# Kiberbiztonsági kompetencia hálózatok Európában – K+F+I lehetőségek a következő évtizedben

Krasznay Csaba

Nemzeti Közszolgálati Egyetem, Budapest

Beérkezett: 2020. szeptember 17.; Elfogadva: 2020. november 19.

**Összefoglalás**

Az elektronikusan tárolt információ biztonsága, általánosabban véve a kiberbiztonság, az egyik legnagyobb kihívás a 21. században. Folyamatosan jelennek meg újabb és újabb fenyegetések, melyekre innovatív és újszerű megoldásokat kell adni. Ezek az innovatív megoldások mindenképpen magukkal hozzák az olyan új típusú technológiák használatát az információbiztonságban, mint például a Nagy Adatokból (Big Data) való építkezés és az erre épülő mesterséges intelligencia. Ennek támogatása érdekében az Európai Unió a 2021 és 2027 közötti időszakban kiemelt fontosságúnak tartja a kiberbiztonsági innovációkat. A tanulmány bemutatja a kiberbiztonsági kompetenciahálózatok tervezetét, illetve ismerteti, hogy milyen kutatás-fejlesztés-innovációs lehetőségek lesznek a következő évtizedben Európában.

**Kulcsszavak**: kiberbiztonság, innováció, Kiberbiztonsági Jogszabály, startup

## Cybersecurity Competence Network in Europe – R&D&I Opportunities in the Next Decade

Csaba Krasznay

National University of Public Service, Budapest, Hungary

**Summary**

Security of stored digital information and more generally, cybersecurity is one of the biggest challenges of the 21st century. Besides the negative effects of cybercrime, cyberespionage, or other state sponsored activities, like cyberwarfare, our society and economy should face the exposure of infocommunication systems all around us. At the dawn of 4th industrial revolution when the whole world is going to be digitalized and will be surrounded by networked digital devices in homes, cities and industry, new threats are constantly emerging that need to be responded with new innovative solutions. These innovative solutions should include the usage of big data and artificial intelligence built onto it. They should also give a response for the inherited risks of legacy systems that can be found in many critical information infrastructures. Meanwhile, they should protect the digital privacy of citizens by not giving out unnecessary user data which is contradictory with the need of big data and AI mentioned before.

Due to the emerging cybersecurity threats and the virtually non-existence of European cybersecurity market, European Union gives high importance for cybersecurity innovation and will support it between 2021 and 2027. In the proposed budget for this period, approximately 3 billion of euros is expected to be spent to cybersecurity related research. On the one hand, that fund may help European research institutes, enterprises, and startups to appear on the global market, on the other hand this is the only possible way to regain Europe's digital independence from the United States and China. In alignment with the European security policy, these innovative solutions may also lead to reducing the amount of cybercrime, ensure the resilience of continental critical information infrastructure and can help to establish strong European cyberwarfare capabilities. As Ursula von der Leyden, president of the European Commission said in her op-ed in February 2020, "The point is that Europe's digital transition must protect and empower citizens, businesses and society as a whole. It has to deliver for people so that they feel the benefits of technology in their lives. To make this happen, Europe needs to have its own digital capacities – be it quantum computing, 5G, cybersecurity or artificial intelligence (AI). These are some of the technologies we have identified as areas for strategic investment, for which EU funding can draw in national and private sector funds." The study presents the draft of cybersecurity competence networks and describes what R&D&I possibilities will be in Europe in the next decade.

**Keywords:** cybersecurity, innovation, Cybersecurity Act, startup

## Bevezetés

Először is ismertessük a trendeket a kiberbiztonságban, hiszen az elmúlt 10–15 évben jelentősen alakultak át azok az alaptechnológiák, melyek információtechnológiai értelemben védelemre szorulnak. Ezek között felsorolhatjuk a kétezres években tömegessé vált közösségi hálózatokat, a hordozható infokommunikációs eszközöket, vagy éppen a felhőszámítástechnikát, de a 2010-es évek közepétől kezdve elterjedtek még a felsoroltakra épülő olyan megoldások is, melyek új szemléletű, új típusú kibervédelmet igényelnek.

