Vijeće
Europske unije

Bruxelles, 6. prosinca 2024.
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Za:	Delegacije
Predmet:	Zaključci Vijeća o ENISA-i

Za delegacije se u prilogu nalaze Zaključci Vijeća o ENISA-I koje je Vijeće odobrilo na sastanku održanome 6. prosinca 2024.

PRILOG

Nacrt zaključaka Vijeća o ENISA-i

VIJEĆE EUROPSKE UNIJE,

1. ISTIČE da izazovi koji proizlaze iz globalnog kibernetičkog prostora nikad nisu bili toliko složeni, raznoliki i ozbiljni kao što su to sada zbog sofisticiranosti novih kibernetičkih prijetnji, sigurnosnog okruženja koje se stalno mijenja i trenutačnih geopolitičkih napetosti. Stoga bi EU i njegove države članice trebali i dalje ulagati napore kako bi postali otporniji s ciljem učinkovitog utvrđivanja trenutačnih i novih prijetnji i izazova te suočavanja s njima. NAGLAŠAVA da bi se rad na povećanju razine kibernetičke otpornosti trebao nastaviti u skladu s pristupom koji obuhvaća cijelo društvo. ISTIČE da bi se u predstojećim godinama EU i njegove države članice trebali usredotočiti na učinkovitu provedbu zakonodavnih i nezakonodavnih inicijativa kojima se podupiru sva djelovanja koja su dosad poduzeta u tom pogledu i kojima se doprinosi tim djelovanjima;

2. PODSJEĆAJUĆI na to da nacionalna sigurnost i dalje ostaje isključiva odgovornost svake države članice, POTVRĐUJE da su EU i njegove države članice posljednjih godina izrazito surađivali na uspostavi potrebnog institucijskog ustroja i oblika suradnje u području kibernetičke sigurnosti na nacionalnoj razini i razini EU-a. POZDRAVLJA različite zakonodavne i nezakonodavne inicijative koje su EU-u i njegovim državama članicama pružile snažan i čvrst okvir u tom području kojim se povećava ukupna kibernetička otpornost Unije. Taj se okvir razvio kako bi obuhvatio nekoliko aspekata kibernetičke domene: sigurnost, diplomaciju, izvršavanje zakonodavstva i obranu. NAPOMINJE da velik broj aktera, uključujući tijela država članica za kibernetičku sigurnost, Skupinu za suradnju u području sigurnosti mrežnih i informacijskih sustava (Skupina za suradnju NIS), mrežu CSIRT-ova, Europsku mrežu organizacija za vezu za kiberkrize (EU-CyCLONe), mrežu nacionalnih koordinacijskih centara, Europsku skupinu za kibersigurnosnu certifikaciju, Komisiju, Europsku službu za vanjsko djelovanje (ESVD), Agenciju Europske unije za kibersigurnost (ENISA), Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti, CERT-EU, Europsku obrambenu agenciju (EDA) i Europolov Europski centar za kiberkriminalitet (EC3), sudjeluje u EU-ovu ekosustavu kibernetičke sigurnosti te svaki od tih aktera obavlja svoju zadaću u provedbi okvira za kibernetičku sigurnost na razini EU-a;

3. PREPOZNAJE da se tijekom posljednja dva desetljeća ENISA pokazala subjektom od neprocjenjive vrijednosti u europskom ekosustavu kibernetičke sigurnosti koji ima ključnu ulogu u aktivnom podupiranju država članica i institucija, tijela, ureda i agencija EU-a u njihovoj provedbi i razvoju politika kibernetičke sigurnosti, u njihovoj izgradnji kapaciteta i pripravnosti, u njihovoj suradnji te promicanju osviještenosti u pogledu kibernetičke sigurnosti i kibersigurnosne certifikacije;

OPĆE PREPORUKE O POLITIKAMA

4. POZIVA Komisiju da iskoristi **evaluaciju Akta o kibersigurnosti** kao priliku za ispitivanje načina na koji se njime može doprinijeti pojednostavnjenju složenog kibernetičkog ekosustava, čime bi se poboljšale djelotvornost i učinkovita upotreba resursa. Stoga POZIVA Komisiju da osigura da mandat ENISA-e za potporu državama članicama i institucijama, tijelima, uredima i agencijama EU-a bude usmjeren i jasno definiran, s konkretnim strateškim ciljevima i prioritetnim zadaćama, uz precizniju podjelu zadaća i nadležnosti u odnosu na druge aktere. U tom pogledu POZIVA Komisiju da ispita i dodatno ojača ulogu ENISA-e u podupiranju operativne suradnje na razini EU-a i među državama članicama u jačanju kibernetičke otpornosti, uzimajući u obzir nadležnosti država članica u tom području. Osim toga, POZIVA Komisiju da ojača savjetodavnu ulogu ENISA-e u pružanju stručnih smjernica i preporuka utemeljenih na dokazima u pogledu provedbe postojećih i budućih zakonodavnih i nezakonodavnih inicijativa EU-a, uz istodobno osiguravanje usklađenog okvira EU-a za kibernetičku sigurnost;

