

Krasznay Csaba – Molnár Dóra

Az Európai Unió digitális stratégiai autonómiája: célok és perspektívák



Bevezetés

Az európai stratégiai autonómiát először az Európai Unió biztonságával és védelmével összefüggésben használták 2013-ban, és ezt a fogalmat mindaddig nem definiálták kifejezetten, amíg a 2016-os uniós Globális Stratégiában szélesebb stratégiai ambíciót nem kapott. Azóta az egymást követő események és fejlemények még nagyobb vonzerőt és aktualitást adtak neki. Elég, ha a Covid-19-világjárványra, az Egyesült Államok nemzetközi politikában betöltött szerepével kapcsolatos aggodalmakra, a transzatlanti és a Csendes-óceánon túli feszültségekre a nemzetek közötti kereskedelemben, Kína stratégiai riválisként való elismerésére vagy a napjainkban is zajló orosz–ukrán háborúra gondolunk, és mindezt súlyosbították a világ digitális piacain való dominancia körüli aggodalmak. Ezek az események, továbbá az, hogy az Unió rájött, hogy saját intelligens digitalizációja az ipar-, energia-, védelmi és fenntarthatósági politikája mellett a stratégiai függetlenségének az előfeltétele, olyan európai kezdeményezések megszületéséhez vezettek, amelyek célja Európa önálló szereplőkénti pozíciójának, valamint a világpolitikában és a globális gazdaságban betöltött státuszának és szerepének megerősítése. Ezek keretét az Európai digitális stratégiai autonómia (European Digital Strategic Autonomy – DSA) jelenti.

A stratégiai autonómia fogalmát Emmanuel Macron francia elnök vezette be az európai köztudatba 2017-ben, a megválasztását követően, majd ezt követően váltak használatossá a digitális autonómia, digitális szuverenitás és technológiai szuverenitás kifejezések is, amelyek mind a politikai diskurzusban, mind a politikai dokumentumokban előkelő helyet foglalnak el. *A stratégiai autonómia nem más, mint a digitális szuverenitás megvalósításának politikai keretrendszere* (TIMMERS 2018). A digitális szuverenitásra való törekvést Európában három különböző diskurzus indokolja (CODAGNONE et al. 2021). Az első a szuverenitás ősi koncepciójára való hivatkozás mind a politikában, mind a geopolitikában. Ezen diskurzus legegységesebb megnyilvánulásai az adatok lokalizálására vonatkozó törvényjavaslatok. A második

diskurzusnak etikai színezete van, és célja a fogyasztók védelme a felhasználói jogokat, valamint a hazai törvényeket és normákat tiszteletben tartó technológiai szolgáltatások nyújtásával. A harmadik diskurzus pedig a jövőbeli gazdasági prosperitással, versenyképességgel és az ellátási láncok rugalmasságával kapcsolatos aggodalmakból fakad.

Autonómnak lenni annyit jelent, hogy kulcsfontosságú stratégiai céljainkat külső felek befolyásától és függőségeitől mentesen tudjuk elérni. Az Európai Unió (EU) digitális autonómiájának elérése tehát attól függ, mennyire lehet megteremteni azt a környezetet, amelyben a szükséges és elégséges mértékben ki lehet zárni a globális versenytársaktól, elsősorban az Amerikai Egyesült Államokból (USA) és Kínából származó technológiákat és versenynyomást. A technológiai függésnek azonban számos dimenziója van, amellyel számolni kell a digitális szuverenitás kivívása érdekében, hiszen a műszaki kérdések mellett gazdasági, jogi, politikai vagy éppen katonai befolyásolás is akadály lehet az önálló és versenyképes európai digitális piac megteremtésének, a két nagyhatalomnak pedig nem érdeke támogatni az EU digitális autonómatörekvéseit.

Két fő kiváltó okot nevesíthetünk, amelyek az Unió digitális szuverenítésra való törekvését – különösen az utóbbi időben – jelentősen felerősítették. Az egyik *a geopolitikai helyzetkép változása és az adatok feletti ellenőrzés kérdéskörét érintő új szabályok* megjelenése (STOLWIJK 2022), míg a másik *a nagy techcégek* (Google, Apple, Facebook, Amazon, Microsoft – avagy GAFAM) *ellen megindult jogi lépések sorozata*, amelyek az uniós jogalkotás speciális irányát jelentik (THIEULIN 2019). Mindezek mentén a tanulmány előbb a változó geopolitikai helyzetképet mutatja be, külön kitérve az Egyesült Államok és Kína azon lépéseire, amelyek döntő jelentőségűek az Unió digitális autonómiája megteremthetőségére nézve, majd felvázolja az EU konkrét lépéseit a főbb területeket érintően, amelyeket a digitális autonómia megteremtése felé vezető út első mérföldköveinek tekinthetünk.

A kibertér geopolitikájának formálódása

A digitális tér világpolitikai jelentősége

A digitális függés kialakulásának egyik legjobb történelmi példája a nemzetállamok közötti küzdelmek egyik legaktuálisabb helyszíne, a kibertér. Míg az olyan hagyományos fizikai dimenziókban, mint a világtengerek, a sarkvidékek vagy éppen a világűr, a történelem során már többször élesedett ki a nagyhatalmak közötti versengés,

a digitális technológiák és az általuk alkotott hálózatok csak az elmúlt harminc évben jelentek meg széles körben és alakították át gyökeresen a világunkat. Ráadásul, szemben a fizikai térrel, amelyet leginkább a természet alakított, a kibertér egy teljesen az emberiség, egészen pontosan az Amerikai Egyesült Államok által megalkotott virtuális tér, amely a kiváló tudósok és az amerikai kormányzati finanszírozás nélkül nem is létezne. A kibertérben emellett nem is azonosíthatók könnyen olyan klasszikus erőforrások, amelyek indokolhatnák azt a megkülönböztetett figyelmet, amit a világpolitika színterén kap ez a nem kézzelfogható helyszín.