Ezen új disztruptív technológiák alatt elsősorban a mesterséges intelligenciát és robotikát, illetve a mindenhol jelen levő informatikát, a Dolgok Internetét (Internet of Things – IoT) lehet érteni. A mesterséges intelligencia különösen fontos, hiszen ez nemcsak lehetőséget ad az új típusú kibervédelem felépítéséhez, de olyan kihívásokat is jelent a mesterséges intelligenciát használó alkalmazások védelme szempontjából, melyeket egyelőre felmérni sem tudunk. A robotika, illetve a mellette megjelenő okos hálózatok, a Dolgok Internete szintén egy korábban nem látott problémát és kihívást okoz az információbiztonsággal foglalkozó szakértők számára.

Észre kell vennünk, hogy az utóbbi időben a kibertámadások a végfelhasználók és az olyan jól ismert iparágak, mint például a bankszektor, illetve a közszolgálat után egyre inkább a gyártás és az alapvető közművek irányába tevődnek át. Megfigyelhető, hogy az olyan speciális rendszerek, melyek a közműszolgáltatásban vagy a gyártásban üzemelnek, szintén meglehetősen védtelenek a kibertéri fenyegetésekkel szemben. Itt azokra az ICS/SCADA rendszerekre kell gondolni, melyeket a gyártásban, illetve a közműszolgáltatásban használnak, és melyeket nem egyszer akár évtizedekkel korábban állítottak üzembe, és adott esetben olyan operációs rendszerek futnak rajtuk, melyek már régen nem támogatottak. Gondolni kell arra is, hogy ezek az iparágak éppen átélik a negyedik ipari forradalom jelentette fejlődést, és itt is megjelennek azok az új típusú megoldások, melyekkel a gyártás, illetve a közműszolgáltatás okossá válik. Megjelennek például az okosvárosok (smart city), melyek mindmind alkalmazzák ezeket a speciális információs rendszereket, sokszor a megfelelő alapfokú védelem nélkül.

Ezeken a területeken tehát – miközben az alapvető információbiztonsági alapelvek változatlanok maradtak – új típusú kibervédelmet és mentalitást kell megvalósítani, miközben az alapvető információbiztonsági alapelvek változatlanok maradnak. Ezt támasztja alá egy másik olyan trend, amire oda kell figyelnünk: egyre több iparágban jelenik meg valamilyen kibervédelmi szabályozás. A pénzintézeteknél és a kormányzati szektorban régóta léteznek olyan szabályozók és jogszabályok, melyeknek meg kell felelniük az ismertetett szempontoknak, viszont az Európai Unió szabályai, ezen belül is elsősorban az európai Általános Adatvédelmi Rendelet (General Data Protection Regulation – GDPR), illetve A hálózati és információs rendszerek biztonságáról szóló irányelv (The Directive on Security of Network and Information Systems – NISD) jelentősen kiterjeszti a megfelelőségi kényszert. Ezek az előírások számos szervezet számára jelöltek ki kötelező információbiztonsági tevékenységet, emellett begyűjtötték őket az állami kibervédelem ernyője alá, függetlenül attól, hogy milyen szektorban működnek.

