EUROPSKA
KOMISIJA

Strasbourg, 18.4.2023.
COM(2023) 207 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije („Akademija za vještine u području kibersigurnosti”)

Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije

(„Akademija za vještine u području kibersigurnosti”)

1. Za smanjenje rizika prijeko je potrebno unaprijediti kibersigurnosne vještine

Kibersigurnost nije samo sastavni dio sigurnosti građana, poduzeća i država članica, već je nužna i kako bi se osigurala politička stabilnost Unije, stabilnost njezinih demokracija te blagostanje našeg društva i naših poduzeća. Kibersigurnosne **prijetnje** proteklih su se godina znatno raširile i pojavio se zabrinjavajući trend: sve je više kibernapada na vojnu i civilnu kritičnu infrastrukturu u Uniji. Prijeteći akteri unapređuju svoje sposobnosti te se javljaju nove, hibridne i inovativne prijetnje, kao što je upotreba botova i tehnika koje se temelje na umjetnoj inteligenciji[1]. Treba posebno istaknuti da prijeteći akteri koji upotrebljavaju ucjenjivački softver subjektima redovito uzrokuju znatnu financijsku i reputacijsku štetu[2].

U brojnim kiberincidentima na meti su također bile javne uprave i vlade država članica te europske institucije, tijela i agencije[3]. Stalne su mete napada i financijski[4] i zdravstveni[5] sektor, koji su okosnice društva i gospodarstva[6]. Geopolitičke napetosti povezane s ruskim agresivnim ratom protiv Ukrajine[7] pridonijele su porastu kibersigurnosnih prijetnji i mogle bi destabilizirati naše društvo. **Sigurnost** Unije nije moguće zajamčiti bez sudjelovanja njezina **najvrednijeg kapitala: njezinih stanovnika.** Uniji su hitno potrebni stručnjaci koji posjeduju vještine i kompetencije za sprečavanje, otkrivanje i odvraćanje kibernapada te za obranu Unije i njezine najkritičnije infrastrukture od njih i izgradnju njezine **otpornosti**.

Manjak stručnjaka za kibersigurnost i dalje ometa **konkurentnost** i **rast** Europe, koji u velikoj mjeri ovise o razvoju i širenju upotrebe strateških digitalnih tehnologija (npr. umjetna inteligencija, 5G tehnologija i računalstvo u oblaku). Kako bi Unija i dalje mogla razvijati ključne napredne tehnologije u globalnom okruženju, potrebna joj je kvalificirana radna snaga u području kibersigurnosti.

Da bi se Unija pripremila za te promjenjive prijetnje i suočila s njima te da bi se potaknula njezina konkurentnost, politika EU-a u području kibersigurnosti proteklih je godina znatno unaprijeđena te je donesen niz inicijativa, kao što su Strategija EU-a za kibersigurnost za

---

[1] ENISA – Pregled prijetnji 2022. – Agencija Europske unije za kibersigurnost (europa.eu).

[2] Europolova ocjena prijetnje organiziranog kriminala na internetu (IOCTA) 2021. Ti akteri primjenjuju model ucjenjivačkog softvera kao usluge. Godišnji trošak za poduzeća 2022. premašio je 18,4 milijardi EUR (Izvješće poduzeća Cybereason o stvarnom trošku ucjenjivačkog softvera 2022.).

[3] Vidjeti npr. Zajednička publikacija ENISA-e i CERT-EU-a, JP-23-01 – Kontinuirana aktivnost određenih prijetećih aktera, TLP:CLEAR, 15. veljače 2023.

[4] Vidjeti npr. u Njemačkoj: krađe identiteta povezane s financijskim uslugama (*phishing*) činile su 90 % prijevara putem e-pošte prijavljenih od 1. lipnja 2021. do 31. svibnja 2022. ili napad na poduzeće u financijskom sektoru u kojem je napadnuto više od 20 000 uređaja iz 125 zemalja, Stanje informatičke sigurnosti u Njemačkoj 2022., Bundesamt für Sicherheit in der Informationstechnik (BSI), 1. siječnja 2023.

[5] Vidjeti npr. u Francuskoj: napadi ucjenjivačkim softverom na javne zdravstvene ustanove, kao što je napad na Centre Hospitalier Sud Francilien, tijekom kojeg je prijeteći akter ugrozio sigurnost 11 GB osobnih i medicinskih podataka te podataka povezanih s osobljem i objavio ih, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023.

[6] ENISA – Pregled prijetnji 2022.

[7] Vidjeti i: CERT-EU – Ruski rat protiv Ukrajine: godina dana kiberoperacija (europa.eu); Ruske kiberoperacije protiv Ukrajine: izjava visokog predstavnika u ime Europske unije, 10. svibnja 2022.; Izjava visokog predstavnika u ime Europske unije o zlonamjernim kiberaktivnostima hakera i hakerskih skupina u kontekstu ruske agresije na Ukrajinu, 19. srpnja 2022.

digitalno desetljeće[8], revidirana Direktiva o sigurnosti mrežnih i informacijskih sustava (Direktiva NIS 2)[9], sektorsko zakonodavstvo EU-a u području kibersigurnosti[10], politika kiberobrane EU-a[11], Akt o kiberotpornosti[12] i Akt o kibersolidarnosti, koji je Komisija predložila zajedno s ovom Komunikacijom. Međutim, ciljevi tih zakonodavnih akata neće se ostvariti bez kvalificiranih osoba potrebnih za njihovu provedbu. Osnovno znanje o kibersigurnosti općoj se populaciji prenosi inicijativama kojima se podupire razvoj općih vještina potrebnih za sudjelovanje u društvu[13], no kompetentna radna snaga u javnom i privatnom sektoru, na nacionalnoj razini i na razini Unije, među ostalim u normizacijskim organizacijama, od presudne je važnosti **za ispunjavanje pravnih i političkih zahtjeva u području kibersigurnosti.**

Sigurnost i konkurentnost Unije stoga ovise o stručnoj i kvalificiranoj radnoj snazi u području kibersigurnosti. Međutim, Unija se suočava s velikim manjkom kvalificiranih stručnjaka za kibersigurnost, zbog čega je zajedno s državama članicama, poduzećima i građanima izložena riziku od kiberincidenata. U Europskoj uniji je 2022. nedostajalo **od 260 000**[14] **do 500 000**[15] stručnjaka za kibersigurnost, a potrebe Unije za radnom snagom u području kibersigurnosti procijenjene su na 883 000 stručnjaka[16], što ukazuje na nesrazmjer između dostupnih i traženih vještina na tržištu rada. Usto, na radnu snagu u području kibersigurnosti negativno utječu pogrešne predodžbe povezane s njezinom tehničkom prirodom te ona i dalje ne uspijeva privući **žene**, koje čine 20 % diplomiranih stručnjaka za kibersigurnost[17] i 19 % stručnjaka za informacijske i komunikacijske tehnologije (IKT)[18]. Kako bi se riješio taj problem, u europskom **programu politike za digitalno desetljeće do 2030.**[19] postavljen je cilj da se do 2030. broj stručnjaka za IKT poveća za 20 milijuna s podjednakim udjelom žena i muškaraca. Nadalje, za provedbu nove politike EU-a potrebna je primjereno kvalificirana i dovoljno velika radna snaga. Na primjer, više od 42 % viših informatičkih rukovoditelja u industriji financijskih usluga istaknulo je nedostatak kibersigurnosnih vještina i stručnosti kao najvažniji izazov za

[8] Zajednička komunikacija Europskom parlamentu i Vijeću, Strategija EU-a za kibersigurnost za digitalno desetljeće, JOIN(2020) 18 final.

[9] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2).

[10] Na primjer, za financijski sektor: Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011.

[11] Zajednička komunikacija Europskom parlamentu i Vijeću, Politika kiberobrane EU-a, JOIN(2022) 49 final.

