EVROPSKA
KOMISIJA

Strasbourg, 18.4.2023
COM(2023) 207 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Zapolnitev vrzeli na področju strokovnjakov za kibernetsko varnost za povečanje konkurenčnosti, rasti in odpornosti EU („akademija za kibernetske veščine“)

Zapolnitev vrzeli na področju strokovnjakov za kibernetsko varnost za povečanje konkurenčnosti, rasti in odpornosti EU
(„akademija za kibernetske veščine“)

1. Nujna potreba po zmanjšanju tveganj z odpravljanjem pomanjkanja kibernetskovarnostnih veščin in zapolnitvijo vrzeli v njih

Kibernetska varnost ni le del varnosti državljanov, podjetij in držav članic. Potrebna je tudi za zagotavljanje politične stabilnosti EU in stabilnosti njenih demokracij ter za blaginjo naše družbe in podjetij. **Krajina kibernetskih groženj** se je v zadnjih letih močno spremenila, pri čemer je zaskrbljujoč porast kibernetskih napadov, usmerjenih v vojaško in civilno kritično infrastrukturo v EU. Akterji groženj povečujejo svoje zmogljivosti, pojavljajo pa se nove in hibridne grožnje, kot je uporaba botov in tehnik, ki temeljijo na umetni inteligenci[1]. Zlasti akterji groženj, ki uporabljajo izsiljevalsko programje, subjektom stalno povzročajo znatno gospodarsko škodo in škodujejo njihovemu ugledu[2].

Tarča v velikem številu kibernetskovarnostnih incidentov so bile tudi javne uprave in vlade držav članic ter evropske institucije, organi, uradi in agencije[3]. Prav tako sta pogosti tarči[4] tudi finančni[5] in zdravstveni[6] sektor, na katerih temeljita družba in gospodarstvo. Zaradi geopolitičnih napetosti, povezanih z rusko vojno agresijo proti Ukrajini, se je povečala kibernetska grožnja[7], te napetosti pa lahko privedejo do destabilizacije naše družbe. **Varnosti** v EU ni mogoče zagotoviti brez **največjega bogastva EU**: **njenih državljanov.** EU nujno potrebuje strokovnjake z znanji, spretnostmi in kompetencami za preprečevanje, odkrivanje in odvračanje kibernetskih napadov ter za obrambo EU in njenih najbolj kritičnih infrastruktur pred njimi ter za zagotavljanje **odpornosti** EU.

Vrzel na področju strokovnjakov za kibernetsko varnost dodatno ovira **konkurenčnost** in **rast** Evrope, ki sta močno odvisni od razvoja in uporabe strateških digitalnih tehnologij (npr. umetna inteligenca, 5G in računalništvo v oblaku). Potrebna je usposobljena delovna sila na področju kibernetske varnosti, da bi lahko EU še naprej zagotavljala ključne napredne tehnologije v globalnem okolju.

---

[1] ENISA Threat Landscape 2022 (Poročilo agencije ENISA o krajini groženj iz leta 2022) – ENISA (europa.eu).

[2] Europol, Internet Organised Crime Threat Assessment (Ocena ogroženosti zaradi internetnega organiziranega kriminala) (IOCTA) 2021. Taki akterji se opirajo na model izsiljevalskega programja kot storitve. Letni stroški podjetij so v letu 2022 presegli 18,4 milijarde EUR (Cybereason 2022 Report on the true cost or Ransomware) (poročilo podjetja Cybereason iz leta 2022 o dejanskih stroških zaradi izsiljevalskega programja).

[3] Glej na primer skupno publikacijo agencije ENISA in skupine CERT-EU, JP-23–01 – Sustained activity by specific threat actors (Trajna dejavnost določenih akterjev groženj), TLP:CLEAR, 15. februar 2023.

[4] ENISA Threat Landscape 2022 (Poročilo agencije ENISA o krajini groženj iz leta 2022).

[5] V Nemčiji je bilo na primer 90 % goljufij z elektronsko pošto, prijavljenih v obdobju od 1. junija 2021 do 31. maja 2022, izvedenih v obliki ribarjenja za pridobitev finančnih informacij ali napada na družbo v finančnem sektorju, pri čemer je bilo vključenih več kot 20 000 okuženih naprav iz 125 držav; glej The State of IT Security in Germany in 2022 (Stanje varnosti IT v Nemčiji v letu 2022), Bundesamt für Sicherheit in der Informationstechnik (BSI), 1. januar 2023.

[6] V Franciji so bili na primer napadi z izsiljevalskim programjem izvedeni na javne zdravstvene ustanove, kot je Centre Hospitalier Sud Francilien, med katerimi je bilo ogroženih 11 GB osebnih in zdravstvenih podatkov ter podatkov o osebju, ki jih je objavil akter groženj; glej Panorama de la Cybermenace 2022 (Pregled kibernetskih groženj v letu 2022), Agence nationale de la sécurité des systèmes d'information (ANSSI), januar 2023.

[7] Glej tudi: CERT-EU – Russia's war on Ukraine:one year of cyber operations (CERT-EU – Ruska vojna v Ukrajini: eno leto kibernetskih operacij) (europa.eu); Ruske kibernetske operacije proti Ukrajini:izjava visokega predstavnika v imenu Evropske unije, 10. maj 2022; Izjava visokega predstavnika v imenu Evropske unije o zlonamernih kibernetskih dejavnostih, ki jih izvajajo hekerji in hekerske skupine v kontekstu ruske agresije v Ukrajini, 19. julij 2022.

V okviru politike EU na področju kibernetske varnosti je bil v zadnjih letih dosežen znaten napredek pri pripravi na to spreminjajočo se krajino groženj in soočanju z njo ter pri spodbujanju konkurenčnosti EU, kar je privedlo do sprejetja številnih pobud, kot so strategija EU za kibernetsko varnost v digitalnem desetletju[8], revidirana direktiva o varnosti omrežij in informacijskih sistemov (direktiva NIS 2)[9], sektorska zakonodaja EU o kibernetski varnosti[10], politika EU za kibernetsko obrambo[11], akt o kibernetski odpornosti[12] in akt o kibernetski solidarnosti, ki ga Komisija predlaga skupaj s tem sporočilom. Vendar cilji iz teh zakonodajnih aktov ne bodo doseženi brez usposobljenih ljudi, potrebnih za njihovo izvajanje. Medtem ko se osnovno znanje splošnega prebivalstva o kibernetski varnosti obravnava v okviru pobud, s katerimi se podpira razvoj splošnih znanj in spretnosti, potrebnih za sodelovanje v družbi[13], je usposobljena delovna sila v javnem in zasebnem sektorju na nacionalni ravni in ravni EU, tudi v organizacijah za standardizacijo, bistvenega pomena za **izpolnitev navedenih pravnih in političnih zahtev na področju kibernetske varnosti**.

Varnost in konkurenčnost EU sta zato odvisni od strokovne usposobljene delovne sile na področju kibernetske varnosti. Vendar pa se EU sooča z zelo velikim pomanjkanjem usposobljenih strokovnjakov za kibernetsko varnost, zaradi česar so EU, njene države članice ter podjetja in državljani izpostavljeni tveganju kibernetskovarnostnih incidentov. Leta 2022 je v Evropski uniji primanjkovalo **med 260 000**[14] **in 500 000**[15] strokovnjakov za kibernetsko varnost, medtem ko so bile potrebe EU po delovni sili na področju kibernetske varnosti ocenjene na 883 000 strokovnjakov[16], kar kaže na neusklajenost med razpoložljivimi kompetencami in kompetencami, potrebnimi na trgu dela. Na delovno silo na področju kibernetske varnosti dodatno slabo vpliva napačno prepričanje, povezano z njeno tehnično podobo, še vedno pa to področje ni privlačno za **ženske**, ki predstavljajo 20 % diplomantov na področju kibernetske varnosti[17] ter 19 % strokovnjakov za informacijsko in

[8] Skupno sporočilo Evropskemu parlamentu in Svetu, Strategija EU za kibernetsko varnost v digitalnem desetletju (JOIN(2020) 18 final).

[9] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2).

[10] Kot na primer v finančnem sektorju Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (uredba o digitalni operativni odpornosti).

[11] Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo (JOIN(2022) 49 final).

[12] Predlog uredbe Evropskega parlamenta in Sveta o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi Uredbe (EU) 2019/1020 (COM(2022) 454 final).