## Innovációs igények a kiberbiztonságban

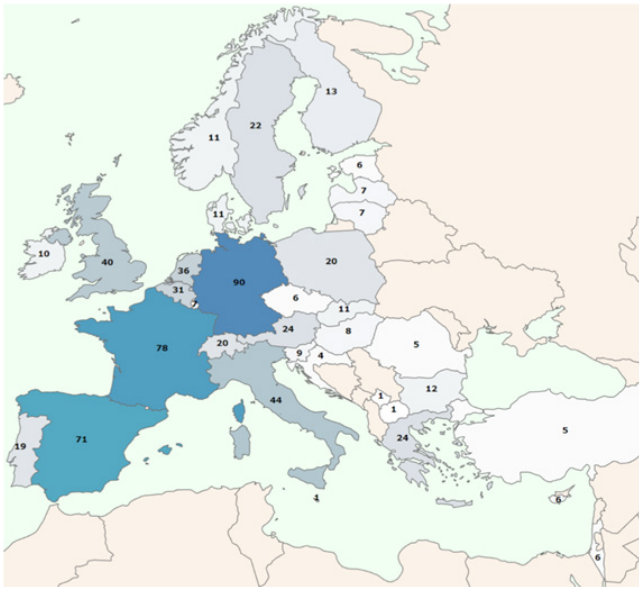
A nagyvállalatoknál azt lehet jelenleg érzékelni, hogy a szabályozói nyomás igen nagy, ezért jellemzően jól működő információbiztonsági kultúra alakult ki az elmúlt évtizedekben. Ezek a vállalati igények egyértelműek, a legtöbb esetben szabályozásokból erednek, illetve azokban az iparágakban, melyek sokkal jobban kitettek a kibertámadásoknak, mint a többiek, megvan az eljárásrendje annak is, hogy milyen módon építsék be akár a legújabb innovatív megoldásokat is a védelmi rendszerükbe.

A nagyvállalatok mellett azonban számos más érintettje is lehet a kibertámadásoknak, kiemelve elsősorban a kis- és közepes vállalkozásokat, melyeknél az információbiztonsággal kevéssé vagy egyáltalán nem foglalkoztak eddig. Ezen a területen is fontossá válnak az említett szabályozások, és főleg a GDPR miatt, elérhető és könnyen használható információbiztonsági megoldások megjelenésére van szükség. Esetükben a szabályozás ugyan megvan, viszont a megfelelőségi nyomás, azaz konkrétan a hatósági ellenőrzések és az ezekből eredő potenciális büntetések egyáltalán nem jellemzőek ebben a pillanatban, bár ez változni látszik. Ennek ellenére mindenképpen fontos látni, hogy a kis- és közepes vállalkozások túlnyomó többsége is információs rendszerekkel dolgozik, működésük információs rendszerekre épül, így esetükben is elengedhetetlenül fontos az információbiztonsági kultúra fölépítése.

Nem szabad megfeledkezni továbbá a magánszemélyekről sem, hiszen jelenleg több mint 4,5 milliárd ember használja az internetet, és a legtöbben olyan eszközökkel kapcsolódnak a világhálóhoz, melyek információbiztonsági felkészültsége kérdéses. A magánszemélyek túlnyomó többsége nem ismeri a kiberhigiénia alapvető fogalmait, így potenciálisan mind saját maguk veszélyben vannak, mind pedig ezekkel a nem megfelelően felkészített eszközökkel és elégtelen tudással veszélyt jelentenek a többi internetezőre, az internet teljes struktúrájára vonatkozóan.

## Kiberbiztonsági K+F+I Európában és a világban

2018-ban az Európai Unió, készülve a kiberbiztonsági szabályozásainak bevezetésére és a 2021-től induló költségvetés megtervezésére, felmérte, hogy hány olyan ku-




**1. ábra** | Európai kiberbiztonsági kutatóközpontok *(Nai-Fovino et al. 2018)*

tatás-fejlesztéssel foglalkozó intézmény van az Európai Unió tagállamaiban, melyek kimondottan kiberbiztonsággal foglalkoznak. *(Nai-Fovino et al. 2018)* Azt lehetett látni a válaszadásokból, hogy míg például Németországban, Franciaországban vagy éppen Spanyolországban meglehetősen sok olyan intézmény van, ahol kiberbiztonsági kutatás-fejlesztés-innovációval foglalkoznak, Kelet-Közép-Európában, így Magyarországon is ezen intézmények száma alacsony. Ez azt is jelenti, hogy a globális versenyben, ahol hatalmas országokkal és tudástőkével kell versenyeznie az európai iparnak, nem igazán van meg az az alap, amire föl lehet építeni a saját információbiztonsági piacot, illetve tudásbázist.

