuk az egyes szereplőket, azoknak tényleges tudása, képzettségi szintjétől függetlenül. E körben az együttműködés állami vonatkozásai és különösen a védelmi-biztonsági szegmense kapcsán is komoly lemaradást kell ma behozni a biztonságtudatosság szintjén,

amivel a kibertérrel összefüggő biztonságfelfogást is szinkronizálni kell.[86]

Ezen államok esetében átfogó oktatási projekteket kell kidolgozni az iskolarendszer minden szintjén, hiszen ma már nemcsak kizárólag a magas kvalifikációt megkövetelő munkakörökben kerülnek az emberek kapcsolatba a kibertérrel és annak egyes alrendszereivel, hanem azok a hétköznapok részévé is váltak.[87] Fájdalmasan kijózanító jelenségként lehetett elkönyvelni, hogy az okoseszközök világában, például a Covid-19 ellen védő vakcinákra történő regisztrációs rendszer elérése, kitöltése egyes egyének számára megoldhatatlan feladatot jelentett (itt nem a rendszer eléréséhez szükséges infrastruktúra hiányára kell gondolni vagy az idős állampolgárokra), míg ugyanők a hétköznapok során számos rendszerhez férnek hozzá. Ma már a felsőoktatásban sincs olyan oktatási terület, amelynek képzésébe ne volna feltétlenül szükséges beépíteni ezeket a készségeket, mert adott esetben vezetőként fog ezek hiányában dönteni az egyén a területet is érintő fontos kérdésekről, vagy ezeket nem ismerve működtett társadalmi alrendszert a potenciális veszélyforrásokat fel nem ismerve, ismertetve (például óvodai, iskolai nevelés). S legalább ugyanilyen fontos ezekben a problémákban a nyomonkövetes kérdése, hiszen a mindenkori új kihívásokhoz kell igazítani magát a képzést is. Ezek megvalósítása tovább már nem várathat magára,[88] hiszen a káros hatások már ténylegesen megindítottak akár deviáns folyamatokat is a társadalmon

[86] BÁNYÁSZ Péter – KRASZNAY Csaba – TÓTH András: *A NATO kibervédelmi szakpolitikája.* In SZENES Zoltán (szerk.) A mai NATO: A szövetség helyzete és feladatai, Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft.,2021, 130-149. o.; Annamária BELÁZ – Csaba KRASZNAY – Zsolt SZABÓ: *Cybersecurity Strategy and Leadership Managment Issues.* In Živan ŽIVKOVIĆ (szerk.): An international serial publication for theory and practice of Management Science - IMCSM Proceedings(2020), Bor, University of Belgrade, Technical Faculty in Bor, Engineering Management Department (EMD), 2020, 242-252. o.; KISS Attila – KRASZNAY Csaba: *A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai.* In Információs Társadalom: Társadalomtudományi Folyóirat, 2017/1. szám, 55-71. o.; FARKAS Ádám: *A védelmi-biztonsági gondolkodás és képzés megújításának elméleti és kulturális alapjai.* In Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/2. szám.

[87] A sérülékenységet és az oktatás szükségességét jól példázza az alábbi megállapítás: „Minden IT-biztonsági szakértő tisztában van vele, hogy a kibertérben a leggyengébb láncszem a humán faktor; a munkavállalók, akik – emberi természetükből fakadóan – jóhiszeműek, megtéveszthetőek, megfélemlíthetőek, nincsenek is tisztában a lehetséges kockázatokkal; éppen azért az ún. social engineering támadások célpontjai. Napjaink digitalizált világában minden munkavállaló kapcsolatba kerül számítógépes rendszerekkel, bizalmas adatokat kezel, és éppen ezért potenciális rizikóforrás. Ez a kockázat tovább növekszik azáltal, ha a munkavállaló a céges környezeten kívül, mérsékelt ellenőrzés mellett tevékenykedik." NÉMETH Richárd: *A COVID-19 járvány okán bevezetett Home Office munkavégzés hatása a munkakörülményekre és szervezeti kommunikációra nagyvállalati környezetben.* In Jog Állam Politika, 2021/4. szám, 101. o.

