Nagy Milada[1]

A kínai „okosváros”-eszközök biztonsági kockázatai

A világszerte üzembe helyezett, kínai eredetű „okosváros”-eszközök nemzet- és kiberbiztonsági kockázatokat rejtenek magukban. Az Amerikai Egyesült Államok kezdeményezésére 2020-ban létrejött Clean Network program – amelyhez bármely állam, szervezet csatlakozhat – biztonságos eszközök használatára szólít fel. Nem hanyagolható el a helyi hatóságok gyakorlatából ezen a téren adódó probléma sem. Ugyanis a települések maguk döntenek az okoseszközök telepítéséről, gyakran a nemzetvédelmi politikát és egyéb biztonsági kérdéseket figyelmen kívül hagyva.

Kulcsszavak: *okosváros, Clean Network, Kína, kiberbiztonság, nemzetbiztonság*

The Security Risks of Chinese Smart City Tools

The worldwide installed Chinese smart city tools involve national and cybersecurity risks. The Clean Network programme announced by the initiative of the United States of America in 2020 calls for the use of secure tools, with free joining of any country and institution. Controversies in the practice of local authorities of security tools installation should also be handled, considering that they often neglect the national security policies and other relevant security issues of their country.

Keywords: *smart city, Clean Network, China, cybersecurity, national security*

A világ népességének rohamos növekedése nélkülözhetetlenné teszi a városok, illetve azok környezeti és egyéb forrásainak hatékony kihasználását. Ez vezetett el az „okos város” elképzeléshez, amely számos alkalmazott, „okos” technológiát hozott magával. A fejlett világ államai elkezdték fejleszteni a nagyvárosaik „smartosítását”, ami például a közösségi terek mesterségesintelligencia-rendszereken alapuló hálózatba kötését eredményezte. Ezek a rendszerek azonban magukban hordoznak kiberbiztonsági és nemzetbiztonsági kockázatokat. A kínai vállalatok már javában exportálják a különböző okosváros-rendszereket, habár a „Nyugat” aggodalmát fejezte ki, hogy ezek a rendszerek az emberi jogokra és nemzetbiztonságra is veszélyt jelentenek.

Az okosváros *(smart city)* elképzelés azért jött létre, hogy a nagyvárosok élhetőbbek legyenek. A városi élet hatékonyabbá tételét technológiai megoldásokkal (adatelemzések a mesterséges intelligencia segítségével; a dolgok internete – *Internet of Things,* IoT; nagy mennyiségű adat feldolgozása – *big data;* kommunikációs hálózatok) próbálják elérni. Ezáltal a város (önkormányzat) által nyújtott szolgáltatások minősége, ütemezése és megvalósítása javul, csökkennek a költségek és a forrásigények, javul a kapcsolattartás

[1] Nagy Milada okleveles nemzetközi kapcsolatok elemző, biztonságpolitikai szakértő, főiskolai docens, a Budapesti Gazdasági Egyetem Külkereskedelmi Kar oktatója. E-mail: nagy.milada@uni-bge.hu

a lakosság és a hatóság között. Mindamellett, hogy ezek a megoldások fejlődést és jelentős hatékonyságot kínálnak, a smartcity-technológiák olyan kihívásokat is rejtenek magukban, amelyek az egyén magánszféráját vagy éppen az adatbiztonságát veszélyeztetik.

Az okosváros (vagy digitális város) koncepció alapjául applikációk széles palettája szolgál, amelyeket az elmúlt években, évtizedekben fejlesztettek ki. Los Angeles tette meg az első lépést a „smart city"-helyzet elérésének irányába, 1974-ben, amikor létrejött ott az első városi big data vállalat. Amszterdamnak további 20 évbe telt, amíg ott megalakult a saját digitális vállalata, a De Digitale Stad, és ezzel a világ első digitális városává vált.[2] 2005-ben a Cisco vállalat fektetett be a legtöbbet (25 millió USD öt éven át) a terület kutatás-fejlesztésébe, és 2008-ban az IBM vállalat bevezette a magát a „smart city" fogalmat. 2010-ben Japán Jokohamát választotta az úgynevezett Jövő Nemzedék Energiainfrastruktúrája és a Közösségi Rendszer Bemutatása Területének. 2011-ben Barcelonában tartották az első Smart City Kiállítás Világkongresszust.[3]

