A nemzetbiztonság fejlődő egyetemi kapcsolatai

Dobák Imre

A nemzetbiztonsági szolgálatok esetében különösen igaznak tekinthető, hogy új, naprakész ismeretek szükségesek feladataik ellátásához, az információk pontos értelmezéséhez, eszközeik, módszereik fejlesztéséhez. A szükséges ismeretek többek között a természettudományok, a társadalomtudományok, a műszaki tudományok vagy akár a bölcsészettudományok tudományterületein jelennek meg. Gondoljunk a már ismertetett, nemzetközi színtereken zajló biztonságpolitikai folyamatok vagy akár az infokommunikáció világában zajló rendkívül gyors fejlődés „megértésének" és „követésének" szükségességére, és az ezek mentén megjelenő tudományok sokoldalúságára.

Központi együttműködési szerep hárul így az egyetemi és tudományos környezetre, amellyel a „titkosszolgálatok" a történelemben visszatekintve is hagyományosan sokrétű kapcsolatokat folytattak. Ezek előzményei a hidegháború időszakáig visszatekintve mind a nyugati, mind a keleti blokk országaiban megtalálhatók, de napjainkban is személyi utánpótlásuk biztosítása, képzése, vagy akár az új ismeretek megszerzése érdekében általánosan fordulnak a civil egyetemi és kutatói közeg felé. Az alábbiakban a nemzetközi színtérre kitekintve – túlnyomórészt az amerikai példát ismertetve – ennek a kapcsolatrendszernek a sajátosságait és jellemzőit mutatjuk be.

Az egyetemi együttműködési felületek

Az egyetemek és nemzetbiztonsági szolgálatok közötti viszonyt tekintve a nemzetközi szakirodalmak alapján az alábbi fő együttműködési irányok, felületek láthatók:

– *képzési együttműködések:* Az egyetemek irányába hagyományos területként jelenik meg a nemzetbiztonsági ágazat munkaerő-utánpótlása biztosításának és az állomány képzésének igénye. Idesorolhatjuk a szolgálatok számára is nélkülözhetetlen civil (például jogi, műszaki, informatikai), valamint az egyre szélesebb körben értelmezhető (nemzet)biztonságot szolgáló képzéseket (például önálló nemzetbiztonsági) szakokat, akár szakosított intézményi formákat;

https://doi.org/10.36250/01005_10

- *kutatási együttműködések:* Ilyenek a kölcsönös előnyöket biztosító tudományos kutatások és fejlesztési együttműködések, amelyek egy része egyéb állami, illetve gazdasági szereplőkével azonos formában valósul meg, más részüknél azonban már szerepet kapnak a tudományos kutatások nemzetbiztonsági szempontjai (például nemzetbiztonsági védelem) is;
- *biztonságtudatosítás területe:* Egyre szélesebb körben látható a fiatal generációkat is veszélyeztető terrorizmus elleni küzdelem feladata, a radikalizáció megakadályozása, de idesorolhatók a kiberbiztonság biztonságtudatosító irányai is. A nemzetközi színtérre kitekintve az elmúlt években számos felsőoktatási program, gyakorlati képzési elem, kutatás jött létre a témakörökben;
- *külföldi hallgatók jelenlétéhez kapcsolódó együttműködés:* Sajátos területként értelmezhetők az egyetemeken tanuló nagyszámú külföldi hallgató jelenlétéhez kapcsolódó (nemzet)biztonsági szempontok. Amíg ezek alapját gyakran diplomáciai, illetve gazdasági jellegű együttműködések és partnerségi lehetőségek teremtik meg, addig egyfajta melléktermékként jelen lehetnek a tudományos eredmények kiáramlásától való félelmek (ipari kémkedés veszélye), vagy akár a nemzetközi hallgatói migráció összetett folyamatai.

A fentiek az egyik oldalról (egyetem) a nyílt tudományos rendszerek és gondolkodás, a másik oldalról (nemzetbiztonság) a szinte minden országban védett működést szükségessé tevő zártabb, biztonsági gondolkodás találkozását mutatják. A témakör áttekintését nehezíti, hogy a nemzetbiztonsági szféra érthető módon kevés információt oszt meg az állományát, képességét, vagy akár a fejlesztési irányait érintő kérdésekben. Igaz, az elmúlt években ezen a téren is változásokat láthattunk, amelyek mögött vagy egyes biztonsági szempontok felerősödése (például terrorizmus jelensége), vagy éppen a nyilvánosságot kapott titkosszolgálati botrányok hatásai álltak.

Képzési kapcsolatok

A nemzetbiztonsági szolgálatok és az egyetemek közötti kapcsolati-intézményi modell fő kereteit keresve Liam Gearon tanulmányában olvasható az a hármas modell[1] *(covert, overt, covert-overt),* amely segíthet a nemzetbiztonsági

[1] Liam Gearon: The counter-terrorist campus: Securitisation theory and university securitisation – Three Models. *Transformation in Higher Education,* 2. (2017), a13. 2519–5638.

szolgálatok egyetemekkel való (esetünkben főként képzési kérdésekre irányuló) kapcsolatát vizsgálni.