[88] Erre is tökéletes példa az infodémia kérdésköre, amikor az emberek jelentős hánya hitt el olyan fake news híreket, amely szerint az oltások HIV-et okoznak, chipet ültetnek az emberi szervezetbe, népírtást követnek el velük stb. Lásd: https://www.webbeteg.hu/cikkek/fertozo_betegseg/17762/tenyek-es-tevhitek-az-oltasokrol.

belül,[89] amelyek a halogatás révén nehezen visszafordíthatóak. Nem feledve az alapfelvetést, ha ezeket a társadalmi, biztonsági kihívásokat nem tudják kezelni a transzatlanti régió államai, abból végső soron az ellenpólus államainak intézményes győzelme is kialakulhat, amellyel önön képét veszítheti el a régió.

ÖSSZEGZÉS HELYETT

A cyberfare state mindegyik modelljében a kiindulópont a kibertérhez kapcsolódó rendszerek által az állam jóléti, szociális rendszereinek reformja, valamint a szolgáltató közigazgatás újradefiniálása. Emellett viszont jelentős eltérések mutatkoznak abban, hogy miként viszonyulnak ezeknek a rendszereknek a védelem és biztonság-szavatolás (angolszász megközelítésben: nemzetbiztonság) területén történő alkalmazásához.

A smart total control cyberfare state államfelfogása e körben visszanyúl a warfare state egyes jegyeihez, fúziót képez a gazdasági szereplők és az állam között, amelynek eredményeként a lehető legteljesebb mértékben kívánja kontrollálni polgárait és a kiberterét. Ennek során kidomborítják az állam hatalmi aspektusait, és saját biztonságuk szavatolását csak a hatalom révén, az erő által látják biztosítottnak. Így a „külső" kibertérben is aktívan használják a modern technológia által biztosított eszközöket.

A nyugati államok esetében is jelentős mértékű volt a digitalizáció, így eme folyamatok jelentős hatást gyakoroltak a társadalomra, gazdaságra és beágyazódtak a közigazgatási alrendszerekbe is. Az államra gyakorolt hatásuknak köszönhetően megteremtették a co-operating cyberfare state alapjait, vagyis a szereplők közötti folyamatos interakciót. Azonban a pozitív hozadékok mellett, mint fentebb láttuk számos negatív biztonsági tapasztalás is hatással volt ezen típusú államokra is, így az állami és nem állami szereplők által képviselt erőszakos, jogellenes fenyegető fellépések és támadások kibereszközökkel való felerősítése, illetve a hagyományos fenyegetések kibertéri lehetőségekkel való kombinálása. Amely szükségszerűvé teszi, hogy ezen államok esetében fokozódjon az egyes szereplők közötti együttműködés. Ebben viszont jelentős eltérés mutatkozik a másik almodellhez képest, hiszen az egyénhez való viszonyulás teljesen más képet mutat, hiszen a jogállami keretek (békeidős) megtartása nem teszik lehetővé a polgárok fenti mértékű korlátozását. Sajátos, hogy szemben a másik almodellel, ebben az almodellben az egyes szereplők alapvetően ellenérdekeltek mégis a megváltozott környezetben szükségszerű az együttműködésük. Ezen kooperációnak a biztonsággal kapcsolatos területek valamennyi szegmensére ki kell terjednie, kiemelten a modern technológia vívmányaira. Az együttműködésnek pedig egy legjobb gyakorlatot kell létrehozni, megújítva a jelenlegi alrendszereket.

Fontos, hogy az ezáltal kialakított rendszernek nem eseti jelleggel, nem pillanatnyi kihívásokat kell kezelnie, hanem átfogó, rendszerszintű és hosszútávú megoldást kell létrehoznia mindezt a jogállami attribútumok fenntartása mellett.

