Szádeczky Tamás

Az ellátórendszerek kiberbiztonsági kitettsége napjainkban, különös tekintettel a víziközmű-infrastruktúrára

Military and Intelligence CyberSecurity Research Paper
2023/5.

UNIVERSITY OF PUBLIC SERVICE

LUDOVIKA

1. BEVEZETÉS

Az információs technológia (IT) kényelmesebbé és hatékonyabbá teszi az életünket, kevesebb manuális, repetatív munkával. A gépek hatékonyan automatizálhatják a folyamatokat. Ez a technológiai váltás az egyén, a szervezet és a társadalom szintjén az IT-től való nagyobb függőséghez vezet. Az egyén szintjén a feladatok túlnyomó többsége ma már valamilyen számítógép használatát igényli.

A termelés és a gyártás automatizálása leginkább az ipari forradalom kifejezéssel írható le. Ezek a forradalmak jelentős előrelépést jelentettek a technológia terén, és jelentős hatást gyakoroltak mind a gazdaságra, mind a társadalomra. Az első ipari forradalmat a gőzgép megjelenésétől számítjuk[1]. A második ipari forradalom a tömegtermelés kialakulását hozta magával. A harmadik ipari forradalom a számítástechnika megjelenése és ezáltal a folyamatok automatizálása volt. Ez egyrészt autonóm szabályozással és irányítással, másrészt a központi koordináció valamilyen formájával, azaz az ipari irányítási rendszerekkel (Imdustrial Control Systems, ICS) járt együtt. Az ICS egyik alapeleme a programozható logikai vezérlő (PLC), amely közvetlen kapcsolatban áll a vezérelt folyamatba integrált szenzorokkal és aktorokkal. Ezek a vezérlők egy megfelelő hálózaton – korábban RS-485, ma ipari ethernet – keresztül összekapcsolhatók. A mérési adatokat például egy felügyeleti vezérlő- és adatgyűjtő rendszer (SCADA) gyűjtheti, vagy az elosztott vezérlést elosztott vezérlőrendszerek (DCS) valósíthatják meg.

A negyedik ipari forradalom, más néven az ipar 4.0 vagy a dolgok ipari internete (IIoT) jelenleg is zajlik. Ezt a digitális, fizikai és biológiai rendszerek konvergenciája, valamint olyan új technológiák megjelenése jellemzi, mint a dolgok internete (IoT), a mesterséges intelligencia (AI), a robotika és a big data adatelemzés. Ez az ipari forradalom ezekre a technológiákra épül, de más, modern informatikai elveket és módszereket alkalmaz, és a gyártás adatvezérelt és hálózatos megközelítése[2]. A 21. század informatikai eszközei korábban elképzelhetetlen mennyiségű adatot képesek összegyűjteni és elemezni, ami az adattudomány vagy data science lényege. Emellett a 2000-es években kialakult tömeges webhasználat - amely az internetet mindenütt jelenlévő eszközzé tette mindannyiunk életében - a gyártásra és a folyamatirányításra is átgyűrűzik. Ez még hatékonyabbá teszi a gyártást. Bármelyik pillanatban valós időben optimalizálhatjuk a folyamatot több millió adatforrás elemzésével, hatékonyabban használhatjuk fel az emberi erőforrásokat, és hatékonyabbá válhatunk a munka elvégzésében. Hogy ez valóban ipari forradalom-e, amelynek gazdasági és társadalmi hatása van, vagy csak egy múló hóbort, amely csak a marketingesek asztalán létezik, azt csak történelmi távlatból

[1] D. WIENECKE-JANZ, Die Chronik der Deutschen (A németek krónikája). Gütersloh-München: Chronik Verlag, 2007.
[2] H. LASI, P. FETTKE, H.-G. KEMPER, T. FELD, and M. HOFFMANN: Industry 4.0, *Business & Information Systems Engineering*, Vol. 6, No. 4, pp. 239-242, 2014, doi: 10.1007/s12599-014-0334-4.

lehet majd eldönteni. Az azonban biztos, hogy az informatika használata, vagy, még pejoratívabban, az informatikától való függés egy megállíthatatlannak tűnő folyamat.

Az intelligens vízgazdálkodás (digital water, water 4.0), mint az ipar 4.0 speciális alkalmazása, a fejlett digitális technológiák és az adatvezérelt megközelítések felhasználásával optimalizálja a vízkészletek és az infrastruktúra tervezését, üzemeltetését és karbantartását, valamint javítja a vízszolgáltatás hatékonyságát, fenntarthatóságát és rugalmasságát. Az elmúlt években az intelligens vízgazdálkodás egyre több kormány (főként a fejlett államokban), közműszolgáltató, ipari és egyes kutatóintézetek részéről világszerte egyre nagyobb figyelmet és pénzügyi beruházást kapott, amit a vízhiány, a szennyezés, az éghajlatváltozás és az elöregedő infrastruktúra jelentette növekvő kihívások, valamint a fogyasztók, a szabályozók és az érdekelt felek növekvő elvárásai motiváltak, amelyek a vízgazdálkodás jobb minőségére, megfizethetőségére és elszámoltathatóságára irányulnak[3].

Az intelligens vízgazdálkodásban az említett digitális technológiákra, automatizálásra és összekapcsolhatóságra való támaszkodás azonban a vízügyi ágazatot új, az informatikai biztonságban jól ismert kiberbiztonsági fenyegetéseknek, sebezhetőségeknek és kockázatoknak is kiteszi, amelyek jelentős következményekkel járhatnak a kritikus vízügyi infrastruktúra és szolgáltatások biztonságára, biztonságára és megbízhatóságára, valamint a közegészségügyre, a környezetre és a gazdaságra nézve. A vízügyi rendszerek növekvő kölcsönös függősége és összetettsége, valamint a technológiai innováció, a telepítés gyors ütemével és a kiberfenyegetések változó természetével együtt a kutatók, a gyakorlati szakemberek és a politikai döntéshozók számára elengedhetetlenné teszi, hogy jobban megértsék, értékeljék és kezeljék az intelligens vízgazdálkodásban felmerülő kiberbiztonsági kihívásokat és lehetőségeket.