A kibertér kiemelt fontosságát a 21. század társadalmi és gazdasági fejlődésében kell keresni. A számítógépek az 1980-as években kezdtek elterjedni, az internet az 1990-es évek terméke. Egészen pontosan a ma ismert internetet (World Wide Web) 1989-ben alkotta meg a brit Tim Berners-Lee, a svájci CERN (Conseil européen pour la Recherche Nucléaire – Európai Nukleáris Kutatási Szervezet) kutatóintézetben. Ezt azért fontos kiemelni, mert ez a világot átalakító felfedezés ugyan egy európai projekt égisze alatt jött létre, de egy jelenleg nem EU-tagállam tudósa egy nem EU-tagállamban hozta létre, ráadásul nem Európa profitált belőle a legjobban. Ekkor az internet még csak néhány millió nyugati tudós és mérnök játszótere volt elsősorban. Ma már közel 5 milliárd internetfelhasználó van globálisan. Bár a számítógépek fontossága egyértelmű volt már a kezdeteknél is, hiszen mind a kormányzati, mind a versenyszférában folyamatosan terjedt a használatuk, a kommunista rezsimek bukása után, a *Pax Americana* globális kiterjesztésének hajnalán kevesen gondoltak arra, hogy a digitális tér egyszer a világpolitika meghatározó kérdése lesz. Az USA korabeli kormányzati politikája azonban előrevetítette, hogy az internetet a globális dominancia egyik eszközének tekinti.

Bill Clinton első elnöki periódusának egyik korai, de talán leglényegesebb stratégiája volt az 1993-ban kiadott *The National Information Infrastructure: Agenda For Action* (NII) című dokumentum. Ebben szerepel a következő célkitűzés:

„Az NII előnyei a nemzet számára óriásiak. A fejlett információs infrastruktúra lehetővé teszi az amerikai cégek számára, hogy versenyezzenek és győzedelmeskedjenek a globális gazdaságban, jó munkahelyeket teremtve az amerikaiak számára és gazdasági növekedést a nemzet számára. Ugyanilyen fontos, hogy az NII átalakíthatja az amerikai emberek életét – enyhítve a földrajzi, fogyatékosági és gazdasági helyzetből adódó korlátokat –, és minden amerikainak tisztességes lehetőséget adva arra, hogy tehetségük és ambícióik szerint olyan messzire jussanak, amilyen messzire csak akarnak. [...] *Az információ a nemzet egyik legkritikusabb gazdasági erőforrása, a szolgáltatóipar és a feldolgozóipar, a gazdaság és a nemzetbiztonság szempontjából*

egyaránt. Egy becslés szerint az amerikai munkavállalók kétharmada az információval kapcsolatos munkakörökben dolgozik, a többiek pedig olyan iparágakban, amelyek nagymértékben támaszkodnak az információra. A globális piacok és a globális verseny korában az információ létrehozására, manipulálására, kezelésére és felhasználására szolgáló technológiák stratégiai jelentőségűek az Egyesült Államok számára. Ezek a technológiák segítik az amerikai vállalkozásokat abban, hogy versenyképesek maradjanak, és kihívást jelentő, jól fizető munkahelyeket teremtsenek. Emellett a gazdasági növekedést is táplálják, ami viszont minden amerikai számára folyamatosan növekvő életszínvonalat teremt.” (BROWN 2003). Az információ tehát hatalom, amely megszerzéséért, birtoklásáért, felhasználásáért ugyanolyan küzdelem folyik, mint bármely más erőforrás esetén. Nem hiába a mondás, miszerint az információ (vagy az adat) a 21. század aranya.

Az Európai Unió a digitális fejlődés útján

Az Európai Unióban a digitális fejlődést, az információs társadalom felé történő legelső lépést megalapozó dokumentumnak a *Bangemann-jelentést* szokták tekinteni.¹ 1994 májusában jelent meg, kijelölve azt az utat, amelyet az Európai Bizottság a következő évtizedekben kisebb korrekciókkal követett. Három évtizeddel később érdekes megállapítani azokat a filozófiai különbségeket, amelyek az amerikai és az európai vízióban rejlenek, és amelyek hosszú távon Európa digitális függőségéhez vezettek. A jelentés vezetői összefoglalója így kezdődik:

„Ez a jelentés sürgeti az Európai Uniót, hogy bízson a piaci mechanizmusokban, mint az információs korszakba való átmenet motorjában. Ez azt jelenti, hogy európai szinten és a tagállamok részéről is lépéseket kell tenni az Európát versenyhátrányba hozó berögzült álláspontok felszámolása érdekében:

- ez a *vállalkozói mentalitás* előmozdítását jelenti, hogy lehetővé váljon a gazdaság új, dinamikus ágazatainak megjelenése,
- ez a *közös szabályozási megközelítés* kidolgozását jelenti az információs szolgáltatások versenyképes, egész Európára kiterjedő piacának megteremtése érdekében,

¹ Martin Bangemann német gazdasági miniszter és európai biztos volt, 1985–88 között pedig a német Szabad Demokrata Párt (FDP) vezetője. 1995 és 1999 között a Santer-bizottság ipari ügyekért, információs és távközlési technológiáért felelős biztosaként volt felelős a hivatkozott jelentés kiadásáért.

- ez NEM jelent több közpénzt, pénzügyi támogatást, szubvenciókat, dirigizmust vagy protekcionizmust” (European Commission 1995).

Az NII-ben megfogalmazott gondolatok előrevetítették, hogy az USA-val versengő hatalmaknak képesnek kell lenniük az információtechnológiai területen is alternatívát nyújtani és saját képességeiket fejleszteni. Azonban ez már a Bangemann-jelentés idejében ismert volt, de az európai politika nem ismerte fel, hogy pusztán szabályozással és a piaci liberalizálással hosszú távon a régió nem lesz versenyképes az amerikai versenytársakkal szemben. Bár szinte minden pontban kiemelik Európa relatív lemaradását az USA-hoz képest, a technológiai területen a következő megállapítást tették a Bangemann-csoport tagjai:

„A jelenlegi európai technológiai bázis elegendő az e jelentésben javasolt alkalmazások késedelem nélküli bevezetéséhez. Elég nagy léptékű, reális rendszerekre kell összpontosítani annak érdekében, hogy azok feltárják a felhasználók számára kínált szolgáltatások értékét, és hogy értékeljék az új információs rendszerek gazdasági megvalósíthatóságát.

Az új technológiákat azonban még ki kell fejleszteni ahhoz, hogy bemutatásukat követően teljeskörűen bevezethetők legyenek. Különösen a rendszerek használhatóságát és költséghatékonyságát kell javítani, és a tömeges használat következményeit tovább kell vizsgálni.

Az Unió és a tagállamok kutatási programjait, különösen a Negyedik Keretprogramot, úgy kell végrehajtani, hogy figyelembe vegyék a piaci követelményeket. A technikai célokat és a projektek időzítését a felhasználók megfelelő bevonásával kell meghatározni” (Európai Bizottság 1993).

Az európai álláspont tehát teljesen egyértelmű volt: lévén, hogy „a jelenlegi európai technológiai bázis elegendő” az Unió szerint, további fejlesztésekre jelenleg nem, legfeljebb a közeli (vagy a távolabbi) jövőben lehet majd szükség. Ugyanakkor a jelentés előremutató – korát meghaladó – gondolata a magán- és közzsféra partnerségének erősítése, amely még harminc év elteltével is részben megoldatlan.