Ez azért lenne fontos, mert a negyedik ipari forradalom robbanásával egyre inkább ki lesz Európa téve azoknak a gyártóknak, akik nem európaiak. A hardvereszközöket jellemzően Kínában gyártják, a szoftverek elsősorban amerikai forrásból jönnek. Éppen ezért az egyes államok által indított kibertámadások előtt gyakorlatilag az európai államok és az európai vállalkozások szinte védtelenül állnak, tekintettel arra, hogy az európai kibervédelem jelenleg nem, vagy nagyon kis számban tud olyan saját gyártású eszközöket használni, melyek felhasználhatók a külső, akár kiberbűnözésből, akár pedig állami forrásból származó támadások ellen.

Az Európai Unió felismerte hiányosságait ezen a területen, és kiemelten fontos stratégiai célkitűzése lett, hogy változtasson a tendencián. Mivel azonban a kutatás-fejlesztéssel foglalkozó intézmények száma meglehetősen alacsony Európában, először is összpontosítani kell az erőfeszítéseket. Az említett felmérés azt is bemutatta, hogy a válaszadók túlnyomó többsége az állami szférából jött, tehát valamilyen közintézményhez kötődnek, a magánkézben lévő, piaci alapon működő kutatás-fejlesztéssel foglalkozó intézmények száma pedig lényegesen alacsonyabb, nagyjából harmada a közfinanszírozású intézményeknek, és még ennél is alacsonyabb azoknak a PPP konstrukcióban működő intézményeknek a száma, akik mind a magán, mind pedig a köz tudását és tőkéjét hasznosítják.

A tervek alapján a következő kutatási érában három pillérre fog épülni a kutatás-fejlesztés-innováció támoga-