[12] Prijedlog uredbe Europskog parlamenta i Vijeća o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020, COM(2022) 454 final.

[13] Ovo su neke od relevantnih inicijativa za razvoj općih digitalnih vještina stanovništva: cilj Akcijskog plana za provedbu europskog stupa socijalnih prava i Digitalnog kompasa da najkasnije do 2030. 80 % stanovništva raspolaže osnovnim digitalnim vještinama, Akcijski plan za digitalno obrazovanje 2021.–2027., okvir digitalnih kompetencija te Prijedlog preporuke Vijeća o poboljšanju prenošenja digitalnih vještina u obrazovanju i osposobljavanju.

[14] (ISC)² u Procjeni vještina u području kibersigurnosti na temelju ECSF-a, webinar ENISA-e, 16. veljače 2023.

[15] Prema Europskoj organizaciji za kibersigurnost (ECSO), kako je navedeno u Zajedničkoj komunikaciji Europskom parlamentu i Vijeću, Politika kiberobrane EU-a, JOIN(2022) 49 final.

[16] (ISC²) u Procjeni vještina u području kibersigurnosti na temelju ECSF-a, webinar ENISA-e, 16. veljače 2023.

[17] Baza podataka o visokom obrazovanju u području kibersigurnosti (CyberHEAD).

[18] Svega 19 % stručnjaka za IKT u Uniji su žene – Indeks gospodarske i društvene digitalizacije (DESI) za 2022. | Izgradnja digitalne budućnosti Europe (europa.eu). Brojke koje se odnose na žensku radnu snagu Unije u području kibersigurnosti nisu dostupne.

[19] Odluka (EU) 2022/2481 Europskog parlamenta i Vijeća od 14. prosinca 2022. o uspostavi programa politike za digitalno desetljeće do 2030., kojom se uspostavlja mehanizam praćenja i suradnje kako bi se ostvarili zajednički ciljevi za digitalnu transformaciju Europe utvrđeni u Digitalnom kompasu 2030., među ostalim u području vještina.

njihovo poduzeće u području kiberobrane i upravljanja incidentima[20], i to u trenutku kad moraju provoditi sektorsko zakonodavstvo u području kibersigurnosti, primjerice Akt o digitalnoj operativnoj otpornosti.

Tržište rada dodatno ograničava i to što poslodavci nerado ulažu u ljudski kapital te traže već osposobljenu i iskusnu radnu snagu[21]. To ograničenje utječe na sve vrste poduzeća, uključujući mala i srednja poduzeća (**MSP-ovi**), koja čine 99 % svih poduzeća u Uniji[22]. **Javne uprave** također se suočavaju s velikim izazovom jer su česta meta kibersigurnosnih incidenata i najviše osjećaju njihove posljedice[23].

Problem nedostatka stručnih kibersigurnosnih kadrova stoga je potrebno hitno riješiti jer o tome ovise sigurnost i konkurentnost Unije.

2. Nedostatak sinergija i koordiniranih mjera za razvoj nedostatnih kibersigurnosnih vještina

Na europskoj i nacionalnoj razini javni i privatni subjekti provode brojne inicijative kako bi se riješio problem nedostatne radne snage na tržištu rada u području kibersigurnosti. Međutim, one nisu objedinjene i dosad nisu uspjele dostići kritičnu masu zahvaljujući kojoj bi se situacija doista promijenila.

Prvo, zajedničko razumijevanje sastava kibersigurnosne radne snage u Uniji i povezanih vještina trenutačno je ograničeno, iako bi profili sličnih zanimanja u području kibersigurnosti trebali uključivati iste vještine. Budući da relevantni akteri ne primjenjuju sustavno zajednički **europski referentni okvir za stručnjake za kibersigurnost**, ne postoje sredstva za komunikaciju među poslodavcima, odgojno-obrazovnim djelatnicima i oblikovateljima politika, pa nedostatke na tržištu rada u području kibersigurnosti zato nije moguće izmjeriti i procijeniti. To dodatno onemogućuje osmišljavanje kurikuluma za obrazovanje i osposobljavanje te oblikovanje mogućnosti za razvoj karijere pri kojima se vodi računa o potrebama politika i tržišta za osobe koje žele raditi u toj struci. **Usavršavanje i prekvalifikacija** radne snage uvelike ovise o osposobljavanjima i certifikatima za kibersigurnost, koje obično pružaju privatni subjekti. Međutim, radnicima nije lako steći pregled nad kvalitetom ponuđenih kibersigurnosnih osposobljavanja i povezanih certifikata koji se potom izdaju.

Obrazovanje i osposobljavanje te mogućnosti za razvoj karijere potrebni su kako bi se povećala ponuda na tržištu rada, no trenutačno se ne pridaje dovoljno važnosti ulozi **potražnje** u osposobljavanju radne snage i njezine prilagodbe kretanjima na tržištu rada. Sektor i javni poslodavci nemaju zajedničke forume i prostor za prikupljanje ideja o tome kako najbolje osposobiti radnu snagu i riješiti pitanje **boljeg ocjenjivanja vještina**, osobito u postupku zapošljavanja. Najtraženije **stručne vještine**, kao što su razvoj softvera ili računalstvo u oblaku[24], možda jesu povezane s kibersigurnošću[25], ali se **transverzalne vještine** i dalje neopravdano zanemaruju. Kritičko mišljenje i analiza, rješavanje problema i organiziranost čine skup vještina koje poslodavci sve više traže[26] i koje će biti sve važnije kako se približavamo 2025.[27]

---

[20] Izvješće poduzeća S-RM o uvidima u kibersigurnost 2022.

[21] Razvoj vještina za kibersigurnost u EU-u, ENISA, prosinac 2019.

[22] Definicija MSP-a (europa.eu).

[23] ENISA – Pregled prijetnji 2022. – Agencija Europske unije za kibersigurnost (europa.eu).

[24] ISACA – Infografika o stanju kibersigurnosti 2022.

[25] LinkedIn – Najtraženije vještine 2023.: steknite vještine koje su poduzećima najpotrebnije.

[26] Kao što je alat CEDEFOP-a: Skills-OVATE | CEDEFOP (europa.eu).

[27] Izvješće o budućnosti radnih mjesta, listopad 2020., Svjetski gospodarski forum.

Brojne inicijative za javna i privatna ulaganja u kibersigurnosne vještine već postoje, a Unija **financira** mnoštvo projekata u okviru raznih instrumenata[28]. Međutim, trajni nedostatak vještina u Uniji dovodi u pitanje njihovu vidljivost i učinak, što znači da one možda sustavno ne odgovaraju potrebama tržišta, koje je treba hitno utvrditi na razini Unije. Usto, zbog višestrukih izvora financiranja nastaju preklapanja te se propušta prilika za širenje i postizanje stvarnog učinka. Nadalje, oni kojima su ulaganja potrebna nisu uvijek sposobni prepoznati najbolje izvore za svoje potrebe.

Dionici pokušavaju riješiti složen i višedimenzionalan problem nedostatka kibersigurnosnih vještina. Agencija Europske unije za kibersigurnost (ENISA) razvija instrumente koji se odnose na profile zanimanja ili visoko obrazovanje[29], Europski stručni centar u području kibersigurnosti (ECCC)[30] okupio je posebnu radnu skupinu za kibersigurnosne vještine, Europska akademija za sigurnost i obranu (ESDC) radi na kibersigurnosnim vještinama civilne i vojne radne snage u kontekstu zajedničke sigurnosne i obrambene politike[31], tim se problemom bave i privatne organizacije[32], a sektor kibersigurnosne certifikacije izrađuje plan i programe osposobljavanja za razvoj nedostatnih vještina[33]. Na rješavanju tog problema rade i države članice, i to pokretanjem raznih inicijativa, koje sežu od regulatornih inicijativa[34] do osnivanja akademija za kibersigurnosne vještine[35], kiberkampusa[36] ili centara izvrsnosti za kiberkriminalitet[37], te uspostavom javno-privatnih partnerstava[38]. Međutim, svi ti dionici često rade bez koordinacije i sinergije te još nisu uspjeli postići stvarni učinak na tržištu rada, što je vidljivo iz sve većeg nedostatka radne snage u području kibersigurnosti u Uniji. Također je potrebno povećati sinergije među kibersigurnosnim zajednicama jer su vještine potrebne za očuvanje kibersigurnosti, borbu protiv **kiberkriminaliteta** i uspostavu **kiberobrane** često slične.