5. u istom duhu POTIČE Komisiju da razmotri racionalizaciju uloge ENISA-e u pogledu zadaća koje nisu u središtu njezine misije. ISTIČE da su **odgovornosti ENISA-e znatno proširene** nedavnim zakonodavnim inicijativama, uključujući, među ostalim, NIS 2, Akt o kibernetičkoj otpornosti i Akt o kibernetičkoj solidarnosti. Iako PRIMA NA ZNANJE da je ENISA dobila dodatne resurse kao rezultat nekih od tih inicijativa, ISTIČE da su proširenje odgovornosti ENISA-e i sve veća složenost kibernetičkih prijetnji i izazova doveli do znatnog povećanja njezinih zadaća, što bi se trebalo odražavati u **odgovarajućim** ljudskim, financijskim i tehničkim resursima, kako bi se Agenciji u potpunosti omogućilo izvršavanje svih zadaća u njezinoj nadležnosti, bez prejudiciranja pregovora o višegodišnjem financijskom okviru. U tu svrhu POZIVA Komisiju da pri pripremi nacrta općeg proračuna Unije utvrdi prioritet djelovanja i da prednost zadaćama povezanima s podupiranjem država članica u jačanju njihove kibernetičke otpornosti, operativne suradnje te razvoja i provedbe prava Unije;

POTPORA ENISA-E RAZVOJU I PROVEDBI POLITIKA

6. PODSJEĆA da je u skladu s postojećim pravnim okvirom za kibernetičku sigurnost ENISA-i povjereno nekoliko ključnih potpornih i savjetodavnih odgovornosti u cijelom EU-u. POZDRAVLJA ulogu ENISA-e u tom pogledu u pružanju **pomoći državama članicama** u učinkovitoj provedbi zakonodavnih i nezakonodavnih inicijativa. Poziva ENISA-u da u bliskoj suradnji sa Skupinom za suradnju NIS i Komisijom nastavi pružati opće uvide i analizu trenutačnog pravnog okružja u pogledu kibernetičke sigurnosti. POTIČE ENISA-u da redovito i strukturirano razmjenjuje i aktivno promiče tehničke smjernice i primjere najbolje prakse pomažući državama članicama u provedbi politike i zakonodavstva u području kibernetičke sigurnosti;

7. PREPOZNAJE ključnu ulogu ENISA-e u razvoju **europskih programa kibersigurnosne certifikacije** kojima se podupire povjerenje u IKT proizvode, usluge i procese te, osim toga, upravljane sigurnosne usluge s obzirom na predstojeću ciljanu izmjenu Akta o kibersigurnosti. NAGLAŠAVA da su države članice i industrija zabrinute zbog dugotrajnog postupka odabira, razrade i donošenja programâ kibersigurnosne certifikacije; stoga POZIVA Komisiju da iskoristi priliku koju pruža evaluacija Akta o kibersigurnosti kako bi pronašla načine za jednostavniji, transparentniji i brži pristup razvoju programâ kibersigurnosne certifikacije EU-a koji se temelji na riziku te istodobno ISTIČE važnu ulogu država članica u tom procesu. Osim toga, ISTIČE važnost izričitog dodjeljivanja odgovornosti za održavanje svakog programa certificiranja. Nadalje PODSJEĆA na to da bi se ENISA trebala pravodobno savjetovati sa svim relevantnim dionicima u okviru formalnog, otvorenog, transparentnog i uključivog postupka pri izradi prijedloga programâ te da bi se Komisija trebala savjetovati na otvoren, transparentan i uključiv način pri procjeni učinkovitosti i upotrebe donesenih programa. POTIČE ENISA-u da dodatno ojača suradnju sa zajednicom za zaštitu podataka, posebno s Europskim odborom za zaštitu podataka, prema potrebi, i nacionalnim nadležnim tijelima, s posebnim naglaskom na poticanju sinergije u kontekstu razvoja budućih europskih programa kibersigurnosne certifikacije;