- A *fedett (covert)* modell a szerző megfogalmazását értelmezve a II. világháború és a hidegháború időszakának terméke, amely a hírszerzés professzionalizálásának időszaka. Idesorolhatók a hírszerzők felkészítésére szakosodott egyetemi szintű oktatási és képzési központok, felölelve a biztonság területeivel és az információgyűjtéssel kapcsolatos elemeket.
- A *nyílt (overt)* modell a felsőoktatási képzés vagy akár a kutatás nagyobb elszámoltathatóságot biztosító nyitott formája, amely rendkívül széles körű együttműködési lehetőségeket jelenthet.
- A *fedett-nyílt (covert-overt)* modellhez sorolja a szerző például a „titokban kémkedéssel foglalkozó egyetemi akadémikusokat, miközben azok teljes mértékben nyitott tudományos feladatokat látnak el".[2]

Leginkább a nyílt modellhez tartozó elemek vizsgálhatók, ahol az egyetemekkel megvalósuló tudományos és képzési kapcsolatokat számos projekt, nyíltan közzétett partnerségi megállapodás, egyetemeken kiírt ösztöndíjak és egyéb pályázati formák is jeleznek. Itt említhetők meg a humán erőforrás biztosítására irányuló képzési célú, akkreditált nyílt felsőoktatási programok, gyakorlati-gyakornoki képzési együttműködések és egyéb közös pályázati formák.

Az egyetemi szféra és a védelmi/nemzetbiztonsági szféra átfogó kapcsolatrendszere vizsgálatának nehézségét jelzi, hogy teljességgel nem nyilvános annak száma és pontos szerkezete. Példaként az Egyesült Államok említhető, ahol az amerikai hírszerzés (CIA) már a 20. század közepén titkos formában jelen volt az egyetemeken, majd az 1960-as évek végén beszivárgott az amerikai Nemzeti Diákszövetségbe is, elősegítve ezzel toborzási tevékenységét és hidegháborús ideológiájának támogatását az egyetemi campusokon. Igaz, válaszként Lyndon Johnson elnök megtiltotta a CIA tevékenységét a felsőoktatásban,[3] de az 1980-as évektől a szervezet visszatért az egyetemek campusaira.

Napjaink viszonyait tekintve nehéz megbecsülni, hogy pontosan hány együttműködés, program létezik,[4] azonban ezek látható módon kiterjednek többek

[2] Gearon (2017): i. m.

[3] Tony Vellela: *New Voices. Student Political Activism in the '80s and '90s.* Boston, South End Press, 1988. 60.

[4] Scott Firsing: The Growing Link between Intelligence Communities and Academia. *The Conversation,* 2015. szeptember 30.

között a nemzetbiztonsági és hírszerzési jellegű új egyetemi képzésekre. Egy 2015-ben megjelent amerikai tanulmány szerint az Egyesült Államokban több mint 250 intézmény kínált diplomákat, tanúsítványokat a tágan értelmezett belbiztonság területén, ahol a képzések több területet is felöleltek (például kiberbiztonság, katonai hírszerzés, rendvédelem). Az állami finanszírozás mellett jelen voltak a magánfinanszírozási elemek, valamint a 2001 utáni megváltozott környezethez és kihívásokhoz igazodva bizonyos területek képzését a biztonsági szféra ki is szervezte, illetve teret nyertek az online programok.[5] A tanulmány „90 ezer személy hírszerző közösséghez (IC) való kapcsolata" alapján állított fel rangsort[6] az Egyesült Államok 100, a védelmi-nemzetbiztonsági szférához leginkább közel álló felsőoktatási intézményéről. Mint megfogalmazzák, a

> „VICE News listáján a felsőoktatási intézmények 4 kategóriája dominál, így azok az iskolák, ahol a hallgatók alapvetően online diplomákat kapnak, amelyek érintettek a védelmi, hírszerzési és biztonsági kutatás-fejlesztésekben, amelyek Washington, D. C.-ben vannak; valamint azok, amelyek a belbiztonságra újonnan helyezik a hangsúlyt".[7]

Érdekesség, hogy „az adathalmazt jelentő 90 000 személy közül kevesebb mint 400 rendelkezett diplomával a nemzetbiztonsági tanulmányokban, kevesebb mint 5%-ának van közép- vagy felsőfokú végzettsége politikai tudományi területen, és még alacsonyabb volt a nemzetközi kapcsolatok aránya".[8]

Egyetemi kutatási kapcsolatok

Már a hidegháború szemben álló feleire jellemző volt az egyetemi tudományos kapcsolatok felhasználása, a biztonság területeihez kapcsolódó kutatóintézeti környezet kialakítása. A különböző fejlesztéseknél azonban törekedtek a nemzeti, illetve szövetségi szinten elért eredmények, megoldások

[5] Firsing (2015): i. m.

[6] A rangsorolás kialakításánál figyelembe vették, hogy a hírszerző közösségben (IC) hány embernek volt diplomája, igazolása az egyes iskolákból, majd 51 további tényező alkalmazásával kiigazították. William M. Arkin – Alexa O'Brien: The Most Militarized Universities in America: *A VICE News,* 2015. november 6.

[7] Arkin–O'Brien (2015): i. m.