Naposljetku, Unijine sposobnosti za procjenu **stanja i kretanja na tržištu rada u području kibersigurnosti** te vještina radne snage danas su ograničene. Države članice te institucije, tijela i agencije Unije oslanjaju se ili na podatke koje prikupljaju privatni subjekti ili na širi skup podataka o stručnjacima u području IKT-a koje prikuplja EU, točnije Eurostat[39] i Europski centar za razvoj strukovnog osposobljavanja (CEDEFOP)[40]. Drugim riječima, Unija ima djelomičan i fragmentiran pregled vlastitih potreba, što je sprečava da stekne cjelovit uvid u stanje na tržištu rada u području kibersigurnosti.

---

[28] Na primjer: Savez za vještine u području kibersigurnosti – Nova vizija Europe – projekt REWIRE (financira se iz programa Erasmus+); projekti kojima se podupire Stručni centar u području kibersigurnosti (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (financira se iz programa Obzor 2020.), projekt Cybersecpro (financira se iz programa Digitalna Europa).

[29] Konkretnije: Europski okvir za vještine u području kibersigurnosti (ECSF); CYBERHEAD – Baza podataka o visokom obrazovanju u području kibersigurnosti; Platforma za kibervježbe (CEP); Europski kibersigurnosni izazov; Europski mjesec kibersigurnosti.

[30] Uredba (EU) 2021/887 Europskog parlamenta i Vijeća od 20. svibnja 2021. o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti i mreže nacionalnih koordinacijskih centara.

[31] Konkretnije platforma za obrazovanje, osposobljavanje, evaluaciju i vježbe u području kibersigurnosti (ETEE).

[32] Na primjer, peta radna skupina Europske organizacije za kibersigurnost (ECSO) za „obrazovanje, osposobljavanje, informiranje, kiberpoligone, ljudske faktore"; organizacija DIGITALEUROPE.

[33] Na primjer, Institut SANS, (ISC)², ISACA.

[34] Na primjer, u nacionalnim strategijama za obrazovanje ili kibersigurnost.

[35] Na primjer, C-Academy u Portugalu.

[36] Na primjer, Campus Cyber u Francuskoj.

[37] Na primjer, Centar izvrsnosti za osposobljavanje, istraživanje i obrazovanje u području kiberkriminaliteta u Litvi (L3CE).

[38] Na primjer, Microsoftova Inicijativa za kibersigurnosne vještine.

[39] Zaposleni stručnjaci u području IKT-a – Objašnjenja statističkih podataka (europa.eu).

[40] Kao što je alat CEDEFOP-a: Skills-OVATE | CEDEFOP (europa.eu).

3. Koordinirani odgovor na razini Unije: Akademija za vještine u području kibersigurnosti

3.1. Cilj

Da bi se prevladali izazovi povezani s manjkom kibersigurnosnih vještina i nadoknadili nedostaci na tržištu rada, Komisija predlaže **Akademiju za vještine u području kibersigurnosti**, koju je predsjednica Europske komisije najavila u Pismu namjere uz Govor o stanju Unije 2022.[41, , 42] i u kontekstu Europske godine vještina.

Cilj je Akademije za vještine u području kibersigurnosti (dalje u tekstu „Akademija") stvoriti **jedinstvenu pristupnu točku i sinergije** za sve ponude obrazovanja i osposobljavanja u području kibersigurnosti, mogućnosti financiranja i konkretne mjere za razvoj kibersigurnosnih vještina. Ona će proširiti inicijative dionika kako bi se postigla kritična masa zahvaljujući kojoj će se situacija na tržištu rada, među ostalim u području obrane, doista promijeniti. Te će se aktivnosti uskladiti pomoću zajedničkih ciljeva i ključnih pokazatelja uspješnosti kako bi se ostvario veći učinak.

Najvažnija zadaća Akademije bit će razvoj vještina **stručnjaka za kibersigurnost**. Njezine aktivnosti pridonijet će politikama Unije u području kibersigurnosti te osposobljavanju i cjeloživotnom učenju. Akademija dopunjuje dvije preporuke Vijeća povezane s digitalnim obrazovanjem i vještinama koje je Komisija predložila u isto vrijeme kad i ovu Komunikaciju[43].

Akademija će se temeljiti na četiri stupa: 1. poticanje **stvaranja znanja putem obrazovanja i osposobljavanja** radom na zajedničkom okviru za profile zanimanja u području kibersigurnosti i povezane vještine, poboljšanjem europske ponude obrazovanja i osposobljavanja tako da odgovara potrebama, pružanjem mogućnosti za razvoj karijere te povećanjem vidljivosti i preglednosti programa osposobljavanja i certifikacija u području kibersigurnosti kako bi se poboljšala ponuda radne snage; 2. bolje usmjeravanje i povećana vidljivost dostupnih **mogućnosti financiranja** za aktivnosti povezane s vještinama kako bi se ostvario najveći mogući učinak; 3. poticanje dionika **na djelovanje** i 4. definiranje pokazatelja koji omogućuju **praćenje kretanja na tržištu** i ocjenjivanje djelotvornosti mjera.

Uspostava Akademije financirat će se sredstvima iz programa Digitalna Europa u iznosu od 10 milijuna EUR[44].

3.2. Upravljanje Akademijom

Kako bi se na raspolaganje stavila infrastruktura koja bi služila kao **jedinstvena pristupna točka** putem koje bi se poticala suradnja akademske zajednice, pružatelja osposobljavanja i industrije i u okviru koje bi se mogli okupljati i osposobljavati subjekti na strani ponude i potražnje kibersigurnosnog sustava Unije, Akademija bi se u konačnici mogla uspostaviti u obliku **konzorcija za europsku digitalnu infrastrukturu (EDIC)**[45]. Taj bi instrument državama članicama omogućio da zajedno rade na problemu nedostatka kibersigurnosnih vještina, usko surađuju s Komisijom, ENISA-om i Europskim stručnim centrom u području

[41] Stanje Unije 2022. – Pismo namjere predsjednici Roberti Metsoli i premijeru Petru Fiali.

[42] Zajednička komunikacija Europskom parlamentu i Vijeću, Politika kiberobrane EU-a, JOIN(2022) 49 final.

[43] Prijedlozi preporuka Vijeća o ključnim čimbenicima koji omogućuju uspješno digitalno obrazovanje i osposobljavanje te o poboljšanju prenošenja digitalnih vještina u obrazovanju i osposobljavanju.

[44] Uredba (EU) 2021/694 Europskog parlamenta i Vijeća od 29. travnja 2021. o uspostavi programa Digitalna Europa te o stavljanju izvan snage Odluke (EU) 2015/2240.