8. Kako bi se spriječilo nepotrebno administrativno opterećenje koje bi moglo proizaći iz složenog okvira za izvješćivanje, POZIVA ENISA-u da u suradnji s Komisijom nastavi razmjenjivati informacije s državama članicama o praktičnim aspektima, pojednostavnjenju i racionalizaciji postupka izvješćivanja. Nadalje, PODSJEĆA na svoj poziv Komisiji da uz potporu ENISA-e i drugih relevantnih subjekata EU-a pripremi pregled relevantnih obveza izvješćivanja utvrđenih u odgovarajućim zakonodavnim aktima EU-a koji se odnose na kibernetička i digitalna pitanja. PODSJEĆA da se razmjena informacija između ENISA-e i država članica temelji na odnosu povjerenja, pri čemu su sigurnost i povjerljivost zajamčene u skladu s Aktom o kibersigurnosti i relevantnim pravilima i protokolima te bi trebala biti ograničena na ono što je relevantno i razmjerno svrsi razmjene. NAGLAŠAVA da je s podacima i informacijama potrebno postupati s dužnom pažnjom;

9. ISTIČE činjenicu da je ENISA **u skladu s Aktom o kibernetičkoj otpornosti** odgovorna za uspostavu i održavanje **jedinstvene platforme za izvješćivanje** koja će imati konkretnu operativnu dodanu vrijednost, posebno za aktivno iskorištene ranjivosti i ozbiljne incidente koji utječu na sigurnost proizvoda s digitalnim elementima. S obzirom na široko područje primjene tog horizontalnog zakonodavstva, jedinstvena platforma za izvješćivanje trebala bi biti učinkovit i siguran alat za olakšavanje razmjene informacija između nacionalnih CSIRT-ova i ENISA-e. Stoga POZIVA ENISA-u da dodijeli dostatne ljudske resurse te da kao ključan prioritet ubrza uspostavu platforme kako bi se osigurala njezina spremnost do roka utvrđenog u Aktu o kibernetičkoj otpornosti;

10. PREPOZNAJE ulogu ENISA-e u uspostavi **europske baze podataka o ranjivostima**, čiji je cilj poboljšati transparentnost u pogledu otkrivanja ranjivosti i istodobno osigurati odgovarajuće postupanje s osjetljivim podacima. S obzirom na kraj razdoblja prenošenja Direktive NIS 2, POZIVA ENISA-u da pojača sav potreban rad kako bi se osigurala neometana funkcionalnost te baze podataka. Istodobno POZIVA Skupinu za suradnju NIS da uz pomoć ENISA-e dodatno promiče smjernice, politike i postupke za otkrivanje ranjivosti;

11. PREPOZNAJE prednosti **djelovanja za potporu kibernetičkoj sigurnosti** koje provodi ENISA, a koje funkcionira kao skup usluga u području kibernetičke sigurnosti dostupnih državama članicama kako bi dopunile svoja nastojanja, kao i iskustvo ENISA-e stečeno njegovom provedbom. U tom pogledu ISTIČE da bi ENISA trebala imati središnju ulogu u upravljanju i radu pričuve EU-a za kibernetičku sigurnost. POZIVA ENISA-u da započne s mapiranjem potrebnih usluga i njihove dostupnosti odmah nakon stupanja na snagu Akta o kibernetičkoj solidarnosti kako bi pričuva EU-a za kibernetičku sigurnost bila što korisnija i prilagođena potrebama korisnika u svim državama članicama. POZIVA ENISA-u da, nakon što joj se povjeri ta zadaća, uključi države članice, posebno prikupljanjem informacija o potrebnim kriterijima i informiranjem o predstojećim natječajima, u ranoj fazi postupka uspostave pričuve EU-a za kibernetičku sigurnost. POZIVA ENISA-u da, nakon što joj se povjeri ta zadaća, osigura da postupak odabira pouzdanih pružatelja upravljanih sigurnosnih usluga bude transparentan, otvoren i pravedan te da omogućuje sudjelovanje pružatelja iz svih država članica, bez obzira na njihovu veličinu. Osim toga PODSJEĆA na to da se od ENISA-e zahtijeva da bez nepotrebne odgode izda smjernice o interoperabilnosti za prekogranične kibernetičke centre;