A smart city világpiaca folyamatosan növekszik, számítások szerint az értéke 2027-re megközelíti az 500 milliárd USD-t. Azoknak a vállalatoknak a száma, amelyek világviszonylatban kapcsolatba hozhatók a smart city applikációkkal egyelőre ismeretlen, de egy 2018-as cikk szerint a top 10 vállalatok között az olyan óriások találhatók, mint a Microsoft, Intel, General Electric, Cisco és IBM.[4]

A smart city technológiák esetében az előnyök mellett kockázatok is jelentkeznek. Ilyen például a településeken üzemelő okos kamerák általi információgyűjtés a lakosság életmódjáról, mobilitásáról, viselkedési mintáiról, amit az arcfelismerő és mesterségesintelligencia-technológiák teszek lehetővé. Azokat az infrastrukturális eszközöket, amelyek érzékelőkön, távirányításon alapulnak egyre szélesebb körben alkalmazzák, egyre több személyiségi adatot gyűjtenek, ezáltal növelik a külső kibertámadás kockázatát, amelyek az ellenőrzés megszerzésére és a károkozásra irányulnak.

Az autokratikus rezsimek ezeket a technológiákat a hatalmuk megerősítésére és a lakosság feletti ellenőrzés szorosabbá tételére használják. Éppen ezért sokkal nagyobb elővigyázatosságra van szükség a demokratikus államok részéről, amikor meghatározzák az okosvárosra vonatkozó szabályokat. A jogszabályok alkotása során el kell kerülniük azt, hogy majdan a gyakorlatban túlságosan nagy hatalom koncentrálódjon a hatóságok kezében, amivel a jogrendszernek, a kormánynak, illetve a lakosságnak kárt okoznának.

A kínai okosvárosok

Napjainkban Kína az egyik legnagyobb jelentőségű ország az okosvárosok terén. Egy 2017-es felmérés alapján Kínában található a világ 1000 okosvárosa közül 500.[5] Kína adatalapú urbanizációs politikájának elterjedése elsősorban a technológia fejlődésének

[2] Peter van den Besselaar: *The Life and Death of the Great Amsterdam Digital City.* [online], 2003. 09. 18–19. Forrás: www.researchgate.net [2021. 08. 02.]

[3] *Smart City Expo World Congress*. [online], 2021. Forrás: smartcityexpo.com [2021. 08. 02.]

[4] A top 15-ös lista és a cikk elérhetősége: Smart Cities World: *Top smart companies named in new index.* [online], 2018. 03. 08. Forrás: smartcitiesworld.net [2021. 08. 02.]

[5] Jamil Anderlini: *How China's smart-city tech focuses on its own citizens.* [online], 2019. Forrás: ft.com [2021. 08. 02.]

és a trendeknek köszönhető, másodsorban nem lehet figyelmen kívül hagyni a Kínai Kommunista Párt álláspontját arra vonatkozóan, hogy a technológia a belső stabilitás és ellenőrzés fenntartását szolgálja. Kína volt az első ország, amelyik az 1990-es években elsőként mutatta be a „digitális város" ötletet, majd a későbbiekben megváltoztatta az elnevezést „információ alapú város"-ra, 2009-ben pedig már okosvárosként emlegették, amikor a 12. gazdasági és fejlesztési ötéves terv (2011–2015) keretében prezentálták. A következő ötéves tervben „új okosváros" fogalom jelent meg, amely elsősorban a big data, az IoT és a felhő alapú informatikai technológiákra fókuszált. A kínai elnök, Hszi Csin-ping is támogatja az ez irányú kezdeményezéseket. 2017-ben hangsúlyozta, hogy Kínának ki kell terjesztenie a városfejlesztést, okossá kell tenni és a 21. századhoz kell igazítani azokat.[6] 2017-ben létrehozták Pekingtől délre a Xiongan új területet, amely a jövőbeli okosváros modellje és az új városi fejlesztések szimbóluma lett.

A mesterséges intelligencia és a smart city területén működő, világviszonylatban is jelentős vállalatok közül jó néhány kínai, mint például a Huawei, Megvii (arcfelismerő technológiát gyártó start-up), Sugon (nagy kapacitású szerverek gyártója), Chengdu Haiguang Microelectronics Technology (mikrochipgyártó), Hikvision (vezető vállalat a CCTV-kamerák piacán) stb. A számuk egyre növekszik, ami tükrözi a terület fontosságát mind a kínai ipar, mind pedig a kormány számára.