[8] Arkin–O'Brien (2015): i. m.

alkalmazására (és megtartására). Általánosságban mind a nyugati, mind a keleti blokk titkosszolgálatainak feladatrendszerében megtalálhatjuk a tudományos és technológiai hírszerzési feladatokat, szervezeti elemeket,[9] továbbá kiemelt szerepet kapott a katonai jellegű kutatás-fejlesztés, amelynek jelentősége a hidegháború végével azonban globálisan csökkent.[10] Ennek az időszaknak a fejlesztési sajátosságaira többek között az alábbiak voltak jellemzők:

- a hidegháborús szembenálláshoz igazodó rendkívüli technológiai verseny;
- a fejlesztések során az állami/védelmi/katonai szempontok meghatározó szerepe;
- az ipari, technológiai, gazdasági jellegű hírszerzés kiemelt jelentősége;
- a nemzeti szinteken rendelkezésre álló K+F képességek és kapacitások felhasználása,
- a nemzeti szintű (állami) „külső" kutatóintézetek, egyetemek nem nyilvános módon történő bevonása;
- a szövetségesi rendszerben partnerként megjelenő országokkal való technikai, technológiai és tudományos együttműködések, tapasztalatcserék.

Az új technológiák, innovatív megoldások kutatása, rendszerbe állítása napjaink nemzetbiztonsági szolgálatainál is jelen van, aminek során a technológiai környezet nyomon követése egyre fontosabbá válik. Ezek sajátos jellemzői között láthatók:

- a zártság, amely a nemzetbiztonsági K+F tevékenységek egész folyamatára kiterjedhet;
- a kutatási tevékenység nemzetbiztonsági jellegű védelme;
- a kutatásokba bekapcsolódó személyek körének korlátozottsága;

[9] A korábbi Szovjetunió szolgálatai esetében bővebben lásd Fredrik Westerlund: *Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?* Stockholm, Defence Analysis FOI Memo 3126, 2010. A tudományos és technológiai hírszerzési tevékenységek jelentősége napjainkban sem csökkent. Nemzetközi példák alapján jól látható, hogy számos titkosszolgálat jelenleg is erőfeszítéseket tesz a technológiai és tudományos hírszerzés érdekében. Ezek közé sorolható, amikor egyes országok ipari szegmensük fejlesztése, a hazai K+F elősegítése és gazdasági versenyképességük növelése érdekében alkalmazzák a hírszerzésnek ezt az irányát.

[10] Csiki Tamás – Tálas Péter: A védelmi beszerzés és kutatás-fejlesztés kapcsolata a védelmi tervezés rendszerében – nemzetközi tapasztalatok. *Nemzet és Biztonság,* (2013), 3–4. 107–142.

- a titoktartás és a tudományos nyitottság gyakran egymásnak ellentmondó szempontjai;
- a kutatásokba bekapcsolódni tudó állomány elvándorlása;
- valamint az egyedi finanszírozási formák, illetve a nyílt és zárt rendszerek (projektek) hatékony együttműködését biztosító működtetési modellek kialakítása.

Az európai védelmi kutatás-szervezés kereteinek védelmi szektorban történő vizsgálatát a Csiki–Tálas szerzőpáros végezte el tanulmányában, ahol több modellt is ismertetnek. Egyrészről a szervezetek minisztériumokhoz való közelsége szerint egy „angolszász" és egy „kontinentális" modellt kategorizáltak.[11] A tanulmányukban hivatkozott[12] védelmi kutatás-fejlesztés súlypontja alapján felállított másik felosztásban a katonai modell és az ügynökség-modell mellett megjelenik az állami vállalati/állami egyetemi kutatási modell, valamint az egyetemi modell. Utóbbi két, egyetemekhez kapcsolódó forma esetében a felsőoktatásban egy-egy témakörben rendelkezésre álló kiemelt kutatási képességre építenek.

A kérdést feltéve, hogy a nemzetbiztonsági szféra számára kutatási kérdésekben miért válik egyre fontosabbá az egyetemek szerepe, a válasz több részből tevődhet össze. Egyrészről, az egyetemek a tudományos és technológiai ismeretek legjelentősebb központjai, azok a helyszínek, ahol multidiszciplináris megoldásokat lehet keresni új problémákra.[13] A különböző tudományterületek képviselői koncentráltan vannak jelen, ami a nemzetbiztonság egyre szélesebb értelmezését tekintve hatékonyan biztosíthatja adott témakörökben új eredmények létrehozását, közvetve a szolgálatok munkájának hatékonyságát. Másrészről, az egyetemek lényegében teret adnak a gazdasági-üzleti élet vagy akár az állam (idesorolva a nemzetbiztonsági szféra) működését elősegítő új

[11] A Csiki–Tálas (2013) szerzőpáros írásukban megállapítják, hogy az angolszász modellt a „kutatás-fejlesztés növekvő mértékű kiszervezése jellemzi a civil fejlesztési források bevonásával", míg a kontinentális modell esetében „a védelmi kutatás-szervezés erősen kötődik a védelmi minisztériumokhoz".

[12] Rudolf Urban –Martin Macko: *Place and Role of the Defense Science in the Czech Research and Development System.* Brno, University of Defence, 2011. idézi Csiki–Tálas (2013): i. m.