A Kína–EU–USA háromszög

Érdekes, hogy míg az 1990-es évek elején Japán tűnt ezen a területen a leginkább kompetitív vetélytársnak mind az USA, mind az EU számára, a 2020-as évtizedre kétségtelenül Kína lett az az ország, amely az egyértelmű második, néhány területen

pedig az első a technológiai területen. Ahhoz képest, hogy Kína az 1990-es évek elején gazdaságilag jelentéktelen ország volt, egészen rendkívüli, ahogy felépítették azt a fejlett digitális gazdaságot, melyet akár Európa is megtehetett volna. Paradox módon ebben sokat segített a Pax Americana jelentette globális nyitás. Kínai diákok tűntek fel tömegesen az USA legjobb egyetemein, eközben pedig amerikai és európai gyártók nyitottak gyártóegységeket Kínában az olcsó munkaerő reményében. Látzólag minden az USA gazdasági előnyéről szólt, hiszen az agyszívás az amerikai tudásintenzív gazdaságot erősítette, miközben az ennek eredményeképp létrejött termékeket a lehető legolcsóbban lehetett előállítani Ázsiában. A 2000-es években viszont a kínai mérnökök és tudósok elkezdtek hazatérni és tudásukat a kínai egyetemeken és vállalatoknál kamatoztatni. A gyártás során Kínába került szellemi tulajdont a helyiek meglehetősen lazán kezelték, akár az ipari kémkedést is kimerítő módon másolták le a nyugati megoldásokat. Nem csoda, hogy a 2010-es évekre Kínában létrejött a digitális képességeket létrehozni képes szellemi tőke és gyártási kapacitás (ZHANG–ZHOU 2015).

Ezzel szemben az európai diákok amerikai tanulmányaik után ott is maradtak, az európai egyetemeken végzett fiatal mérnököket tömegesen csábították el amerikai vállalatok, a legjobb európai egyetemi oktatók pedig jelentős ösztöndíjakat kaptak azért, hogy kutatásaikat az USA-ban folytassák. 2022-ben a QS World University Rankings egyetemi rangsorban a mérnöki és technológiai területen mindösszesen egy európai egyetem szerepel a top 10-ben és kilenc a top 50-ben. Ugyanebben a rangsorban három top 10-es és 14 top 50-es amerikai, valamint két top 10-es és 13 top 50-es ázsiai egyetem található. A brexit jelentette veszteséget és Svájc EU-n kívülségének problémáját mi sem mutatja jobban, mint hogy Svájc és Nagy-Britannia egyetemei a rangsorban négy top 10-es és hat top 50-es egyetemet tudhatnak magukénak (QS Top Universities [é. n.]).

Kínában már egy évtizede erőltetik a digitális iparba történő állami befektetéseket. A 2012-ben elfogadott 12. Ötéves Terv például már kimondottan támogatja a feltörekvő technológiák gyártási képességeinek megerősítését, a 2017-es 13. Ötéves Terv pedig komoly hangsúlyt helyez az olyan technológiák elterjesztésére, mint a mobiltechnológia, a *cloud computing* vagy az Internet of Things. A China 2025 stratégiából pedig egyértelműen kiderül, hogy Kína célja a legerősebb „kiberhatalommá” válni (GODEMENT et al. 2018). Rob Joyce, az amerikai Nemzeti Biztonsági Szolgálat (National Security Agency – NSA) kiberbiztonságért felelős igazgatójának 2023. áprilisi előadása jelzi, hogy ezért a célért jelentős erővel dolgoznak. Meglátása szerint Kína maratont fut a kibertérben, rengeteg erőforrástallokálnak a területre. Az USA

szempontjából ezért Kína a legnagyobb fenyegetés, de folyamatos a kínai kiberhírszerzés az őt körülvevő országokban is. Aktívak a technológiai szabványosításban, nem támogatják a nyugati szabványokat, helyette a saját technológiai szabványaik globális elfogadásán dolgoznak, összhangban a China Standards 2035 stratégiával. A hackelései technikája egyre kifinomultabb. Az USA elleni támadások során az utolsó, detektálható számítógép rendszeresen az USA-ban van, és nagyon gyorsan változtatják ezeket, olyannyira, hogy gyakran, mire kinyomozzák, hogy mi ez a végpont, már mást használnak. Ezzel kihasználják az USA azon gyengeségét, hogy az NSA, amely a legmélyebb technológiai képességgel rendelkező titkosszolgálat, az USA területén nem folytathat műveletet. Nagyon kitartóak, ha egy célpontot fel akarnak törni: akkor addig dolgoznak, amíg sikerrel nem járnak. Alapvetően ismert sebezhetőségeket használnak ki, de mivel ezeket egyre hatékonyabban frissítik a technológiai cégek, meg kellett jelenniük a korábban nem ismert, *o-day* (*zero-day*) támadásokkal. Ezt támogatja a Tienfu Cup, a kínai „hackerverseny” és az, hogy minden, a kínaiak által felfedezett új szoftveres sérülékenységet két napon belül be kell jelenteni a kínai hatóságoknak. Ezzel rengeteg olyan potenciális támadókhöz hozzájuthatnak, amelyet a kiberhírszerzés során fel tudnak használni (JOYCE 2023).

Ismét az európai lemaradást jelzi az, hogy ugyanezeket az irányokat csak évekkel később lehetett megtalálni az EU stratégiai dokumentumaiban (lásd részletesebben az *Uniók szakpolitika a digitális autonómia megteremtéséért* c. alfejezet 2. pontjában), és az is tény, hogy a minimum évtizedes lemaradás ledolgozása nagyságrendileg több költségvetési forrást igényel az európai tagállamoktól, ami a háborús időszakban nem feltétlenül fog a legfontosabb feladatok közé tartozni, és számolni kell a politikai akadályokkal is. Az USA már Barack Obama elnöksége alatt felismerte a technológiai területen megjelenő kínai fenyegetést, és elkezdte blokkolni Kína ez irányú tevékenységét. Donald Trump elnöksége alatt például kemény szankciókkal igyekezett visszavetni a kínai technológiai cégek piaci megjelenését, gondoljunk csak az 5G technológiák kitiltására, egyes kínai mobilgyártók amerikai szoftverektől való elzárására és az egyik legnépszerűbb, kínai tulajdonú közösségi hálózat felvásárlására tett kísérletre. Joe Biden elnöksége alatt ez a trend tudatosan folytatódik, az USA számára Kína az elsődleges stratégiai ellenfél, és mindent megtesz azért, hogy globális pozícióját tartani tudja, és letörje Kína (kiber)hatalommá válását (The White House 2022). Az Európai Unió tagállamai ezekben a kérdésekben meglehetősen megosztottak, a kínai 5G technológia kitiltását például csak a leghűségesebb USA-szövetséges országokban sikerült elérni, annak ellenére, hogy jelentős európai 5G gyártók (például Ericsson, Nokia) vannak, és ez a lépés a potenciális nemzetbiztonsági fenyegetés csökkentése mellett az európai

digitális ipar fejlődéséhez és szuverenítéséhez is hozzájárulhatna. Az egységes európai politikai válasz helyett azonban ebben az esetben is csak egy szabályozási lépés, az 5G kiberbiztonságra irányuló uniós eszköztár létrehozása történt meg, mellyel évekre el lehetett tolni a probléma megoldását.