Kína diktatórikus berendezkedésű állam, a Kommunista Párt abszolút ellenőrzése alatt áll, amely irányítja a közigazgatási hatóságokat és az élet minden területét – a politikától a technológiai fejlesztésig. Ez mindenképpen rányomja a bélyegét az okosváros milyenségére az egész országban.

Egy 2020-as felmérés szerint a leginkább „felügyelt" (kamerákkal ellátott) városok közül 18 Kínában található. Az ország területén 2000–2018 között közel 200 millió úgynevezett CCTV (*closed-circuit television*, zárt láncú televízió rövidítése) biztonsági kamerából álló, relatíve sűrű hálózatot építettek ki, és azóta további több millió kamerát telepítettek, illetve kívánnak telepíteni.[7] A napjainkban közel 300 millió kamerával rendelkező kínai nemzeti biztonsági hálózat a Skynet elnevezést kapta.

A mesterséges intelligencia, arcfelismerés és big data technológiáknak köszönhetően Kína kidolgozta az úgynevezett társadalmi kreditrendszert, amely – a „mézesmadzag és furkósbot" hasonlatával élve – jutalmazza, illetve bünteti a lakosságot.[8] A rendszer – az okosvároshoz hasonlóan – azokat az „okos" infrastruktúrákat használja, amelyeket a lakosság megfigyelésére telepítettek közterületekre. A kreditrendszert illetően azonban az „elfogadhatatlan magaviseletre" vonatkozó teljes listát még nem hozták nyilvánosságra, ennek ellenére napvilágot láttak olyan hírek, amelyek szerint a vétkesek

[6] HSBC: *Smart cities are taking over, and over 50% of them are in China*. [online], 2018. 03. 28. Forrás: cnbc.com [2021. 08. 02.]

[7] Összehasonlításképpen, az Amerikai Egyesült Államokban körülbelül 50 millió CCTV-kamera működik.

[8] A kínai állampolgárok magatartásának, viselkedésének és adatainak gyűjtése révén a rendszer jutalmazza, illetve bünteti az embereket. A vörös listára kerülőknek például lakásbérlés esetében nem kell kauciót fizetni, különböző engedményeket kaphatnak a kommunikációs szolgáltatóktól stb. Feketelistára például olyan magatartással lehet kerülni, ha az illető az adósságát ki tudná fizetni, de nem teszi meg, vagy megpróbál kibújni a bírósági ítélet végrehajtása alól.

megtorlásban részesültek (például repülő-, vasúti, tömegközlekedési jegy vagy éppen ingatlan vásárlásának megtiltása).[9]

A közbiztonságért felelős minisztérium kezelése alá tartozó rendszerben az üzleti szféra és a hatóságok – beleértve a rendőrséget – közötti kapcsolat létezik. Néhányat a fentebb említett vállalatok közül az a vád ért, hogy segítik a kínai rendszert a helyi kisebbségek elnyomásában.[10] Ezt támasztja alá az interneten is közzétett felvétel, amely szerint egy Kínában telepített kamera arcfelismerő rendszere képes volt kiszűrni a rendőrség által körözött személyt.[11]

Napjainkban az úgynevezett „megnevezés és megszégyenítés" technológiájának fejlesztése zajlik, amelyet a kínai állam a közeljövőben igyekszik majd alkalmazni. A megvalósulásakor például egy nagyváros központi kereszteződésében kihelyezett kivetítőn – amely arcfelismerő kamerákkal van összekötve – keresztül bemutatnák a törvényszegőket arccal, névvel, igazolványszámmal.[12]

Egy másik új technológia, amelyet már néhány város rendőrségi állománya tesztel: az arcfelismerő szemüveg.

A kínai smartcity-rendszerek exportja

Kína nemcsak a területén alkalmazza a smartcity-rendszereket, hanem elkezdte ezek exportját is. Az Egy Övezet Egy Út Kezdeményezés keretén belül létrehozták a Digitális Selyemút stratégiai kezdeményezést 2015-ben.[13] Ennek célja a kínai technológiai óriások a világ minden táján történő megkapaszkodása volt, továbbá a kínai gyártású digitális infrastruktúra kiépítése, valamint a globális adat- és kommunikációs ellátó láncok feletti kínai ellenőrzés növelése. A kínai elnök egyik 2017-es beszédében arra mutatott rá, hogy a részvételük más országok smart city fejlesztésében a partnerország és Kína gazdasági együttműködésének kiterjesztését jelentette.[14]