[13] Pomembne pobude, s katerimi se obravnavajo splošna digitalna znanja in spretnosti prebivalstva, vključujejo naslednje: akcijski načrt za evropski steber socialnih pravic in digitalni kompas (s ciljem, da 80 % odraslih do leta 2030 pridobi osnovne digitalne spretnosti in znanja), akcijski načrt za digitalno izobraževanje 2021–2027, orodje evropski okvir digitalnih kompetenc ali predlog priporočila Sveta za izboljšanje zagotavljanja digitalnih spretnosti v izobraževanju in usposabljanju.

[14] (ISC)² v Assessing Cyber Skills on the basis of the ECSF (Ocenjevanje kibernetskih veščin na podlagi evropskega okvira za kibernetskovarnostne veščine (ECSF)), spletni seminar agencije ENISA, 16. februar 2023.

[15] Po ocenah Evropske organizacije za kibernetsko varnost (ECSO), kot je navedeno v Skupnem sporočilu Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo (JOIN(2022) 49 final).

[16] (ISC)² v Assessing Cyber Skills on the basis of the ECSF (Ocenjevanje kibernetskih veščin na podlagi evropskega okvira za kibernetskovarnostne veščine (ECSF)), spletni seminar agencije ENISA, 16. februar 2023.

[17] Podatkovna zbirka o visokošolskem izobraževanju za kibernetsko varnost (CyberHEAD).

komunikacijsko tehnologijo (IKT)[18]. V evropskem **programu politike Digitalno desetletje do leta 2030**[19] je za odpravo te težave določen cilj povečanja števila strokovnjakov na področju IKT za 20 milijonov do leta 2030, pri tem pa se bo odpravila tudi razlika med deležem žensk in moških. Poleg tega izvajanje nastajajoče politike EU zahteva zadostno število ustrezno usposobljene delovne sile. Več kot 42 % višjih vodij IT v industriji finančnih storitev je na primer poudarilo, da je pomanjkanje kibernetskovarnostnih veščin in strokovnega znanja ključni izziv, s katerimi se srečuje njihovo podjetje pri kibernetskovarnostni obrambi in obvladovanju kibernetskovarnostnih incidentov[20], in to v času, ko bodo morali izvajati sektorsko zakonodajo o kibernetski varnosti, kot je uredba o digitalni operativni odpornosti (DORA).

Delodajalci omahujejo pri vlaganju v človeški kapital ter iščejo že usposobljeno in izkušeno delovno silo, kar dodatno prispeva k omejevanju trga dela[21]. To pomanjkanje vpliva na vse vrste družb, vključno z malimi in srednjimi podjetji (**MSP**), ki predstavljajo 99 % vseh podjetij v EU[22]. Z velikim izzivom se srečujejo tudi **javne uprave**, ki so velikokrat tarče kibernetskovarnostnih incidentov in na katere ti najbolj vplivajo[23].

Zato je treba nujno odpraviti vrzel na področju strokovnjakov za kibernetsko varnost v EU, saj sta ogroženi varnost in konkurenčnost EU.

2. Pomanjkanje sinergij in usklajenega ukrepanja za zapolnitev vrzeli v kibernetskovarnostnih veščinah

Na evropski in nacionalni ravni se pojavlja vse več čedalje uspešnejših pobud, ki jih izvajajo javni in zasebni subjekti, da bi odpravili pomanjkanja delovne sile na področju kibernetske varnosti. Vendar so te razpršene in doslej še niso dosegle kritične mase, ki bi privedla do resnične spremembe.

Prvič, skupno razumevanje sestave delovne sile EU na področju kibernetske varnosti ter s tem povezanih veščin je trenutno omejeno, medtem ko bi morali podobni profili delovnih mest na področju kibernetske varnosti vključevati enak nabor veščin. Ker zadevni akterji premalo uporabljajo skupni **evropski referenčni okvir za strokovnjake za kibernetsko varnost**, ni komunikacijskega orodja med delodajalci, izobraževalci in oblikovalci politik, prav tako pa ni mogoče izmeriti in oceniti vrzeli na trgu dela na področju kibernetske varnosti. To dodatno preprečuje oblikovanje učnih načrtov za izobraževanje in usposabljanje ter oblikovanje poklicnih poti, ki bi ustrezale potrebam politike in trga, za tiste, ki želijo začeti opravljati poklic. **Izpopolnjevanje in preusposabljanje** delovne sile sta v veliki meri odvisna od usposabljanj in pridobivanja certifikatov na področju kibernetske varnosti, ki jih običajno nudijo zasebni ponudniki. Vendar pa se delovna sila srečuje s težavami pri pridobivanju pregleda nad kakovostjo ponujenih usposabljanj na področju kibernetske varnosti in certifikatov, ki se izdajajo v povezavi z njimi.

---

[18] Le 19 % strokovnjakov na področju IKT v EU je žensk, glede na indeks digitalnega gospodarstva in družbe (indeks DESI) za leto 2022 | Oblikovanje digitalne prihodnosti Evrope (europa.eu). Podatki o številu ženske delovne sile Unije na področju kibernetske varnosti niso na voljo.

[19] Sklep (EU) 2022/2481 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o vzpostavitvi programa politike Digitalno desetletje do leta 2030, s katerim je vzpostavljen mehanizem spremljanja in sodelovanja za doseganje skupnih ciljev za digitalno preobrazbo Evrope, določenih v digitalnem kompasu do leta 2030, vključno s področjem znanj in spretnosti.

[20] S-RM Cyber Security Insights Report 2022 (Poročilo S-RM o uvidih na področju kibernetske varnosti za leto 2022).

[21] Cybersecurity Skills Development in the EU (Razvoj kibernetskovarnostnih veščin v EU), ENISA, december 2019.

[22] Opredelitev MSP (europa.eu).

[23] ENISA Threat Landscape 2022 (Poročilo agencije ENISA o krajini groženj iz leta 2022) – ENISA (europa.eu).

Čeprav so izobraževanje, usposabljanje ter oblikovanje poklicnih poti potrebni za izboljšanje ponudbe na trgu dela, je vloga **povpraševanja** pri usposabljanju delovne sile na trgu dela in pri prilagajanju na razvoj tega trga trenutno podcenjena. Industrija in delodajalci iz javnega sektorja nimajo na voljo skupnih forumov in mest za združevanje zamisli o tem, kako najbolje usposobiti delovno silo ter **bolje oceniti veščine**, zlasti med postopkom zaposlovanja. Najbolj iskane **trde veščine** so lahko povezane s kibernetsko varnostjo[24], kot sta razvoj programske opreme ali računalništvo v oblaku[25], vendar pa so **prečne veščine** še vedno neupravičeno prezrte. Vrste veščin, ki jih delodajalci vse bolj zahtevajo, so kritično razmišljanje, analiziranje, reševanje težav ter samoiniciativnost in samostojnost pri delu[26], ki bodo do leta 2025 postajale vse pomembnejše[27].

Obstajajo že številne javne in zasebne naložbene pobude za kibernetskovarnostne veščine, pri čemer EU obsežno **financira** projekte v okviru različnih instrumentov[28]. Ker pa v EU še vedno primanjkuje veščin, se porajajo vprašanja glede prepoznavnosti in učinka teh projektov, kar kaže na to, da se morda ne ujemajo sistematično s potrebami trga, ki jih je treba nujno opredeliti na ravni EU. Poleg tega več virov financiranja vodi k podvajanju, zaradi česar se ne izkoristijo priložnosti za širitev in doseganje dejanskega učinka. Hkrati pa tisti, ki potrebujejo naložbo, ne znajo vedno opredeliti najprimernejših virov za svoje potrebe.

Deležniki že nekaj časa poskušajo odpraviti zapleteno in večplastno težavo pomanjkanja kibernetskovarnostnih veščin. Agencija EU za kibernetsko varnost (ENISA) razvija instrumente, povezane s profili vlog ali visokošolskim izobraževanjem[29], Evropski kompetenčni center za kibernetsko varnost (ECCC)[30] obravnava kibernetskovarnostne veščine v okviru posebne delovne skupine, Evropska akademija za varnost in obrambo (EAVO) se ukvarja s kibernetskovarnostnimi veščinami civilne in vojaške delovne sile v okviru skupne varnostne in obrambne politike[31], hkrati pa si to težavo prizadevajo rešiti zasebne organizacije[32], v sektorju za certificiranje kibernetske varnosti pa se pripravljajo časovni načrt in usposabljanja za odpravo pomanjkanja veščin[33]. Države članice poskušajo to težavo obravnavati tudi z različnimi pobudami, ki segajo od regulativnih pobud[34] do ustanavljanja akademij za kibernetskovarnostne veščine[35] ali kibernetskih kampusov[36] in

[24] LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most (Najbolj iskane veščine po izboru portala LinkedIn v letu 2023: osvojite tiste, ki jih podjetja najbolj potrebujejo).