A két nagyhatalom, az USA és Kína közötti viszonyban eközben viszont számos olyan pont van, amely a következő évtizedekben nyitottá teszi a kibertér feletti dominancia kérdését, és amely masszívan befolyásolja az EU digitális autonómia irányába tett lépéseit. Ezek közül talán a legfontosabb kérdés az, hogyan alakul át a második világháború után kialakult, multilaterális kapcsolatokra és nemzetközi szervezetekre épülő világpolitika. Oroszország Ukrajna elleni katonai agressziója és a szuverén ukrán területek annektálása az ENSZ Biztonsági Tanácsának egyik tagja által egyértelműen megrengeti a nemzetközi rendet, felborítja a *status quót* és erősítheti Kína szándékait a 21. századi erőviszonyoknak megfelelő nemzetközi rend kialakítására, beleértve a globális (amerikai dominanciájú) kibertér nemzeti irányú elmozdítását, segítve ezzel a nemzeti hálózatok (*splinternet*) kialakítását. Európa ebben nem érdekelt, minden nemzetközi fórumon támogatja a jelenlegi kibertér fenntartását, ezzel viszont kialakulni látszik egy olyan szembenállás Kelet és Nyugat között a digitális technológiákat érintő kérdésekben is, amelynek keretében az európai érdekek képviselése igen nehéznek ígérkezik.

További fontos kérdés Kína szándéka Oroszországgal és Tajvannal kapcsolatban. Oroszország háborús agresszióját a nyugati világ erőteljes technológiai szankciókkal bünteti, így amennyiben Oroszország bent kívánja tartani a gazdaságát a 21. században, egyedül Kínára támaszkodhat. A kiberteret tekintve Oroszország évtizedek óta küzd az USA dominanciája ellen és használja ki a technológia jelentette befolyásolási lehetőségeket saját céljai elérése érdekében, ám ezektől a lehetőségektől a háborús cselekedetei miatt hosszabb időre el fogják vágni mind diplomáciai, mind műszaki értelemben. A kiberdiplomáciában azonban jellemzően együtt mozgott Kínával, így valószínűsíthető, hogy a szándékok nem fognak változni, de azokat Kína fogja a jövőben artikulálni, elsősorban saját érdekeinek megfelelően. Így Oroszország minden valószínűség szerint elveszíti kiberhatalmi pozícióját, és Kína-függővé fog válni. Viszont az egységes európai kiállás, például a technológiai szankciók területén prognosztizálhatóan ellenlépéseket fog szülni orosz részről. Nem elég tehát, hogy az EU digitális ipara jelentős piacot veszít, de kibertámadások formájában még ellenséges lépésekre is számíthat orosz részről.

Uniók szakpolitika a digitális autonómia megteremtéséért

Az Unió hosszú évek óta fáradozik a szabályozási keretek megteremtésén, amelyek mentén a következő években, évtizedekben a célként kiűzött digitális stratégiai autonómiáját megteremteni szándékozik. A már említett *Európai digitális stratégiai autonómiának* (European Digital Strategic Autonomy, DSA)² – amely megvalósulásának előfeltétele a határozott uniós politikák megléte – az alábbi jellemzői vannak (POGOREL–NESTORAS–CAPPELLETTI 2022: xi-xii):

- A DSA-nak hosszú távúnak és innovációorientáltnak kell lennie.
- A DSA nem működhet a partnerekkel és szövetségekkel kialakított erős konszenzusos keret nélkül, valamint a jelenlegi geopolitikai átrendeződések miatt a partnerek és szövetségek közötti erős együttműködés kiépítése is elengedhetetlen.
- A DSA szigorú szabályozási elvárásokat feltételez az adatok, a hálózatok és a kiberbiztonság tekintetében.
- A távközlési piac szabályozását felül kell vizsgálni, hogy a szolgáltatók nagyobb mértékben járulhassanak hozzá a digitális infrastruktúra kiépítéséhez.
- A közpolitikáknak minden eddigénél jobban a kutatóközpontok és az iparágak által felhalmozott és kifejlesztett tudásra kell épülniük.
- A DSA egyben kényes erőegyensúlyt jelent Kínával. Tekintettel az Európa és Kína közötti kölcsönös függőségre, egy egyértelmű, a fejlődésre gyorsan reagálni képes politikai keretet kell létrehozni, és annak hatásait valós időben nyomon kell követni.

Ezt a politikai keretet jelenti a digitális autonómia megteremtését célul kitűző ún. *Digitális Iránytű* elnevezésű uniós dokumentum. A továbbiakban ennek legfontosabb megállapításait rögzítjük, majd rávilágítunk arra, hogy az EU elmaradottsága mire vezethető vissza, mely területeket érinti és milyenek a jövőbeli kilátások.

A már meglévő uniós jogi eszközök számos rendelkezést tartalmaznak a nyomon követésre (monitoring), az információmegosztásra és a kockázatértékelésre vonatkozóan. A jövőbeli szabályozási kezdeményezéseknek ezen túllépve továbbra is gondosan

² Ennek részeként az elműlt éveken felgyorsult az uniós jogalkotás is. 2022-ben olyan mérföldkőnek tekinthető jogszabályokat fogadtak el, mint például az Európai Parlament és a Tanács 2022/1925 rendelete a digitális ágazat vonatkozásában a versengő és tisztességes piacokról (a digitális piacokról szóló jogszabály, Digital Market Act – DMA) vagy az Európai Parlament és a Tanács 2022/2065 rendelete a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló jogszabály, Digital Services Act – DSA).