A tanulmány célja, hogy hozzájáruljon a kiberbiztonsággal és az intelligens vízgazdálkodással kapcsolatos egyre bővülő ismeretekhez és vitákhoz azáltal, hogy megvizsgálja az intelligens vízgazdálkodás jelenlegi helyzetét Magyarországon és Közép-Európában, valamint elemzi a különböző kiberbiztonsági fenyegetéseket, sebezhetőségeket és kockázatokat ebben a kritikus infrastruktúrákból álló ágazatban. A tanulmány emellett kutatási kérdéseket és ajánlásokat fogalmaz meg a jövőbeli tanulmányokhoz és intézkedésekhez az intelligens vízgazdálkodás

kiberbiztonságának és ellenálló képességének javítása érdekében a régióban. A tanulmány a szerző korábbi kutatásain és az azokból született cikkeken alapul.[4]

---

[3] A. D. GUPTA, P. PANDEY, A. FEIJÓO, Z. M. YASEEN és N. D. BOKDE: Smart Water Technology for Efficient Water Resource Management: A Review, *Energies (Basel)*, Vol. 13, No. 23, p. 6268, Nov. 2020, doi: 10.3390/en13236268.

[4] SZÁDECZKY, Tamás: Víz 4.0? A digitális víziközmű-infrastruktúra kiberbiztonsági kitettsége, *Hadtudomány*, 31 : 4 pp. 111-117. , 7 p. (2021); SZÁDECZKY, Tamás: Water 4.0 in Hungary: Prospects and Cybersecurity Concerns, *Acta Polytechnica Hungarica*, 20: 7 pp. 211-230. , 20 p. (2023)

2. ELLÁTÓRENDSZEREK DIGITALIZÁLÁSA

Ha valaki az ipar 4.0-ra gondol, először talán egy autógyárra vagy valamilyen űrtechnológiai központra asszociál. Tény azonban, hogy a megvalósításához szükséges eszközök a gazdaság és a társadalom széles rétegei számára válnak elérhetővé, mivel az áruk drasztikusan csökkent. Elég csak arra gondolni, hogy felhasználók milliói telepítettek okosotthon-megoldásokat. Néhány százezer forintos beruházásért tucatnyi érzékelővel és egy felhőalapú személyi asszisztenssel automatizálhatjuk és hangvezérelhetjük családi otthonunkat. Továbbá az okos város koncepciója alapján az önkormányzati közszolgáltatások optimalizálhatók és hatékonyabban használhatók. Ilyen megoldás lehet például az intelligens parkolás bevezetése, ahol a járdaszegélyekbe épített szenzorok továbbítják az adatokat az autósok navigációs rendszerének, és lehetővé teszik számukra, hogy egy mobilalkalmazáson keresztül lássák az úti céljukhoz legközelebbi szabad parkolóhelyeket, és így minimalizálják a parkolóhely keresésére fordított időt.

Ez gyakorlatilag minden ellátórendszerre, illetve kritikus infrastruktúrára igaz, de a technikai előnyök bemutatását a víziközmű-infrastruktúrán szeretném bemutatni.

1994-ben a VITUKI világméretű felmérést végzett arról, hogy a különböző országokban hogyan használják a számítástechnikát a víz- és csatornaszolgáltatásban[5]. A fő területeket a földrajzi információs rendszer (GIS) alkalmazásai, a műveletek folyamatirányítása, a vízdíjszámlázás és a szakértői rendszerek alkalmazása jelentette. A két és fél évtizeddel ezelőtt leírt francia gyakorlathoz képest még ma is gyakran elmarad egy-egy kisebb magyar víziközmű-szolgáltató. Ez a fejlődés azonban gyakran nem szerves piaci fejlődés, hanem kormányzati döntés. A térinformatika tekintetében például az elektronikus közműnyilvántartás és -egyeztetés folyamata jól ismert az iparágban. A hatóság az adatok elektronikus formában történő bekérésével építi fel adatbázisát, ami jelentősen leegyszerűsíti a közműtervezés és -üzemeltetés folyamatát. Mindemellett ezen túlmenően a megfelelő adatok birtokában okosmérőkből webes tudásbázis-rendszerek építhetők, amelyek megkönnyítik az építőmérnökök feladatát a víziközmű-infrastruktúra építésében[6].

A víz- és szennyvíztisztító telepek irányítási folyamatainak összetettsége számos szenzor és aktor használatát teszi szükségessé. A digitalizálás a következő folyamatokban alkalmazható:

1) A nyersvízfelvétel számszerűsítése és optimalizálása
2) Energiahatékonyság a szivattyú üzemeltetésében
3) A tározó vízminőségének ellenőrzése
4) A kezelendő víz mennyiségének meghatározása és minőségének elemzése
5) A vízkezelési folyamat optimalizálása (vegyszer, klórgáz használata)
6) Lehetőség nyílhat a hálózatba való betáplálás helyén az optimális szivattyúzási kapacitás meghatározására, a hálózatba táplált víz nyomásának nyomon követésére.

---

[5] DÉRI J., Számítógépesített technológiák víz- és csatornaműveknél. Budapest: Vituki Innosystem, 1994.

[6] R. A. STEWART, R. WILLIS, D. GIURCO, K. PANUWATWANICH, and G. CAPATI: Web-based knowledge management system: linking smart metering to the future of urban water planning, *Australian Planner*, Vol. 47, No. 2, pp. 66-74, Jun. 2010, doi: 10.1080/07293681003767769.

7) Csőtörések és szivárgások felderítése
8) A fogyasztói kereslet valós idejű értékelése
9) Nyomásnövelés toronyházakban
10) A vízművek infrastruktúrájának védelme

Annak ellenére, hogy számos adatforrás áll rendelkezésre, a hidraulikai hálózatnak számos olyan eleme van, amely nem mérhető. Ezekre virtuális érzékelőket alkalmazhatunk, hogy valós idejű dinamikus hidraulikai modellt alkossunk a vízveszteség csökkentése érdekében[7].