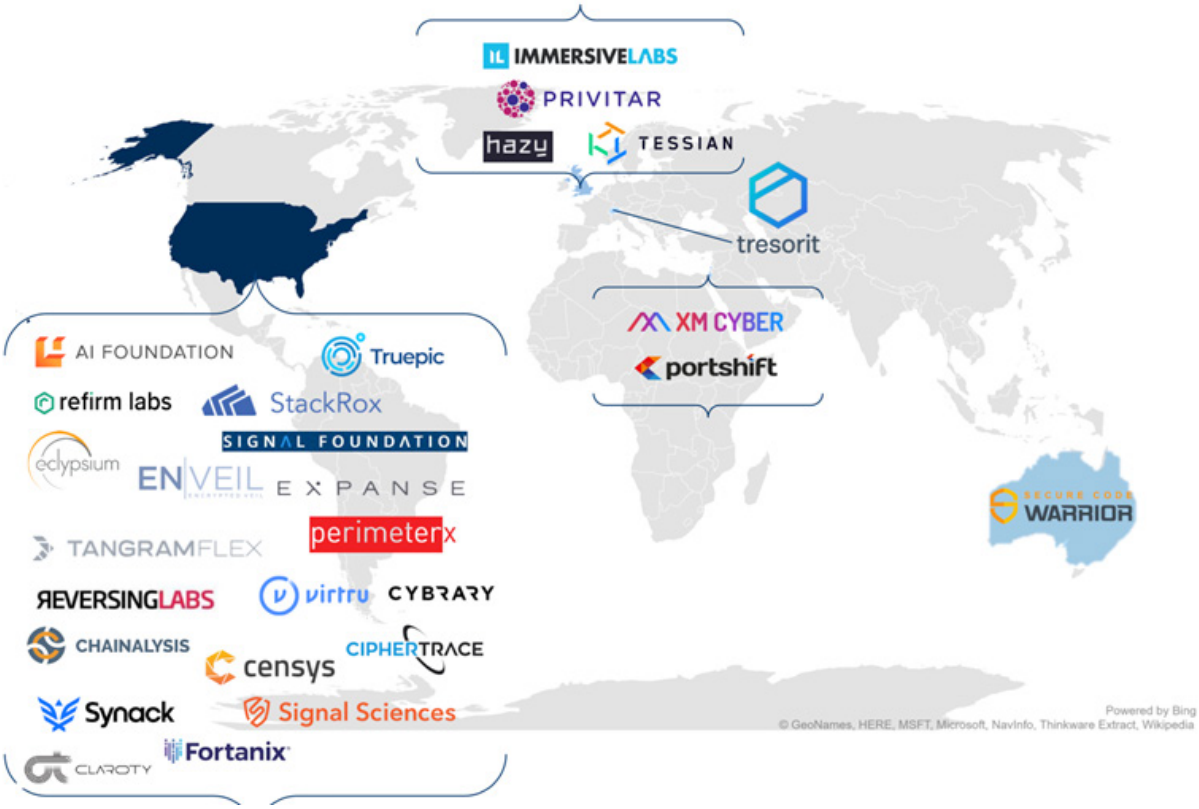

**2. ábra** | EU-finanszírozás a kutatás és az innováció területén (2021–2027) *(Európai Bizottság 2018)*

tása. Ebből az első a kiváló tudomány, a második a globális kihívások és az európai ipar versenyképessége, míg a harmadik pillér az innovatív Európáról fog szólni. *(Európai Bizottság 2018)* A második pillérben *A társadalmat szolgáló polgári biztonság* nevű klaszterben a kiberbiztonság nevesítve szerepel, ez pedig meglehetősen pozitív jövőképet fest azoknak a kutatás-fejlesztés-innovációval foglalkozó intézményeknek és szakembereknek, akik szeretnék az európai kiberbiztonsági ipart megteremteni. Az Európai Bizottság tervei alapján a 2021–27 közötti szakaszban 100 milliárd euró nagyságrendű összeg áll majd rendelkezésre a kutatás-fejlesztés-innovációra, ezen belül a Globális kihívások és az európai ipar versenyképessége pillér 52,7 milliárd euróra számíthat. Tovább bontva, *A társadalmat szolgáló polgári biztonság* klaszterben szerepel a kiberbiztonság, mely a jelenlegi tudásunk szerint körülbelül 2 milliárd euróval fog részesülni ebből a hatalmas összegből. *(Digital Single Market 2018)*

## Startup ökoszisztéma a kiberbiztonságban

Az tehát kétségtelen, hogy a forrás meglesz arra, hogy az európai kutatás-fejlesztés-innováció a kiberbiztonsági területen fejlődjön. A kérdés az, hogy hogyan lehet mindezt elérni. A CB Insight nevű kutatócég 2019-es felmérése alapján ugyanis jelen pillanatban a kontinentális Európában, tehát az Európai Unió jelenlegi országai között nagyon kevés olyan startup van, melynek terméke megfelel a globális igényeknek, illetve a piaci potenciálja olyan, hogy ezekkel hosszú távon lehet számolni. *(CB Insight 2019)* A CB Insight felmérése alapján napjainkban a legígéretesebb kiberbiztonsági startupok elsősorban az Egyesült Államok területén találhatók, emellett Nagy-Britannia és Izrael a két másik olyan szereplő, amelyekre érdemes odafigyelni. Európában egyedül egy svájci bejegyzésű cég, a Trezorit szerepel a listán, mint ígéretes startup. A Trezorit egyébként magyarországi alapítású, de jelen pillanatban ők is az Európai Unió területén kívüli jogi entitásnak számítanak.

Ez a felmérés is mutatja, hogy a startup jellegű, piacorientált innováció a kiberbiztonsági szakmában, az Európai Unió területén belül meglehetősen alacsony szinten van és igen komoly versenyhátránnyal indul a nagy versenytársakhoz képest. Természetesen számos startup létezik, nem is az a probléma, hogy ne lenne meg az innovációs képesség ezeken a területeken, viszont a piacra jutásuk valószínűsége lényegesen alacsonyabb, mint hogyha ezeket a startupokat az Egyesült Államokban, vagy éppen Izraelből indulva jegyeznék be. Meg kell továbbá jegyezni, hogy az ígéretes startupok egy része ettől függetlenül európai alapítású, csak a finanszírozás, illetve a piaci környezet miatt elsősorban az Egyesült Államokban indították ezeket útnak, tehát az európai ipar kevésbé fog profitálni ezek sikeréből.