ügyelniük kell a túlszabályozás és a *laissez-faire* megközelítések közötti kényes egyensúly megtartására, és követniük kell a technológia-agnosztikus szabályozás elvét, amely a jövőbeli technológiák elfogadását biztosítaná. Ez utóbbi esetben azonban – többek között – a finansziális akadályokat is le kellene küzdeni.

A Digitális Iránytű és végrehajtása

A direkt állami támogatással kapcsolatos hibás európai megközelítést a 2021. március 9-én elfogadott *Európa digitális évtizede: a 2030-ra kitűzött célok* program felülírni látszik. A *Digitális Iránytű*nek nevezett dokumentum meghatározza az Európa sikeres digitális átalakulására vonatkozó célkitűzéseket, és kiemeli Európának a digitális szuverenitás megteremtésére irányuló törekvését: „Az EU arra törekszik, hogy digitálisan szuverén legyen egy nyílt és összekapcsolt világban, és olyan digitális politikákat folytasson, amelyek lehetővé teszik az emberek és a vállalkozások számára, hogy emberközpontú, fenntartható és virágzó digitális jövőt valósítsanak meg. Ez magában foglalja a sebezhetőségek és függőségek kezelését, valamint a beruházások felgyorsítását” (Európai Bizottság 2021b). Ez jelentős előrelépés a korábbi évtizedek megközelítéséhez képest, és elismeri, szükség van a stratégiai európai beruházásokra a digitális technológiák területén. A program a következő négy beavatkozási területet és célokat azonosította:

- Szakértelem – digitálisan képzett polgárok és magasan képzett digitális szakemberek:
 - IKT³-szakemberek: 20 millió, továbbá a nemek közötti kiegyensúlyozottság megteremtése,
 - Digitális alapkészségek: a népesség legalább 80%-a.
- Biztonságos, hatékony és fenntartható digitális infrastruktúrák:
 - Konnektivitás: gigabit mindenkinek, 5G mindenütt,
 - A csúcstechnológiát képviselő félvezetők: az EU részesedésének megkészszerzése a világ össztermeléséből,
 - Adatok – peremhálózat és felhő: 10 000 klímasemleges, rendkívül biztonságos peremcsomópont,
 - Számítástechnika: az első számítógép, amely kvantumgyorsulással rendelkezik.

³ IKT – Információs és kommunikációs technológia.

- A vállalkozások digitális átalakítása:
 - Technológiafejlesztés: az uniós vállalkozások 75%-a használja a felhőszolgáltatásokat, a mesterséges intelligenciát és a nagy adathalmazokat,
 - Innovátorok: a növekvő innovatív vállalkozások erősítése és az EU-beli uniokornisok finanszírozása,
 - Kései csatlakozók: a kkv-k több mint 90%-a használja intenzíven a digitális eszközöket, legalább alapszinten.
- A közszolgáltatások digitalizálása:
 - Kulcsfontosságú közszolgáltatások: 100%-ban online,
 - E-egészségügy: minden európai polgárnak hozzáférése van egészségügyi adataihoz,
 - Digitális személyazonosság: a polgárok 80%-a használ digitális azonosítót (Európai Bizottság 2021a).

Nem véletlen, hogy az első helyen az oktatás és a szakképzés szerepel, hiszen ez képezi Európa digitális autonómiájának alfáját és omegáját. A kérdést két oldalról kell megközelíteni: egyrészt meg kell teremteni a feltételeket ahhoz, hogy a kiberbiztonsági oktatás koncepciója biztosítsa a szükséges szintű ismereteket és működési gyakorlatokat, másrészt pedig elegendő szakképzett munkavállalót kell képezni a kiberbiztonsági ágazat és minden olyan ágazat igényeinek kielégítésére, amelynek kapcsolódnia kell a kiberbiztonsági szolgáltatásokhoz és megoldásokhoz, illetve azokat alkalmazni kell (European Organization for Security 2019). Ezt felismerve már számos uniós kezdeményezés született a digitális munkaerő-képesség növelésére. Ezek között említhető a Digitális készségek és munkahelyek koalíciója (Digital Skills and Jobs Coalition) 2016-ban vagy az Ágazati Együttműködési Terv (Blueprint for Sectorial Cooperation) a képességhiányosságok azonosítására.

Bár az *Iránytű* célkitűzéseket és célokat határoz meg, hiányoznak belőle az egyértelműen integrált és koherens politikai intézkedések, továbbá a célkitűzések és a célok között is vannak ellentmondások. E hiányosságokat részben orvosolandó, 2021. szeptember 15-én az Európai Bizottság bemutatta az *Út a digitális évtizedhez* című szakpolitikai programját, amely célja, hogy kiegészítse, teljesítse és megvalósítsa a *Digitális Iránytű* jövőképét, céljait és intézkedéseit. Az új programmal a Bizottság négy elemből álló éves együttműködési mechanizmust javasol a tagállamokkal, hogy támogassa őket a 2030-ra kitűzött célok elérésében: 1. egy továbbfejlesztett digitális gazdasági és társadalmi indexen (Digital Economy and Society Index – DESI) alapuló, átlátható nyomon követési rendszer a célok elérésének mérésére; 2. évente jelentés

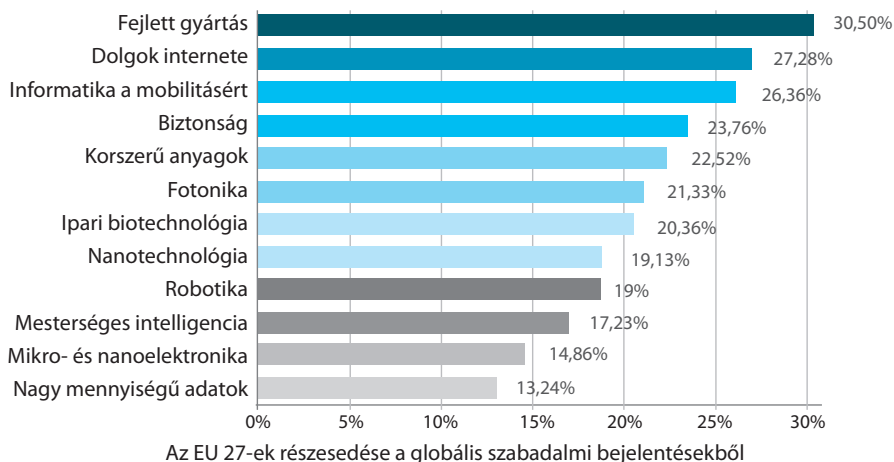
a „Digitális évtized helyzetéről”, amely értékeli az elért eredményeket és ajánlásokat fogalmaz meg; 3. többéves stratégiai ütemtervek az egyes tagállamok számára; és 4. több országot érintő projektek végrehajtását támogató mechanizmus.