[45] EDIC-i su uspostavljeni Odlukom (EU) 2022/2481 Europskog parlamenta i Vijeća od 14. prosinca 2022. o uspostavi programa politike za digitalno desetljeće do 2030., članak 13. i dalje.

kibersigurnosti (ECCC), u skladu s njihovim nadležnostima i kompetencijama, uključe sve relevantne dionike te usmjere europska, nacionalna i privatna ulaganja prema zajedničkom cilju. Zainteresirane države članice stoga se potiču da Komisiji do 30. svibnja 2023. dostave prethodnu obavijest o budućem zahtjevu za EDIC. Na temelju tih dobrovoljnih prethodnih obavijesti Komisija bi mogla objaviti rane primjedbe o nacrtu zahtjeva za EDIC, što bi omogućilo njegovu bržu izradu i službeno slanje. Komisija će tijekom cijelog postupka i u mjeri u kojoj to budu tražile države članice omogućiti ubrzanje višedržavnih projekata i pomagati u pripremi zahtjeva za EDIC. Zatim, nakon što pozitivno ocijeni zahtjev i on dobije odobrenje Odbora za program digitalnog desetljeća, Komisija će izdati Odluku o uspostavi EDIC-a i nastaviti pomagati u koordinaciji njegove provedbe[46].

U međuvremenu, dok se EDIC službeno uspostavlja, Komisija će uvesti virtualnu jedinstvenu pristupnu točku tako što će nadograditi svoju **platformu za digitalne vještine i radna mjesta**[47] uz pomoć projekta potpore europskoj zajednici za kibersigurnost (ECCO)[48].

ENISA će uspostavi Akademije doprinijeti u skladu sa svojim ciljevima[49], posebno u vezi s potporom obrazovanju i osposobljavanju u području kibersigurnosti, i uzimajući u obzir svoje obveze izvješćivanja u okviru Direktive NIS 2[50]. Kako bi pridonio uspostavi Akademije za vještine u području kibersigurnosti, **ECCC** će djelovati u skladu sa svojim strateškim programom. Konkretnije, provodit će treći strateški cilj (kibersigurnost) programa Digitalna Europa, a Komisija i države članice podupirat će ga putem **nacionalnih koordinacijskih centara**. **Skupina za suradnju** osnovana Direktivom NIS 2[51] angažirat će se prema potrebi. Naposljetku, da bi se uspješno riješio problem nedostatka kibersigurnosnih vještina, Akademija će trebati udružiti snage s **industrijom** i **akademskom zajednicom**.

4. Stvaranje znanja i osposobljavanje: uspostava zajedničkog pristupa EU-a osposobljavanju u području kibersigurnosti

U okviru stupa Akademije za vještine u području kibersigurnosti koji se odnosi na stvaranje znanja i osposobljavanje osmislit će se strukturirani pristup s jasnim ciljem da se poveća **broj** osoba s kibersigurnosnim vještinama u Uniji, osposobljavanje bolje uskladi s **potrebama tržišta** i poveća vidljivost **mogućnosti za razvoj karijere**.

4.1. Zajednički jezik: zajednički pristup profilima zanimanja u području kibersigurnosti i povezanim vještinama

ENISA je već počela raditi na definiranju profila zanimanja stručnjaka za kibersigurnost u okviru Europskog okvira za vještine u području kibersigurnosti (**ECSF**)[52]. To bi trebala biti

---

[46] Isto, članak 12.

[47] Početna stranica | Platforma za digitalne vještine i radna mjesta (europa.eu).

[48] Vidjeti Europski stručni centar i mreža u području kibersigurnosti: novi projekt za potporu zajednici za kibersigurnost financiran sredstvima EU-a (europa.eu). Europska komisija je u prosincu 2022. potpisala ugovor vrijedan 3 milijuna EUR za potporu zajednici za kibersigurnost u Uniji putem Europskog stručnog centra u području kibersigurnosti. Taj će projekt pridonijeti ciljevima Unije koji se odnose na proširenje zajednice i povećanje kapaciteta za istraživanje, inovacije, širenje primjene i industrijsku bazu u području kibersigurnosti.

[49] „ENISA podupire jačanje kapaciteta i pripravnosti u cijeloj Uniji na način da institucijama, tijelima, uredima i agencijama Unije, kao i državama članicama te javnim i privatnim dionicima pomaže da [...] razviju vještine i sposobnosti u području kibersigurnosti.” Članak 4. stavak 3. Akta o kibersigurnosti.

[50] Članak 18. Direktive NIS 2.

[51] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2).

[52] Europski okvir za vještine u području kibersigurnosti (ECSF) – ENISA (europa.eu). ECSF pomaže u identifikaciji i artikulaciji zadaća, kompetencija, vještina i znanja povezanih sa zanimanjima europskih stručnjaka za kibersigurnost. U

osnova na kojoj će Akademija definirati i ocjenjivati relevantne vještine, pratiti kretanja u pogledu njihova nedostatka i ukazivati na nove potrebe. Kao element opisa za svaki profil zanimanja u području kibersigurnosti iz ECSF-a[53] naveden je skup primjenjivih vještina iz europskog okvira e-kompetencija[54].

ENISA će stoga preispitati ECSF i **utvrditi novonastale potrebe za vještinama i nedostatne vještine** radne snage u području kibersigurnosti, među ostalim primjenom naprednih alata (npr. umjetna inteligencija, velika količina podataka[55], rudarenje podataka). U tu će svrhu pod vodstvom EDIC-a, kad se on uspostavi, i ECCC-a, surađivati s nacionalnim koordinacijskim centrima, Komisijom, projektom ECCO i sudionicima na tržištu[56]. U pogledu radne snage za kiberobranu ENISA će uzeti u obzir rad koji je obavio ESDC. Slično tome, u području borbe protiv kiberkriminaliteta uzet će u obzir aktivnosti koje Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva (CEPOL) i Europol provode pri izradi analize potreba za operativnu obuku[57] u području kibernapada.

ECSF će se redovito dopunjavati i preispitivati u dvogodišnjem ciklusu u okviru Akademije. Usto, Komisija i Europska služba za vanjsko djelovanje doprinijet će definiranju specifičnih profila i povezanih vještina za sektore prema potrebi, uz potporu agencija i tijela EU-a kao što su ESDC[58], Europol i CEPOL[59].

ECSF će se također povezati s relevantnim instrumentima politike zapošljavanja Unije[60], i to na način da će se profili zanimanja i povezane vještine iz ECSF-a uvrstiti u **klasifikaciju ESCO-a**. Time će se poboljšati klasifikacija i povezanost zanimanja i vještina u području kibersigurnosti, pa će se pojedincima olakšati usavršavanje i strukovna prekvalifikacija, kao i pronalaženje odgovarajućeg posla na temelju vještina koje posjeduju te prekogranična mobilnost.

4.2. Poticanje suradnje u izradi kurikuluma za obrazovanje i osposobljavanje u području kibersigurnosti

Nakon što se uspostavi EDIC, države članice trebale bi pomoći Akademiji kako bi postala **referentno mjesto u Europi za osmišljavanje i pružanje osposobljavanja u području kibersigurnosti** u cilju razvoja najtraženijih vještina te kako bi *start-up* poduzećima, MSP-ovima i javnim upravama mogla ponuditi osposobljavanja na radnom mjestu i pripravništva u

njemu je svako zanimanje povezano s kibersigurnošću sažeto u profil u kojem se detaljno analiziraju pripadajuće obveze, vještine, sinergije i međuovisnosti.

[53] U vezi s tim vidjeti Korisnički priručnik – Europski okvir za vještine u području kibersigurnosti (ECSF) – rujan 2022.

[54] Europski okvir e-kompetencija (e-CF) | ESCO (europa.eu). U e-CF-u se navode dosljedne poveznice u kontekstu kvalifikacija u području IKT-a i drugih okvira relevantnih za sektor, uključujući DigComp.

[55] Vidjeti, na primjer, Skills-OVATE, koji je razvio CEDEFOP.

[56] Agencija će dodatno iskoristiti rezultate drugih projekata koji se financiraju sredstvima EU-a (npr. REWIRE, Prostor za podatke o vještinama (DS4S), CyberSecPro, Concordia) i metodologije proizišle iz sličnih inicijativa (npr. *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States* (Stvaranje kvalificirane radne snage u području kibersigurnosti u pet zemalja: iskustva iz Australije, Kanade, Novog Zelanda, Ujedinjene Kraljevine i Sjedinjenih Američkih Država), izvješće OECD-a, objavljeno 21. ožujka 2023.) kako bi se u budućnosti mogao dobiti uvid u stvarno stanje potreba u okruženju u kojem se potražnja neprestano mijenja.