[25] Infografika združenja ISACA o stanju kibernetske varnosti v letu 2022.

[26] Kot je orodje CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

[27] The Future of Jobs Report (Poročilo o prihodnosti zaposlitev), oktober 2020, Svetovni gospodarski forum.

[28] Na primer: Zveza za kibernetskovarnostne veščine – Nova vizija za Evropo – Projekt REWIRE (financiran iz programa Erasmus+); projekti za podporo kompetenčnemu centru za kibernetsko varnost (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (financirani iz programa Obzorje 2020) in projekt Cybersecpro (financiran iz programa za digitalno Evropo).

[29] Zlasti: evropski okvir za kibernetskovarnostne veščine (ECSF); CYBERHEAD – podatkovna zbirka o visokošolskem izobraževanju za kibernetsko varnost; platforma za kibernetske vaje (CEP); evropski izziv na področju kibernetske varnosti; evropski mesec kibernetske varnosti.

[30] Uredba (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov.

[31] Zlasti prek platforme za kibernetsko izobraževanje, usposabljanje, ocenjevanje in kibernetske vaje.

[32] Na primer delovna skupina 5 za „izobraževanje, usposabljanje, ozaveščenost, kibernetsko varnost in človeške dejavnike“ Evropske organizacije za kibernetsko varnost (ECSO); organizacija DIGITALEUROPE.

[33] Na primer SANS Institute, (ISC)² in ISACA.

[34] Na primer v nacionalnih strategijah za izobraževanje ali kibernetsko varnost.

[35] Na primer C-Academy na Portugalskem.

[36] Na primer kibernetski kampus v Franciji.

centrov odličnosti za kibernetsko kriminaliteto[37], ali z javno-zasebnimi partnerstvi[38]. Vendar pri delu vseh teh deležnikov pogosto manjkajo usklajevanje in sinergije, zato še ni doseglo svojega potenciala, da bi se bistveno spremenil trg dela, kar dokazuje vse večje pomanjkanje delovne sile na področju kibernetske varnosti v EU. Potrebne so tudi večje sinergije med kibernetskimi skupnostmi, saj so za ohranjanje kibernetske varnosti, boj proti **kibernetski kriminaliteti** ali oblikovanje odzivov v okviru **kibernetske obrambe** pogosto potrebne podobne veščine.

Nazadnje, EU ima danes omejena sredstva za ocenjevanje **stanja in razvoja trga dela na področju kibernetske varnosti** ter veščin svoje delovne sile. Države članice ter institucije, organi, uradi in agencije EU se opirajo na podatke, ki jih zbirajo zasebni subjekti, ali na širši sklop podatkov, zbranih v EU, zlasti podatkov Eurostata[39] in Evropskega centra za razvoj poklicnega usposabljanja (CEDEFOP)[40] o strokovnjakih na področju IKT. Povedano drugače, EU ima delen in razdrobljen pregled nad svojimi potrebami, kar ji preprečuje, da bi utrdila skupno vizijo glede stanja trga dela na področju kibernetske varnosti.

3. Usklajen odziv na ravni EU: akademija za kibernetske veščine

3.1.Cilj

Komisija za premagovanje izziva v zvezi z obravnavanjem kibernetskovarnostnih veščin ter zapolnitvijo vrzeli na trgu dela predlaga ustanovitev **akademije za kibernetske veščine**, kot jo je napovedala predsednica Evropske komisije v svojem pismu o nameri k stanju v Uniji v letu 2022 [41, , 42] ter kot je bila napovedana v okviru evropskega leta spretnosti.

Namen akademije za kibernetske veščine (v nadaljnjem besedilu: akademija) je ustvariti **enotno vstopno točko in sinergije** za vse ponudbe izobraževanja in usposabljanja na področju kibernetske varnosti, pa tudi za priložnosti za financiranje in specifične ukrepe za podporo razvoju kibernetskovarnostnih veščin. Z akademijo se bodo okrepile pobude deležnikov, da bo dosežena kritična masa, ki bo prinesla spremembe na trgu dela, tudi na področju obrambe. Te dejavnosti bi se za večji učinek uskladile s skupnimi cilji in ključnimi kazalniki uspešnosti.

Poudarek akademije bo na usposabljanju **strokovnjakov za kibernetsko varnost**. Dejavnost akademije bo prispevala k politikam EU na področju kibernetske varnosti, pa tudi k izobraževanju in vseživljenjskemu učenju. Akademija dopolnjuje dve priporočili Sveta v zvezi z digitalnim izobraževanjem in spretnostmi, ki ju Komisija predlaga hkrati s tem sporočilom[43].

Akademija bo temeljila na štirih stebrih: (1) spodbujanju **ustvarjanja znanja z izobraževanjem in usposabljanjem**, tako da se bo oblikoval skupni okvir za profile vlog na področju kibernetske varnosti ter s tem povezane veščine, izboljšala evropska ponudba

[37] Na primer litovski center odličnosti za usposabljanje, raziskave in izobraževanje na področju kibernetske kriminalitete v Litvi (L3CE).

[38] Na primer Microsoftova pobuda za pridobivanje kibernetskovarnostnih veščin.

[39] ICT specialists in employment - Statistics Explained (Zaposleni strokovnjaki za IKT – Vodnik po statističnih podatkih) (europa.eu).

[40] Kot je orodje CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

[41] Pismo o nameri k stanju v Evropski uniji v letu 2022, naslovljeno na predsednico Roberto Metsola in predsednika vlade Petra Fialo.

[42] Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo (JOIN(2022) 49 final).

[43] Predloga za priporočila Sveta o ključnih dejavnikih, ki omogočajo uspešno digitalno izobraževanje in usposabljanje, ter o izboljšanju zagotavljanja digitalnih spretnosti v izobraževanju in usposabljanju.

izobraževanja in usposabljanja za zadovoljitev potreb, ustvarile poklicne poti ter zagotovili prepoznavnost in jasnost v zvezi z usposabljanjem in certificiranjem na področju kibernetske varnosti, da se okrepi ponudba na trgu dela; (2) zagotavljanju boljšega usmerjanja in prepoznavnosti razpoložljivih **priložnosti za financiranje** za dejavnosti, povezane z veščinami, da se čim bolj poveča njihov učinek; (3) pozivu deležnikom **k ukrepanju** ter (4) opredelitvi kazalnikov za **spremljanje razvoja trga** in razvoju zmogljivosti za ocenjevanje učinkovitosti ukrepov zadevnih deležnikov.

Delovanje akademije bo podprto s sredstvi v višini 10 milijonov EUR iz programa Digitalna Evropa[44].

3.2. Upravljanje akademije

Da bi se zagotovila infrastruktura, ki bi služila kot **enotna vstopna točka** za spodbujanje sodelovanja med znanstveno skupnostjo, ponudniki usposabljanja in industrijo, v njenem okviru pa bi se lahko srečevali in usposabljali subjekti na strani ponudbe in povpraševanja v ekosistemu kibernetske varnosti EU, bi se akademija lahko oblikovala kot **konzorcij evropske digitalne infrastrukture (EDIC)**[45]. Ta instrument bi državam članicam omogočil sodelovanje pri zapolnitvi vrzeli v kibernetskovarnostnih veščinah ter tesno sodelovanje s Komisijo, agencijo ENISA in Evropskim kompetenčnim centrom za kibernetsko varnost (ECCC) v skladu z njihovimi mandati in pristojnostmi, hkrati pa bi jim omogočil, da vključijo vse ustrezne deležnike ter tudi to, da evropske, nacionalne in zasebne naložbe usmerijo v skupni cilj. V ta namen so zainteresirane države članice pozvane, naj Komisiji do 30. maja 2023 predložijo predhodno obvestilo o svoji prihodnji vlogi za ustanovitev takega konzorcija evropske digitalne infrastrukture. To prostovoljno predhodno obvestilo bi Komisiji omogočilo, da zgodaj poda pripombe k osnutku vloge za ustanovitev konzorcija evropske digitalne infrastrukture, kar bo omogočilo hitrejši nadaljnji razvoj in uradno predložitev. Komisija bo v vlogi pospeševalke večdržavnih projektov med celotnim postopkom in v obsegu, ki ga bodo zahtevale države članice, nudila pomoč pri pripravi vloge za ustanovitev konzorcija evropske digitalne infrastrukture. Komisija bo po tem, ko bo vlogo ocenila pozitivno, in po tem, ko bo vlogo odobril programski odbor za Digitalno desetletje, izdala sklep o ustanovitvi konzorcija evropske digitalne infrastrukture ter nato pomagala usklajevati izvajanje tega konzorcija[46].