Szennyvíztisztítási folyamat esetén az üzemeltető optimalizálhatja a szivattyúk működését a nyomás alatt álló csatornarendszerekben, értékelheti a szaghatásokat a szennyvíztisztító telepeken, és optimalizálhatja a szennyvíztisztítási folyamatokat. A közműszolgáltató optimalizálhatja a szennyvíztisztító telepek működését, racionalizálhatja az iszapkezelési folyamatot, növelheti a biogázfelhasználás energiahatékonyságát, és mérheti a tisztított szennyvíz minőségét a befogadóba való bevezetés előtt[8].

A digitalizáció legegyszerűbben bevezethető eleme az intelligens fogyasztásmérők használata, amelyhez ma már számos technológia áll rendelkezésre az európai piacon. Aknába vagy pincébe szerelhető az okos vízmérő, amely a távközlési szolgáltató által biztosított NB-IoT technológia segítségével alacsony sebességgel, de nagy megbízhatósággal képes kommunikálni a vízszolgáltató rendszereivel egy olyan helyről, amely korábban semmilyen más rádiós eszközzel nem volt elérhető[9]. Az intelligens fogyasztásmérők lehetővé teszik a fogyasztási szokások valós idejű elemzését és a víztisztítási és vízellátási technológia igény szerinti beállítását a tényleges igényekhez, ami a hagyományos megoldásoknál hatékonyabbá teszi a vízszámlázási folyamatot, mivel a számla mindig a tényleges fogyasztási adatokon alapulhat.[10] A szolgáltató helyszíni beavatkozás nélkül is korlátozhatja a vízfogyasztást a fogyasztó számára. Az adatok közvetlenül elérhetők az ERP-rendszerrel integrált számlázási rendszer számára.

Az iparág ezeket a megoldásokat Water 4.0, Digital Water, Smart Water és Internet of Water (IoW) elnevezésekkel illeti, és az ehhez hasoló megoldások megjelentek a többi ellátórendszer esetében is.

3. Biztonsági problémák

A digitalizáció számos pozitív előnnyel jár az egyének, a szervezetek és a társadalom számára, amelyeket nap mint nap érzékelünk. Nem szabad azonban megfeledkeznünk a technológiának

[7] M. S. Osman, A. M. Abu-Mahfouz és P. R. Page, "A Survey on Data Imputation Techniques: Water Distribution System as a Use Case, *IEEE Access*, Vol. 6, pp. 63279-63291, 2018, doi: 10.1109/ACCESS.2018.2877269.
[8] Patziger Miklós: Közepes és kis szennyvíztisztító telepek hatékony üzemeltetése. Budapest: Magyar Víziközmű Szövetség, 2018.
[9] S. Alvisi et al., Wireless Middleware Solutions for Smart Water Metering, *Sensors*, Vol. 19, No. 8, p. 1853, Apr. 2019, doi: 10.3390/s19081853.
[10] S. D. B. Moraes, C. Langhi, and M. Crivelaro: How an existing telecommunications network can support the deployment of smart meters in a water utility?, *Independent Journal of Management & Production*, Vol. 6, No. 4, 2015, doi: 10.14807/ijmp.v6i4.351

való kiszolgáltatottság veszélyeiről sem. Különösen az informatikai alkalmazások és szolgáltatások elvesztésével, a folyamatok automatizálásával és a rendszerek összetettségéből adódó nehézségekkel kell számolnunk.

3.1. Kiberbiztonsági fenyegetések

A digitális infrastruktúrát érintő kiberbiztonsági fenyegetések, sebezhetőségek és kockázatok jelentősen befolyásolhatják a kritikus vízügyi infrastruktúra és szolgáltatások biztonságát és megbízhatóságát, valamint kritikus infrastruktúraként a közegészségügyet, a környezetet és a nemzetgazdaságot. Az intelligens vízellátást érintő legfontosabb kiberbiztonsági kihívások és veszélyek a jelen alfejezetben kerülnek bemutatásra.

3.1.1. Kiber-fizikai támadások

Ezek olyan támadások, amelyek a vízrendszerek fizikai összetevőit és automatizálási folyamatait, például szivattyúkat, szelepeket, tisztítóműveket és elosztóhálózati elemeket veszik célba, a digitális vezérlőrendszereik, például a felügyeleti rendszerek manipulálása vagy megzavarása révén. Ennek célpontjai jellemzően a vezérlő és adatgyűjtő (SCADA) rendszerek, elosztott vezérlőrendszerek (DCS), programozható logikai vezérlők (PLC-k) és humán-gép interfészek (HMI-k), vagy távoli terminálegységek (RTU-k)[11]. A támadás történhet valamilyen hardver, szoftver vagy firmware sérülékenysége vagy gyenge biztonsági konfigurációja kihasználása útján.

A kiberfizikai támadások a víziközmű infrastruktúra fizikai károsodását, meghibásodását vagy rendelkezésre állásának csökkenését okozhatják, ami a vízszolgáltatás megszakadásához, szennyeződéshez, szivárgáshoz vagy vízkárokhoz vezethet, ami súlyos következményekkel járhat a közegészségügyre, a környezetre és a gazdaságra nézve.

3.1.2. Adatvédelmi incidensek

Az adatvédelmi incidensek a vízgazdálkodási rendszerekben például ügyfélnyilvántartási, számlázási rendszerekben, eszközkezelő rendszerekben vagy felügyeleti és ellenőrzési rendszerekben tárolt vagy továbbított érzékeny vagy bizalmas adatok, például személyes adatok vagy üzleti titkok, pénzügyi tranzakciók vagy üzemi adatok jogosulatlan hozzáférése, közzététele vagy ellopása[12]. Az adatsértések (data breach), a személyes adatok védelméhez fűződő jog megsértéséhez, büntető- és polgári jogi következményekhez, személyazonosság-lopáshoz, pénzügyi csaláshoz vagy ipari kémkedéshez vezethetnek, aláásva a víziközművekkel és a hatóságokkal szembeni bizalmat, a szervezet hírnevét és a jogszabályi megfelelőségét.