[57] CEPOL-ova procjena potreba za operativnu obuku (OTNA).

[58] U vezi s tim vidjeti Zajedničku komunikaciju Europskom parlamentu i Vijeću, Politika kiberobrane EU-a, JOIN(2022) 49 final.

[59] U vezi s tim u obzir će se uzeti rad na okviru kompetencija za osposobljavanje u području borbe protiv kiberkriminaliteta (TCF), koji je trenutačno u izradi.

[60] Kao što su europska klasifikacija vještina, kompetencija, kvalifikacija i zanimanja (ESCO), Europass i Europska mreža službi za zapošljavanje (EURES).

inovativnim poduzećima koja se bave kibersigurnošću i stručnim centrima u području kibersigurnosti. Kako bi postao primjer dobre prakse za sve programe osposobljavanja u području kibersigurnosti, EDIC bi u osmišljavanju programa osposobljavanja trebao surađivati sa svim relevantnim dionicima, uključujući industriju, te temeljiti svoj rad na projektima kao što je **CyberSecPro**[61], koji se financira iz programa Digitalna Europa i okuplja 17 visokih učilišta i 13 zaštitarskih društava iz 16 država članica.

Akademija će surađivati sa svim relevantnim dionicima kako bi **potaknula mlađe generacije** da se odluče na karijeru u području kibersigurnosti. Države članice bi, u skladu s prijedlogom Preporuke Vijeća o poboljšanju prenošenja digitalnih vještina u obrazovanju i osposobljavanju, trebale uspostaviti i podupirati mjere za zapošljavanje i osposobljavanje kvalificiranih nastavnika i voditelja osposobljavanja te olakšavati stjecanje kibersigurnosnih vještina, među ostalim putem naukovanja. Trebalo bi poticati sljedeće: uključivanje kibersigurnosti u obrazovne programe i programe osposobljavanja i jamčenje njihove pristupačnosti, razvoj ponude **naukovanja** i pripravništva, promicanje inovativnih pristupa, kao što su ozbiljne igre i zajedničke platforme za simulaciju, organiziranje tjedana za stjecanje iskustva na radnim mjestima u području kibersigurnosti i objašnjavanje profila netehničkih zanimanja. Također bi trebalo podupirati da u tim mogućnostima za učenje sudjeluju skupine do kojih je teško doprijeti, kao što su mladi s invaliditetom, osobe koje žive u udaljenim ili ruralnim područjima ili pripadnici manjina.

Komisija će nastaviti podupirati razvoj programa mikrokvalifikacija, strukovnog obrazovanja i osposobljavanja. Konkretnije, **zajednički preddiplomski i diplomski programi, zajednički kolegiji ili moduli za ostvarivanje mikrokvalifikacija** te **kombinirani intenzivni programi**[62] u svim područjima, uključujući **kibersigurnost**, i dalje će se financirati u okviru programa Erasmus+. Podupirat će se i daljnja provedba **inicijative Europska sveučilišta**[63] te uspostava **centara strukovne izvrsnosti**[64] kako bi se potaknula bolja suradnja među visokim učilištima i relevantnim ustanovama za strukovno obrazovanje i osposobljavanje u cijeloj Europi. Tom će se cilju pojačane suradnje doprinijeti iz EU-ovih programa financiranja, među ostalim iz programa Erasmus+ i Digitalna Europa, te sredstvima EU-a za razvoj **individualnih računa za učenje**[65].

Kako bi se olakšala suradnja akademske zajednice, pružatelja osposobljavanja u području kibersigurnosti i poslodavaca u privatnom i javnom sektoru na nacionalnoj razini te kako bi se potaknula sinergija između javnog i privatnog sektora, nacionalni koordinacijski centri pozivaju se da istraže mogućnost osnivanja **kiberkampusa** u državama članicama. Oni bi imali za cilj stvoriti nacionalne centre izvrsnosti za kibersigurnosnu zajednicu, a Akademija bi pomogla u njihovu povezivanju i daljnjoj koordinaciji njihovih aktivnosti.

ENISA će također poboljšati svoju ponudu programa osposobljavanja u području kibersigurnosti te će uskladiti svoj **katalog kolegija**[66] s profilima zanimanja iz ECSF-a i razraditi module osposobljavanja za svaki profil, što bi moglo poboljšati ponudu programa

[61] U okviru projekta CyberSecPro će se, na primjer, analizirati programi, kolegiji i ljetne škole u području kibersigurnosti u ponudi na sveučilištima te tablice ocjenjivanja iz Europskog sustava prijenosa i prikupljanja bodova (ECTS); usto će se osigurati sudjelovanje ciljnog broja pripravnika (više od 530) u trogodišnjem razdoblju te provesti osposobljavanje vanjskih suradnika iz raznih industrija i sektora.

[62] Kombinirani intenzivni programi objedinjuju učenje putem interneta i kratko razdoblje fizičke mobilnosti.

[63] Inicijativa Europska sveučilišta | Europski prostor obrazovanja (europa.eu).

[64] Centri strukovne izvrsnosti | Erasmus+ (europa.eu).

[65] U skladu s Preporukom Vijeća od 16. lipnja 2022. o individualnim računima za učenje.

[66] Tečajevi osposobljavanja – ENISA (europa.eu).

osposobljavanja u državama članicama. Usto, proširit će svoj **program „osposobljavanja voditelja osposobljavanja"**[67] kako bi se odgovorilo na profesionalne potrebe institucija, tijela i agencija Unije, javnih tijela država članica te **javnih i privatnih operatora ključnih usluga** u okviru Direktive NIS 2.

Nadalje, druge će agencije i tijela EU-a poboljšati svoju ponudu programa osposobljavanja u području kibersigurnosti. Na primjer, **ESDC** će pri provedbi politike kiberobrane EU-a osmisliti novi skup tečajeva o kibersigurnosti i uskladiti neke od postojećih tečajeva s ECSF-om. Po završetku tih tečajeva izdavat će se certifikat o ishodima učenja[68]. ESDC će u suradnji s Komisijom istražiti mogućnost dodavanja certifikata u lisnicu EU-a za elektroničku identifikaciju. Dodatno će istražiti potencijalne mehanizme ocjenjivanja vještina za koje će se moći dobiti certifikati. Slično tome, u području borbe protiv kiberkriminaliteta nastojat će se uspostaviti bliske veze s **CEPOL-ovom akademijom za kiberkriminalitet**[69] kako bi se potaknule sinergija i komplementarnost u osmišljavanju i provedbi kurikuluma za osposobljavanje.

4.3. Stvaranje sinergija i povećanje vidljivosti programa osposobljavanja i certifikacija u državama članicama

Akademija bi trebala raditi na pitanju vidljivosti i sinergija programa osposobljavanja i certifikacija. To bi donijelo koristi civilnoj, obrambenoj, kaznenoj i diplomatskoj zajednici za kibersigurnost jer su u mnogim slučajevima u svim sektorima potrebne iste vještine, koje se temelje na sličnim kurikulima i ishodima učenja.