Komisija bo medtem in v času uradnega ustanavljanja konzorcija evropske digitalne infrastrukture vzpostavila virtualno enotno vstopno točko, tako da bo izboljšala svojo **platformo za digitalne spretnosti in delovna mesta**[47] s podporo iz projekta za podporo evropski skupnosti za kibernetsko varnost[48].

---

[44] Uredba (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa Digitalna Evropa in razveljavitvi Sklepa (EU) 2015/2240.

[45] Konzorciji evropske digitalne strukture so bili vzpostavljeni v Sklepu (EU) 2022/2481 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o vzpostavitvi programa politike Digitalno desetletje do leta 2030, člen 13 in naslednji.

[46] Prav tam, člen 12.

[47] Domača stran | Platforma za digitalne spretnosti in delovna mesta (europa.eu).

[48] Glej Evropski kompetenčni center za kibernetsko varnost in Mreža nacionalnih koordinacijskih centrov: nov projekt za podporo skupnosti za kibernetsko varnost, ki ga financira EU. Evropska komisija je decembra 2022 podpisala pogodbo v višini 3 milijonov EUR za podporo skupnosti za kibernetsko varnost EU v okviru Evropskega kompetenčnega centra za kibernetsko varnost. Ta projekt bo prispeval k ciljem EU glede krepitve skupnosti in zmogljivosti v zvezi z raziskavami, inovacijami, uvajanjem ter industrijsko bazo na področju kibernetske varnosti.

Agencija ENISA bo prispevala k delovanju akademije v skladu s svojimi cilji[49], zlasti kar zadeva pomoč pri izobraževanju in usposabljanju na področju kibernetske varnosti, ter ob upoštevanju svojih obveznosti poročanja na podlagi direktive NIS 2[50]. **Evropski kompetenčni center za kibernetsko varnost** bo deloval v skladu s svojim strateškim programom, da bo podprl delovanje akademije za kibernetske veščine. Izvajal bo zlasti strateški cilj 3 (kibernetska varnost) programa Digitalna Evropa. Pri tem ga bodo podprle Komisija in države članice prek **nacionalnih koordinacijskih centrov**. Po potrebi bo k sodelovanju povabljena **skupina za sodelovanje**, ustanovljena na podlagi direktive NIS 2[51]. Nazadnje bo treba združiti moči z **industrijo** in **znanstveno skupnostjo**, da bi se dosegel cilj akademije, tj. zapolniti vrzel v kibernetskovarnostnih veščinah.

4. Ustvarjanje znanja in usposabljanje: vzpostavitev skupnega pristopa EU k usposabljanju na področju kibernetske varnosti

Na akademiji kibernetskih veščin bo v okviru stebra ustvarjanja znanja in usposabljanja razvit strukturiran pristop z jasnim ciljem povečanja **števila** oseb s kibernetskovarnostnimi veščinami v EU, boljše prilagoditve usposabljanja **potrebam trga** ter zagotovitve prepoznavnosti v okviru **poklicnih poti**.

4.1. V slogi je moč: skupni pristop k profilom vlog na področju kibernetske varnosti ter s tem povezanim veščinam

Agencija ENISA je že opravila delo za opredelitev profilov vlog strokovnjakov za kibernetsko varnost na podlagi evropskega okvira za kibernetskovarnostne veščine **(ECSF)**[52]. Akademija bi morala na podlagi tega opredeliti in oceniti ustrezne veščine, spremljati razvoj vrzeli v veščinah ter zagotoviti informacije o novih potrebah. Za vsako vlogo na področju kibernetske varnosti[53] v evropskemu okviru za kibernetskovarnostne veščine je kot element opisa vključen sklop ustreznih informacij iz evropskega okvira za e-usposobljenost[54].

Agencija ENISA bo zato pregledala evropski okvir za kibernetskovarnostne veščine ter **opredelila spreminjajoče se potrebe po veščinah ter njihovo pomanjkanje** pri delovni sili na področju kibernetske varnosti, tudi z uporabo naprednih orodij (npr. umetne inteligence, velepodatkov[55], podatkovnega rudarjenja). Agencija ENISA bo v ta namen delovala pod vodstvom konzorcija evropske digitalne infrastrukture, ko bo ta ustanovljen, in Evropskega kompetenčnega centra za kibernetsko varnost (ECCC), skupaj z nacionalnimi koordinacijskimi centri, Komisijo, projektom za podporo evropski skupnosti za kibernetsko

[49] „Agencija ENISA podpira krepitev zmogljivosti in pripravljenosti v vsej Uniji, tako da institucijam, organom, uradom in agencijam Unije, pa tudi državam članicam ter javnim in zasebnim deležnikom pomaga […] razvijati znanja in spretnosti na področju kibernetske varnosti.“ Člen 4(3) Akta o kibernetski varnosti.

[50] Člen 18 direktive NIS 2.

[51] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2).

[52] Evropski okvir za kibernetskovarnostne veščine (ECSF) – ENISA (europa.eu). Evropski okvir za kibernetskovarnostne veščine podpira opredelitev in opis nalog, kompetenc, veščin in znanja, povezanih z vlogami evropskih strokovnjakov za kibernetsko varnost. V njem so vse vloge, povezane s kibernetsko varnostjo, povzete v profile, ki so posamično razčlenjeni na podrobnosti o ustreznih odgovornostih, veščinah, sinergijah in soodvisnostih.

[53] Evropski okvir za e-usposobljenost (e-CF) | Esco (europa.eu). Evropski okvir za e-usposobljenost zagotavlja dosledne povezave v okviru kvalifikacij na področju IKT in drugih okvirov, pomembnih za sektor, med katere sodi okvir digitalnih kompetenc za državljane.

[54] V zvezi s tem glej uporabniški priročnik – evropski okvir za kibernetskovarnostne veščine – september 2022.

[55] Glej na primer orodje Skills-OVATE, ki ga je razvil Cedefop.

varnost ter akterji na trgu[56]. Kar zadeva delovno silo na področju kibernetske obrambe, bo agencija ENISA ustrezno upoštevala delo, ki ga opravlja EAVO. Podobno bo na področju boja proti kibernetski kriminaliteti upoštevala dejavnosti, ki jih izvajata Agencija Evropske unije za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (CEPOL) ter Europol za pripravo analize potreb po operativnem usposabljanju[57] v zvezi s kibernetskimi napadi.

Evropski okvir za kibernetskovarnostne veščine se bo v celotnem dvoletnem ciklu v okviru akademije redno dopolnjeval in pregledoval. Poleg tega bosta Komisija in Evropska služba za zunanje delovanje po potrebi prispevali k opredelitvi posameznih profilov ter s tem povezanih veščin za sektorje, pri čemer ju bodo podprli agencije, uradi in organi EU, kot so EAVO[58], Europol in CEPOL[59].

Vzpostavljene bodo tudi povezave med evropskim okvirom za kibernetskovarnostne veščine in ustreznimi instrumenti politike zaposlovanja EU[60]. Zlasti bodo profili delovnih mest iz evropskega okvira za kibernetskovarnostne veščine ter s tem povezane veščine vključeni v **klasifikacijo ESCO**. S tem se bodo izboljšale klasifikacija poklicev in veščin na področju kibernetske varnosti ter povezave med njimi, s čimer se bo posameznikom omogočilo lažje izpopolnjevanje in preusposabljanje ter se bosta podprla usklajevanje ponudbe delovnih mest in povpraševanja po njih ter čezmejna mobilnost.