3.1.3. Szolgáltatásmegtagadási (DoS) támadások

E támadások célja a vízellátási rendszerek, közműhálózatok vagy szolgáltatások rendelkezésre állásának, teljesítményének vagy funkcionalitásának megzavarása, túlterhelése vagy minimalizálása azáltal, hogy túlzott mennyiségű adat, kérés vagy forgalom árasztja el azokat,

[11] Y. CHERDANTSEVA et al.: A review of cyber security risk assessment methods for SCADA systems, *Comput Secur*, Vol. 56, pp. 1-27, Feb. 2016, doi: 10.1016/J.COSE.2015.09.009.
[12] CHERDANTSEVA i.m.

vagy kihasználja sebezhetőségüket és gyengeségeiket vagy tervezési hibáikat[13]. A DoS-támadások a vízgazdálkodásban a hozzáférés, az irányítás vagy a kommunikáció ideiglenes vagy végleges elvesztését okozhatják, és növelik a rendszer helyreállításának és helyreállításának munkaterhelését, költségeit és késedelmét.

3.1.4. Belső fenyegetések

Ezek olyan kiberbiztonsági kockázatok, amelyek a szervezeten belülről erednek, például olyan alkalmazottak, vállalkozók vagy partnerek részéről, akik jogos hozzáféréssel és ismeretekkel rendelkeznek a vízgazdálkodási rendszerekhez, irányelvekhez vagy eljárásokhoz, de szándékosan vagy véletlenül (pl. hiba) visszaélnek, visszaélnek vagy veszélyeztetik azokat hanyagság, anyagi haszonszerzés, bosszú vagy más indítékok miatt[14]. A bennfentes vagy belső fenyegetések felderítése kihívást jelenthet, alapvetően nehezebb megelőzni, és reagálni rá, mint egy külső támadásra. A támadások gyakran a bizalom, a tekintély vagy az ismertség kihasználásával járnak, és képesek megkerülni vagy kijátszani a biztonsági ellenőrzéseket és intézkedéseket.

Incidens következhet be gondatlanságból is, ilyen például az alapértelmezett jelszavak használata az ICS-rendszerekben, ami triviális hibának tűnik, de mégis gyakran előfordul, mivel az ICS-rendszerek általában le vannak választva az internettől, ami téves biztonságérzetet adhat az üzemeltetőnek. Ezért kiemelkedő fontosságú, hogy a digitalizálási folyamatot megfelelő kiberbiztonsági felméréssel és az ebből következően szükséges információbiztonsági ellenőrző intézkedések végrehajtásával támogassuk. Az informatikával kapcsolatos területeken magasabb szintű kiberbiztonsági szakértelemmel rendelkező munkatársakat kell alkalmazni, ami a víz- és csatornaszolgáltatóknál általában nem áll rendelkezésre.

3.1.5. Ellátási lánc kockázatok

Az ellátórendszerek maguk is egy ellátási lánc részét képezik. Az ellátási lánccal kapcsolatos kockázatok olyan kiberbiztonsági kockázatok, amelyek a vízgazdálkodási rendszerek ellátási láncának különböző szereplői és összetevői közötti kölcsönös függőségekből és kapcsolatokból erednek. Ezek a szereplők lehetnek az eladók, beszállítók, integrátorok, üzemeltetők és karbantartók, illetve akik olyan hardvert, szoftvert, firmware-t vagy szolgáltatásokat biztosítanak, gyártanak, szerelnek, telepítenek, karbantartanak vagy frissítenek, amelyek sebezhetőségeket, hibákat vagy hátsó ajtókat tartalmazhatnak, vagy amelyek manipulálhatók, szabotálhatók vagy hamisíthatók[15]. Mivel a folyamat működése nagymértékben függ az érzékelők, a működtető elemek és a vezérlőrendszer működőképességétől, a műszaki okok miatti leállás valószínűsége nagyobb, mint a hagyományos rendszerek esetében[16]. A dolgok internete (IoT), a felhőalapú számítástechnikai infrastruktúra és az adatfeldolgozás szintén

---

[13] CHERDANTSEVA i.m.
[14] CHERDANTSEVA i.m.
[15] CHERDANTSEVA i.m.
[16] M. MOY DE VITRY, M. Y. SCHNEIDER, O. WANI, L. MANNY, J. P. LEITÃO, S. EGGIMANN, Smart urban water systems: what could possibly go wrong?, *Environmental Research Letters*, Vol. 14, No. 8, p. 081001, Aug. 2019, doi: 10.1088/1748-9326/ab3761.

jelentős kockázatnövelő tényezők[17], amelyeket csak egy komplex, összekapcsolt vezérlőrendszerrel lehet hatékonyan mérsékelni[18] . Ráadásul a rendszer egyetlen elemének meghibásodása könnyen a szolgáltatás teljes kieséséhez vezethet. Az ellátási lánc kockázatai veszélyeztethetik a vízgazdálkodási rendszerek biztonságát, minőségét és megbízhatóságát, és lehetőséget teremtenek a támadók számára, hogy kihasználják vagy manipulálják ezeket a rendszereket különböző belépési pontokon, szakaszokon vagy csatornákon keresztül.

3.2. Kiberbiztonsági incidensek és trendek a víziközmű ágazatban

Az elmúlt években a víziközmű ágazatban több nagy visszhangot kiváltó kiberbiztonsági incidensről számoltak be, ami jól mutatja a vízügyi rendszerek kiberfenyegetettségét és kibertámadásokkal szembeni sebezhetőségét és hatását.