Egy 2020-ban megjelent tanulmány szerint a kínai vállalatok mintegy 116 (köztük 38 ázsiai, 30 európai, 15 közel-keleti, 15 afrikai) országba exportálták az okoseszközöket.[15] Példának okáért a kirgiz fővárosban egy különleges irányítási központot állítottak fel a rendőrség részére, amelyet a kínai kormány CEIEC elektronikai vállalatának „smart" eszközeivel szereltek fel – ingyen. Ugandában a Huawei kötött szerződést 126 millió USD értékben okosvárosrendszerekre, Üzbegisztánban pedig 883 kamera és az okta-

[9] Yau Tsz Yan: *Exporting China's Social Credit System to Central Asia.* [online], 2020. 01. 17. Forrás: thediplomat.com [2021. 08. 02.]

[10] Louise Lucas: *China steps up surveillance on Xinjiang Muslims.* [online], 2018. Forrás: ft.com [2021. 08. 02.]

[11] Zack Whittaker: *Security Lapse Exposed a Chinese Smart City Surveillance System. Thousands of Facial Recognition Scans Were Matched against Chinese Policy Record.* [online], 2019. 05. 03. Forrás: techcrunch.com [2021. 08. 02.]

[12] Paul Mozur: *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras.* [online], 2018. 07. 08. Forrás: nytimes.com [2021. 08. 12.]

[13] Richard Ghiasy – Rajeshwari Krishnamurthy: *China's Digital Silk Road and the Global Digital Order.* [online] 2021. 04. 13. Forrás: thediplomat.com [2021. 08. 02.]

[14] *Full text of President Xi's speech at opening of Belt and Road forum.* [online], 2017. 05. 14. Forrás: xinhuanet.com [2021. 08. 02.]

[15] James Kynge – Nian Liu: *From AI to facial recognition: how China is setting the rules in new tech.* [online], 2020. Forrás: ft.com [2021. 08. 02.]

tásban az arcfelismerő technológia telepítésére kapta meg a jogot, mintegy egymilliárd USD értékben. Malajziában az Alibaba Cloud big data rendszert épített ki, ezáltal Kuala Lumpurban valósult meg először a rendszer Kínán kívüli telepítése. A Huawei Európába is „betört": Olaszországba, Hollandiába, Németországba, Franciaországba, Spanyolországba is exportálta a smart city rendszerét, míg a Hikvision az USA-t, az Egyesült Királyságot, Dániát és Japánt célozta meg. 2016-ban a sydneyi UTS egyetem írt alá megállapodást a CETC biztonsági vállalattal.

Az Egy Övezet – Egy Út Kezdeményezés részeként 2018 októberében Kína multilaterális megállapodást hozott tető alá a nemzetközi „társadalmi kreditrendszer szövetség"-ről, amelyben 35 kínai város mellett Olaszország, Franciaország, Mongólia, Mianmar, Szaúd-Arábia és Thaiföld voltak az aláíró felek.[16] A cél egy olyan platform megvalósítása, amely koordinálja a társadalmi kreditrendszer megalkotását. A kreditrendszer koncepciójának exportja túlmutat a technológiák vagy áruk kereskedelmén. Ráadásul önkormányzati szinten „lazábbak" a védelmi intézkedések, és nem igazán tartják szem előtt az országuk kül- és biztonságpolitikai szempontjait.

A koronavírus-járvány további lehetőséget adott a Huawei számára a mesterséges intelligencián alapuló rendszereinek terjesztésére. A kínai vállalat a szaúdi kormányt látta el különböző 5G és mesterségesintelligencia-alapú rendszerekkel, és a kórházakban, egyetemeken hőérzékelő kamerákat szerelt fel. Az Egyesült Arab Emírségekben Sardzsa (Sharjah) hatóságának önvezető járműveket adott el, hogy csökkentsék a tömegközlekedési eszközök megállóiban várakozni kényszerülő emberek létszámát. Chilében a Hikvision segített közel 700 hőérzékelő kamerát felállítani országszerte.[17]

A kínai smartcity-rendszerekkel szembeni fenntartások

Kínát sok kritika érte, hogy terjeszti a saját rezsimjének a normáit, értékeit és módszereit. A Szerbiában felszerelt Huawei térfigyelő kamerák arcfelismerő rendszerrel is rendelkeznek, és ott azt hozták fel ellenük, hogy ugyan a bűnözés visszaszorítására helyezték ki azokat, de az újságírók, ellenzéki politikusok és emberjogi aktivisták rezsim általi megfigyelésére is alkalmasak.[18] Egy 2019-es cikk állítása szerint a kínai vállalat alkalmazottai segítettek egyes afrikai kormányoknak az ellenzékiek nyomon követésében.[19] Az Amerikai Egyesült Államok Kereskedelmi Minisztériuma 28 kínai entitást és technológiai vállalatot tett feketelistára, köztük néhány, a fentiekben említett vállalatot, mert kapcsolatba hozhatók a kínai elnyomó politikával, a kisebbségi emberi jogok megsértésével.