[13] Gearon (2017): i. m. 192.

tudományos eredmények létrehozásának,[14] innovatív megoldások kidolgozásának. A közegben adottak a nemzetközi szintű, rendkívül gyors, tudományos információcserét biztosító kapcsolatok, valamint jól működnek a hagyományos szervezeti formákon kívüli virtuálisnak tekinthető nemzetközi tudományos közösségek, kutatócsoporti keretek.[15]

A látható kutatási irányokat tekintve napjaink egyik legmeghatározóbb együttműködési iránya a kiberbiztonság témaköre, amelyben az egyén, a gazdasági élet szereplői és az állami szféra érdeke kölcsönösen találkozik, elősegítve ezzel a közös innovatív gondolkodást. Az egyetemi együttműködések számos formája jött létre (kiválósági központok, oktatási kiválósági központok, felsőoktatási képzések és akkreditált képzési helyek vagy akár a vállalati szféra bevonásával járó közös projektek, programok), ahol a partnerek közös céljai a kiberbiztonsági kutatás, innováció vagy akár új „kiberbiztonsági termékek és szolgáltatások" fejlesztése.

Az egyetemek irányába is megmutatkozó (nemzet)biztonsági célzatú K+F együttműködésre széles körben ismert példaként a globális nagyhatalom Amerikai Egyesült Államok 1958-ban létrehozott DARPA szervezete említhető, amely a mindennapi életünket meghatározó új technológiák létrejöttében vált közismertté. A kutatókat, egyetemeket, kutatóközpontokat, PhD-kutatásokat szponzoráló, projekteket indító szervezet története[16] és az élet számos területén napjainkban már nélkülözhetetlen alkalmazásai jól példázzák a védelmi/nemzetbiztonsági struktúrákon belüli innovatív gondolkodás szükségességét. A szervezet jelentősége a fejlett technológiákhoz kapcsolódó új tudományos eredmények létrehozásában, a kutatásokba bevonásra kerülő civil szereplők, intézetek, egyetemek kutatási, innovációs munkáján keresztül meghatározó.[17]

[14] A világ egyetemeinek rangsora alapján (QS rangsor) 2019-ben 19 egyesült államokbeli és nyolc nagy-britanniai egyetem szerepel a legjobb 50 egyetem között. A külön mért kutatási intenzitást tekintve ezek mindegyike nagyon magas értékkel jelölt intézmény. A magán finanszírozású, illetve széles körben nyitva álló állami kategóriákat tekintve közel megegyezik a megoszlásuk. A világ legjobb 50 egyeteme között megjelenő amerikai és brit egyetemek hivatalos weboldalait áttekintve is jól látható, hogy jelen vannak a (nemzet)biztonsági kérdéskörök, képzési felületek, vagy akár a (nemzet)biztonsági célú kutatási kapcsolatok. Lásd Top Universities: www.topuniversities.com/university-rankings/world-university-rankings/2019

[15] Lásd például: www.researchgate.net/, www.academia.edu/

[16] William Regli: Universities in Service to National Security, DARPA's Call to Academia. In *DARPA Defense Advanced Research Projects Agency 1958–2018 (60 years).* Faircount Media Group, 2018. 134–136.

[17] Kadtke–Wharton (2018): i. m.

A megoldás nem egyedülálló, és mint Major Milán kutatásában részletesen ismerteti, 2012-ben Oroszország is létrehozta az amerikai DARPA-hoz hasonló „Perspektivikus Kutatások Alapját", elősegítve ezzel új technológiák fejlesztését (kiemelten a robotika, a pilóta nélküli repülőeszközök [UAV-k], valamint a nanotechnológia területén).[18]

A nemzetbiztonsági szolgálatok K+F együttműködéseit tekintve, visszatérve az amerikai példához, a Nemzetbiztonsági Ügynökség (NSA) emelhető ki, ahol hagyományosan jelentős szerepet játszik a partnerségi forma. A szervezet 2012-ben közzétett, *Access to innovation: NSA's Technology Transfer Program*[19] című tanulmánya alapján az NSA már 1990-ben létrehozta TTP-programját „az NSA feltalálóinak a szövetségileg finanszírozott szellemi tulajdon megosztására és együttműködő kutatások végzésére a magánvállalatokkal, tudományos helyekkel, nonprofit szervezetekkel, más szövetségi ügynökségekkel, valamint állami és helyi önkormányzatokkal".[20] Az NSA programja esetében olyan megoldásokat láthatunk, mint a szabadalmi licencmegállapodások,[21] amelyek lehetővé tehetik a partnerekkel való közös kutatási és fejlesztési tevékenységet,[22] biztosíthatják a tapasztalatok megosztását, képzések nyújtását,[23] valamint technológiatranszfert nyújthatnak[24] más kormányzati ügynökségek számára.[25]

Az Egyesült Államokban a 2000-es évek közepe óta erősödött fel annak a kormányzati igénye, hogy a nemzetbiztonsági szervezetek fokozottabban működjenek együtt külső, tudományos felekkel az innováció és képességeik továbbfejlesztése érdekében. A szervezet az elmúlt időszakban is folyamatosan bővítette a nemzetbiztonsággal, kriptográfiával, kiberbiztonsággal kapcsolatos egyetemi együttműködéseit. 2013-ban például ötéves partnerséget alakítottak ki a North Carolina State Universityvel az analitikai tudományok laboratóriumának

[18] Mint Major Milán kutatásában részletesen ismerteti, Oroszország esetében a rendkívül összetett portfólióval rendelkező védelmi ipar elmúlt évtizedekben történt átszervezéseit követően jelenleg is több millió alkalmazottat foglalkoztat. Az idesorolható cégek és szereplők esetében is fontos szempont a kutatás-fejlesztés, és ezen keresztül az Oroszországi Föderáció innovációs előrehaladásához való hozzájárulás. Lásd Major Milán: Az orosz védelmi ipari komplexum a Szovjetunió szétesésétől napjainkig. *NKE Stratégiai Védelmi Kutatóintézet Nézőpontok,* (2020), 2. 1–10.