Akademija bi služila kao **jedinstvena pristupna točka** za osobe koje su zainteresirane za karijeru u području kibersigurnosti. U kratkom će se roku to ostvariti nadogradnjom Komisijine **platforme za digitalne vještine i radna mjesta** uz potporu projekta ECCO. U posebnom odjeljku o karijerama u području kibersigurnosti postojeći će se alati, koji sežu od programa visokog obrazovanja do mogućnosti osposobljavanja, među kojima su i tečajevi za stjecanje mikrokvalifikacija te programi strukovnog obrazovanja i osposobljavanja, povezivati s ponudama radnih mjesta. U tu će se svrhu na platformi navoditi ili u nju integrirati trenutačne aktivnosti i inicijative, kao što je rad ENISA-e, koja je u suradnji s akademskom zajednicom izradila **pregled obrazovnih institucija** koje nude programe u području kibersigurnosti. Dodatna poboljšanja postići će se uz potporu nacionalnih koordinacijskih centara. Usto, ENISA će uz potporu nacionalnih koordinacijskih centara, Komisije i projekta ECCO razviti i konsolidirati dva **repozitorija postojećih programa osposobljavanja u javnom i privatnom sektoru te kibersigurnosnih certifikacija**, a u suradnji sa subjektima koji izdaju certifikacije uključit će i druge relevantne inicijative[70]. Ti će repozitoriji biti dostupni i putem jedinstvene pristupne točke na platformi za digitalne vještine i radna mjesta. Koristi od toga imat će i nacionalni koordinacijski centri, čija je zadaća promicanje i širenje obrazovnih programa u području kibersigurnosti[71].

---

[67] Program osposobljavanja voditelja osposobljavanja – ENISA (europa.eu).

[68] U skladu s člankom 20. stavkom 4. Odluke Vijeća (ZVSP) 2020/1515 od 19. listopada 2020. o osnivanju Europske akademije za sigurnost i obranu te o stavljanju izvan snage Odluke (ZVSP) 2016/2382.

[69] CEPOL-ova akademija za kiberkriminalitet osnovana je 2019. kao najsuvremenija platforma za poboljšanje znanja o kiberkriminalitetu i povećanje kiberkapaciteta u Europi.

[70] Na primjer, Akademija W4C – Women4Cyber ili projekt Globalnog certificiranja za borbu protiv kiberkriminaliteta za tijela za izvršavanje zakonodavstva i pravosudna tijela.

[71] „1. Nacionalni koordinacijski centri imaju sljedeće zadaće: [...] (g) ne dovodeći u pitanje nadležnosti država članica za obrazovanje i uzimajući u obzir relevantne zadaće ENISA-e, surađuju s nacionalnim tijelima u vezi s mogućim doprinosima

Potrebno je i stručnjacima pružiti jamstvo da su programi osposobljavanja koje pohađaju odgovarajuće kvalitete. Stoga će ENISA pokrenuti **pilot-projekt** za istraživanje mogućnosti uspostave europskog programa za certifikaciju vještina u području kibersigurnosti.

Nadalje, utvrđivanje vještina i programa osposobljavanja te njihovo povezivanje s profilom zanimanja iznimno je važno, no važno je i osigurati da se kibersigurnosne usluge pružaju uz nužne kompetencije, vještine i iskustvo. To se posebno odnosi na pružatelje upravljanih sigurnosnih usluga u područjima kao što su odgovor na incidente, penetracijska testiranja, revizije sigurnosti i savjetovanje. U Direktivi NIS 2 i prijedlogu Akta o kibersolidarnosti za pružatelje upravljanih sigurnosnih usluga utvrđene su specifične zadaće. Komisija stoga predlaže i **ciljanu izmjenu Akta o kibersigurnosti**[72] kako bi na razini Unije bili dostupni programi certifikacije za pružatelje upravljanih sigurnosnih usluga. Ti bi programi certifikacije trebali biti imati za cilj da, među ostalim, predmetne usluge pružaju zaposlenici s vrlo visokom razinom tehničkog znanja i kompetencija u relevantnim područjima.

Osiguranje kvalitete i mehanizmi priznavanja mikrokvalifikacija[73] doprinose transparentnosti, usporedivosti i prenosivosti ishoda učenja. Države članice potiču se da u skladu s Preporukom Vijeća o europskom pristupu mikrokvalifikacijama[74] uključe mikrokvalifikacije u području kibersigurnosti u svoje nacionalne kvalifikacijske okvire. To bi im omogućilo da te mikrokvalifikacije povežu s Europskim kvalifikacijskim okvirom[75]. Za izdavanje kibersigurnosnih kvalifikacija i mikrokvalifikacija s digitalnim potpisom pojedincima dostupna je infrastruktura europskih digitalnih vjerodajnica za učenje. Te kvalifikacije sadržavaju opširne podatke, među ostalim o ishodima učenja u području kibersigurnosti, i mogu se pohraniti u buduću **lisnicu EU-a za elektroničku identifikaciju**[76].

Mjere u okviru Akademije

Države članice i industrija

- Pružanje potpore za osmišljavanje i priznavanje kibersigurnosnih **mikrokvalifikacija** u skladu s Preporukom Vijeća o europskom pristupu mikrokvalifikacijama.
- Uvrštavanje kibersigurnosnih kvalifikacija i mikrokvalifikacija u **nacionalne kvalifikacije okvire.**
- Pružanje **mogućnosti osposobljavanja na radnom mjestu** u obliku naukovanja za osobe koje sudjeluju u inicijativama za razvoj kibersigurnosnih vještina.

Komisija

- U kratkom roku, uspostava **jedinstvene pristupne točke** za kibersigurnosne programe, postojeća osposobljavanja i kibersigurnosne certifikacije putem **platforme za digitalne vještine i radna mjesta** do kraja 2023.

promicanju i širenju obrazovnih programa u području kibersigurnosti", članak 7. stavak 1. točka (g) Uredbe o ECCC-u. Vidjeti i povezanu uvodnu izjavu 28.

[72] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti).

[73] Na primjer, potvrda ili certifikat o ishodima učenja stečeni nakon kratkog osposobljavanja.

[74] Preporuka Vijeća o europskom pristupu mikrokvalifikacijama za cjeloživotno učenje i zapošljivost.

[75] Preporuka Vijeća od 22. svibnja 2017. o Europskome kvalifikacijskom okviru za cjeloživotno učenje i o stavljanju izvan snage Preporuke Europskog parlamenta i Vijeća od 23. travnja 2008. o uspostavi Europskoga kvalifikacijskog okvira za cjeloživotno učenje.

[76] Prijedlog uredbe Europskog parlamenta i Vijeća o izmjeni Uredbe (EU) br. 910/2014 u pogledu uspostavljanja europskog okvira za digitalni identitet.

- Prijedlog izmjene **Akta o kibersigurnosti** 18. travnja 2023. kako bi se omogućila certifikacija pružatelja upravljanih sigurnosnih usluga.

Tijela i agencije EU-a

- Uspostava **ECSF-a** kao zajedničkog pristupa profilima zanimanja u području kibersigurnosti i povezanim vještinama do kraja 2023.
- ENISA će u drugom tromjesečju 2023. pokrenuti pilot-projekt za uspostavu **europskog programa za certifikaciju** kibersigurnosnih vještina.
- ENISA će do kraja 2023. preispitati svoj **katalog kolegija**, a **program „osposobljavanja voditelja osposobljavanja"** otvorit će za javne i privatne ključne subjekte.
- Dovršetak **usklađivanja kurikuluma ESDC-a s ECSF-om** do sredine 2023.

5. Sudjelovanje dionika: obveza unapređivanja kibersigurnosnih vještina

U odgovoru na nedostatak kibersigurnosnih vještina u okviru Akademije razvit će se koordinirani pristup sudjelovanju dionika. Cilj će biti povećati vidljivost i učinak obveza koje razni dionici preuzimaju kako bi se ublažio nedostatak stručnih kadrova u području kibersigurnosti.