[89] KISS Tibor: Agresszió a cybertérben. Budapest, Nemzeti Közszolgálati Egyetem, 2020.; KISS Tibor – PARI Katalin – PRAZSÁK Gergő: *Cyberdeviancia.* Budapest, Dialóg Campus, 2019.

„Rendeltetése ugyanis a totálissá váló biztonsági kihívások megelőzésén, elhárításán, illetve felszámolásán túl pontosan az, hogy kitörjünk a my lai-i, abu ghraibi, guantanamoi és egyéb árnyékokból, s valóban rendezett, átgondolt, a kor kihívásaihoz igazodó, de egyben jogállami"90 biztonsági modellt, legjobb gyakorlatot teremtsünk meg.

Ennek során azt is látni kell, hogy univerzális, minden államra, régióra alkalmazható megoldások nincsenek. A transzatlanti térség államai kulturálisan és történeti hagyományaikat tekintve rendkívül sokszínűek, így a kialakítandó rendszer esetében a nemzeti sajátosságokat, történeti, társadalmi tradíciókat szükséges figyelembe venni. Emellett az egyes megoldásoknak idomulniuk kell az alkalmazott szinthez, hiszen más igény formálódik meg egy multinacionális vállalatnál és egy KKV esetében, illetve egy helyi önkormányzat vagy országos szervnél esetében. Az ellenőrzés, visszacsatolás, elemzés szükségszerű velejárója a rendszernek. A co-operating cyberfare state legjelentősebb kihívása az egyén elhelyezése ebben a rendszerben, tudatosságának kialakítása, megerősítése alapvető fontosságú a rendszer fenntartása, védelme és működtetése érdekében, amelyben a képzés, oktatás kiemelten hangsúlyos szerephez jut.

Ezen co-operating cyberfare state rendszereinek kialakítása átfogó reformot igényel, ami nélkül az átalakult biztonsági környezet kihívásaival (például hibrid konfliktusok ezen belül is kibertámadások, dezinformációk, radikalizmus, (kiber)terrorizmus stb.) hosszú távon nem tudnak eredményesen megküzdeni a transzatlanti térség államai. *A reformnak pedig ténylegesnek és átfogónak kell lennie és az orosz-ukrán háború geopolitikai történéseit látva azonnal meg kell indítani, ahol –az elmúlt évtizedek tapasztalásaival szemben – a reform nem abban rejlik, hogy a múlt fáradt és kopott ötleteit leporoljuk és újracsomagoljuk. Az igazi reform csak akkor valósulhat meg, ha elfogadjuk az új paradigmát és újradefiniáljuk az állam szerepét.*[91]

FELHASZNÁLT FORRÁSOK

[1] Aar Aaron F. BRANTLY – Nerea M. CAL – Devlin P. WINKELSTEIN: *Defending the Borderland - Ukrainian Military Experiences with IO, Cyber, and EW.* Army Cyber Institute at West Point, West Point, 2017.

[2] Abishur PRAKASH: *Go. AI – A mesterséges intelligencia geopolitikája.* Budapest, Pallas Athéné Könyvkiadó, 2018.

[3] Amaël CATTARUZZA: *A digitális adatok geopolitikája – A hatalom és konfliktusok a big data korában.* Budapest, Pallas Athéné Könyvkiadó, 2020.

[4] Annamária BELÁZ – Csaba KRASZNAY – Zsolt SZABÓ: *Cybersecurity Strategy and Leadership Managment Issues.* In Živan ŽIVKOVIĆ (szerk.): An

[90] FARKAS Ádám: *A totálitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 70. o.

[91] KALADIJAN: i. m. 103. o.

international serial publication for theory and practice of Management Science - IMCSM Proceedings(2020), Bor, University of Belgrade, Technical Faculty in Bor, Engineering Management Department (EMD), 2020, 242-252. o.