**3. ábra** | 2019 legígéretesebb kiberbiztonsági startupjai *(CB Insight 2019)*

Még aggasztóbb kép, hogyha megnézzük a CB Insight azon elemzését, mely 2014 és 2019 között mutatja be, hogy melyik országokban mekkora beruházások történtek a kiberbiztonsági kutatás-fejlesztés-innovációban. Ebből látszódik, hogy a kiberbiztonsági K+F+I-re elköltött összegek túlnyomó többsége, kétharmada az Egyesült Államokban jelent meg, mögötte pedig egy kis ország, Izrael áll, ahol nagyon jól működik a gyakorlatilag az iskolától a piacig tartó kutatás-fejlesztés-innovációs támogatás. A beruházásokból Izrael 6,7 százalékkal részesül, ezután következik az Egyesült Királyság 6,5%-os aránnyal, majd Kína jön 5,6%-kal. Utána 14,4%-kal részesül az említetteken kívül minden más ország a világon a beruházásokból, beleérve az Európai Uniót is.

## Lehetőségek Kelet-Közép-Európában

Magyarországon, illetve kicsit tágabb értelemben véve a kelet-közép-európai régióban hatalmas innovációs potenciál rejtőzik. Tehetségeket, jó ötleteket a környező országokban, így elsősorban Romániában, Ukrajnában, Lengyelországban, Csehországban, valamint Észtországban is lehet látni. A régió elsőszámú komoly kihívása az, hogy bár tehetségekből jól állunk, a kelet-közép-európai gondolkodásmód nagyon sokban és nagyon jól támogatja a mérnöki gondolkodást, ezek azonban általában nem konvertálódnak üzleti sikerré. Azt lehet tapasztalni, hogy a nyugati nagyvállalatoknál mérnöki pozícióban számos esetben Kelet-Közép-Európából származó szakembereket alkalmaznak, de a vállalati hierarchiában ritkán jutnak el a régiós szakemberek magasabb, üzleti jellegű pozícióba.

Éppen ezért kétségtelen, hogy tehetségekből jól állunk. A kérdés csak az, hogy ezeket a tehetségeket hogyan lehet bátorítani. Ennek lehet egyik alapköve az, hogy egy olyan ökoszisztéma épül ki ezekben az országokban, mely már akár középiskolában, vagy legkésőbb az egyetemeken segíti a tehetségek fejlesztését, és a mérnöki tudás mellé egy jól meghatározott üzleti, vállalkozásfejlesztési tudást is ad a mérnököknek. Éppen ezért bátorítani kell az iskolai, akár egyetemi szinten történő innovációs képességek fejlesztését. Magyarországon egyébként 2020 szeptembertől indul több egyetemen is olyan innovációs képzés, mely segítheti ezeknek a tehetségeknek a piacra jutását, cégalapítását, illetve segíteni kell azt, hogy a különböző diszciplínákban, különböző tudományterületeken dolgozó szakértők egymással tudjanak dolgozni. *(NFKIH 2020)*

Fontos állami fejlesztéspolitikai lépés lehet az, hogy létrejöjjenek azok az úgynevezett Science Parkok, melyekben több egyetem együttesen tudja fölépíteni a saját innovációs ökoszisztémáját, beleértve ebbe a kiberbiztonságot is. A Nemzeti Közszolgálati Egyetem például a Semmelweis Egyetem által vezetett Science Park részese, és ezen Science Park fejlesztés, innovációs központ egyik eleme a kiberbiztonság az orvosi technológiákban, mely potenciálisan piacképes ötleteket tud majd eredményezni. *(Dobozi 2019)*