Egy korai – és áttételes – példa erre az Egyesült Államok északkeleti részét és Kanada középső részét 2003 augusztusában sújtó áramkimaradás[19] [20]. A világ második legnagyobb áramszünete 55 millió embert érintett, és két napig szinte teljes áramszünetet, valamint két hétig rendellenes szolgáltatási szintet jelentett. Számunkra az az izgalmas, hogy az incidens egy szolgáltató szoftverhibájával kezdődött, és az egyébként redundáns rendszerben bekövetkezett hiba más rendszerekre is átterjedt, és a kapcsolódó rendszereket is kiiktatta. Ekkor ezen a területen részlegesen a vízszolgáltatás is kimaradt. A víziközmű-szolgáltatások könnyen megszűnhetnek, ha valamely más kritikus infrastruktúraelem meghibásodik, ugyanis a kritikus infrastruktúrák között kölcsönös függés, interdependencia van. Például áram nélkül nem működnek a szivattyúk, így nem lesz elérhető az ivóvíz (nem lesz betermelve a hálózatba). Mindemellett még az internetszolgáltatás kiesése is problémát jelenthet a vízművek számára a kommunikáció, a távvezérlés és az adatgyűjtés elvesztésével. Szolgáltatás-leállást okozhat a rendszer megbízhatatlansága és természeti jelenségek is, de a legnagyobb veszélyt jellemzően a szándékos emberi támadás jelenti. Ez a személy lehet egy külső támadó, aki kiberbűnözés vagy kiberháború révén akarja megzavarni az ipari vezérlőrendszereket. Az ipari automatizálási és vezérlőrendszerek a katonai kiberműveletek célpontjai is, például az Advanced Persistent Threats (APT) révén[20].

Az Egyesült Államokban 2016-ban egy víztisztító telepen kiber-fizikai támadással manipulálták a vízkezelési folyamatban használt fertőtlenítő vegyszereket, amelyek potenciálisan veszélyeztetik a közegészséget és a közbiztonságot[21]. Egy másik példa, hogy az izraeli kormány szerint palesztin hackerek 2020 áprilisában egy izraeli vízműben a klórozó

---

[17] R. O. ANDRADE, S. G. YOO, L. TELLO-OQUENDO és I. ORTIZ-GARCÉS, A Comprehensive Study of the IoT Cybersecurity in Smart Cities, *IEEE Access*, Vol. 8, pp. 228922-228941, 2020, doi: 10.1109/ACCESS.2020.3046442.

[18] TÓTH András: Cloud of Things Security Challenges and Solutions; Cloud of Things Security Challenges and Solutions, in *Communication and Information Technologies (KIT)*, Vysoke Tatry, Slovakia, 2021, pp. 1-6. doi: 10.1109/KIT52904.2021.9583760.

[19] M. TABIBZADEH and S. MIRZAEI, "A system-oriented framework for risk and resiliency analysis of power blackouts," in *Proceedings of the 2016 Industrial and Systems Engineering Research Conference, ISERC 2016*, 2020, pp. 582-587.

[20] W. STEINGARTNER és D. GALINEC, Cyber Threats and Cyber Deception in Hybrid Warfare, *Acta Polytechnica Hungarica*, Vol. 18, No. 3, pp. 25-45, 2021, doi: 10.12700/APH.18.3.2021.3.2.

[21] CHERDANTSEVA i.m.

rendszer manipulálásával próbáltak tömeges klórmérgezést okozni, de a támadást megakadályozták. A palesztin fél tagadta a vádat[22]. Más források azt állítják, hogy a vezérlőrendszer mellett működő Safety Instrumented System (SIS) akadályozta meg a támadást. A SIS egyébként szintén az irányítórendszer tervezési követelménye.

A közelmúltban az orosz-ukrán fegyveres konfliktusban több példát is láthattunk. A konfliktus során számos hackercsoport támadta az ICS/SCADA-rendszereket mindkét oldalon, amit egyelőre csak nem megerősített háborús jelentésekből, illetve a hackercsoportok közösségi média oldalairól láthatunk.

A vízművek vonzó célpontok, mivel annak ellenére, hogy kritikus infrastruktúráról van szó, a védelem szintje általában alacsonyabb, mint a villamosenergia-ellátásé. Ezek az incidensek azt mutatják, hogy a víziközmű ágazatban fokozott éberségre, felkészültségre és ellenálló képességre van szükség a kiberbiztonsági fenyegetésekkel és kockázatokkal szemben.

A szakirodalmi áttekintés és a másodlagos adatok elemzése számos újonnan kialakuló kiberbiztonsági tendenciát tárt fel a vízügyi ágazatban, mint például a bejelentett kiberbiztonsági incidensek növekvő száma, a kiberfenyegetések (például APT-k) növekvő kifinomultsága és összetettsége, a dolgok internetének elterjedése miatt bővülő támadási felület és vektorok, a fejlődő szabályozási és megfelelési környezet, valamint a kiberbiztonsági intézkedések és legjobb gyakorlatok iránti növekvő tudatosság és beruházások. Ezek a tendenciák azt jelzik, hogy a kiberbiztonság egyre fontosabb kérdéssé és prioritássá válik a víziközművek, hatóságok és érdekelt felek, valamint az intelligens vízügyi technológiák és megoldások kutatói, fejlesztői és szolgáltatói számára.

3.3. Kiberbiztonsági ellenintézkedések

A kutatás számos olyan kiberbiztonsági intézkedést és bevált gyakorlatot azonosított, amelyeket a vízügyi ágazatban javasoltak vagy alkalmaztak az információbiztonsági kockázatok és sebezhetőségek kezelésére és mérséklésére. Ezen intézkedések közé tartoznak a kockázatértékelések, auditok és tanúsítások, amelyek segítenek a kiberbiztonsági kockázatok és ellenőrzések azonosításában, értékelésében és rangsorolásában; a biztonsági politikák, eljárások és iránymutatások, amelyek meghatározzák és kommunikálják a kiberbiztonsági szerepeket, felelősségeket és elvárásokat; a biztonsági képzés, oktatás és tudatossági képzés, amelyek fejlesztik és fenntartják a kiberbiztonsági készségeket, ismereteket és kultúrát; technikai ellenőrzések, például tűzfalak, vírusirtók, titkosítás és hozzáférés-ellenőrzés, amelyek védik és felügyelik az információs rendszereket és hálózatokat; valamint az incidensekre való reagálásra, helyreállításra és folyamatosságra vonatkozó tervek, amelyek felkészítik és irányítják a szervezeteket a kiberbiztonsági incidensek kezelésére és helyreállítására[23]. A kiberfizikai támadások kockázatának minimalizálása érdekében meg kell határozni az