Komisija poziva dionike da preuzmu konkretne obveze u smislu usavršavanja i prekvalifikacije radnika putem posebnih mjera, koje će se u najvećoj mogućoj mjeri temeljiti na utvrđenom nedostatku kibersigurnosnih vještina. **Obveze koje dionici preuzmu u pogledu kibersigurnosti** trebale bi se objavljivati na **platformi za digitalne vještine i radna mjesta**, kao i druge digitalne obveze koje su ondje već prikazane. Komisija dodatno potiče dionike koji na platformi preuzmu obveze u pogledu kibersigurnosti da se pridruže **velikom digitalnom partnerstvu u okviru Pakta za vještine**[77]. Potiče se da se obveze u pogledu kibersigurnosti preuzete u okviru velikog digitalnog partnerstva objave na platformi za digitalne vještine i radna mjesta. Isto tako, potiče se da se o obvezama preuzetima na platformi za digitalne vještine i radna mjesta izvješćuje u okviru velikog digitalnog partnerstva u okviru Pakta za vještine.

Usto, Komisija poziva države članice da **nastoje ispuniti obveze preuzete u pogledu „žena u digitalnom dobu"**[78] kako bi potaknule žene da preuzmu aktivnu i istaknutu ulogu u sektoru digitalne tehnologije te kako bi se ostvarila rodna konvergencija radnih mjesta u sektoru kibersigurnosti. Komisija potiče države članice i da razviju sinergije sa svojim programima u okviru **Europskog socijalnog fonda plus** (ESF+) kako bi dodatno podržale cilj rodne ravnopravnosti na tržištu rada[79], na primjer, osnivanjem **mentorskih programa za djevojčice i žene.** Tim programima može se potaknuti stvaranje uzora kako bi kibersigurnosna struka postala privlačnija djevojčicama i kako bi se istovremeno eliminirali rodni stereotipi. Na taj se način također potiču usavršavanje i prekvalifikacija žena te se pridonosi razvoju zajednice koja može poduprijeti žene pri ulasku na tržište rada u području kibersigurnosti ili u njihovu promaknuću na tom tržištu.

[77] Pokrenuta nova europska partnerstva radi ostvarenja ambicija EU-a za digitalno desetljeće | Izgradnja digitalne budućnosti Europe (europa.eu); to partnerstvo je uspostavljeno u okviru Pakta za vještine u odgovoru na nedostatke u području informacijske i komunikacijske tehnologije (IKT).

[78] Države članice EU-a obvezuju se na povećanje sudjelovanja žena u digitalnom sektoru | Izgradnja digitalne budućnosti Europe (europa.eu).

[79] Uredba (EU) 2021/1057 Europskog parlamenta i Vijeća od 24. lipnja 2021. o uspostavi Europskog socijalnog fonda plus (ESF+) i stavljanju izvan snage Uredbe (EU) br. 1296/2013, članak 4. stavak 1. točka (c).

Države članice bi u okviru **svojih nacionalnih strategija za kibersigurnost trebale donijeti posebne mjere kako bi ublažile nedostatak kibersigurnosnih vještina**[80], utvrdile mjere za njihovo unapređenje i učinkovitije ih provodile te se u konačnici pobrinule za odgovarajuću provedbu vlastitih obveza iz Direktive NIS 2.

Neke države članice iskorištavaju **sinergije među civilnim, obrambenim i kaznenim** inicijativama. Primjerice, da bi povećale radnu snagu, na radna mjesta u oružanim snagama povezana s kibersigurnošću zapošljavaju obveznike služenja vojnog roka ili pak pripadnike pričuvnog sastava, tj. građane s vojnom obukom[81], pa ti građani, osobito mladi, imaju priliku unaprijediti svoje kibersigurnosne i kiberobrambene vještine. To vrijedi i za područje **borbe protiv kiberkriminaliteta** jer postoje mnoge sličnosti između općih kibersigurnosnih zadaća i aktivnosti izvršavanja zakonodavstva u odgovoru na kiberincidente. Komisija potiče države članice da međusobno raspravljaju o tim inicijativama i poziva ih da procijene kako kvalificirana radna snaga može najbolje doprinijeti zajednicama za vojnu i civilnu kibersigurnost.

Komisija će razmotriti prijedloge o tome kako nadoknaditi trenutačne i očekivane nedostatke koji su utvrđeni preispitivanjem potreba institucija, tijela i agencija Unije. Posebno će poticati zaposlenike da iskoriste nadolazeću **zajedničku stipendiju EU-a i Sjedinjenih Američkih Država za kibersigurnost**, koja je uspostavljena u okviru dijaloga EU-a i SAD-a.

Mjere u okviru Akademije

Industrija

- Predlaganje **preuzimanja konkretnih obveza** na platformi za digitalne vještine i radna mjesta od 18. travnja 2023.

Države članice

- Uvrštavanje posebnih mjera za razvoj nedostatnih kibersigurnosnih vještina u **nacionalne strategije za kibersigurnost**.

Države članice i industrija

- Ispunjavanje obveza u pogledu „žena u digitalnom dobu” i postizanje **rodne konvergencije radnih mjesta u sektoru kibersigurnosti** do 2030.

6. Financiranje: stvaranje sinergija radi povećanja učinka financijskih sredstava za razvoj kibersigurnosnih vještina

Učinak ulaganja u kibersigurnosne vještine u okviru Akademije povećat će se uspostavom zajedničke pristupne točke, olakšavanjem prilagodbe financijskih ulaganja potrebama tržišta i konsolidacijom njihova korištenja te omogućivanjem sinergija među instrumentima i izbjegavanjem udvostručivanja napora[82].

6.1. Povezivanje sredstava i potreba

[80] Direktiva NIS 2, članak 7. stavak 2. točka (f).

[81] Izvješće – kibersigurnosna vojna služba: iskustvo i najbolji primjeri iz prakse iz odabranih zemalja, Martin Hurt i Tiia Sõmer, Međunarodni centar za obranu i sigurnost (ICDS), veljača 2021.

[82] Mogućnosti financiranja (europa.eu). Pomoćne usluge Pakta za vještine uključuju jedinstvenu pristupnu točku za informacije o financiranju vještina, među ostalim za Digitalni ekosustav. Ondje su dostupne opće informacije o instrumentima financiranja koji nisu posebno usmjereni na kibersigurnosne vještine, no Akademija bi trebala voditi računa o njima kako bi se izbjeglo udvostručivanje.

ECCC će u okviru Akademije i uz potporu Komisije, projekta ECCO i nacionalnih koordinacijskih centara prikupiti **informacije o iskorištavanju sredstava EU-a za financiranje kibersigurnosnih vještina** te će procijeniti kako ta sredstva doprinose ublažavanju nedostatka kibersigurnosnih vještina. Na temelju tih zbirnih informacija nastojat će bolje usmjeriti sredstva EU-a prema utvrđenim potrebama. Financirat će mjere za ublažavanje gorućih nedostataka stručnih kibersigurnosnih kadrova, među ostalim onih povezanih s provedbom politike kibersigurnosti.

6.2. Postizanje vidljivosti dostupnih sredstava i partnerske inicijative za kibersigurnosne vještine

Platforma za digitalne vještine i radna mjesta kratkoročno će postati jedinstvena pristupna točka za dionike na kojoj će biti dostupne sve informacije o mogućnostima financiranja kibersigurnosnih vještina.

Unija ulaže u ljude i njihove vještine te uspostavlja partnerstva, posebice s industrijom, kako bi potaknula usavršavanje i prekvalifikaciju putem nekoliko instrumenata utvrđenih u **Programu vještina za Europu**[83], konkretnije **Pakta za vještine**[84] i **Akcijskog plana za digitalno obrazovanje**[85]. Iz **programa Digitalna Europa** financiraju se mogućnosti za stjecanje kibersigurnosnih vještina, osobito putem višedržavnih inicijativa, čime se jasno dopunjuje potpora Obzora Europa za istraživanja i inovativna tehnološka rješenja u području kibersigurnosti. Iz **Europskog fonda za obranu**[86] financiraju se istraživanje i razvoj tehnologija za provedbu djelotvornih kiberoperacija, uključujući obuke i vježbe[87]. Te inicijative nastavit će se podupirati u okviru programa **Erasmus+**, među ostalim putem kombiniranih intenzivnih programa i projekata suradnje.