[5] ÁRVA László – PÁSZTOR Szabolcs – Victoria PYANATOVA: *A multinacionális vállalati stratégiák és a változó világkereskedelem kapcsolatáról.* In Gazdaság és Pénzügy, 2020/1. szám, 57-81. o.

[6] Asa BRIGGS: *The Welfare State in Historical Perspective.* In Christopher PIERSEN – Francis G. CASTEl (szerk.): The Welfare State Reader (Second Edition), Cambridge, Polity Press, 2006.

[7] Atanu BHUYAN: *Designing optimal welfare policies for intermediate publictransportation systems: A developing country perspective*. In Academia Letters.

[8] Aurel SARI: *Legal Resilience in an Era of Grey Zone Conflicts and Hybrid Threats*. In Exeter Centre for International Law Working Paper 2019/1. szám.

[9] BÁNYÁSZ Péter – KRASZNAY Csaba – TÓTH András: *A NATO kibervédelmi szakpolitikája.* In SZENES Zoltán (szerk.) A mai NATO: A szövetség helyzete és feladatai, Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft.,2021, 130-149. o.

[10] Ben DUBOW – Edward LUCAS – Jake MORRIS: *Jabbed in the Back: Mapping Russian and Chinese Information Operations During Covid-19.* The Center for European Polidy Analysis (CEPA), 2020.

[11] BŐGEL György: *A big data ökoszisztémája,* Budapest, Typotex, 2015.

[12] Bruce D. PORTER: *The Warfare State*. In American Heritage, 1994/4. szám (https://www.americanheritage.com/warfare-state#1).

[13] Bruce D. PORTER: *War and the Rise of the State – The Military Foundations of Modern Politics.* New York, The Free Press, 1994, 7. fejezet War and the American Goverment.

[14] BUDAI Balázs: *Az e-közigazgatás fogalma, jogi és stratégiai keretei.* Budapest, Dialóg Campus, 2017.

[15] Catalin CIMPANU: *Sweden and UK's surveillance programs on trial at the European Court of Human Rights.* In ZDNet, 2019. 07. 12.

[16] CSITEI Béla: *Az önvezető járművek és az Európai Unió joga.* In LÉVAYNÉ FAZEKAS Judit – KECSKÉS Gábor (szerk.): Az autonóm járművek és intelligens rendszerek jogi vonatkozásai, Győr, Universitas-Győr Nonprofit Kft, 2020, 55-73. o.

[17] David EDGERTON: *Warfare State – Britain, 1920-1970.* Cambridge, Cambridge University Press, 2006, 59-107. o.

[18] Douglas MURRAY: *A tömegek tébolya – Áldozatok a politikai korrektség oltárán?* Budapest, Alexandra, 2020.

[19] DUSEK Tamás: *Az okos városok komplex mutatószámainak egyes*

tartalmi és módszertani problémái. In KOVÁCS Gábor – VÖLGYI Katalin (szerk.): Üzleti vállalkozások, makro- és mikrokörnyezetük gazdálkodási és menedzsment sajátosságai" c. kutatás tanulmányai. Győr, Széchenyi István Egyetem Kautz Gyula Gazdaságtudományi Kar, 2018, 1-3. o.

[20] ENGEL Péter: *A Bundeskartellamt Facebook-döntése – az adatgyűjtés versenyjogi kockázatai.* In Verseny Tükör, 2019/1. szám, 70-76. o.

[21] FARKAS Ádám – RESPERGER István: *Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai.* In FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020, 132-149. o.

[22] FARKAS Ádám – SPITZER Jenő: *Az információs korszak és az állami reziliencia egyes kérdései.* In Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok, 2021/18. szám.

[23] FARKAS Ádám: *A fegyveres védelem mint állami alrendszer és annak szabályozási sajátosságai.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

[24] FARKAS Ádám: *A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben.* In Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata, 2012/elektronikus szám.