12. ISTIČE da je **praćenje trendova u pogledu tehnologija u nastajanju** u području koje se brzo mijenja, kao što je kibernetička domena, od ključne važnosti za održavanje i daljnje jačanje stanja naše kibernetičke sigurnosti. PREPOZNAJE rad ENISA-e na skretanju pozornosti javnosti na rizike i mogućnosti tehnologija kao što su umjetna inteligencija i kvantno računalstvo, čime se olakšava bolje razumijevanje trenutačnih izazova. POTIČE ENISA-u da dodatno doprinese tim zadaćama, da se aktivno zalaže za provedbu svojih preporuka te da, prema potrebi, savjetuje Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti i surađuje s njime;

POTPORA ENISA-E DRŽAVAMA ČLANICAMA U JAČANJU KIBERNETIČKO OTPORNOSTI I OPERATIVNE SURADNJE

13. ISTIČE da ENISA ima važnu ulogu **tajništva dviju mreža za kibernetičku suradnju na razini EU-a koje vode države članice, mreže CSIRT-ova i mreže EU-CyCLONe**. NAGLAŠAVA vrijedno sudjelovanje ENISA-e u Skupini za suradnju NIS, posebno njezinim aktivnim sudjelovanjem i tehničkim doprinosima u različitim područjima rada. POTIČE ENISA-u da nastavi podupirati funkcioniranje i suradnju tih mreža u budućnosti jer one državama članicama pružaju temeljne kanale za suradnju na različitim razinama;

14. PONOVNO ISTIČE potrebu za poboljšanjem **zajedničke informiranosti o stanju** na razini EU-a, čime se doprinosi EU-ovu stanju kibernetičke sigurnosti, u vezi s otkrivanjem, sprečavanjem i odgovorom na kibernetičke incidente. U tom pogledu ISTIČE važnost ENISA-inih aktivnosti predviđanja, redovitih izvješća i procjena prijetnji, koji svi doprinose poboljšanju informiranosti o stanju. POTIČE ENISA-u da blisko surađuje s državama članicama kako bi doprinijela razvoju informiranosti o stanju na razini EU-a. U tom kontekstu PREPOZNAJE važnu ulogu koju ENISA ima, zajedno s CERT-EU-om i Europolom, u pružanju potpore Vijeću u obliku informativnih sastanaka o stanju u kontekstu paketa instrumenata za kiberdiplomaciju kojima se dopunjuje informiranost o stanju koju pruža Služba za jedinstvenu obavještajnu analizu (SIAC) te NAGLAŠAVA potrebu za izradom sveobuhvatnog pregleda prijetnji iz različitih izvora, uključujući privatni sektor. U tom pogledu POTIČE daljnji razvoj suradnje ENISA-e s ESVD-om, a posebno s INTCEN-om, uz potpuno poštovanje njihovih mandata;

15. ISTIČE da Komisijin centar za situaciju i analizu u kibernetičkom prostoru ima internu funkciju unutar Komisije te da se podupire putem svoje suradnje s ENISA-om i CERT-EU-om. Kako bi se stvorio najveći mogući potencijal za sinergiju i smanjila složenost u kibernetičkom ekosustavu EU-a, POZIVA Komisiju da uzme u obzir rezultate evaluacije Akta o kibersigurnosti i rasprave o evaluaciji Plana za kibernetičku sigurnost kako bi se racionalizirale zadaće Komisijina centra za situaciju i analizu u kibernetičkom prostoru te povezane zadaće ENISA-e. POTIČE Komisiju da izbjegava nepotrebno udvostručavanje zadaća, štiteći pritom središnju ulogu ENISA-e u doprinosu razvoju zajedničke informiranosti o stanju na razini Unije radi potpore državama članicama, uz dužno poštovanje njihovih nacionalnih nadležnosti;

16. NAGLAŠAVA da je razvoj zajedničke informiranosti o stanju preduvjet za pravodobno i učinkovito upravljanje krizama u Uniji kao cjelini. ISTIČE da su na razini EU-a različiti ključni akteri uključeni u **odgovor na kibernetičke incidente velikih razmjera** te da se u slučaju takvih incidenata učinkovita suradnja među državama članicama uglavnom temelji na mreži CSIRT-ova i mreži EU-CyCLONe. ENISA ima važnu ulogu u upravljanju kibernetičkim krizama kao tajništvo mreže CSIRT-ova i mreže EU-CyCLONe. POZIVA Komisiju da iskoristi evaluaciju Plana za kibernetičku sigurnost kako bi se na odgovarajući način uzele u obzir dodatne zadaće i odgovornosti za doprinos razvoju kooperativnog odgovora na prekogranične kibernetičke incidente ili kibernetičke krize velikih razmjera, kao i uloga dodijeljena ENISA-i kao tajništvu mreže CSIRT-ova i mreži EU-CyCLONe te nedavno doneseno zakonodavstvo o kibernetičkoj sigurnosti;