Mindez azonban csak az elmélet, gyakorlatba való átültetése még kérdéses. Akadályt nemcsak az Unió bürokratikus rendszeréből fakadó tényezők jelenthetnek, hanem a szükséges anyagi erőforrások megteremtése is. Az Európai Beruházási Bank a digitális átalakulásból származó potenciális előnyök eléréséhez az uniós beruházási hiányt évi 65 milliárd euróra becsüli (European Investment Bank 2016). Ráadásul a Bizottság becslése szerint a digitális átalakulás terén Európa beruházási lemaradása az Egyesült Államokkal és Kínával szemben évi 125 milliárd euró (European Commission 2020a). Ugyanakkor a beruházások megvalósulásából az Unió nemcsak politikai és stratégiai tőkét kovácsolhatna, hanem számottevő gazdasági fellendüléssel is számolhatna, ugyanis az új digitális technológiák kumulatív GDP-hozzájárulása elérheti a 2,2 billió eurót, ami igen jelentős, 14%-os növekedést jelentene a 2017-es bázisához képest (European Commission 2020b).

*A kritikus területek: big data, mikro- és nanoelektronika,
mesterséges intelligencia, robotika*

Az Európai Bizottság fejlett ipari technológiákra vonatkozó projektje⁴ a jövője szempontjából stratégiai jelentőségűnek tekintett technológiákat követi nyomon. Idetartozik – többek között – a fejlett gyártás, a mesterséges intelligencia, a big data, a felhőszolgáltatások, az ipari biotechnológia, a dolgok internete (Internet of Things – IoT), a mikro- és nanoelektronika, beleértve a félvezetőket, a nanotechnológia, a robotika és a kiberbiztonság is. A technikai fejlődéssel való folyamatos lépéstartás elengedhetetlen feltétele a digitális szuverenitás megteremtésének az Unió számára is, ezért ennek valamennyi szegmensre vonatkozóan kiemelt uniós célnak kell lennie.

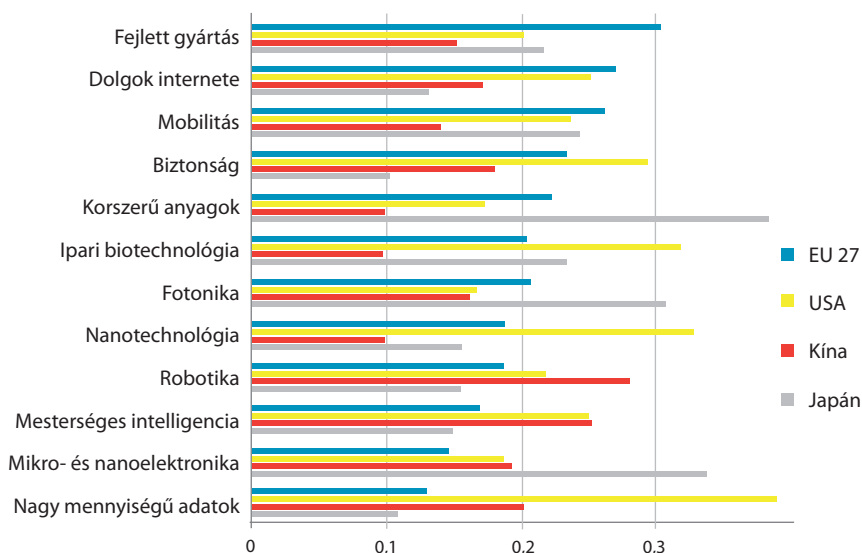
⁴ Advanced Technologies for Industry [é. n.].



1. ábra: Az EU 27 tagállamának erősségei és gyengeségei a fejlett technológiák előállításában

Forrás: Advanced Technologies for Industry [é. n.]

A 1. ábrán jól látható, hogy az egyes technológiák vonatkozásában az EU mennyire eltérő teljesítményt nyújt jelenleg: a fejlett gyártás terén kiemelkedően jó eredményeket ért el, és a dolgok internete, a mobilitás és a biztonság kategóriákban is jó a teljesítménye. Ugyanakkor hatalmasnak mutatkozik a lemaradás négy olyan területen, amely a digitális autonómia megteremtése szempontjából is kulcsfontosságú: a big data, a mikro- és nanoelektronika, a mesterséges intelligencia és a robotika. (Ezek közül különös jelentősége okán a félvezetők kérdéskörével alább részletesen foglalkozunk.) Összességében a fejlett technológiák globális szabadalmi bejelentéseinek mindössze 21,94%-a van az EU 27 tagállamának tulajdonában, ami meglehetősen alacsony érték. A lemaradás azonban talán még szembetűnőbb akkor, ha az Unió teljesítményét az Egyesült Államok, Kína és Japán teljesítményével vetjük össze. A 2. ábra a vizsgált szegmensekben tárja elénk e négy entitás teljesítményét, jól mutatva az EU sebezhető pontjait.