4.2.Spodbujanje sodelovanja za oblikovanje učnih načrtov za izobraževanje in usposabljanje na področju kibernetske varnosti

Po vzpostavitvi konzorcija evropske digitalne infrastrukture bi morala akademija prejeti podporo držav članic, da bi postala **referenčno mesto v Evropi za oblikovanje in izvajanje usposabljanj na področju kibernetske varnosti**, s čimer bi se obravnavale najpotrebnejše veščine ter zagotovile priložnosti za usposabljanja na delovnem mestu in pripravništva za zagonska podjetja in MSP ter javne uprave v inovativnih podjetjih na področju kibernetske varnosti in kompetenčnih centrih za kibernetsko varnost. Konzorcij evropske digitalne infrastrukture bi moral sodelovati z vsemi ustreznimi deležniki, vključno z industrijo, in graditi na projektih kot je **CyberSecPro**[61], ki se financira iz programa Digitalna Evropa ter v katerem sodeluje 17 visokošolskih ustanov in 13 varnostnih podjetij iz 16 držav članic, da bi postal primer dobre prakse za vse programe usposabljanja na področju kibernetske varnosti.

---

[56] Agencija bo še naprej uporabljala rezultate iz drugih projektov, ki jih financira EU (REWIRE, Data Space For Skills (DS4S), CyberSecPro, Concordia), in metodologije, ki izhajajo iz podobnih pobud (npr. „Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States“ (Ustvarjanje usposobljene delovne sile na področju kibernetske varnosti v petih državah: spoznanja iz Avstralije, Kanade, Nove Zelandije, Združenega kraljestva in Združenih držav Amerike), poročilo OECD, objavljeno 21. marca 2023), da bi v prihodnosti zagotovila posodobljeno vizijo potreb v okolju, v katerem se povpraševanje nenehno spreminja.

[57] CEPOL, Ocena potreb po operativnem usposabljanju (OTNA).

[58] V zvezi s tem glej Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo (JOIN(2022) 49 final).

[59] Glede tega bo pozornost namenjena delu v zvezi z okvirom kompetenc na področju usposabljanja o kibernetski kriminaliteti, ki je trenutno v pripravi.

[60] Kot so evropska klasifikacija spretnosti, kompetenc, kvalifikacij in poklicev (ESCO), Europass ter mreža evropskih služb za zaposlovanje (EURES).

[61] CyberSecPro V okviru projekta se bodo na primer analizirali programi, tečaji in poletne šole za kibernetsko varnost, ki so na voljo na univerzah, ter uporabljene preglednice ocenjevanja evropskega sistema prenašanja in zbiranja kreditnih točk (ECTS), zagotovilo se bo sodelovanje ciljnega števila več kot 530 pripravnikov v triletnem obdobju ter usposabljale se bodo zunanje osebe iz različnih panog in sektorjev.

Akademija bo sodelovala z vsemi ustreznimi deležniki, da bi **mlade generacije pritegnila** k izbiri poklicnih poti na področju kibernetske varnosti. Države članice bi morale v skladu s predlogom za priporočilo Sveta o izboljšanju zagotavljanja digitalnih spretnosti v izobraževanju in usposabljanju vzpostaviti in okrepiti ukrepe za zaposlovanje in usposabljanje specializiranih učiteljev in mentorjev ter olajšati pridobivanje kibernetskovarnostnih veščin, tudi z vajeništvom. Spodbujati bi bilo treba vključevanje kibernetske varnosti v programe izobraževanja in usposabljanja ter hkrati zagotavljati dostopnost teh programov, razvijati ponudbo **vajeništev** in pripravništev, spodbujati inovativne pristope, vključno na primer z resnimi igrami in skupnimi simulacijskimi platformami, organizirati izkustvene tedne na delovnih mestih na področju kibernetske varnosti ter pojasniti profile netehničnih vlog. Podpirati bi bilo treba tudi sodelovanje težko dosegljivih skupin, kot so mladi invalidi, ki živijo na oddaljenih ali podeželskih območjih, in posamezniki iz drugih manjšinskih skupin, pri teh priložnostih za učenje o kibernetski varnosti.

Komisija bo še naprej zagotavljala podporo za razvoj mikrodokazil ter programov poklicnega izobraževanja in usposabljanja. V okviru programa Erasmus+ se bodo še naprej financirali zlasti **programi skupnega diplomskega in magistrskega študija**, **skupni tečaji ali moduli, s katerimi se lahko pridobijo mikrodokazila**, ter **kombinirani intenzivni programi**[62] o vseh temah, vključno **s kibernetsko varnostjo**. Prav tako se bo podprlo nadaljnje izvajanje **pobude Evropske univerze**[63] in **centrov poklicne odličnosti**[64], da bi se spodbudilo tesnejše sodelovanje med visokošolskimi ustanovami ter ustreznimi ustanovami poklicnega izobraževanja in usposabljanja po vsej Evropi. Ta cilj tesnejšega sodelovanja se bo podprl s programi financiranja EU, vključno s programom Erasmus+ in programom Digitalna Evropa, ter s sredstvi EU za razvoj **individualnih učnih računov**[65].

Da bi se na nacionalni ravni olajšalo sodelovanje med znanstveno skupnostjo in ponudniki usposabljanj za kibernetskovarnostne veščine ter delodajalci iz zasebnega in javnega sektorja ter da bi se spodbudile sinergije med javnim in zasebnim sektorjem, so nacionalni koordinacijski centri pozvani, naj preučijo ustanovitev **kibernetskih kampusov** v državah članicah. Namen kibernetskih kampusov bi bil zagotoviti centre odličnosti na nacionalni ravni za skupnost za kibernetsko varnost, akademija pa bi tem kampusom pomagala pri mreženju in nadaljnjem usklajevanju njihovih dejavnosti.

Agencija ENISA bo prav tako izboljšala svojo ponudbo usposabljanja na področju kibernetske varnosti, tako da bo **svoj katalog tečajev**[66] uskladila s profili iz evropskega okvira za kibernetskovarnostne veščine ter dopolnila module usposabljanja za vsak profil, kar bi lahko izboljšalo ponudbe usposabljanj v državah članicah. Razširila bo tudi svoj **program „usposabljanja izvajalcev usposabljanja“**[67], pri čemer se bo osredotočila na poklicne potrebe institucij, organov, uradov in agencij EU ter javnih organov in **javnih in zasebnih kritičnih izvajalcev** iz držav članic, ki spadajo na področje uporabe direktive NIS 2.

[62] Kombinirani intenzivni programi združujejo poučevanje na daljavo s kratkim obdobjem fizične mobilnosti.

[63] Pobuda Evropske univerze |Evropski izobraževalni prostor (europa.eu).

[64] Centri poklicne odličnosti | Erasmus+ (europa.eu).

[65] V skladu s Priporočilom Sveta z dne 16. junija 2022 o individualnih učnih računih.

[66] Tečaji usposabljanja – ENISA (europa.eu).

[67] Program usposabljanja izvajalcev usposabljanja – ENISA (europa.eu).

Poleg tega bodo tudi druge agencije, uradi in organi EU okrepili svojo ponudbo usposabljanja na področju kibernetske varnosti. **EAVO** bo na primer z izvajanjem politike EU za kibernetsko obrambo razvila nov sklop tečajev o kibernetski varnosti in nekatere svoje sedanje tečaje uskladila z evropskim okvirom za kibernetskovarnostne veščine. Ti tečaji bodo privedli do certificiranja učnih rezultatov[68]. EAVO bo v sodelovanju s Komisijo preučila možnost vključitve spričeval v denarnico evropske digitalne identitete. EAVO bo nadalje preučila možne mehanizme ocenjevanja veščin, na podlagi katerih bodo izdana spričevala. Podobno bodo na področju boja proti kibernetski kriminaliteti potekala prizadevanja za tesnejše sodelovanje z **akademijo za kibernetsko kriminaliteto agencije CEPOL**[69], da bi se spodbudile sinergije in dopolnjevanja pri oblikovanju in izvajanju učnih načrtov za usposabljanje.

4.3. Oblikovanje sinergij in zagotavljanje prepoznavnosti usposabljanj in certificiranja na področju kibernetske varnosti v državah članicah

V okviru akademije bi bilo treba obravnavati vprašanje prepoznavnosti usposabljanja in certificiranja ter sinergij med njima. To bi koristilo civilnim, obrambnim in diplomatskim kibernetskim skupnostim ter kibernetskim skupnostim organov kazenskega pregona, saj je v številnih primerih v vseh sektorjih potrebno enako strokovno znanje, ki temelji na podobnih učnih načrtih in učnih rezultatih.