Države članice potiču se da iskoriste financijska sredstva EU-a kojima izravno upravljaju kako bi poduprle vještine i radna mjesta u području kibersigurnosti. Fondovi kohezijske politike, kao što su **Europski fond za regionalni razvoj (ERDF)** i **ESF+**, imaju velik potencijal za sinergije[88]. Područje primjene mjera u okviru **Mehanizma za oporavak i otpornost** (RRF)[89] i **programa InvestEU**[90] ostavlja prostora za dodatne važne komplementarnosti u ostvarenju ciljeva Akademije.

Mjere u okviru Akademije

Europski stručni centar u području kibersigurnosti i ENISA

[83] Program vještina za Europu – Zapošljavanje, socijalna pitanja i uključenost – Europska komisija (europa.eu).

[84] Instrumenti EU-a za financiranje usavršavanja i prekvalificiranja – Zapošljavanje, socijalna pitanja i uključenost – Europska komisija (europa.eu).

[85] Akcijski plan za digitalno obrazovanje 2021.–2027.

[86] Uredba (EU) 2021/697 Europskog parlamenta i Vijeća od 29. travnja 2021. o uspostavi Europskog fonda za obranu i stavljanju izvan snage Uredbe (EU) 2018/1092.

[87] Države članice obvezne su sudjelovati u zajedničkim obukama i vježbama, na primjer, pokretanjem projekata za kibersigurnosnu obuku i vježbe u okviru stalne strukturirane suradnje (PESCO) i sudjelovanjem u njima, a među njima su, primjerice, Kiberakademija i inovacijski centar EU-a (EU CAIH) i savezni kiberpoligoni.

[88] Uredba (EU) 2021/1058, članak 3. stavak 1. i Uredba (EU) 2021/1057, članak 4. stavak 1. točka (g).

[89] Na primjer, estonskim planom za oporavak i otpornost predviđeno je ulaganje (10 milijuna EUR) u digitalne vještine koje će uključivati reviziju osposobljavanja za stručnjake za IKT, financiranje usavršavanja i prekvalifikacije stručnjaka za IKT u stručnjake za kibersigurnost te razvoj pilot-programa za ponovno osmišljavanje kvalifikacijskog okvira stručnjaka za IKT.

[90] Dionici (npr. pružatelji osposobljavanja i poduzeća koja žele osmisliti ili unaprijediti aktivnosti osposobljavanja u području kibersigurnosti) mogu se javiti savjetodavnom centru InvestEU, koji pruža tehničku potporu i pomoć, među ostalim izgradnjom kapaciteta za nositelje projekata i subjekte, te potražiti informacije na portalu InvestEU.

- **Izrada pregleda** postojećih financijskih sredstava EU-a za kibersigurnosne vještine u odnosu na potrebe tržišta, procjena **djelotvornosti** i utvrđivanje **prioriteta** za financiranje do kraja 2024.

Komisija

- Uspostava **jedinstvene pristupne točke** za mogućnosti financiranja kibersigurnosnih vještina na platformi za digitalne vještine i radna mjesta do kraja 2023.

7. Mjerenje napretka: sustavna odgovornost

U okviru Akademije osmislit će se **metodologija** za **mjerenje napretka u rješavanju problema nedostatnih kibersigurnosnih vještina**.

7.1. Definiranje kibersigurnosnih pokazatelja radi praćenja kretanja na tržištu rada u području kibersigurnosti

Indeks gospodarske i društvene digitalizacije (DESI) sažima pokazatelje digitalne uspješnosti Europe i prati napredak država članica EU-a. ENISA će u okviru Akademije za vještine u području kibersigurnosti i u suradnji s Komisijom i Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava[91] osmisliti **pokazatelje**, među ostalim one koji se odnose na rod, za praćenje napretka država članica EU-a u povećanju broja stručnjaka za kibersigurnost, pri čemu će se također savjetovati s relevantnim sudionicima na tržištu i nacionalnim koordinacijskim centrima. Kao početnu točku upotrijebit će metodologiju DESI-ja[92] te će se pobrinuti da pokazatelji budu usklađeni s europskim digitalnim ciljevima o stručnjacima za IKT i postizanju rodne konvergencije u IKT-u. Komisija će zatim raditi na integraciji tih pokazatelja u DESI, što će omogućiti godišnje praćenje stanja u pogledu kibersigurnosnih vještina i tržišta rada.

7.2. Prikupljanje podataka i izvješćivanje

ENISA će uz potporu projekta ECCO i nacionalnih koordinacijskih centara prikupiti podatke o pokazateljima. Na temelju prikupljenih podataka izradit će **godišnje izvješće** koje će doprinijeti izvješću o stanju digitalnog desetljeća[93], a ono će pak zajedno s DESI-jem poslužiti za analizu i preporuke za pojedine zemlje u okviru **europskog semestra**[94]. Nadalje, pokazatelji kibersigurnosnih vještina doprinijet će **dvogodišnjem izvješću** ENISA-e o stanju kibersigurnosti u Uniji, koje je predviđeno Direktivom NIS 2, a obuhvaća kibersigurnosne kapacitete, informiranost o kibersigurnosti i kiberhigijenu u Uniji.

7.3. Priprema ključnih pokazatelja uspješnosti za kibersigurnost

Kako bi se riješio problem nedostatka stručnjaka za kibersigurnost u Europi, ENISA će u bliskoj suradnji s Komisijom i nacionalnim koordinacijskim centrima Komisiji predložiti ključne pokazatelje uspješnosti koji će se temeljiti na metodologiji iz programa politike za digitalno desetljeće do 2030. i iskustvu industrije. U obzir će uzeti ključne pokazatelje

[91] Na temelju metodologije koju će ENISA osmisliti u svrhu dvogodišnjeg izvješća o stanju kibersigurnosti u Uniji i kao dopuna toj metodologiji, u skladu s člankom 18. stavkom 3. Direktive NIS 2.

[92] Vidjeti Metodološku napomenu Indeksa gospodarske i društvene digitalizacije (DESI) 2022., dostupnu na: Indeks gospodarske i društvene digitalizacije (DESI) | Izgradnja digitalne budućnosti Europe (europa.eu).

[93] Odluka (EU) 2022/2481 Europskog parlamenta i Vijeća od 14. prosinca 2022. o uspostavi programa politike za digitalno desetljeće do 2030.

[94] Isto, uvodna izjava 25.

uspješnosti koje države članice upotrebljavaju za procjenu nacionalnih strategija za kibersigurnost[95].

Mjere u okviru Akademije

ENISA

- Priprema **pokazatelja i ključnih pokazatelja uspješnosti** za kibersigurnosne vještine do kraja 2023.
- **Prikupljanje podataka** o pokazateljima i izvješćivanje o njima, uz prvo prikupljanje do 2025.

Komisija

- Rad na uključivanju **pokazatelja kibersigurnosti u DESI** i **izvješće o stanju digitalnog desetljeća**.

8. Zaključak

U ovoj se Komunikaciji utvrđuju temelji za promjenu načina na koji Unija pristupa poboljšanju kibersigurnosnih vještina svojih stručnjaka. Cilj je smanjiti nedostatak tih vještina i Uniji osigurati potrebnu radnu snagu kako bi se mogla nositi s prijetnjama koje se neprekidno mijenjaju, provoditi politike čiji je cilj zaštita Unije od kibernapada te povećati poslovne prilike i konkurentnost. Kvalificirana kibersigurnosna radna snaga može donijeti koristi **civilnoj, obrambenoj, kaznenoj i diplomatskoj** zajednici te doprinosi sinergiji među njima.

Komisija poziva države članice i sve dionike da sudjeluju u ostvarenju ambicioznog cilja uspostave Akademije za vještine u području kibersigurnosti.

[95] Direktiva NIS 2, članak 7. stavak 4.