2. ábra: Az Európai Unió teljesítménye más államokkal összevetve

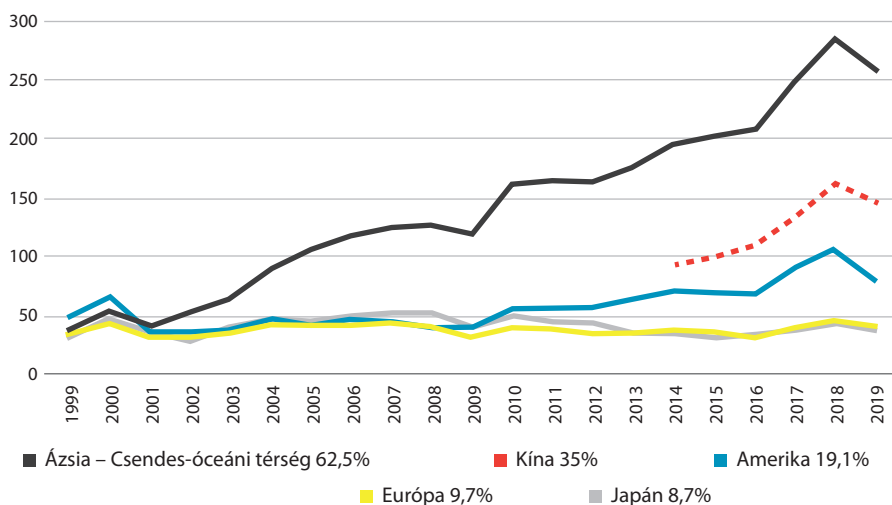
Forrás: CODAGNONE et al. 2021: 20

A félvezetők

A félvezetőket azért is övezi kiemelt figyelem, mert minden digitális termék építőkövei és ezáltal az egyre gyorsuló digitalizációs ipar fő mozgatórugói. Az elmúlt harminc évben az Európai Unió igen nagy hanyatláson ment keresztül e téren, ugyanis míg 1990-ben az európai félvezetők világpiaci részesedése még 44% volt (Bloomberg 2021), addig ez mára drasztikusan lecsökkent, és mindössze 8–13% között mozgott (Semiconductor Industry Association 2020) míg az ázsiai térség kiemelkedő, több mint 60%-os részesedéssé (lásd 3. ábra). Ennek eredményeképpen a piacot néhány vezető chipgyártó uralja: 2020-ban mindössze két cég, a TSMC (Tajvan) és a Samsung (Dél-Korea) gyártott 5 nm-es chipet, Európában pedig egyáltalán nincs olyan vállalat, amely 22 nm alatti alkatrészeket gyártana (European Commission 2021). Az amerikai Intel is 2022-re halasztotta a 7 nm-es alkatrészek gyártásának bevezetését, ami jól mutatja a chipgyártás technológiai bonyolultságát (European Commission 2021). Ugyanakkor az Intel lehet az a vállalat, amely megmenti Európát: 2021-ben bejelentette, hogy

2026-ra a legmodernebb félvezetők gyártására gyárat létesít Európában, lehetővé téve az uniós vállalkozások számára, hogy az általuk előállított saját félvezető-tervezéseik alapján saját chipeket gyárthassanak Európában (BERTUZZI 2021). Ha ez megvalósul, az európai ellátási láncok megerősödése várható középtávon.

Tajvan esete a digitális függetlenség szempontjából azért különösen fontos, mert jelenleg a világ chipjeinek nagyjából kétharmadát a szigeten gyártják. Egyebek mellett ezért is adtak aggodalomra okot a tajvani fejlemények 2020 nyarán. Amennyiben ugyanis Kína akár blokáddal, akár direkt katonai csapással avatkozik be a tajvani kereskedelembe, annak minden bizonnyal hosszabb távú hatása lesz az USA, Európa és a teljes világ digitális gazdaságára, tekintettel arra, hogy a kibertér alapvető infrastruktúra-elemeinek, számítógépeknek, mobileszközöknek vagy éppen hálózati megoldásoknak a gyártása és szállítása válik kérdésessé, nem is beszélve az európai ipar számára számottevő gépjárműiparról. A digitális autonómia szempontjából éppen ezért a *legsürgetőbb lépés a félvezetőipar (újra)építése Európában* (HASS-BLANCHETTE 2022).



3. ábra: A félvezetők piacának megoszlása (milliárd USD)

Megjegyzés: A táblázatban a 2014–2019 közötti kínai piaci adatok a teljes ázsiai és csendes-óceáni piac egyik részhalmozát alkotják.

Forrás: Semiconductor Industry Association 2020: 16.

Végezetül kiemeljük, hogy ez a szektor rendkívül intenzíven igényli a kutatás-fejlesztést, akár a bevételek egy harmadát is kutatásba fordíthatják vissza, ezért jelentős tőkebefektetésekre van szükség. Nem meglepő, hogy e területen is Kína jár az élen. Célja, hogy 2025-re 70%-os önállóságot érjen el a chipgyártásban, és ehhez 10 évre 150 milliárd dollárt különített el a Made in China 2025 program keretében. Dél-Korea 17 milliárd dollárt tervez befektetni 2029-ig a következő generációs chippekbe, míg az Egyesült Államok 25 milliárd dolláros tervet dolgozott ki 5 évre a K+F és a gyártás területén történő beruházásokra (European Commission 2021).

Következtetések

Jelenleg tehát az USA és Kína az a két szereplő, aki érdemben bele tud szólni az európai digitális autonómia alakításának kérdésébe. Az Európai Unió is aktívan próbálja alakítani a kibertér szabályait, de a jól érzékelhetően kialakult Kelet–Nyugat szembenállás jelentősen csökkenti az önálló stratégiai célok elérése sikerességének lehetőségét. Ugyanakkor a digitális stratégiai autonómia kihívásai közül csak egy a geopolitikai feszültségek növekedése, különösen az USA és Kína közötti kapcsolatok vonatkozásában. Emellett a jövő fenyegetései között számolni kell egyrészt a dolgok internetének (IoT), az 5G-nek, a mesterséges intelligenciának, a felhő- és adatvezérelt üzleti modelleknek a széles körű elterjedésével a gazdaságban és a társadalomban egyaránt, valamint az oligopolisztikus, billió dolláros platformok felé történő (szuverén) hatalomváltással járó zavaró változásokkal; és ezzel együtt a kiberbűnözés és a kiberfenyegetések támadási felületének robbanásszerű növekedésével is. Másrészt pedig a már említett radikálisan új technológiák, mint a mesterséges intelligencia, az 5G/6G, a fejlett félvezetők, az intelligensebb tárgyak internete és a kvantumtechnológia, amelyek többsége többé-kevésbé egy időben jelenik meg, mind alapvető fontosságúak az EU jövője szempontjából (TIMMERS 2022). Ezek fényében nem véletlen, hogy az Európai Unió Kiberbiztonsági Ügynöksége, az ENISA⁵ 2021-ben a következő hét területet azonosította mint az uniós digitális stratégiai autonómia fejlesztésének kulcsterületeit: adatbiztonság, megbízható szoftverplatformok, megfelelő incidensmenedzsment, megbízható hardverplatformok, poszt-kvantumkriptográfia, felhasználóbarát biztonsági eszközök és gyakorlatok, valamint a digitális kommunikáció biztonsága. Ugyanakkor az ENISA azt is hozzátette, hogy bár a digitális autonómia és szuverenitás a technológiai

⁵ European Union Agency for Cybersecurity.

vezető szerepre – és legfőképpen a jelentős kutatás-fejlesztésre – támaszkodik, a technikai vezetés önmagában nem elegendő ahhoz, hogy biztosítsa a fenntartható stratégiai autonómiát hosszú távon. Ezért az Uniónak a digitális autonómia társadalomtudományi dimenzióira úgy, mint a képzett munkaerőre és a megfelelő jogi-szabályozási környezet kialakítására is nagy szüksége van (ENISA 2021).