[19] Access to innovation: NSA's Technology Transfer Program. *The Next Wave,* 19. (2012), 3.

[20] Access to innovation (2012): i. m.

[21] *Patent License Agreements* (PLAs).

[22] *Cooperative Research and Development Agreements* (CRADAs).

[23] *Educational Partnership Agreements* (EPAs).

[24] *Technology Transfer Sharing Agreements* (TTSAs).

[25] Access to innovation (2012): i. m.

(LAS) létrehozására, amely küldetése a szolgálat, a tudományos szféra és az ipar közötti együttműködés a big data kérdéskörrel kapcsolatos kihívások megoldására.[26]

A nyíltnak tekinthető együttműködési formákhoz sorolva, az amerikai mellett a brit GCHQ[27] mint technikai feladatkörrel rendelkező nemzetbiztonsági szolgálat esetében is kiemelt hangsúlyt fordítanak a fiatal generációkat megcélzó utánpótlásra, a kapcsolódó képzésekre, kapcsolatrendszerekre. Egyetemi partnerségi programokkal rendelkeznek a kiberbiztonság területein, elősegítve a témakör külső felekkel történő közös kutatását.[28] Példaként említhető, hogy a GCHQ már évekkel ezelőtt „nyolc egyetemet választott partnerévé a kiberbiztonsági tevékenységben",[29] de itt emelhető ki az Alan Turing Intézettel fennálló együttműködés is, amely a GCHQ-val közösen indította el az egyetemi tudományos vagy akár a vállalati szféra felé is kapcsolatot biztosító működését az adattudományok terén.[30]

Az együttműködések védelmének szükségessége

A (nemzet)biztonsági ágazat jellegéből adódóan a szféra érdeklődési körébe tartozó kutatások és infrastruktúra sajátos védelmet igényel.[31] Ez a védelem

[26] Christopher Kampe et al.: Bringing the National Security Agency into the Classroom: Ethical Reflections on Academia-Intelligence Agency Partnerships. *Science and Engineering Ethics,* (2019), 25. 869–898.

[27] GCHQ *(Government Communications Headquarters)* Nagy-Britannia technikai feladatrendszerű nemzetbiztonsági szolgálata. Széles körben ismertek a brit titkosszolgálatok keretei között fejlődő SIGINT-képességek történeti előzményei, így például a híres Bletchley Parkban a II. világháború idején folytatott kódfejtési tevékenység. Összetett feladatrendszere mentén, a GCHQ feladataival már 1946 óta segíti a brit kormány és szövetségesei katonai, diplomáciai és bűnüldöző szerveinek tevékenységét. Lásd GCHQ: *Bletchley Park & WWII* (é. n.).

[28] GCHQ: *Education & Outreach* (é. n.).

[29] Richard Tyler: GCHQ Recruits Eight Universities to Counter Cyber Attacks*. The Telegraph,* 2012. április 1.

[30] Secure Trend 2015, valamint The Alan Turing Institute: *Current Partnerships and Collaborations* (é. n.).

[31] David Dwaine Cornely: *Leadership and Security: Factors that Support or Prevent Successful Integration into Research and Development Organizations.* Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Management in Organizational Leadership. University of Phoenix, 2003.

azonban nem pusztán ágazati sajátosság, hiszen a profitorientált gazdasági környezetben zajló, üzleti titkokat, új innovációkat érintő kutatások terén hasonló kritériumokkal találkozhatunk. Mivel az új technológiák, megoldások mindig is a másik fél hírszerző szervezetének érdeklődési körét képezték, nem lehet kétségünk afelől, hogy a tudományos és technológiai hozzáértés megszerzésének célja napjainkban is jelen van[32] (akár az idegen államok érintett szervei, akár a vállalatok oldaláról jelentkező ipari kémkedés előtt). Megjelenésük az új tudományos eredmények, innovációk létrehozásával párhuzamosan erősödhet fel, akár a humán információgyűjtés, akár a kibertérben végzett információgyűjtési megoldásokon keresztül.

A védett tudományos információk megszerzésére irányuló törekvések azonban hosszú távon negatív hatással lehetnek annak elkövetőjére, hiszen tudományos partnerei részéről bizalomvesztést eredményezhetnek. Ennek következményeként – akár jelentős gazdasági hátrányokat okozva – elzárulhatnak az új tudományos eredményekhez való hozzáférés forrásai. Az ipari kémkedés lehetőségének ellensúlyozására, a zárt tudományos kutatási területeknél érthető módon így jelen kell lennie a biztonságtudatos szemléletnek, valamint hatékony biztonsági programokat kell beágyazni a K+F szervezetekbe.[33] Az új eredmények, innovációk nemzetbiztonság célú felhasználása mellett fontossá válik az ott keletkező információk védelmének kialakítása,[34] a szükséges információvédelmi protokollok kidolgozása, a minősített információk megfelelő kezelése.