Z akademijo bi se zagotovila **enotna vstopna točka** za tiste, ki se zanimajo za poklicno pot na področju kibernetske varnosti. To bo kratkoročno doseženo z okrepitvijo **platforme** Komisije **za digitalne spretnosti in delovna mesta** s podporo iz projekta za podporo evropski skupnosti za kibernetsko varnost. V posebnem oddelku o poklicnih poteh na področju kibernetske varnosti bodo zagotovljene povezave z obstoječimi orodji, od visokošolskih programov do priložnosti za usposabljanje, vključno s tečaji za pridobitev mikrodokazil ter programi poklicnega izobraževanja in usposabljanja, ter do ponudb za zaposlitev. To bo doseženo s sklicevanjem na tekoče delo in pobude, kot so tiste v okviru agencije ENISA, ki je v sodelovanju z znanstveno skupnostjo pripravila **podatkovno zbirko izobraževalnih ustanov**, ki ponujajo programe na področju kibernetske varnosti, ter z vključevanjem tega dela in pobud na platformo.. To bo dodatno okrepljeno s podporo nacionalnih koordinacijskih centrov. Poleg tega bo agencija ENISA s podporo nacionalnih koordinacijskih centrov, Komisije ter projekta za podporo evropski skupnosti za kibernetsko varnost in v sodelovanju s subjekti, ki zagotavljajo certificiranje, ter na podlagi drugih ustreznih pobud razvila in utrdila dva **repozitorija obstoječih usposabljanj iz javnega in zasebnega sektorja ter certificiranj na področju kibernetske varnosti**[70]. Ta repozitorija bosta vključena tudi v enotno vstopno točko platforme za digitalne spretnosti in delovna mesta. To delo bo koristilo tudi nacionalnim koordinacijskim centrom, katerih naloga je zlasti spodbujati in razširjati izobraževalne programe na področju kibernetske varnosti[71].

---

[68] V skladu s členom 20(4) Sklepa Sveta (SZVP) 2020/1515 z dne 19. oktobra 2020 o ustanovitvi Evropske akademije za varnost inobrambo ter razveljavitvi Sklepa (SZVP) 2016/2382.

[69] Akademija za kibernetsko kriminaliteto agencije CEPOL je bila ustanovljena leta 2019, da bi se zagotovila najsodobnejša platforma za izboljšanje znanja o kibernetski kriminaliteti in kibernetskih zmogljivosti v Evropi.

[70] Na primer W4C Academy – Women4Cyber ali projekt Global Cybercrime Certification za organe kazenskega pregona in pravosodne organe.

[71] „1. Nacionalni koordinacijski centri imajo naslednje naloge: […] (g) brez poseganja v pristojnosti držav članic za izobraževanje in ob upoštevanju ustreznih nalog agencije ENISA, sodelovanje z nacionalnimi organi v zvezi z morebitnim prispevkom k promoviranju in razširjanju izobraževalnih programov na področju kibernetske varnosti“,

Prav tako je treba strokovnjakom dati zagotovilo, da so usposabljanja, ki se jih udeležijo, zahtevane kakovosti. Zato bo agencija ENISA razvila **pilotni projekt**, v okviru katerega bo preučila vzpostavitev evropskega sistema potrdil za kibernetskovarnostne veščine.

Poleg tega je bistveno opredeliti veščine in usposabljanja ter jih povezati s profilom delovnega mesta, vendar je prav tako pomembno zagotoviti, da imajo ponudniki storitev kibernetske varnosti potrebne kompetence, strokovno znanje in izkušnje. To velja zlasti za ponudnike upravljanih varnostnih storitev na področjih, kot so odzivanje na incidente, penetracijsko testiranje, varnostne presoje in svetovanje. V direktivi NIS 2 in predlogu akta o kibernetski solidarnosti so določene posebne naloge za take ponudnike upravljanih varnostnih storitev. Komisija zato predlaga tudi **ciljno usmerjeno spremembo Akta o kibernetski varnosti**[72], da se omogočijo certifikacijske sheme upravljanih varnostnih storitev na ravni EU. Take certifikacijske sheme bi morale biti med drugim namenjene zagotovitvi, da te storitve opravlja osebje z zelo visoko stopnjo tehničnega znanja in kompetenc na ustreznih področjih.

Mehanizmi za zagotavljanje kakovosti in priznavanje mikrodokazil[73] omogočajo boljšo preglednost, primerljivost in prenosljivost učnih rezultatov. Države članice se v skladu s priporočilom Sveta o evropskem pristopu k mikrodokazilom[74] spodbuja, naj mikrodokazila za kibernetsko varnost vključijo v svoja nacionalna ogrodja kvalifikacij. To bi jim omogočilo, da mikrodokazila za kibernetsko varnost povežejo z evropskim ogrodjem kvalifikacij[75]. Infrastruktura za evropska digitalna potrdila za učenje je na voljo za izdajanje digitalno podpisanih kvalifikacij in mikrodokazil na področju kibernetske varnosti posameznikom. Ti vsebujejo veliko podatkov, tudi o učnih rezultatih na področju kibernetske varnosti, in jih je mogoče shraniti v prihodnji **digitalni denarnici evropske digitalne identitete**[76].

Ukrepi v okviru akademije

Države članice in industrija

- Zagotoviti podporo za razvoj in priznavanje **mikrodokazil** za učenje na področju kibernetske varnosti v skladu s priporočilom Sveta o evropskem pristopu k mikrodokazilom.
- Vključiti kvalifikacije in mikrodokazila na področju kibernetske varnosti v **nacionalna ogrodja kvalifikacij**.
- Zagotoviti **priložnosti za učenje na delovnem mestu** v obliki vajeništva za osebe, ki so vključene v pobude za razvoj kibernetskovarnostnih veščin.

Komisija

člen 7(1), točka (g), uredbe o Evropskem kompetenčnem centru za kibernetsko varnost. Glej tudi s tem povezano uvodno izjavo 28.

[72] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti).

[73] Na primer evidenca ali potrdila o učnih rezultatih, ki jih osebe pridobijo po manjših usposabljanjih.

[74] Priporočilo Sveta o evropskem pristopu k mikrodokazilom za vseživljenjsko učenje in zaposljivost.

[75] Priporočilo Sveta z dne 22. maja 2017 o evropskem ogrodju kvalifikacij za vseživljenjsko učenje in razveljavitvi Priporočila Evropskega parlamenta in Sveta z dne 23. aprila 2008 o uvedbi evropskega ogrodja kvalifikacij za vseživljenjsko učenje.

[76] Predlog uredbe Evropskega parlamenta in Sveta o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo okvira za evropsko digitalno identiteto.

- Kratkoročno do konca leta 2023 prek **platforme za digitalne spretnosti in delovna mesta** vzpostaviti **enotno vstopno točko** za programe na področju kibernetske varnosti, obstoječa usposabljanja in certificiranja na področju kibernetske varnosti.
- 18. aprila 2023 predlagati spremembo **Akta o kibernetski varnosti**, da se omogoči certificiranje ponudnikov upravljanih varnostnih storitev.

Organi, uradi in agencije EU

- Vzpostaviti **evropski okvir za kibernetskovarnostne veščine** kot skupni pristop k profilom vlog na področju kibernetske varnosti ter s tem povezanim veščinam do konca leta 2023.
- Agencija ENISA začne v drugem četrtletju 2023 razvijati pilotni projekt za vzpostavitev **evropskega sistema potrdil** za kibernetskovarnostne veščine.
- Agencija ENISA pregleda svoj **katalog tečajev** ter do konca leta 2023 omogoči, da se v njen **program „usposabljanja izvajalcev usposabljanja“** vključijo javni in zasebni kritični izvajalci.
- Končati **usklajevanje učnih načrtov EAVO z evropskim okvirom za kibernetskovarnostne veščine** do sredine leta 2023.

5. Vključenost deležnikov: zaveza za zapolnitev vrzeli v kibernetskovarnostnih veščinah

V okviru akademije bo razvit usklajen pristop k vključevanju deležnikov za zapolnitev vrzeli v kibernetskovarnostnih veščinah. Cilj bo čim bolj povečati prepoznavnost in učinek zavez različnih deležnikov, namenjenih zmanjševanju vrzeli v kibernetskovarnostnih veščinah.