Azonban az ökoszisztéma nemcsak az egyetemistáknak segít. Észre kell venni, hogy csakúgy, mint Magyarországon, a környező országokban is számos, úgynevezett Security Operation Center (SOC), azaz biztonsági felügyeleti központ működik, melyek feladata a globális nagyvállalatok információbiztonsági támogatása. Ezekben számos olyan mérnök dolgozik, akik rálátnak a legfejlettebb, legjobban működő információbiztonsági technológiákra, illetve első kézből tapasztalják meg az aktuális kibertéri problémákat. A startup ökoszisztéma segíthet abban is, hogy az akár öt-tíz év tapasztalattal rendelkező mérnököknek adjon egy olyan hátteret, melyen belül ők a saját ötletüket meg tudják valósítani, és ezt a lehető legjobban a piacra tudják vinni.

További kérdés a finanszírozás rendelkezésre állása. Startupokra rengeteg pénz van, a tőke alapvetően keresi a jó ötleteket. Ez Európában is így van, de nagy aránytalanságokat lehet észrevenni a startup-finanszírozásban. Magyarországon például az izgalmas ötletekhez 1 millió forint kockázati tőke bevonást aránylag könnyen el lehet érni egy startup ötletre, addig ez az összeg Nyugat-Európában már 10 millió forint, míg az Egyesült Államokban akár 100 millió forintos nagyságrendet is elérhet. Ez az aránytalanság mindenképpen azt szüli, hogy az ötleteket inkább az Egyesült Államokban célszerű megvalósítani, nem pedig itt, Kelet-Közép-Európában.

Látszódik, hogy a régiónkban is vannak kezdeményezések, ezek azonban tőke- és kapcsolatszegényebbek, mint a nyugati és elsősorban az amerikai befektetők kínálatai. Éppen ezért fontos a régiós együttműködés, és fontos az is, hogy európai szinten is minél jobban megjelenjenek a kelet-közép-európai kezdeményezések. A finanszírozási igény alapvetően kevesebb, mintha Nyugaton történne az indulás, viszont éppen ezért szükségesek azok az állami támogatások is, melyek piacra tudják juttatni a nyugat-európai uniós tagországokban is az itt létrejövő megoldásokat és ötleteket.

Sokat segíthet, ha 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, azaz a Kiberbiztonsági Jogszabályból egyelőre még hiányzó kutatás-fejlesztés-innovációs terület végre elfogadásra kerülne az Európai Unióban. A tervek szerint a Tanács kiberbiztonsági hálózatokat hoz létre, melyek három szinten épülnének ki. Elsősorban létrejönne valamelyik európai uniós tagországban egy olyan központ, melynek feladata a kutatás-fejlesztés-innovációval kapcsolatos források koordinálása, annak érdekében, hogy a Horizont Európa programban rendelkezésre álló összeg jól kerüljön elköltésre. Ez az Európai Kiberbiztonsági Ipari Technológiai és Kutatási Központ nevet viseli, és a tanulmány írásának pillanatában tagországi tárgyalás folyik arról, hogy pon-

tosan milyen felhatalmazással működjön ez a központ. Figyelembe véve, hogy az ENISA-val, az Európai Hálózatbiztonsági Ügynökséggel párhuzamosan kéne ennek működnie, gondoskodni kell arról, hogy ne legyenek olyan átfedések a hatáskörökkel kapcsolatban, melyek nehezítenék a központ működését. Ennek a központnak a székhelye egyelőre nem ismert, több európai ország is bejelentkezett annak érdekében, hogy a központot vendégül láthassa. *(EU Tanácsa 2019)*