[25] FARKAS Ádám: A *kortárs technológia-fejlődés és innováció viszonya a honvédelmi szabályozással.* In MTA Law Working Paper, 2021/4. szám, 4. o.

[26] FARKAS Ádám: *A multidiszciplinaritás helye, szerepe a védelem és biztonság szabályozásának és szervezésének komplex kutatásaiban.* In Közjogi Szemle 2021/4. szám, 22-28. o.

[27] FARKAS Ádám: *A totálitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

[28] FARKAS Ádám: *A történelmi tapasztalat és a tudomány helye, szerepe a 21. századi védelmi és biztonsági gondolkodásban.* In Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/1. szám.

[29] FARKAS Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

[30] FARKAS Ádám: *A védelmi-biztonsági gondolkodás és képzés megújításának elméleti és kulturális alapjai.* In Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/2. szám.

[31] FARKAS Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2019.

[32] FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei.* In SmartLaw Research Group Working Paper, 2021/1. szám, 1-13. o.

[33] FARKAS Ádám: *Gondolatok a totalitás 21. századi esszenciájához.* In PONGRÁCZ Alex (szerk.): Ünnepi tanulmányok a 65 éves Cs. Kiss Lajos tiszteletére. Út vocatio scientia, Budapest, Ludovika Egyetemi Kiadó, 2021, 65-80. o.

[34] FARKAS Ádám: *Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán.* In Military and Intelligence CyberSecurity Research Paper, 2021/1. szám.

[35] FERENCZ Jácint: *Az információ és a technológia kettős arca a munkajogban.* In Baranyiné Kóczy Judit – Fehér Ágota (szerk.): Pedagógusképzés, oktatás a Kárpát-medencében, társadalmi kontextusok. XXII. Apáczai-napok Tudományos Konferencia tanulmánykötet, Győr, Széchenyi István Egyetem Apáczai Csere János Kar, 2019.

[36] Fred J. COOK: *The Warfare State.* In The Annals of the American Academy of Political and Social Scince, 1964/1. szám, 102-109. o.

[37] G. KARÁCSONY Gergely: *A videójátékok adatkezelési gyakorlata: kommunikáció és profilalkotás.* In G., KARÁCSONY Gergely (szerk.): A videojátékok jogi kérdései. Győr, Széchenyi István Egyetem, 2021, 25-38. o.

[38] G. KARÁCSONY Gergely: *Okoseszközök - okos jog?* Budapest, Ludovika Egyetemi Kiadó, 2020.

[39] GELLÉN Klára: *Tisztességtelen kereskedelmi gyakorlatok az online térben – fókuszban a közösségi média*. In In Medias Res, 2020/1. szám, 127-140. o.

[40] Gøsta ESPING-ANDERSEN: *A Welfare State for the Twenty-first Century.* In: Christopher PIERSEN – Francis G. CASTEL (szerk.): The Welfare State Reader (Second Edition), Cambridge, Polity Press, 2006.

[41] Gøsta ESPING-ANDERSEN: *Towards the Good Society, Once Again?* In Gøsta ESPING-ANDERSEN (szerk.): Why We Need a New Welfare State, Oxford – New York, Oxford University Press, 2002.

[42] GOSZTONYI Gergely: *Az internetes tartalomszabályozással kapcsolatos új gondolkodási irányok az Amerikai Egyesült Államokban.* In Miskolci Jogi Szemle, 2021/4. szám, 40-54. o.

[43] GOSZTONYI Gergely: *Az internet-hozzáférés korlátozásának gyakorlata az Emberi Jogok Európai Bírósága előtt.* In In Medias Res, 2021/1. szám, 91-101. o.

[44] GOSZTONYI Gergely: *Special Models of Internet and Content Regulation on*

China and Russia. In ELTE Law Journal, 2021/2. szám, 87-99. o.

[45] Gregory M. KALADIJAN: *Welfare vs Cyberfare*. In Journal of Children and Proverty, 1996/1. szám, 93-104. o.