Nyugati források azt állították, hogy a nemcsak a kínai állami vállalatok számára, hanem a magánvállalatoknak is előírja a jog a Kommunista Párttal és a minisztériumokkal való együttműködést. Például a nemzeti hírszerzésre vonatkozó jogszabály 7. cikkelye

[16] Yau Tsz Yan (2020) i. m.

[17] *Feature: Chinese facial recognition technology fully backs Chile's anti-pandemic fight.* [online], 2020. 07. 15. Forrás: xinhuanet.com [2021. 08. 02.]

[18] *Chinese facial recognition tech installed in nations vulnerable to abuse.* [online], 2019. 10. 16. Forrás: cbsnews.com [2021. 08. 02.]

[19] Joe Parkinson – Nicholas Bariyo – Josh Chin: *Huawei Technicians Helped African Governments Spy on Political Opponents.* [online], 2019. 08. 15. Forrás: wsj.com [2021. 08. 02.]

(2017) kimondja, hogy minden szervezet vagy állampolgár a törvényi keretek között köteles együttműködni a hírszerzési szervezettel, annak tevékenységét segíteni. A kínai kiberbiztonsági törvény 28. cikke szerint szükség van hálózati operátorokra, hogy technikai segítséget nyújtsanak – a joggal összhangban – az állami és nem állami biztonsági szerveknek, amelyek a nemzetbiztonságért felelősek és a bűnüldözésben részt vesznek.[20] Mivel a kínai gyártású kamerák információkat továbbítanak a kínai hatóságok felé, néhány nyugati ország úgy döntött, csökkentik azok használatát. Például Ausztrália és az USA a különösen érzékeny helyszíneken (katonai létesítmények, diplomáciai épületek) leszereltette ezeket a kamerákat, hogy megakadályozza a hírszerzést.

Habár a kínai vállalatok sorban cáfolták, hogy a kormányuk kémkedésre használná őket, az Amerikai Egyesült Államok kormánya 2018-ban úgy döntött, hogy bojkottálja a Dahua és a Hikvision vállalatok termékeit – nemzetbiztonsági okokra hivatkozva. 2019 augusztusában továbbment, és kiterjesztette a tilalmat a Huaweire és további 118 hozzá kapcsolható vállalatra. A feketelistát októberben hozták nyilvánosságra, amely megtiltja az amerikai vállalatoknak az „érzékenynek" minősített technológia, szoftver és egyéb felszerelés, alkatrész szállítását külföldi partnereknek, kiemelve a Huaweit és mellette más technológiai vállalatot is, amelyek termékei elsősorban az okosváros kiépítését szolgálják. 2020 novemberében az amerikai kormány továbbment, és megtiltotta az amerikai vállalatoknak a befektetési együttműködéseket 31 kínai vállalattal (a Hikvisiont és a Huaweit is beleértve), amelyek állítólag szoros kapcsolatban állnak a kínai biztonsági szolgálatokkal.[21]

Még 2020 augusztusában az USA Külügyminisztériuma meghirdette a Clean Network[22] program kiterjesztését, aminek az volt a célja, hogy létrehozzák azon államok technológiai koalícióját, amelyek szükségesnek tartják a kommunikációs infrastruktúrájuk biztonságossá tételét, beleértve a jövő technológiáit is. Külön kiemelték a forgalmazó megbízhatóságának fontosságát, aki nem állhat olyan autokratikus rezsim ellenőrzése alatt, amely megkerüli a jogszabályokat. A kezdeményezés szövege külön megemlíti a Kínai Kommunista Pártot mint e veszély hordozóját.[23]

A Clean Network egyik szempontja, hogy kivédje az amerikai állampolgárok személyes és vállalati adatainak kínai kézbe jutását. Hat különböző területen tiltja a kínai vállalatok részvételét: kommunikációs hálózatok, kommunikációs szolgáltatás, alkalmazás-áruházak (app store-ok), applikációk, felhőalapú adattárolás, víz alatti kábelek. Habár a kezdeményezés szövegében az okosváros fogalma nincs szó szerint feltüntetve, de a működtetéséhez olyan alrendszerek szükségesek, amelyek viszont a tilalom hatálya alá esnek. Az okosváros számtalan kiber- és adattárolási kockázatot rejt magában – függetlenül attól, hogy ki szállítja a technológiát.