Az viszont biztosnak tűnik, hogy minden országban létrejön majd egy nemzeti koordinációs központ, mely felelős lesz azért, hogy az országon belül a forrásokhoz minél többen hozzáférhessenek. Ez pedig a kiberbiztonsági kiválósági központok hálózatán keresztül lesz majd lehetséges. A jelenlegi elképzelések alapján ezek olyan állami kutatás-fejlesztési-innovációs intézmények lesznek, mint például a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Kutatóintézete, melyek segítik azt, hogy az európai kutatási pénzek el tudjanak jutni a piaci szereplőkhöz, a privát szférához is, és egyben erősítik azt az elképzelést, hogy az egyetemeken és a kutatóintézetekben rendelkezésre álló tudás és a piaci igény találkozhasson. Éppen ezért nagyon fontos, hogy nemzeti szinten még a jogszabály elfogadása és a következő költségvetési időszak megkezdése előtt a kiberbiztonságban érdekelt szereplők egymással együttműködve kialakítsák azt a laza hálózatot, melyen keresztül az európai kutatási pénzek hozzáférhetővé válnak majd a jövőben.

## Összefoglalás

Ennek az elképzelésnek a pilotolására, kipróbálására az Európai Bizottság 2019-től kezdve négy kiemelt projektet indított el. Ezek a Concordia, a Cyber Security for Europe, az ECHO, illetve a Sparta nevű kezdeményezések, melyek számos európai uniós tagországot egyesítenek és fognak össze, és próbálják kialakítani, hogyan tud majd működni ez a háromszintű felosztás, hogyan valósítható meg az, hogy az európai kutatási pénzek a leghatékonyabban jussanak el az innovációval foglalkozó magán és közfinanszírozású szereplőkhöz. *(Európai Bizottság 2019)*

A kutatás-fejlesztés-innováció tehát fontos, a lehetőség itt van előttünk, viszont ezzel tudni kell élni, és ehhez a legfontosabb az, hogy a tudatosság meglegyen minden szereplőben. Remélhetőleg jelen tanulmány segített abban, hogy felhívja a figyelmet ennek a fontosságára és minden érintett szereplő figyelemmel fogja követni a következő évek fejlesztését, egyben keresni fogja a kapcsolatot azokkal az intézményekkel, akik részeivé válnak majd a következő évek információbiztonsági kutatás-fejlesztés-innovációs tevékenységének.

## Irodalomjegyzék


CB Insight (2019) *2019 Cyber Defenders.* CB Insight. https://www.cbinsights.com/research/report/cyber-defenders-2019/ [Letöltve: 2020. március 30.]

Digital Single Market (2018) *New Digital Europe Programme brings €9.2 billion investment between 2021–2027* https://ec.europa.eu/isa2/news/european-commission-has-announced-investment-%E2%82%AC92-billion-align-next-long-term-eubudget-2021_en [Letöltve: 2020. március 30.]

Dobozi, P. (2019) *Bemutatták a Science Park tervezett szakmai tartalmát.* https://www.uni-nke.hu/hirek/2019/10/24/bemutattak-a-science-park-tervezett-szakmai-tartalmat [Letöltve: 2020. március 30.]

Európai Bizottság (2018) EU-finanszírozás a kutatás és az innováció területén (2021–2027) https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-research-innovation_hu.pdf [Letöltve: 2020. március 30.]

Európai Bizottság (2019) *Four EU pilot projects launched to prepare the European Cybersecurity Competence Network* https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network [Letöltve: 2020. március 30.]

EU Tanácsa (2019) *Az EU összefogja és hálózatba szervezi kiberbiztonsági szakértelmét – a Tanács megállapodott a kiberbiztonsági központokkal kapcsolatos álláspontjáról* https://www.consilium.europa.eu/hu/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/ [Letöltve: 2020. március 30.]

Nai-Fovino, I.; Neisse, R.; 'Lazari, A. & Ruzzante, G. (2018) European Cybersecurity Centre of Expertise – Cybersecurity Competence Survey. Luxembourg, Publications Office of the European Union, ISBN 978-92-79-92954-0, doi:10.2760/42369, JRC111211.

NKFIH (2020) *Szeptemberben startol a Hungarian Startup University Program* https://nkfih.gov.hu/hivatalrol/online-sajto/szeptemberben-startol [Letöltve: 2020. március 30.]