[22] Iranian Cyberattack Aimed to Raise Chlorine Level in Israeli Water, Report Says (Az iráni kibertámadás célja az izraeli víz klórszintjének emelése volt, állítja a jelentés), *Haaretz*, 2020. jún. 01., [Online]. Elérhető: https://www.haaretz.com/israel-news/iranian-cyberattack- aimed-to-raise-chlorine-level-in-israeli-water-report-resays-1.8886235

[23] CHERDANTSEVA i.m.

információvagyont és a kritikus erőforrásokat, hogy megerősítsük védelmüket[24]. A számítógépes hálózatokra és rendszerekre vonatkozó kockázatok és ellenintézkedések többsége az ipari vezérlőrendszerekre is vonatkozik, de elfogultan. A hozzáférés-ellenőrzés, azaz a hozzáférés korlátozása az engedélyezett felhasználókra alapvető az informatikai biztonságban, de az ipari vezérlőrendszerekben (ICS) problémásabb. Ennek oka az, hogy sok ICS-eszköz nem rendelkezik hozzáférés-szabályozási képességekkel. A belső fenyegetésekkel szemben a megoldást egy jól megtervezett hozzáférés-ellenőrzési stratégia jelentheti[25]. A szoftverhibákat javító frissítések az ICS-ben ritkák és rendszertelenek, ellentétben az informatikai rendszerekkel. Az ICS-ben hagyományosan a funkcionális biztonság élvez prioritást minden más szempont felett. Egy jól konfigurált, futó ipari vezérlőrendszer patchelése nyilvánvalóan kockázatot jelent a funkcionális biztonság szempontjából, csakúgy, mint az informatikai rendszerek esetében. Bár az informatikai rendszerekben jól megtervezett javítás-ellenőrzési folyamat van központi kezeléssel (pl. Windows Server Update Services, WSUS), visszaállítási funkciókkal, tesztrendszerekkel és tesztelési csoportokkal. Még a szoftverfejlesztési és üzemeltetési gyakorlatok, mint például a Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), Enhanced Mitigation Experience Toolkit (EMET) és Control Flow Enforcement (CFE) is alkalmazhatók a szoftver sebezhetőségek kihasználásának kockázatának minimalizálása érdekében[26]. Az ICS-rendszerekben ezek a módszerek és eszközök nem léteznek. Ráadásul az időkritikus alkalmazásokban sem engedélyezett az újraindítás. A hálózat alapú védelem alapesetben a légréseken (air gap), tehát a hálózatok fizikai szétkapcsolásán alapul. Történelmileg nem volt közvetlen kapcsolat az informatikai hálózat és az üzemeltetési technológiai (OT) hálózat között, amely az IKT-rendszereket kezeli. Ezért a hálózati védelemre nem volt szükség. A hálózattal kapcsolatos problémák akkor merülnek fel, amikor a korábban légréses hálózat az ipar 4.0 jellemzői miatt már nem csak IT-hálózat, hanem internetkapcsolat is van[27]. Emellett az IT hálózatbiztonsági technológiák csak részben használhatók az OT-hálózaton. Mivel a funkciók többnyire időkritikusak, nem megengedett a késleltetés, így az állapotfüggő csomagellenőrzés (stateful packet inspection) vagy az alkalmazásszintű tűzfalak (application level firewall) nem feltétlenül használhatók. A behatolásmegelőző rendszerek (IPS) a csomagok eldobása során megzavarhatják az üzemi kommunikációt, ezért különös óvatossággal használhatók.

---

[24] A. MASSEL és D. GASKOVA, A kritikus objektumok azonosítása a kiberfenyegetések függvényében az energiaágazatban, *Acta Polytechnica Hungarica*, Vol. 17, No. 8, pp. 61-73, 2020, doi: 10.12700/APH.17.8.2020.8.5.

[25] B. LEANDER, A. ČAUŠEVIĆ, H. HANSSON, és T. LINDSTRÖM, Toward an Ideal Access Control Strategy for Industry 4.0 Manufacturing Systems, *IEEE Access*, Vol. 9, pp. 114037-114050, 2021, doi: 10.1109/ACCESS.2021.3104649.

[26] L. ERDŐDI és A. JØSANG, Exploitation vs. Prevention: The ongoing saga of software vulnerabilities, *Acta Polytechnica Hungarica*, Vol. 17, No. 7, pp. 199-218, 2020, doi: 10.12700/APH.17.7.2020.7.11.

[27] E. D. KNAPP és J. T. LANGILL, Ipari hálózatbiztonság: Az intelligens hálózat, a SCADA és más ipari vezérlőrendszerek kritikus infrastrukturális hálózatainak biztosítása. Waltham, MA: Syngress, 2015.

4. KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

A szakirodalmi áttekintés és a másodlagos adatok elemzéséből származó megállapítások és meglátások, valamint a magyarországi és közép-európai kontextus és körülmények alapján a következő következtetések és ajánlások vezethetők le az intelligens vízgazdálkodás kiberbiztonságának és ellenálló képességének nemzeti szintű, vagy akár a régióbeli fokozására:

4.1. Stratégiák, politikák, irányítás és együttműködés

A magyarországi és közép-európai kormányoknak és hatóságoknak olyan átfogó, koherens és összehangolt kiberbiztonsági stratégiákat és politikákat kell kidolgozniuk és végrehajtaniuk (vagy a jelenlegieket a víziközmű ágazatra alkalmazniuk), amelyek az intelligens vízgazdálkodás sajátos kockázatait, kihívásait és lehetőségeit kezelik, és amelyek összhangban vannak a nemzetközi, nemzeti és ágazati kiberbiztonsági keretekkel, szabványokkal és iránymutatásokkal, és azokat támogatják.