A nemzetbiztonsággal való egyetemi együttműködések során felmerülhetnek egyéb bizalmatlansági kérdések is. Idesorolhatók akár egyes tudósok, kutatók azon félelmei, hogy a nemzetbiztonsági szférával való együttműködés rányomhatja a bélyegét (például ipari kémkedés gyanúja) megjelenésükre a nemzetközi környezetben és tudományos kapcsolataikra is, így kevesebb eséllyel válhatnak részeseivé az új tudományos eredményeket létrehozó nemzetközi projekteknek. Mint Fredrik Westerlund felveti tanulmányában: „A hírszerző szolgálatokkal való kapcsolattartás valószínűleg nem csak tönkreteheti az egyes tudósok, vagy vállalkozók nemzetközi helyzetét, hanem megzavarhatja a kutató szervezetet és korlátozza a külföldi szereplőkkel folytatott szoros együttműködés lehetőségeit."[35] A legrosszabb esetben aláássa a bizalmat az adott intézmény irányába.

[32] Westerlund (2010): i. m.
[33] Cornely (2003): i. m. 4.
[34] Peter McPherson – Mary Sue Coleman: We Must Have Both. *Inside Higher Ed,* 2019. augusztus. 5.
[35] Westerlund (2010): i. m.

A nemzetbiztonsági területen nem ismeretlen annak gyakorlata sem, hogy a szférába kerülő, korábban nyílt tudományos életet és kapcsolatrendszert folytató kutató számára a védett kutatásokon alapuló tudományos eredményeinek nyílt publikálása érthető módon elmarad.

Az új tudományos eredmények kiáramlásához kapcsolódó félelmek

Az új tudományos eredmények kiáramlásához kapcsolódó félelmek, az egyetemeken folyó kutatások irányába megjelenő „indokolatlan érdeklődés" (így például egy másik ország által motivált információszerzés) témaköre az elmúlt években egyre nagyobb visszhangot kapott a nemzetközi politikai színtéren. Az Egyesült Államok esetében a „félelmek" közvetlenül érintették az egyetemi és tudományos szférát is, egyrészről a „veszélyesnek" ítélt országok (például Kína, Irán, Oroszország, Észak-Korea) diákjainak és kutatóinak jelenléte, másrészről az ezen országokhoz köthető „tehetséggondozási" programokban való részvételek miatt. Ezek közül a legjelentősebb veszélynek az országban tudományos kutatásokban részt vevő nagyszámú kínai hallgatói és kutatói közösséget tekintik. John Negroponte[36] szerint Kínából „évente 250 000 hallgatót küldenek az Egyesült Államokba", akik egy részéről feltételezhető, hogy a világ legjelentősebb gazdasági hatalmává válni akaró Kína nyomást gyakorol rájuk, hogy hazatérésükkor jelentsenek a kínai kormánynak.[37] Kína egyébként is egyre emelkedő létszámú hallgatót küld a világ különböző országainak oktatási intézményeibe, így amíg 2008-ban közel 180 ezer, addig 2018-ban már 662 ezer hallgató tanult külföldön.[38] Ebből az Egyesült Államokban a 2009/2010-es tanévben több mint 127 ezer, de a 2018/2019-es tanévben már több mint 369 ezer hallgató tanult, amivel Kína a nemzetközi hallgatók elsődleges forrása.[39]

Általánosan elmondható, hogy a mérnöki, a matematikai és a számítástechnikai tudományok területén a nemzetközi hallgatók teszik ki az amerikai egyetemeken a doktori fokozatot szerző hallgatók többségét. 2017-ben például

[36] Az USA első Nemzeti Hírszerzési Igazgatója (DNI) 2005–2007 között.

[37] Green (2019): i. m.

[38] Adatok forrása: Number of Students from China Going Abroad for Study from 2008 to 2018. *Statista,* (2020).

[39] Adatok forrása: Number of College and University Students from China in the United States from Academic Year 2009/10 to 2019/20, *Statista*.

a Kínából érkező hallgatók 5157 tudományos és mérnöki doktori fokozatot szereztek, ami abban az évben az USA-ban szerzett 41 438 doktori fokozat több mint 12%-a volt.[40]

Idesorolhatók az USA és Kína 2018–2020 közötti gazdasági háborújának légkörében felszínre került egyéb sérelmek,[41] illetve a kínai technológiai nagyvállalatok térnyerése[42] elleni szankciók is, amelyek hátterében az Egyesült Államok attól való félelmei állnak, hogy kínai távközlési gyártók eszközein keresztül a kínai kormány számára lehetővé válik az USA elleni kémkedés. A válaszként 2018-ban aláírt amerikai jogszabály (*National Defense Authorization Act,* NDAA) létrehozása azonban jelentős hátrányt okozhat az egyetemi-tudományos szférának, hiszen az amerikai egyetemeken évek óta meghatározók a kínai támogatások, a kínai hallgatói és kutatói állomány létszáma, valamint számos területen közös érdek az új kutatási eredmények létrehozása. Az egyetemek számára így a kínai féltől való eltávolodás egyik oldalról akár adott kutatási projektek visszaesését, másik oldalról a jogszabály 2020 augusztusáig történő nem teljesítése esetén az állami kutatási támogatások elvesztését jelentheti.[43] Mindez jól jelzi a gazdasági és nemzetbiztonsági érdekek, valamint az egyetemi kutatások „nemzetközi" határokon átnyúló jellegét, összetett megjelenését.