A Covid-19-világjárvánnyal járó digitális transzformáció, a globális felmelegedés elleni küzdelem és az orosz–ukrán háború azonban olyan társadalmi és gazdasági változásokat hozott, amelyek egyben lehetőséget is jelentenek Európa digitális szuverenitásának kivívására. A globális ellátási láncok ellehetetlenülése, az alapvető erőforrásoktól való elzáródás, az olcsó ázsiai munkaerőre épülő gyártás megnehezülése, az európai perifériaországok integrációs törekvéseinek felgyorsulása vagy éppen a csúcstechnológiás hadiipari gyártás széles körű beindítása mind abba az irányba mutatnak, hogy az európai iparnak sebességet kell váltania, és néhány éven belül meg kell teremtenie saját képességeit, különben függősége hosszú évtizedekre megmarad. Függetlenül attól, hogy az európai politika milyen irányba halad előre, hogy az európai állampolgárok a föderalista, a nemzetállami vagy a kétsebességes Európa mellett döntenek, a *digitális autonómia megteremtése az összehangolt tagállami lépések nélkül nem kivívható*. A digitális szuverenitás elvesztése pedig azzal jár, hogy Európa kiesik a 21. század hatalmi központjai közül, és bizonytalan időre befolyásolási övezetté válik. Kína példája azonban azt mutatja, hogy két-három évtized elég lehet egy európai digitális reneszánsz eléréséhez.

Felhasznált irodalom

- Advanced Technologies for Industry* [é. n.] Online: <https://ati.ec.europa.eu/>
- BERTUZZI, Luca (2021): Leading Chip-Maker Answers EU Call to Scale Up European Capacity. *Euractiv*, 2021. június 10. Online: www.euractiv.com/section/digital/news/leading-chip-maker-answers-eu-call-to-scale-up-european-capacity/
- Bloomberg (2021): Europe Looks to Secure Chips Supply After 'Naive' past Approach. *Automotive News Europe*, 2021. május 5. Online: <https://europe.autonews.com/suppliers/europe-looks-secure-chip-supply-after-naive-past-approach>
- BROWN, Ronald Harmon (1993): *The National Information Infrastructure: Agenda for Action*. Executive Office of the President Information Infrastructure Task Force.
- CODAGNONE, Cristiano et al. (2021): *Europe's Digital Decade and Autonomy*. Online: [www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU\(2021\)695465_EN.pdf](https://europe.eu/RegData/etudes/STUD/2021/695465/IPOL_STU(2021)695465_EN.pdf)

- ENISA (2021): *Cybersecurity Research Directions for the EU's Digital Strategic Autonomy*. Online: <https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy>
- Európai Bizottság (2021a): *Európa digitális évtizede: a 2030-ra kitűzött célok*. Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_hu
- Európai Bizottság (2021b): *Javaslat az Európai Parlament és a Tanács határozata „A digitális évtizedhez vezető út” elnevezésű, 2030-ig szóló szakpolitikai program létrehozásáról*. COM(2021) 574. Online: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021PC0574>
- European Commission (1995): *Europe and the Global Information Society: Recommendations to the European Council: Conference G7 – Raport BANGEMANN*. Publications Office.
- European Commission (2020a): *Commission Staff Working Document. Identifying Europe's Recovery Needs*. SWD(2020) 98 final/2. Brüsszel, 2020. május 27. Online: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0098\(01\)&rid=3](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0098(01)&rid=3)
- European Commission (2020b): *Shaping the Digital Transformation in Europe*. Online: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69479
- European Commission (2021): *Commission Staff Working Document. Strategic Dependencies and Capacities*. Online: https://commission.europa.eu/system/files/2021-05/swd-strategic-dependencies-capacities_en.pdf
- European Investment Bank (2016): *Restoring EU Competitiveness. 2016 Updated Version*. Online: www.eib.org/attachments/efs/restoring_eu_competitiveness_en.pdf
- GODEMENT, Francois et al. (2018): *The China Dream Goes Digital: Technology in the Age of Xi*. *European Council on Foreign Relations*, 2018. október 25. Online: https://ecfr.eu/publication/the_china_dream_digital_technology_in_the_age_of_xi/
- HASS, Ryan – BLANCHETTE, Jude (2022): *Central Questions in U.S.-China Relations amid Global Turbulence*. *Center for Strategic & International Studies*, 2022. július 21. Online: www.csis.org/analysis/central-questions-us-china-relations-amid-global-turbulence
- JOYCE, Rob (2023): *State of the Hack 2023. RSA Conference*, 2023. április 26. Online: www.rsa-conference.com/library/presentation/usa/2023/state%20of%20the%20hack%202023%20%20nsas%20perspective
- POGOREL, Geral – NESTORAS, Antonios – CAPPELLETTI, Francesco szerk. (2022): *Decoding EU Digital Strategic Autonomy. Sectors, Issues, and Partners*. European Liberal Forum, Techno-Politics Series, 1. Online: https://liberalforum.eu/wp-content/uploads/2022/06/Decoding-EU-Digital-Strategic-Autonomy_ELF-Study_Techno-Politics_vol.1-2.pdf

- QS Top Universities [é. n.]: *QS World University Rankings by Subject 2022: Engineering & Technology*. Online: www.topuniversities.com/university-rankings/university-subject-rankings/2022/engineering-technology
- Semiconductor Industry Association (2020): *Factbook 2020*. Online: www.semiconductors.org/wp-content/uploads/2020/04/2020-SIA-Factbook-FINAL_reduced-size.pdf
- STOLWIJK, Claire (2022): Strengthening Digital Sovereignty Makes Europe Less Vulnerable Both Politically and Economically. *TNO*, 2022. június 14. Online: www.tno.nl/en/tno-insights/articles/strengthening-digital-sovereignty-makes-europe-less-vulnerable-politically-and-economically
- The White House (2022): *National Security Strategy*. Online: www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
- THIEULIN, Benoît (2019): *Towards a European Digital Sovereignty Policy*. ESEC's opinion. Online: www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf
- TIMMERS, Paul (2018). *Cybersecurity is forcing a rethink of strategic autonomy*. OXPOL. Online: <https://echalliance.com/news/cybersecurity-is-forcing-a-rethink-of-strategic-autonomy/>
- TIMMERS, Paul (2022): Cybersecurity and Resilience from a Strategic Autonomy Perspective. In POGOREL, Geral – NESTORAS, Antonios – CAPPELLETTI, Francesco (szerk.) (2022): *Decoding EU Digital Strategic Autonomy. Sectors, Issues, and Partners*. European Liberal Forum, Techno-Politics Series, 1, 37–49. Online: https://liberalforum.eu/wp-content/uploads/2022/06/Decoding-EU-Digital-Strategic-Autonomy_ELF-Study_Techno-Politics_vol.1-2.pdf
- ZHANG, Yingying – ZHOU, Yu (2015): *The Source of Innovation in China*. London: Palgrave Macmillan.