A települési vízgazdálkodás egyes elemei de facto kritikus infrastruktúrák Magyarországon, ahogyan azt a kritikus rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.)[28], valamint a vízgazdálkodási rendszerelemekről és a vízilétesítményekről szóló 541/2013 (XII. 30.) Kormányrendelet[29] is meghatározza Magyarországon. A vízellátás tehát közérdek, és a szennyvízgyűjtést és -tisztítást, mint közegészségügyi kérdést, szintén folyamatosan biztosítani kell. Az édesvíz stratégiai kérdés, és számos földrajzi régióban (pl. Izrael, Tibet, Kasmír, Nílus-völgy) a korlátozott édesvízkészletek használata jelenleg fegyveres konfliktusokat okoz[30]. A vízhiány miatt az ország rendkívül kiszolgáltatott a feljebb fekvő országokkal szemben, ha nem rendelkezik megfelelő tárolókapacitással. Ez a legtöbb közép-európai országban aktuális probléma, elsősorban társadalmi okokból, azaz a földhasználat miatt. A tárolás mind gazdasági (védelmi költségek, hasznosítás), mind stratégiai (közvetett biztonsági kockázatok) szempontból fontos[31].

A magyarországi és közép-európai víziközmű-szolgáltatóknak, hatóságoknak és érdekelt feleknek ki kell alakítaniuk és meg kell erősíteniük kiberbiztonsági irányításukat és kapacitásukat azáltal, hogy egyértelmű szervezeti szerepeket, felelősségeket és erőforrásokat jelölnek ki a kiberbiztonság irányítására, a kiberbiztonsági szempontokat beépítik a szervezeti kultúrába, folyamatokba és rendszerekbe, valamint folyamatos tanulást, fejlesztést és innovációt folytatnak a kiberbiztonsági gyakorlatok és technológiák terén[32].

---

[28] *A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló* 2012. évi CLXVI. törvény.

[29] *A létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló* 541/2013. (XII. 30.) Korm. rendelet. Magyar Közlöny, 2013/223. sz. p. 89511.

[30] PADÁNYI József: Vízkonfliktusok, *Hadtudomány*, Vol. 25, No. e, pp. 272- 284, 2015. doi: 10.17047/HADTUD.2015.25.E.272

[31] LIGETVÁRI Krisztina, Magyarország vízbiztonsági problémái az uniós és világtendenciákkal összevetve, *Hadtudomány*, Vol. 23, No. 1, pp. 4-13, 2013.

[32] CHERDANTSEVA i.m.

A magyarországi és közép-európai kormányoknak, közműszolgáltatóknak, iparágaknak és kutatóintézeteknek elő kell mozdítaniuk és meg kell könnyíteniük a kiberbiztonsági együttműködést és információcserét a vízügyi ágazatban különböző mechanizmusok és platformok - például partnerségek, hálózatok, konferenciák, műhelyek és kiadványok - révén, amelyek lehetővé teszik a kiberbiztonsági fenyegetésekkel, sebezhetőségekkel, incidensekkel és ellenintézkedésekkel kapcsolatos ismeretek, tapasztalatok és információk cseréjét, valamint a kiberbiztonsági irányítás és kutatás terén a legjobb gyakorlatok és tanulságok azonosítását és terjesztését[33].

Szakmai folyamatok indultak a villamosenergia-ellátási és -elosztási infrastruktúrára vonatkozó jogszabályi ellenőrzés fokozása érdekében, részben a korábbi incidensek, részben pedig az informatikai kitettség magasabb szintje miatt. Ez a jogalkotás az Egyesült Államokban már egy évtizeddel ezelőtt elkezdődött, Európában azonban csak az utóbbi években. Mivel azonban ez a jogalkotói szándékkal párosul, az ágazat fokozott ellenálló képességére számíthatunk a kibertámadásokkal szemben[34].

Mivel ez már nem kizárólag az egyes országok problémája, az Európai Unió és a NATO különböző megközelítésekkel foglalkozik ezzel a problémával. A NATO a stratégiai aspektussal foglalkozik, és sürgeti a tagállamok felkészítését a kiberműveletekre, mint a hadviselés különálló dimenziójára[35] Az EU inkább az operatív irányzattal foglalkozik: a Kiberbiztonsági jogszabályban[36] az egyik konkrét alkalmazás az ICS komponensek információbiztonsággal kapcsolatos tanúsítása, ahogyan azt az Európai Bizottság Közös Kutatóközpontja által kiadott Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)[37] írja. Mivel a fent leírt digitalizáció Közép-Európában még gyerekcipőben jár, célszerű nyugat-európai modellt használni az ilyen irányú tanulmányokhoz. Jó példa lehet a német piac, ahol szintén sok a kis közműszolgáltató. A német szabályozó hatóságok már foglalkoznak a víziközművek kiberbiztonságával, a KRITIS stratégia és az abból következő jogszabály a teljes német kritikus infrastruktúra kiberbiztonsági felelősségét határozza meg[38].

---

[33] BEDERNA Zsolt és RAJNAI Zoltán, Analysis of the cybersecurity ecosystem in the European Union, *International Cybersecurity Law Review*, 3. kötet, 1. szám, pp. 35-49, Jun. 2022, doi: 10.1365/s43439-022-00048-9.

[34] E. D. KNAPP és R. SAMANI, Alkalmazott kiberbiztonság és az intelligens hálózat: A biztonsági ellenőrzések bevezetése a modern villamosenergia-infrastruktúrába. Waltham, MA: Syngress, 2013.

[35] BÁNYÁSZ Péter, KRASZNAY Csaba és TÓTH András: A NATO kibervédelmi szakpolitikája, in: SZENES Zoltán (szerk.): *A mai NATO: A szövetség helyzete és feladatai*, HM Zrínyi, 2021, pp. 130-149.

[36] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (EGT-vonatkozású szöveg). http://data.europa.eu/eli/reg/2019/881/oj

[37] THERON P. et al.: Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS), *Ispra*, 2020. https://ec.europa.eu/jrc

[38] FETTIG Joachim és OLDENBURG Martin: Overview: Preparedness in the Water Supply and the Sanitation and Sewarege Sectors in Germany and Europe. In RATNAWEERA, H., PIVOVAROV O. A. (szerk.): *Physical and Cyber Safety in Critical Water Infrastructure*. Amsterdam: IOS Press, 2019.