[46] HÓDOS László: *A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai.* In Honvédségi Szemle, 2020/4. szám, 49-64. o.

[47] HOLLÓ Bettina: *Földi László a háborúról: Állásfoglalásra késztetnek, de az igazság magjától is eltántoríthatnak.* In Index (https://index.hu/belfold/2022/03/06/haboru-ukrajna-alhirek-biztonsagpolitika-foldi-laszlo-demko-attila/).

[48] HUSZÁK Dániel: *Példátlan információs háború zajlik Ukrajna körül – Elképesztő mennyiségű hazugság ömlik a világra.* In Portfolio (https://www.portfolio.hu/global/20220226/peldatlan-informacios-haboru-zajlik-ukrajna-korul-elkepeszto-mennyisegu-hazugsag-omlik-a-vilagra-529377).

[49] *Iran creates „Halal Internet" to control online information.* In RSF – Reporters without Borders. 2016. szeptember (https://rsf.org/en/news/iran-creates-halal-internet-control-online-information).

[50] James A. LEWIS: *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,* In Center for Strategic and International Studies, 2002 (https://www.steptoe.com/images/content/4/5/v1/4586/231a.pdf).

[51] James T. SPARROW: *Warfare State – World War II Americans and the Age of Big Government*. Oxford, Oxford University Press, 2011.

[52] Jarmo MAKELA: *Countering Disinformation: News Media and Legal Resilience.* In Hybrid CoE Paper. 2019/1. szám.

[53] Jessika ARO: *Putyin trolljai – Igaz történetek az orosz infoháború frontvonalából*. Budapest, Corvina, 2021.

[54] Joe TIDY: *Ukraine crisis: 'Wiper' discovered in latest cyber-attacks*. In BBC News, 2022. 02. 24. (https://www.bbc.com/news/technology-60500618).

[55] KÁNCZ Csaba: *Az orosz titkosszolgálatok és a szervezett bűnözés ijesztő kapcsolatrendszere.* In privátbankár.hu, 2021. (https://privatbankar.hu/cikkek/makro/az-orosz-titkosszolgalatok-es-a-szervezett-bunozes-ijeszto-kapcsolatrendszere.html).

[56] Keith L. NELSON: *The Warfare State: History of Concept.* In Pacific Historical Review, 1971/2. szám, 127-143. o.

[57] KELEMEN Roland – PATAKI Márta: *A kibertámadások nemzetközi jogi értékelése.* In Katonai Jogi és Hadijogi Szemle, 2015/1. szám, 53-90. o.

[58] KELEMEN Roland: *A polgári kor társadalombiztosítása - Társadalombiztosítási bíráskodás a polgári korban.* In Molnár Andrea – Széplaki László (szerk.): Tanulmányok a győri felsőbíráskodás történetéből a XIX-XX. század fordulóján, Győr, Győri Ítélőtábla, 2019, 149-174. o.

[59] KELEMEN Roland: *Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben.* In Jog Állam Politika, 2021/3. szám, 71-85. o.

[60] KESERŰ Barna: *A mesterséges intelligencia néhány magánjogi aspektusáról.* In GLAVANITS Judit (szerk.): A gazdasági jogalkotás aktuális kérdései. Budapest, Dialóg Campus, 2019, 109-123. o.

[61] KESZELY László: *Hibrid hadviselés és nemzeti ellenálló képesség (resilience), avagy átfogó megközelítés újratöltve.* In Katonai Jogi és Hadijogi Szemle, 2018/1. szám, 29-62. o.

[62] KISS Álmos Péter: *A hibrid hadviselés természetrajza.* In Honvédségi Szemle, 2019/4. szám.

[63] KISS Attila – KRASZNAY Csaba: *A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai.* In Információs Társadalom: Társadalomtudományi Folyóirat, 2017/1. szám, 55-71. o.