Komisija poziva deležnike, naj se s konkretnimi zavezami obvežejo k izpopolnjevanju in preusposabljanju delavcev z namenskimi ukrepi, pri čemer naj se čim bolj oprejo na ugotovljeno vrzeli v kibernetskovarnostnih veščinah. O takih **zavezah deležnikov glede kibernetske varnosti** bi bilo treba poročati na **platformi za digitalne spretnosti in delovna mesta**, podobno kot o drugih digitalnih zavezah, ki so že vidne na platformi. Komisija nadalje spodbuja deležnike, ki so na platformi podali zavezo glede kibernetske varnosti, naj se pridružijo **obsežnemu digitalnemu partnerstvu v okviru Pakta za spretnosti**[77]. Spodbuja se, da se zaveze glede kibernetske varnosti, sprejete v okviru obsežnega digitalnega partnerstva, predložijo na platformi za digitalne spretnosti in delovna mesta. Podobno se spodbuja, da se zaveze, sprejete v okviru platforme za digitalne spretnosti in delovna mesta, sporočijo v okviru obsežnega digitalnega partnerstva Pakta za spretnosti.

Komisija nadalje poziva države članice, naj si **prizadevajo za izvajanje izjave o ženskah na digitalnem področju**[78], da bi se ženske spodbudile k dejavni in pomembni vlogi v sektorju digitalne tehnologije ter da bi se odpravile razlike med deležem žensk in moških na delovnih mestih na področju kibernetske varnosti. Komisija države članice prav tako spodbuja, naj razvijejo sinergije s svojimi programi **Evropskega socialnega sklada plus** (ESS+), da bi

[77] Ustanovitev novih evropskih partnerstev za uresničitev ambicij EU v okviru digitalnega desetletja | Oblikovanje digitalne prihodnosti Evrope (europa.eu), ki so nastala v okviru Pakta za spretnosti za odpravo pomanjkanja informacijske in komunikacijske tehnologije (IKT).

[78] Države EU se zavezujejo h krepitvi udeležbe žensk na digitalnem področju | Oblikovanje digitalne prihodnosti Evrope (europa.eu).

dodatno podprle cilj enakosti spolov pri udeležbi na trgu dela[79], na primer z vzpostavitvijo **programov mentorstva za dekleta in ženske**. S temi programi se lahko lažje pridobijo vzorniki, ki bi dekleta pritegnili k poklicem na področju kibernetske varnosti, hkrati pa bi se z njimi odpravljali spolni stereotipi. S temi programi se tudi spodbujajo izpopolnjevanje in preusposabljanje žensk ter razvoj skupnosti, ki lahko ženske podpira pri njihovem vstopu na trg dela na področju kibernetske varnosti ali pri napredovanju na njem.

Države članice bi morale v okviru svojih **nacionalnih strategij za kibernetsko varnost sprejeti posebne ukrepe, s katerimi bi ublažile pomanjkanje kibernetskovarnostnih veščin**[80], opredelile in bolje usmerjale prizadevanja za zapolnitev vrzeli v veščinah ter nazadnje zagotovile ustrezno izvajanje svojih obveznosti iz direktive NIS 2.

Nekatere države članice izkoriščajo **sinergije med civilnimi in obrambnimi pobudami ter pobudami na področju kazenskega pregona**. Na primer z razvojem delovne sile na podlagi nacionalnega obveznega služenja vojaškega roka ali z vključitvijo kibernetskih rezervistov, ki so vojaško usposobljeni državljani na položajih na področju kibernetske varnosti v oboroženih silah[81], se prebivalcem, zlasti mladim odraslim, omogoči izboljšanje veščin na področju kibernetske varnosti in kibernetske obrambe. Enako velja za področje **boja proti kibernetski kriminaliteti**, saj so si splošna prizadevanja na področju kibernetske varnosti in dejavnosti kazenskega pregona pri odzivanju na kibernetskovarnostne incidente v marsičem podobni. Komisija spodbuja razprave o takih pobudah med državami članicami ter jih poziva, naj ocenijo, kako lahko usposobljena delovna sila najbolje služi obrambnim in civilnim skupnostim za kibernetsko varnost.

Komisija bo razmislila o predlogih glede tega, kako odpraviti sedanje in pričakovane vrzeli , ki so bile ugotovljene pri njenem pregledu potreb institucij, organov, uradov in agencij EU. Zlasti bo spodbujala osebje, naj izkoristi prihodnja **nepovratna sredstva za kibernetsko varnost EU-Združene države Amerika (ZDA)**, vzpostavljena v okviru dialoga med EU in ZDA.

Ukrepi v okviru akademije

Industrija

- Do 18. aprila 2023 predlagati posebne **zaveze glede kibernetske varnosti** na platformi za digitalne spretnosti in delovna mesta.

Države članice

- V **nacionalne strategije za kibernetsko varnost** vključiti posebne ukrepe za odpravo vrzeli v kibernetskovarnostnih veščinah.

Države članice in industrija

- Izvajati izjavo o ženskah na digitalnem področju ter do leta 2030 **odpraviti razliko med deležem žensk in moških na delovnih mestih na področju kibernetske varnosti**.

[79] Uredba (EU) 2021/1057 Evropskega parlamenta in Sveta z dne 24. junija 2021 o vzpostavitvi Evropskega socialnega sklada plus (ESS+) in razveljavitvi Uredbe (EU) št. 1296/2013, člen 4(1), točka (c).

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

[81] Report – Cyber Conscription: Experience and Best Practice from Selected Countries (Vpoklic na kibernetskem področju: izkušnje in dobra praksa izbranih držav), Martin Hurt in Tiia Sõmer, International Centre for Defence and Security, februar 2021.

6. Financiranje: vzpostavitev sinergij za čim večji učinek porabljenih sredstev za razvoj kibernetskovarnostnih veščin

V okviru akademije se bo čim bolj povečal učinek naložb v kibernetskovarnostne veščine, in sicer tako da se bo zagotovila skupna vstopna točka, omogočilo boljše usmerjanje sredstev k potrebam trga, spodbudila poraba sredstev in olajšale sinergije med različnimi instrumenti, hkrati pa preprečilo podvajanje prizadevanj[82].

6.1. Usklajevanje sredstev s potrebami

Evropski kompetenčni center za kibernetsko varnost bo v okviru akademije in ob podpori Komisije, projekta za podporo evropski skupnosti za kibernetsko varnost in nacionalnih koordinacijskih centrov zbiral **informacije o tem, kako se s sredstvi EU financirajo kibernetskovarnostne veščine**, ter ocenil, kako se s temi sredstvi podpira zmanjševanje vrzeli v teh veščinah. Ob upoštevanju teh zbranih informacij si bo Evropski kompetenčni center za kibernetsko varnost prizadeval zagotoviti boljše usmerjanje sredstev EU k ugotovljenim potrebam. Financiral bo ukrepe, s katerimi se bodo zapolnila najpomembnejše vrzelipri delovni sil na področju kibernetske varnosti, tudi tista, ki so povezana z izpolnjevanjem potreb politike na področju kibernetske varnosti.

6.2. Zagotavljanje prepoznavnosti razpoložljivih sredstev ter partnerskih pobud za kibernetskovarnostne veščine

Platforma za digitalne spretnosti in delovna mesta bo kratkoročno postala enotna vstopna točka za deležnike, kjer bodo na voljo vse informacije o priložnostih za financiranje za kibernetskovarnostne veščine.

EU vlaga v ljudi ter njihova znanja in spretnosti ter uporablja zlasti partnerstva z industrijo, da izvaja ukrepe za izpopolnjevanje in preusposabljanje, pri čemer izkorišča več instrumentov, opredeljenih v **evropskem programu znanj in spretnosti**[83], zlasti **Pakt za spretnosti**[84] ter **akcijski načrt za digitalno izobraževanje**[85]. S **programom Digitalna Evropa** se financirajo priložnosti za kibernetskovarnostne veščine, zlasti s pobudami za večdržavne projekte ob jasnem dopolnjevanju s podporo iz programa Obzorje Evropa za raziskave in inovativne tehnološke rešitve na področju kibernetske varnosti. Iz **Evropskega obrambnega sklada**[86] se financirajo raziskave in tehnološki razvoj za izvajanje učinkovitih kibernetskih operacij, vključno z usposabljanji in vajami[87]. Take pobude se bodo še naprej podpirale s **programom Erasmus+**, tudi s kombiniranimi intenzivnimi programi in projekti sodelovanja.