---

[20] William Evanina: *Keynote Remarks As Prepared For Delivery.* [online], 2019. 06. 04. Forrás: dni.gov [2021. 08. 02.]

[21] A bojkottált 31 kínai vállalat listája itt (is) olvasható: Rebecca Choong Wilkins: *Here's a List of 31 Chinese Firms Named in U.S. Investment Ban*. [online], 2020. 11. 18. Forrás: bloomberg.com [2021. 08. 04.]

[22] A programot 2020 áprilisában fogadták el.

[23] Több mint 30 állam (pl. Csehország, Izrael, Észtország, Japán, Norvégia, Lengyelország, Franciaország stb.) csatlakozott a „tiszta országokhoz" *(clean countries),* amelyeknek szándékában áll megvédeni saját 5G hálózataikat a veszélyes és rosszindulatú beszállítóktól. Vö. U.S. Deapartment of State: *The Clean Network Safeguards America's Assets*. [online], 2020. 08. 11. Forrás: state.gov [2021. 08. 14.]

2020 májusában az Amerikai Egyesült Államok a *United States Strategic Approach to the People's Republic of China*[24] című dokumentumban Kínát kihívásként nevezi meg az USA gazdaságára, értékeire, biztonságára és a világrendre általában. Továbbá megvádolta Kínát, hogy az amerikai egyetemeket és vállalatokat arra kényszeríti, hogy alkalmazott technológiákat adjon át számára, vagy éppenséggel kibertámadásokkal szerzi meg ezeket. Ahogy az USA viszonya hűvössé vált Kínával szemben, úgy próbálta rávenni a szövetségeseit arra, hogy csatlakozzanak az USA Kína-politikájához és támogassák a kockázatkezelési mechanizmusait. A Clean Network terv is meghívja az USA szövetségeseit a csatlakozásra. 2020 novemberében Mike Pompeo a Twitteren tette közzé, hogy 53 országot, 180 telekommunikációs és több tucat vezető vállalatot tudnak már a kötelékben, amely a megbízható 5G-t tartja szem előtt.[25]

Azzal, hogy az Amerikai Egyesült Államok blokkolta a saját és a szövetségesei területén a Huawei részvételét az 5G hálózat kiépítésében, elérte, hogy a vállalat ne lehessen a vezeték nélküli technológia új generációjának globális éllovasa. Ebben az értelemben a jól ismert kínai és más országok technológiai vállalatai (például Samsung) között óriási verseny zajlik.

Ha tágabb körben vizsgáljuk a kérdést, nyilvánvalóvá válik, hogy a Clean Network az Amerikai Egyesült Államok és Kína viszonyában az elmúlt években (főleg a Trump-adminisztráció alatt) beállt hanyatlásnak az egyik következménye. Az USA lépései előrevetítik a technológiák megkettőződését, vagyis a párhuzamos fejlesztéseket. Ebben az esetben a globális rendszer szétválhat technológiai szövetségekre. Ez behatárolná az együttműködéseket olyan vállalatokkal és országokkal, amelyeket kockázati tényezőnek kiáltanak ki.

Természetesen a technológia megkettőződése kihat a kínai iparra is. A Skynet épp az amerikai bojkott miatt komoly akadályokkal küzd. Mivel az alkatrészellátása függ egyes amerikai és európai vállalatoktól, a kereskedelmi szigorítások miatt a beszállítások elmaradnak, így a Skynet fejlesztéséhez szükséges alkatrészek (például a mesterséges intelligenciával felszerelt kamerák komponensei, chipek) sem érkeznek Kínába. A Hikvision részvényeinek értéke látványosan esett, amikor az amerikai kormány bejelentette, hogy megtiltja a központi kormányzatnak a cég termékeinek használatát.[26]