17. ISTIČE važnost organiziranja redovitih **vježbi u području kibernetičke sigurnosti** kojima se znatno povećava pripravnost EU-a za odgovor na incidente i krize. PREPOZNAJE da je ENISA prikupila vrijedno i bogato iskustvo u tom području kojim se podupiru države članice. PREPOZNAJE važnu ulogu ENISA-e u fazama planiranja, pripreme, provedbe i evaluacije vježbi u području kibernetičke sigurnosti te NAGLAŠAVA da bi ona trebala ostati jedan od središnjih aktera na razini EU-a, imajući na umu da bi se takve vježbe trebale provoditi na temelju strukturiranih okvira i zajedničkih terminologija. POZIVA ENISA-u, mrežu CSIRT-ova i mrežu EU-CyCLONe da na najučinkovitiji način iskoriste postojeće redovite vježbe za testiranje i poboljšanje okvira EU-a za odgovor na krizu te da osiguraju maksimalno iskorištavanje stečenih iskustava;

SURADNJE ENISA-E S DRUGIM AKTERIMA U KIBERNETIČKOM EKOSUSTAVU

18. PONAVLJA da je zbog horizontalne prirode kibernetičke sigurnosti ključna **suradnja među svim akterima na razini država članica i Unije** te stoga NAGLAŠAVA da je za povećanje ukupne kibernetičke otpornosti na europskoj razini potreban i zajednički rad ENISA-e i drugih relevantnih subjekata u području kibernetičke sigurnosti;

19. ISTIČE da je sposobnost institucija, tijela, ureda i agencija EU-a da ostanu kibernetički sigurna važna za sveukupnu kibernetičku otpornost na razini EU-a, u čemu je uloga CERT-EU-a neprocjenjiva. U tom pogledu POZDRAVLJA uspostavljenu strukturiranu suradnju između CERT-EU-a i ENISA-e te ih POTIČE da i u budućnosti nastave blisko surađivati;

20. Zahvaljujući postignutoj financijskoj autonomiji Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti znatno će doprinijeti razvoju snažnog europskog istraživačkog, industrijskog i tehnološkog ekosustava u kibernetičkom području, što obuhvaća vještine za razvoj radne snage u skladu s njegovim mandatom. Potiče ENISA-u i Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti da nastave blisko surađivati, posebno u vezi s potrebama i prioritetima u području istraživanja i inovacija, kao i kibernetičkim vještinama, kako bi se povećala konkurentnost Unijine industrije kibernetičke sigurnosti. POZIVA Komisiju da ispita kako se sinergija u radu ENISA-e i Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti može dodatno optimizirati i kako bolje racionalizirati aktivnosti u skladu s njihovim mandatima;

21. ISTIČE da redovito pružanje ažuriranih informacija o prijetnjama doprinosi boljem utvrđivanju mjera i alata potrebnih za učinkovitu borbu protiv kibernetičkog kriminaliteta. NAGLAŠAVA dodanu vrijednost izvješća o EU-ovoj zajedničkoj kibernetičkoj procjeni (J-CAR), koja su rezultat zajedničke suradnje ENISA-e, Europolova Europskog centra za kiberkriminalitet i CERT-EU-a te su već pružila vrijedan doprinos rješavanju različitih izazova, uključujući borbu protiv kibernetičkog kriminaliteta. POZIVA ENISA-u i Europol da nastave strukturiranu suradnju u budućnosti;