Magyarországon úttörő kezdeményezés a SeConSys, a kritikus energetikai infrastruktúrák kiberbiztonságán együtt dolgozó szakemberek és szabályozók csoportja. Az ebben a keretben készült, a villamosenergia-ipari vezérlőrendszerek kiberbiztonsági kézikönyve[39] hiánypótló munka, amely útmutatást nyújt a védelem szabályozási, tervezési és üzemeltetési szintű fejlesztéséhez. Emellett a magyar tudományos szakirodalomban is találhatók esettanulmányok a megfelelő kibervédelem kialakításáról az energiaszektorban[40].

4.2. Kutatás, fejlesztés és innováció

A magyarországi és közép-európai kormányoknak, közműszolgáltatóknak, iparágaknak és kutatóintézeteknek ösztönözniük és támogatniuk kell a kiberbiztonsági kutatást, fejlesztést és innovációt a vízügyi ágazatban a tervezésre összpontosító multidiszciplináris és együttműködésen alapuló kutatási projektek, programok és központok finanszírozásával (vagy pályázatok benyújtásával), a biztonságos, rugalmas és megbízható intelligens vízügyi technológiák, rendszerek és szolgáltatások tervezésére, értékelésére és bevezetésére, valamint a fejlett kiberbiztonsági módszerek, eszközök és technikák - például kockázatértékelés, fenyegetésmodellezés, sebezhetőségi elemzés, behatolás-felderítés és incidensek elhárítása - fejlesztésére és alkalmazására irányulnak[41].

A víziközmű-szolgáltatók irányítási és informatikai rendszereinek érettsége és az ebből eredő kiberbiztonsági kockázatok – bár attól időben kissé lemaradva – a villamosenergia-ágazatéhoz hasonlóan fognak alakulni. A digitalizáció előrehaladása ezen a területen elkerülhetetlen, ami új típusú kockázatok megjelenésével is jár. Emellett a jelenlegi instabil geopolitikai helyzet még fontosabbá teszi a kritikus infrastruktúrák védelmét. Annak érdekében, hogy az üzemeltetők, a jogalkotók és a szabályozók felkészüljenek az ezzel járó kihívásokra, elengedhetetlen, hogy európai szakmai és tudományos kezdeményezéseket hozzanak létre a kérdés átfogó kutatására.

Az egyetemi kutatások is megkezdődtek ezen a területen. A CYBERWATER NATO Advanced Research Workshop például Harsha Ratnaweera, a Norvég Élettudományi Egyetem professzorának vezetésével végzett kutatásokat[42].

5. KÖVETKEZTETÉSEK

Ez a tanulmány az intelligens vízgazdálkodás növekvő jelentőségét elemezte a negyedik ipari forradalom és a hozzá kapcsolódó kiberbiztonsági kockázatok összefüggésében, különösen Magyarországon és Közép-Európában. Az intelligens vízgazdálkodás jelenlegi helyzetének

---

[39] ANGYAL István, ARATÓ György, BAKOS Béla, BARANYA Zsolt, BOCSOK Viktor, BOGÁNCS Tamás János, BONNYAI Tünde, BUTTYÁN Levente, CSATÁR János, DANYEK Miklós et al.: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve. Budapest: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, 2020.

[40] KRASZNAY Csaba, DANYEK, Miklós: Protecting the National Electricity System in the Cyberspace – A Case Study. In: TÖRÖK Bernát (szerk.): *Információ- és kiberbiztonság : Fenntartható biztonság és társadalmi környezet tanulmányok V.* Budapest: Ludovika Egyetemi Kiadó, 2020.

[41] CHERDANTSEVA i.m.

[42] NATO SPS: NATO Newsroom, 2018. https://www.nato.int/cps/en/natohq/news_157806.htm

vizsgálatával és az e kritikus ágazatot érintő különböző kiberbiztonsági fenyegetések, sebezhetőségek és kockázatok elemzésével a tanulmány arra törekedett, hogy felhívja a figyelmet a fokozott biztonsági intézkedések és gyakorlatok szükségességére az intelligens vízgazdálkodásban, valamint hogy alapot és irányt adjon a jövőbeli kutatásoknak.A kutatás a szakirodalomra és a hivatkozásokban felsorolt forrásokra korlátozódott. Egy szélesebb körű, több (köztük nagy) vízművön végzett kutatás megerősíthetné a megállapításokat.

A kiberbiztonság és az intelligens vízgazdálkodás jövőbeli kutatási irányai a következők lehetnek: empirikus és összehasonlító tanulmányok készítése a különböző kiberbiztonsági intézkedések, gyakorlatok és technológiák hatékonyságáról és eredményességéről a vízügyi ágazatban; a kiberbiztonság és a magánélet védelmének etikai, jogi és társadalmi vonatkozásainak és kihívásainak feltárása az intelligens vízgazdálkodásban, mint például az adatok hozzáférhetősége, a személyes adatok védelme, a hozzájárulás és az elszámoltathatóság.

Ezen és más kutatási kérdések és hiányosságok kezelésével a tudományos és szakmai közösségek hozzájárulhatnak a tudás és a gyakorlat fejlesztéséhez a kiberbiztonság és az intelligens vízgazdálkodás területén. Ez hozzájárul ahhoz, hogy a vízellátási ágazatban a digitális átalakulás és innováció előnyei és lehetőségei megvalósuljanak és fenntarthatóak legyenek, anélkül, hogy a kritikus víziközmű infrastruktúra, a vízellátási- és szennyvízkezelési szolgáltatások biztonsága, rugalmassága és bizalma sérülne.

UNIVERSITY OF PUBLIC SERVICE

LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2023/5.

Szerző(k) / Author(s):
Dr. Szádeczky Tamás PhD

Kézirat lezárásának ideje / Manuscript closing time:
2023.08.15.

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:
Dr. Magyar Sándor 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.

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.
The opinions and resolutions included in each issue of the series reflect the authors' own opinions. They should not be construed as an official point of view of either the publisher or the institutions employing the author.