Az áttekintett forrás alapján 2019-ben az FBI, a kínai diákok és kutatók részvételével zajló, védelmi iparban felhasználható kutatások felülvizsgálatát kérte több egyetemtől, és tájékoztattak több vállalatot, kutatóintézetet a kínai hírszerzési és kiberbiztonsági fenyegetésekről.[44] Egyes egyetemek megszakították

[40] A tudomány és biztonság kapcsolatát vizsgáló tanulmány megfogalmazza, „ha az akadémikusok és a csúcstechnológia más őrzői nem lesznek óvatosabbak, az USA azt kockáztatja, hogy más országoknak – nevezetesen Kínának – lehetővé teszi, hogy ellopják az amerikai adófizetők által finanszírozott kutatás gyümölcseit, és megalapozzák, hogy technikai előnyt szerezzenek bizonyos kritikus tudományos és technológiai területeken". Elizabeth Redden: Science vs. Security. *Inside Higher Ed,* 2019. április 16.

[41] Deák András György: Kevés egyezmény, kívánt eredmény? – Trump kínai „vámháborújának" mérlege. *NKE Stratégiai Védelmi Kutatóintézet Elemzések,* (2020), 8. 1–12.

[42] „Peking hivatalos célja Kínát egy innováció-alapú országgá tenni 2020-ig, illetve a világ vezető innovációs központjainak egyikévé válni 2030-ig." Forrás: Külgazdasági és Külügyminisztérium Magyarország Nagykövetsége, Peking, Vezetői összefoglaló, 2017–18 TET éves beszámoló.

[43] Heather Somerville – Jane Lanhee Lee: U.S. Universities Unplug from China's Huawei under Pressure from Trump. *Reuters,* 2019. január 24.

[44] Diákmunka: Az FBI diákokkal figyelteti a kínaiakat. (MTI) *Librarius,* 2019. június 30.

a Kínával folytatott közös kutatásaikat, együttműködéseiket,[45] mások azonban ellenérzéseket fogalmaztak meg a nemzetbiztonsági szervek kéréseivel kapcsolatosan. Jelen pillanatban még nem látható, hogy a 2020 elején kirobbant világjárvány elleni küzdelem közös, országokon túlmutató érdeke hogyan fogja formálni ezeket a nemzetközi kutatási együttműködéseket.

Összességében a nemzetbiztonság részeként jól láthatók a K+F+I területek védelmének indokai és ellentmondásai, az egyetemi „tudományos nyitottság" és a „nemzetbiztonsági érdekek" találkozásának komplex kérdései. A biztonságpolitikai színtéren zajló folyamatok pedig napjainkra tovább erősítették a tudomány és kutatás szabadságához, valamint a nemzetbiztonsági-gazdasági érdekek biztosításához kapcsolódó teoretikus vitákat.

Egyetemek vs. nemzetközi hallgatói migráció

Szinte minden jelentősebb egyetem képzési-kutatási területein és hallgatói létszámában meghatározó a külföldi hallgatók jelenléte. Egy-egy nagyobb egyetem akár többezres külföldi hallgatói létszám fogadására és folyamatos képzésére is vállalkozik, amely sajátos, egyes elemeiben a nemzetbiztonsági szféra feladatrendszeréhez sorolható kérdésköröket is eredményezhet. Mint M. Császár Zsuzsa és szerzőtársai tanulmányukban megfogalmazzák, „a nemzetközi hallgatói migráció napjaink felsőoktatásának egyik leginkább kutatott jelensége".[46] Az előző kínai hallgatói példán is látva tényként kezelhető, hogy a külföldi hallgatók jelenléte a képzést kínáló országoknak és maguknak az egyetemeknek is rendkívül fontos, nemcsak az államok nemzetközi kapcsolatainak erősítése, hanem az intézmény tudományos hírnevének erősítése terén is. Vitathatatlanul fontos, hogy a külföldi hallgatók által „befizetett tandíjak közvetlen gazdasági hasznot jelentenek".[47] Érthető tehát az egyetemek nyitottsága, fogadókészsége a külföldi diákok iránt, amely folyamat azonban biztonsági szempontból is

[45] Itt említhetők meg a Konfuciusz Intézetek bezárásához kapcsolódó viták, amelyek a hasonló nemzetközi intézményekhez képest nem önállóan, hanem együttműködések révén adott egyetemeken belül jöttek létre.

[46] A nemzetközi hallgatói migráció biztonságpolitikai kockázatait részletesen vizsgálja tanulmányában M. Császár Zsuzsa et al.: A nemzetközi hallgatói migráció biztonságpolitikai kockázatainak egyes aspektusai. *Nemzetbiztonsági Szemle,* 6. (2018), 3. 49–64.