Hosszú távon azonban az amerikai tilalom a kínai ipar előnyére változhat. A válság következményeként a kutatás-fejlesztésre fordított befektetések növekedhetnek, ahogy az amerikai/nyugati vállalatokkal folytatott verseny is erősödhet. A kínai vállalatok felkészültek a legrosszabbra és elkezdték az ellátó láncaikat bővíteni, hogy csökkentsék az amerikai és európai beszállítóktól való függésüket. Nagy valószínűség szerint ebben a technológiai versenyben a kínai vállalatok komoly segítséget kapnak a kormányuktól, mivel a smartcity-fejlesztések a vezetés prioritásai között szerepelnek, és a gazdaságnak is jelentős ágazatáról van szó. Ez a pénzügyi támogatás egyre jobban látható, akár az állam

[24] White House: *United States Strategic Approach to the People's Republic of China*. [online], 2020. 05. Forrás: trumpwhitehouse.archives.gov [2021. 08. 02.]

[25] Mike Pompeo: *Twitter-bejegyzés*. [online], 2020. Forrás: twitter.com [2021. 08. 14.]

[26] Sherisse Pham: *Chinese surveillance firm's stock plunges after reports of possible US ban*. [online], 2019. 05. 22. Forrás: cnn.com [2021. 08. 14.]

által támogatott befektetési alapok tevékenysége, akár a szubvenciók esetében. A Megvii 2019-ben 460 millió USD értékben jutott hozzá befektetésekhez, ebből az egyik egy állami hátterű alap volt.[27]

A közelmúltban a kínai kormány a civil-katonai együttműködést kezdte el erősíteni a mesterségesintelligencia-iparban. Ahogy a smartcity-technológia beszivárog a védelmi ipar eszközállományába, úgy fog növekedni a kutatás-fejlesztés állami támogatása. Általánosságban elmondható, hogy nemcsak Kínában, más országokban is a smart city növekvő fejlődést mutat, amelyet a védelmi ipar erőteljes K+F támogatása jellemez.

Az Amerikai Egyesült Államok smart city ambíciói is jelentősek. A Kereskedelmi Minisztérium segíti az ország vállalatait abban, hogy bővítsék ügyfélkörüket külföldön is a városi szolgáltatások terén, mivel úgy tűnik, az amerikai vállalatok inkább hazai településeken tevékenykednek, és lényegesen kisebb mértékben vannak jelen a nemzetközi piacon, mint a kínai vetélytársaik. A kivételek közül említhető az AT&T, amely Mexikóvárossal kötött megállapodást 2017-ben.[28]

Következtetés

Az okosváros-technológiák számtalan előnyük (a helyi hatóságok forrásainak hatékonyabb ellenőrzése, a közélet javítása stb.) mellett kockázatok sorát is magukban rejtik, elsősorban a nemzetbiztonságra és a magánéletre vonatkozóan. Az okosváros-koncepció aggodalmakat vált ki a demokratikus értékek sérülése miatt, mert az a vélemény alakult ki, hogy túl nagy hatalom kerül a helyi hatóságok és a politikai erők kezébe. A kormányoknak át kellene gondolniuk, milyen és mekkora hatalmat juttattak egyes szerveknek azáltal, hogy azok adatgyűjtési joggal rendelkeznek, és hozzáférésük is van ezekhez az adatokhoz.

Szükség lenne minden állam számára – amelyek alkalmazzák az okosvároseszközöket – saját vizsgálatra, továbbá egy minden részletre kiterjedő tervre és technológiára a közterületeken alkalmazott okos technológiákat illetően, hogy képet kaphassanak a jelenlegi helyzetükről „okosváros"-viszonylatban. Mindezt azért, hogy megfelelő elemzések készülhessenek a nemzetbiztonságra, magánéletre, kiberbiztonságra, adatvédelemre vonatkozó kockázatokról, valamint hogy miképpen tudják alkalmazni a Clean Network alapelveit.

A kormányzatoknak további feladata lenne a helyi hatóságok külkapcsolatainak fokozottabb ellenőrzése, hogy csökkentsék azokat a nemzetbiztonsági kockázatokat, amelyek például az okostechnológiák felhasználása során jelentkezhetnek. Ugyanakkor nem lehet szem elől téveszteni, hogy Kínával a kereskedelmet folytatni kell, lehetőség szerint a kétoldalú kapcsolatok sérülése nélkül.

Az okosváros fogalma nemcsak a vállalatok közötti gazdasági és technológiai verseny emblémája, hanem politikai és társadalmi rendszerek közötti versengést is jelent, de tekinthetjük a befolyásgyakorlás és a geostratégiai vetélkedés új területének is. Ezeken

[27] Mozur (2018) i. m.