[64] KISS Tibor – PARI Katalin – PRAZSÁK Gergő: *Cyberdeviancia.* Budapest, Dialóg Campus, 2019.

[65] KISS Tibor: Agresszió a cybertérben. Budapest, Nemzeti Közszolgálati Egyetem, 2020.

[66] KOLLÁR Csaba: *Kína és a társadalmi kredit rendszere.* In Hadtudomány, 2020/2. szám, 79-97. o.

[67] KOLTAY András: *A social media platformok jogi státusa a szólásszabadság nézőpontjából.* In In Media Res. 2019/1. szám, 1-56.o.

[68] KOVÁCS László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

[69] Lásd: MOLNÁR Ferenc: A *reziliencia kérdése és a NATO.* In Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok, 2021/15. szám.

[70] Lina ROSENSTEDT: *Improving Cooperation with Social Media Companies to Counter Electoral Interference.* In Hybrid Coe Paper, 2021/5. szám.

[71] MÁRAI Sándor: *A gyetyák csonkig égnek.* Budapest, Helikon Kiadó, 2008, 47.o.

[72] Mary AIKEN: *Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést?* Budapest, Harmat – Új Ember, 2020.

[73] MEZEI Kitti: *A szervezett bűnözés az interneten.* In MEZEI Kitti (szerk.): A bűnügyi tudományok és az informatika, Pécs, Budapest, Pécsi Tudományegyetem, MTA TK, 2019, 125-147. o.

[74] NÉMETH Richárd: *A COVID-19 járvány okán bevezetett Home Office munkavégzés hatása a munkakörülményekre és szervezeti*

kommunikációra nagyvállalati környezetben. In Jog Állam Politika, 2021/4. szám.

[75] NÉMETH Richárd: *A kibertérből érkező fenyegetések elleni védekezés vállalati környezetben.* In GIKOF Journal, 2021.

[76] NÉMETH Richárd: *Kiberfenyegetettség nagyvállalati környezetben.* In Magyar Bűnüldöző, 2020/2. szám, 23-41. o.

[77] NÉMETH Richárd: *Kibertámadások gazdasági vonatkozásai a vállalati szférában.* In: DERNÓCZY-POLYÁK Adrienn (szerk.): Kutatási jelentés 1. Győr, Universitas-Győr Nonprofit Kft., 2019, 307-325. o.

[78] *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. Department of Justice, 2018. szeptember 6. (https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and).

[79] PATÓ Viktória Lila: *A háború hatása a közösségi médiára.* In Nemzeti Közszolgálati Egyetem Európai Stratégia Kutatóintézet (https://eustrat.uni-nke.hu/hirek/2022/03/01/a-haboru-hatasa-a-kozossegi-mediara).

[80] PESCHKA Vilmos: *A jog sajátossága*, Budapest, Akadémia Kiadó, 1988, 33. o.

[81] PETRUSKA Ferenc – VIKMAN László: *Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából.* In Military and Intelligence CyberSecurity Research Paper, 2021/4. szám, 1-18. o.

[82] PONGRÁCZ Alex – TÉGLÁSI András: *Szociális állam, jóléti állam – Elméleti és történeti alapvetés.* In BÓDI Stefánia – SCHWEITZER Gábor (szerk.): Az emberi jogok alkotmányos védelme Magyarországon, Budapest, Ludovika Egyetemi Kiadó, 2021.

[83] PONGRÁCZ Alex: *A politika folytatása más eszközökkel? Avagy gondolatok az állam és az erőszak kérdésköréről.* In Államtudományi Műhelytanulmányok, 2017/17. szám.

[84] PONGRÁCZ Alex: *Az állam gazdaságpolitikai szerepvállalásának változásai.* In Pro Publico Bono, 2017/3. szám, 168-195. o.

[85] PONGRÁCZ Alex: *Nemzetállamok és új szabályozó hatalmak a globális erőtérben – avagy megszelídíthető-e a globalizáció?* Budapest, Dialóg Campus, 2019.