[47] M. Császár et al. (2018): i. m.

megközelíthető. A kapcsolatok pozitívumainak részletes bemutatásától eltekintve, a biztonsági szervek munkáját igénylő feladatként azonosíthatók:

- egyes tudományos kutatási területeken a gazdasági hátrányokat és nemzetbiztonsági érdekeket sértő, versenyhátrányt okozó lehetséges információszerzési tevékenységek (tudományos-gazdasági hírszerzés, ipari kémkedés) felderítése, megakadályozása;
- a távoli, akár terrorizmussal sújtott térségekből (például tanulói vízummal) érkező, biztonsági kockázatot jelentő személyek kiszűrése,[48] vagy akár az egyetemeken esetlegesen felbukkanó radikalizáció nyomon követése.

Befejező gondolatok

A nemzetbiztonsági struktúrák számára egyre fontosabbá válnak az egyetemi, tudományos környezet nyújtotta lehetőségek. A kialakuló együttműködési felületek a hagyományos képzési területeken túl katalizátorszerepet tölthetnek be a tudományos kutatások és új innovatív technológiák mentén. A közös érdekeken alapuló együttműködések lehetőségeket teremthetnek az alapvetően zártan működő nemzetbiztonsági szolgálatok számára a társadalom felé történő nyitására, a bizalmatlanság csökkentésére, valamint a gazdasági szereplők szükséges mértékű bevonására a K+F tevékenységek, az új technológiák és műszaki megoldások fejlesztése terén.

A hidegháború időszakának „nemzetbiztonsági célzatú" fejlesztési modelljeinek felhasználása a 21. század technológiai versenyben számos elemében már idejétmúltnak tekinthető, és a nyílt, globális tudományos környezetben rendkívül gyorsan formálódó innovációk megjelenését a zárt struktúrák nem tudják kellően lekövetni. Mint O'Connell megfogalmazza, egyetlen „titkosítási/minősítési" rendszer „sem akadályozhatja meg a tudomány fejlődését",[49] hiszen a fejlődés lehetősége a hírszerzési/információgyűjtési, valamint az elhárítási/védelmi technológiák innovációjának lehetőségét is magában hordozza.

[48] Példaként említhető, hogy a 2001. szeptember 11-i Egyesült Államokbeli terrortámadás előkészítői között külföldről, diákvízummal érkező személy is megtalálható volt.

[49] Kevin M. O'Connell: The Role of Science and Technology in Transforming American Intelligence. In Peter Berkowitz (szerk.): *The Future of American Intelligence.* Hoover Press, 2005. 153.

Napjainkra a nemzetközi szintű kutatási kapcsolatok, a különböző projektek mentén alakuló új együttműködési formák jelentős része már a virtuális térbe tolódott át. Megszűntek a fizikai értelemben vett zárt határok a tudományos eredmények megosztásában és

> „a különböző tudományágak technológiai közösségei egymást elősegítve, eredményeit felhasználva új tudományterületeket hozhatnak létre, a hatékonyság maximalizálása érdekében a multinacionális kutatóintézetek ötleteket, embereket és erőforrásokat mozgathatnak könnyedén nemzeti határokon át".[50]

Az együttműködések jelentőségére és a változásokra felhívva a figyelmet, William Regli 2018-ban a DARPA-ról szóló kiadványban fogalmazza meg, hogy az új technológiák egyidejűleg furcsának, csodálatosnak és zavarónak bizonyulnak, sőt a változások gyorsasága kapcsán felveti, hogy a technológiai fejlődéshez és az új eredmények megjelenéséhez kapcsolódó kihívások közül „sok meghaladja a kormányzati válaszidőket, az egyetemek ciklusait"[51] is. Mindez új megközelítéseket kíván, és mindkét oldalról megköveteli, hogy új mechanizmusokat találjanak a nem nyilvános kutatások és ösztöndíjak támogatására, amelyek érzékeny kérdéseket érinthetnek – biztosítva mind az akadémiai és kutatói szabadságot, mind a nemzeti érdekeket.[52]

Ezek jelentősége a nemzetbiztonsági szervezetek számára is kiemelten fontos, hiszen lehetővé válhat, hogy a technológiailag hagyományosan meghatározó nagy nemzetek mellett a korábban fejletlenebb képességekkel rendelkező országok is egy-egy kutatási területen jelentős eredményeket érjenek el. A partnerségek révén új, a nemzetbiztonsági szolgálatok feladatait támogató kutatási források jelenhetnek (például pályázati konzorciumok) meg, amelyek közvetve hozzájárulhatnak a szervezeteknél az állomány megtartásához, a tudományos munkatapasztalatok beépüléséhez és a szakértelem növekedéséhez.

A változások a nemzetbiztonságért felelős szervezetektől is innovatív gondolkodást, a változó környezet nyomon követését igénylik, utat nyitva a nemzetbiztonsági szempontokat szem előtt tartó jövőbeli együttműködések létrehozásának.

[50] Kadtke–Wharton (2018): i. m.
[51] Regli (2018): i. m. 134–136.
[52] Regli (2018): i. m. 134–136.