[28] A fővárosi piactér vezeték nélküli internethálózatának kiépítésére vonatkozó megállapodás a vállalkozások lehetőségeit növelte, a tranzakciók lebonyolításának könnyítését jelentette. *Mexico City and AT&T Sign a Smart City Agreement*. [online], 2017. 11. 30. Forrás: att.com [2021. 08. 02.]

kívül, ahogyan jelentősége a védelmi iparban növekszik, úgy kerül át az államok közötti biztonsági rivalizálás területére is.

Felhasznált irodalom

Anderlini, Jamil: *How China's smart-city tech focuses on its own citizens.* [online], 2019. Forrás: ft.com [2021. 08. 02.]

Besselaar, Peter van den: *The Life and Death of the Great Amsterdam Digital City*. [online], 2003. 09. 18–19. Forrás: www.researchgate.net [2021. 08. 02.] Online: https://doi.org/10.1007/11407546_4

Chinese facial recognition tech installed in nations vulnerable to abuse. [online], 2019. 10. 16. Forrás: cbsnews.com [2021. 08. 02.]

Evanina, William: *Keynote Remarks As Prepared For Delivery.* [online], 2019. 06. 04. Forrás: dni.gov [2021. 08. 02.]

Feature: Chinese facial recognition technology fully backs Chile's anti-pandemic fight. [online], 2020. 07. 15. Forrás: xinhuanet.com [2021. 08. 02.]

Full text of President Xi's speech at opening of Belt and Road forum. [online], 2017. 05. 14. Forrás: xinhuanet.com [2021. 08. 02.]

Ghiasy, Richard – Rajeshwari Krishnamurthy: *China's Digital Silk Road and the Global Digital Order*. [online] 2021. 04. 13. Forrás: thediplomat.com [2021. 08. 02.]

HSBC: *Smart cities are taking over, and over 50% of them are in China*. [online], 2018. 03. 28. Forrás: cnbc.com [2021. 08. 02.]

Kynge, James – Nian Liu: *From AI to facial recognition: how China is setting the rules in new tech.* [online], 2020. Forrás: ft.com [2021. 08. 02.]

Lucas, Louise: *China steps up surveillance on Xinjiang Muslims*. [online], 2018. Forrás: ft.com [2021. 08. 02.]

Mexico City and AT&T Sign a Smart City Agreement. [online], 2017. 11. 30. Forrás: att.com [2021. 08. 02.]

Mozur, Paul: *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*. [online], 2018. 07. 08. Forrás: nytimes.com [2021. 08. 12.]

Parkinson, Joe – Nicholas Bariyo – Josh Chin: *Huawei Technicians Helped African Governments Spy on Political Opponents*. [online], 2019. 08. 15. Forrás: wsj.com [2021. 08. 02.]

Pham, Sherisse: *Chinese surveillance firm's stock plunges after reports of possible US ban*. [online], 2019. 05. 22. Forrás: cnn.com [2021. 08. 14.]

Pompeo, Mike: *Twitter-bejegyzés*. [online], 2020. Forrás: twitter.com [2021. 08. 14.]

SmartCitiesWorld: *Top smart companies named in new index*. [online], 2018. 03. 08. Forrás: smartcitiesworld.net [2021. 08. 02.]

Smart City Expo World Congress. [online], 2021. Forrás: smartcityexpo.com [2021. 08. 02.]

U.S. Deapartment of State: *The Clean Network Safeguards America's Assets*. [online], 2020. 08. 11. Forrás: state.gov [2021. 08. 14.]

White House: *United States Strategic Approach to the People's Republic of China*. [online], 2020. 05. Forrás: trumpwhitehouse.archives.gov [2021. 08. 02.]

Whittaker, Zack: *Security Lapse Exposed a Chinese Smart City Surveillance System. Thousands of Facial Recognition Scans Were Matched against Chinese Policy Record*. [online], 2019. 05. 03. Forrás: techcrunch.com [2021. 08. 02.]

Wilkins, Rebecca Choong: *Here's a List of 31 Chinese Firms Named in U.S. Investment Ban*. [online], 2020. 11. 18. Forrás: bloomberg.com [2021. 08. 04.]

Yan, Yau Tsz: *Exporting China's Social Credit System to Central Asia.* [online], 2020. 01. 17. Forrás: thediplomat.com [2021. 08. 02.]