[86] PÓTI László: *Minszk-2 után két évvel: Hol tart a békefolyamat?* In KKI Elemzések, 2017/5. szám.

[87] RAB Judit – SZEMEREY Samu: *Az okos város fejlesztési modell módszertani alapjai.* Budapest, Lechner Nonprofit Kft, 2018.

[88] Richard TITMUSS: *Universal versus Selection.* In Christopher PIERSEN –

Francis G. CASTEL (szerk.): The Welfare State Reader (Second Edition), Cambridge, Polity Press, 2006, 42-43. o.

[89] Sascha-Dominik BACHMANN – Hakan GUNNERIUSSON: *Hybrid Wars: The 21st Century's New Threats to Global Peace and Security.* In South African Journal of Military Studies, 2015/1. szám.

[90] SEPSI Tibor: *GDPR útikalauz adatkezelőknek.* Budapest, Wolters Kluwer, 2019.

[91] SOMKUTAS Péter – KŐHIDI Ákos: *Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó?* In In Media Res, 2017/2. szám, 232-269. o.

[92] SZALAI Ádám: *Az okosváros-koncepciók kritikai földrajzi vizsgálata – elméleti háttér és lehetséges kutatási irányok.* In Tér és Társadalom, 2020/2. szám, 88-107. o.

[93] SZÉPVÖLGYI Enikő: *A dualizmuskori állami gyermekvédelem és a szegényügy összefüggései*. In Jog Állam Politika, 2020/3. szám, 101-116.

[94] SZÉPVÖLGYI Enikő: *Gondolatok az állami gyermekvédelemről szóló törvénycikkek 120. évfordulójára.* In MEZEY Barna (szerk.): Kölcsönhatások. Európa és Magyarország a jogtörténelem sodrásában, Budapest, Gondolat Kiadó, 2021, 316-323. o.

[95] SZIGETI Péter: *Kapitalizmus és a tőkés termelési mód elmélete.* In Eszmélet, 2019, 1-59. o.

[96] SZIGETI Péter: *Társadalomkutatás – Mi végre? Politikatudomány, alkotmányjog, világrendszerelmélet*, Győr, Universitas, 2011.

[97] SZIGETI Péter: *Vázlat a közbiztonság három dimenziójáról: világrendszer – nemzetállami szint és lokalitás.* In SZIGETI Péter: A valóság vonzásában – Jogelméleti és Jogtudományi Közlöny, Győr, ELTE-SZIF ÁJK, 2001. (https://mek.oszk.hu/04200/04241/04241.htm#16).

[98] TILESCH György – Omar HATAMLEH: *Mesterséges intelligencia – Vegyük kezünkbe a sorsunkat az MI korában.* Budapest, Libri, 2021.

[99] VIKMAN László: *A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra,* In Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14. szám.

[100] VIKMAN László: *A műveletszervezés jogi feladatai.* In Honvédségi Szemle, 2021/2. szám, 44-56. o.

[101] VIKMAN László: *A német kiberbiztonsági szisztéma áttekintése: Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására.* In Military and Intelligence CyberSecurity Research Paper, 2021/2. szám.

[102] VIKMAN László: *Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi*

útmutató kapcsán. In SmartLaw Research Group Workin Paper 2022/1. szám.

[103] Vincent MOSCO: *Okosvárosok a digitális világban.* Budapest, Pallas Athéné Könyvkiadó, 2019.

[104] *Yellow Vests Flooded by Fake News – Over 100M Views of Disinformation on Facebook. Avaaz Report.* 15.03.2019. (https://avaazimages.avaaz.org/Report%20Yellow%20Vests%20FINAL.pdf).

[105] Yvonne HOFSTETTER: *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Budapest, Corvina, 2020.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2022/1.

Szerző(k) / Author(s):
Dr. Kelemen Roland

Kézirat lezárásának ideje / Manuscript closing time:
2022.03.06.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.