22. NAGLAŠAVA da je kibernetička obrana važan element suzbijanja prijetnji koje proizlaze iz kibernetičkog prostora, a taj se element stalno razvija. ISTIČE potrebu da ENISA surađuje s ESVD-om i Komisijom u slučajevima u kojima ENISA ima ulogu u podupiranju provedbe politike kibernetičke obrane EU-a, u bliskoj suradnji s EDA-om, Europskim stručnim centrom za industriju, tehnologiju i istraživanja u području kibersigurnosti i zajednicom za kibernetičku obranu. NAGLAŠAVA ulogu ENISA-e kao civilne agencije. ISTIČE važnost produbljivanja i racionalizacije civilno-vojne suradnje u području kibernetičke sigurnosti u EU-u, uključujući jasnu podjelu uloga i odgovornosti između dviju zajednica te između EU-a i NATO-a, uz potpuno poštovanje načela uključivosti, reciprociteta, uzajamne otvorenosti i transparentnosti, kao i autonomije obiju organizacija u pogledu donošenja odluka. POTIČE ENISA-u da nastavi s radnim dogovorom s Agencijom NATO-a za komunikaciju i informacije;

23. POTIČE EU da nastavi promicati naše zajedničke vrijednosti i zajedničke napore u okviru globalnih foruma kako bi se zaštitio slobodan, globalan, otvoren i siguran kibernetički prostor. NAGLAŠAVA da prekogranična priroda kibernetičkih prijetnji i kibernetičkih incidenata zahtijeva snažnu i učinkovitu suradnju, ne samo na razini EU-a, već i **s međunarodnim organizacijama i partnerima**. NAPOMINJE da bi se međunarodno sudjelovanje ENISA-e trebalo usredotočiti na strateške partnere i zemlje kandidatkinje za članstvo u EU-u, u skladu sa zajedničkom vanjskom i sigurnosnom politikom EU-a. ISTIČE da bi ENISA u okviru svoje međunarodne uključenosti trebala djelovati u skladu sa svojim mandatom i odgovarajućim odredbama Akta o kibersigurnosti. PREPOZNAJE potrebu da se, u skladu s relevantnim postupcima, pojasni međunarodna uključenost ENISA-e, posebno osiguravajući da njezin upravni odbor bude propisno i pravodobno obaviješten o povezanim aktivnostima. POTIČE uključenost ENISA-e u relevantne međunarodne okvire za suradnju u području kibernetičke sigurnosti, uključujući organizacije kao što su NATO i OESS;

24. PONAVLJA da su EU i njegove države članice često isticali nedostatke u **vještinama u području kibernetičke sigurnosti**. PODSJEĆA da su Komisija i ENISA uvele širok i sveobuhvatan okvir za pružanje smjernica svim dionicima, kao što su Europski okvir za vještine u području kibernetičke sigurnosti, Komunikacija o Akademiji za vještine u području kibersigurnosti i Europska konferencija o vještinama u području kibernetičke sigurnosti, koja se svake godine organizira, te POTIČE Komisiju i ENISA-u da se nadovežu na te inicijative, posebno uzimajući u obzir tekuću raspravu o konzorciju za europsku digitalnu infrastrukturu (EDIC). U tu svrhu POZIVA Komisiju da se poveže s državama članicama zainteresiranima za uspostavu EDIC-a. POTVRĐUJE da su ENISA i Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti obvezni promicati vještine u cijeloj Uniji. POZIVA ENISA-u da prednost dâ podupiranju napora država članica u području vještina i obrazovanja, jačanju svijesti opće javnosti i, prema potrebi, suradnji s Europskim stručnim centrom za industriju, tehnologiju i istraživanja u području kibersigurnosti;

25. POTVRĐUJE da je ENISA posljednjih godina razvila **suradnju s privatnim sektorom**. PODSJEĆA da bi, s obzirom na to da privatni sektor kontinuirano prati kibernetičke prijetnje, informacije koje prikuplja industrija mogle doprinijeti poboljšanju zajedničke informiranosti o stanju. Stoga POTIČE ENISA-u da u bliskoj suradnji s državama članicama i svim subjektima EU-a ojača suradnju s privatnim sektorom;

26. POZIVA Komisiju i ENISA-u da razmotre načine za poboljšanje suradnje između ENISA-e i europskih tijela za **normizaciju**. NAGLAŠAVA potrebu da ENISA poveća svoje stručno znanje za europsku normizaciju u području kibernetičke sigurnosti, među ostalim praćenjem normizacijskih aktivnosti i sudjelovanjem u njima;

27. POZIVA Komisiju i ENISA-u da ispitaju kako dodatno optimizirati funkcioniranje okvira EU-a za kibernetičku sigurnost, uzimajući u obzir preporuke i prijedloge iz ovih zaključaka. Stalna suradnja, određivanje prioriteta u pogledu zadaća i resursa te pojednostavnjenje složenog kibernetičkog prostora bit će ključni elementi za suočavanje s trenutačnim i budućim izazovima.