Države članice se spodbuja k zagotovitvi sredstev EU, ki jih upravljajo neposredno, za podporo kibernetskovarnostnim veščinam in delovnim mestom. V zvezi s tem imajo skladi

---

[82] Priložnosti za financiranje (europa.eu). Podporne storitve v okviru Pakta za spretnosti zagotavljajo enotno vstopno točko za informacije o financiranju za veščine, tudi za digitalni ekosistem. Podporne storitve Pakta za spretnosti zagotavljajo splošne informacije o instrumentih financiranja, ki niso posebej namenjeni kibernetskovarnostnim veščinam, vendar pa bilo treba v okviru akademije upoštevati delo, ki se izvaja v okviru teh instrumentov, da bi se izognili podvajanju.

[83] Program znanj in spretnosti za Evropo – Zaposlovanje, socialne zadeve in vključevanje – Evropska komisija (europa.eu).

[84] Instrumenti financiranja EU za strokovno izpopolnjevanje in prekvalifikacijo – Zaposlovanje, socialne zadeve in vključevanje – Evropska komisija (europa.eu).

[85] Akcijski načrt za digitalno izobraževanje 2021–2027.

[86] Uredba (EU) 2021/697 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi Evropskega obrambnega sklada ter razveljavitvi Uredbe (EU) 2018/1092.

[87] Države članice so zavezane k skupnim usposabljanjem in vajam, na primer tako, da vzpostavijo projekte kibernetskega usposabljanja in vaj v okviru stalnega strukturnega sodelovanja (PESCO), kot sta akademsko in inovacijsko vozlišče EU za kibernetsko varnost (EU CAIH) ter Zveza virtualnih poligonov za kibernetsko varnost, ter v njih sodelujejo.

kohezijske politike, kot sta **Evropski sklad za regionalni razvoj (ESRR)** in **ESS+**, velik potencial za sinergije[88]. Področja uporabe ukrepov v okviru **mehanizma za okrevanje in odpornost**[89] ter **programa InvestEU**[90] se med seboj prekrivajo na način, ki je ključen za izpolnjevanje ciljev akademije.

Ukrepi v okviru akademije

Evropski kompetenčni center za kibernetsko varnost in agencija ENISA

- Obstoječa sredstva EU za kibernetskovarnostne veščine **povezati** s potrebami trga, oceniti **učinkovitost** in opredeliti **prednostne naloge** na področju financiranja do konca leta 2024.

Komisija

- Do konca leta 2023 na platformi za digitalne spretnosti in delovna mesta vzpostaviti **enotno vstopno točko** za priložnosti za financiranje za kibernetskovarnostne veščine.

7. Merjenje napredka: vgrajena odgovornost

V okviru akademije bo razvita **metodologija**, s katero bo mogoče **meriti napredek pri zapolnitvi vrzeli v kibernetskovarnostnih veščinah**.

7.1. Opredelitev kazalnikov kibernetske varnosti za spremljanje razvoja trga dela na področju kibernetske varnosti

V **indeksu digitalnega gospodarstva in družbe** so povzeti kazalniki digitalne uspešnosti Evrope, z njim pa se spremlja napredek držav članic EU. Agencija ENISA bo v okviru akademije za kibernetske veščine ter v sodelovanju s Komisijo in skupino za sodelovanje na področju varnosti omrežij in informacij[91] razvila **kazalnike**, povezane tudi s spolom, za spremljanje napredka v državah članicah EU pri povečanju števila strokovnjakov za kibernetsko varnost, pri tem pa se bo posvetovala tudi z ustreznimi akterji na trgu in nacionalnimi koordinacijskimi centri. Agencija ENISA se bo oprla na metodologijo indeksa digitalnega gospodarstva in družbe[92] ter zagotovila, da bodo kazalniki v skladu z evropskimi digitalnimi cilji glede strokovnjakov na področju IKT in glede odprave razlike med deležem žensk in moških na področju IKT. Komisija si bo nato prizadevala za vključitev takih kazalnikov v indeks digitalnega gospodarstva in družbe, kar bo omogočilo letno spremljanje stanja kibernetskovarnostnih veščin in trga dela.

7.2. Zbiranje podatkov in poročanje

[88] Člen 3(1) Uredbe (EU) 2021/1058 in člen 4(1), točka (g), Uredbe (EU) 2021/1057.

[89] V estonskem načrtu za okrevanje in odpornost je na primer predvidena naložba (10 milijonov EUR) v digitalne spretnosti, ki bo vključevala revizijo usposabljanj, ki so na voljo strokovnjakom na področju IKT, ter s katero se bosta financirala izpopolnjevanje in preusposabljanje za kibernetsko varnost za strokovnjake na področju IKT ter ki bo prispevala k razvoju pilotnega programa za preoblikovanje ogrodja kvalifikacij za strokovnjake na področju IKT.

[90] Deležniki (npr. ponudniki usposabljanja in družbe, ki želijo zasnovati ali izboljšati svoje dejavnosti usposabljanja na področju kibernetske varnosti) lahko obiščejo portal InvestEU ter se obrnejo na svetovalno vozlišče InvestEU, ki razvijalcem projektov in subjektom zagotavlja tehnično podporo in pomoč, vključno s krepitvijo zmogljivosti.

[91] Na podlagi in ob dopolnjevanju metodologije, ki jo bo agencija ENISA razvila za namene svojega dvoletnega poročila o stanju kibernetske varnosti v Uniji v skladu s členom 18(3) direktive NIS 2.

[92] Glej metodološko opombo indeksa digitalnega gospodarstva in družbe za leto 2022, ki je na voljo na spletni strani Indeks digitalnega gospodarstva in družbe | Oblikovanje digitalne prihodnosti Evrope (europa.eu).

Agencija ENISA bo podatke o kazalnikih zbirala ob podpori projekta za podporo evropski skupnosti za kibernetsko varnost in nacionalnih koordinacijskih centrov. Na podlagi zbranih podatkov bo pripravila **letno poročilo**, ki bo vključeno v poročilo o stanju digitalnega desetletja[93], to poročilo pa se bo nato skupaj z indeksom digitalnega gospodarstva in družbe upoštevalo pri analizi in priporočilih za posamezne države v okviru **evropskega semestra**[94]. Poleg tega bodo kazalniki o kibernetskovarnostnih veščinah prispevali k **dvoletnemu poročilu** agencije ENISA o stanju kibernetske varnosti v EU, ki je predvideno v direktivi NIS 2 ter zajema zmogljivosti, ozaveščenost in higieno na področju kibernetske varnosti po vsej EU.

7.3.Priprava ključnih kazalnikov uspešnosti za kibernetsko varnost

Agencija ENISA bo v tesnem sodelovanju s Komisijo in nacionalnimi koordinacijskimi centri Komisiji predlagala ključne kazalnike uspešnosti za zapolnitev vrzeli na področju strokovnjakov za kibernetsko varnost v Evropi, pri čemer se bo oprla na metodologijo iz programa politike Digitalno desetletje do leta 2030 ter na izkušnje industrije. Agencija ENISA bo ustrezno upoštevala ključne kazalnike uspešnosti, ki jih države članice uporabljajo za ocenjevanje svojih nacionalnih strategij za kibernetsko varnost[95].

Ukrepi v okviru akademije

Agencija ENISA

- Do konca leta 2023 pripraviti **kazalnike in ključne kazalnike uspešnosti** za kibernetskovarnostne veščine.
- **Zbirati podatke** o kazalnikih in poročati o njih, pri čemer bo prvo zbiranje izvedeno do leta 2025.

Komisija

- Prizadevati si za vključitev **kazalnikov kibernetske varnosti v indeks digitalnega gospodarstva in družbe** ter v **poročilo o stanju digitalnega desetletja**.

8. Sklep

V tem sporočilu so postavljeni temelji za prenovitev pristopa EU k izboljšanju kibernetskovarnostnih veščin za strokovnjake v EU. Cilj je zmanjšati vrzel v kibernetskovarnostnih veščinah in EU zagotoviti potrebno delovno silo, da se bo lahko odzivala na nenehno spreminjajočo se krajino groženj, izvajati politike EU, ki so namenjene zaščiti EU pred kibernetskimi napadi, pa tudi povečati poslovne priložnosti in konkurenčnost. Usposobljena delovna sila na področju kibernetske varnosti lahko koristi **civilnim, obrambnim in diplomatskim skupnostim ter skupnostim na področju kazenskega pregona**, saj olajšuje sinergije med njimi.

Komisija poziva države članice in vse deležnike, naj uresničijo ambicije akademije za kibernetske veščine.

[93] Sklep (EU) 2022/2481 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o vzpostavitvi programa politike Digitalno desetletje do leta 2030.

[94] Prav tam, uvodna izjava 25.

[95] Direktiva NIS 2, člen 7(4).