EIROPAS REVĪZIJAS PALĀTA

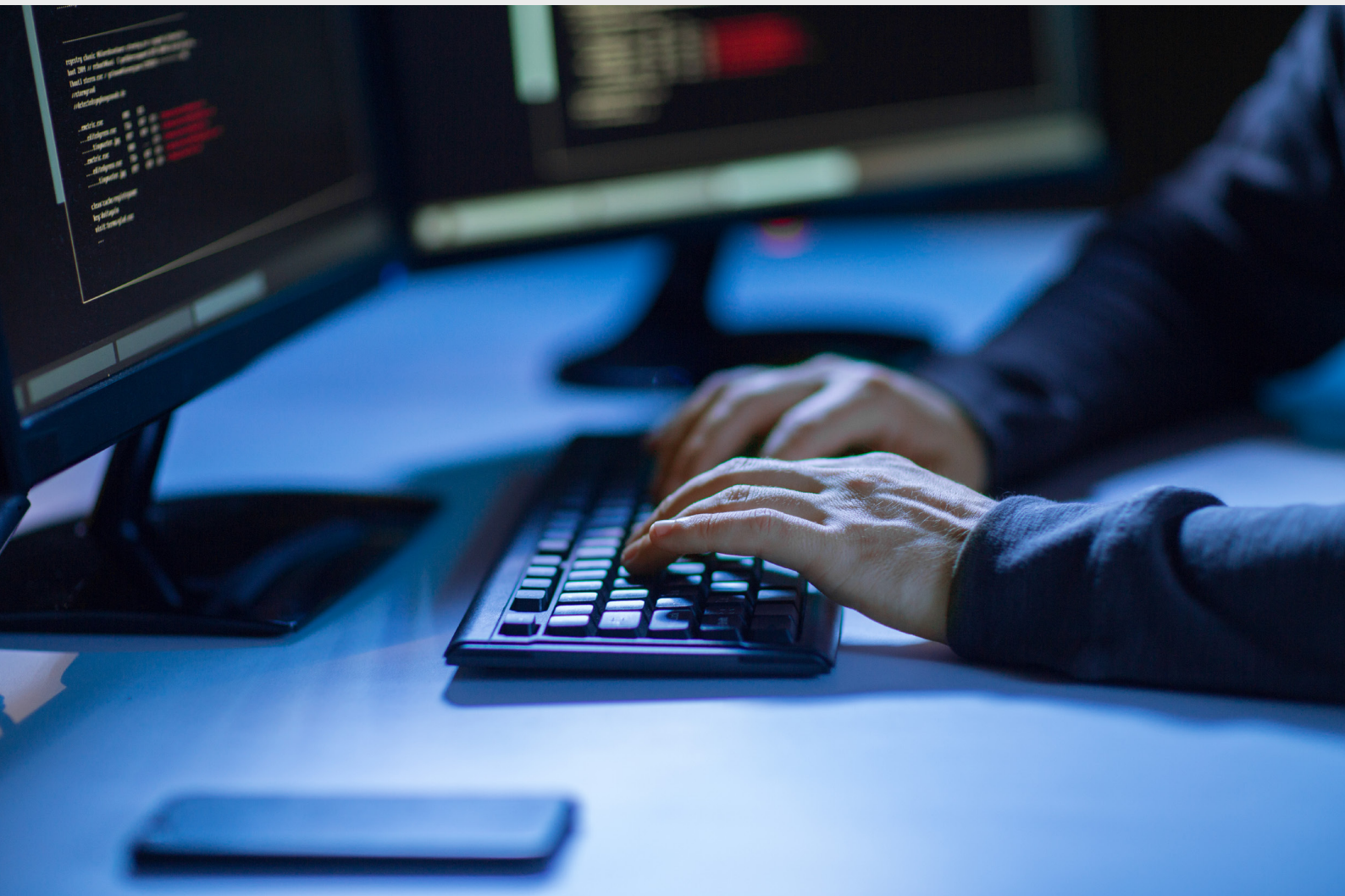
LV

2019

Problēmas, kas traucē īstenot efektīvu ES kiberdrošības politiku

Informatīvais apskats

2019. gada marts



Par apskatu

Šis informatīvais apskats nav revīzijas ziņojums, un tā mērķis ir sniegt pārskatu par sarežģīto situāciju ES kiberdrošības politikas jomā un noteikt galvenās problēmas, kas traucē efektīvi īstenot politiku. Tajā ir skatīti jautājumi, kas attiecas uz tīklu un informācijas drošību, kibernoziedzību, kiberaizsardzību un dezinformāciju. Apskatā iekļautā informācija tiks ņemta vērā arī turpmākajā revīzijas darbā šajā jomā.

Mēs veicām analīzi, pamatojoties uz publiski pieejamo informāciju, kas iekļauta oficiālos dokumentos, nostājas dokumentos un trešo pušu pētījumos. Praktiskais darbs tika veikts no 2018. gada aprīļa līdz septembrim, un ir ņemtas vērā norises līdz 2018. gada decembrim. Papildus šim darbam veicām dalībvalstu revīzijas iestāžu aptauju un iztaujājām galvenās ieinteresētās personas ES iestādēs, kā arī privātā sektora pārstāvjus.

Konstatētās problēmas ir sagrupētas četrās plašās kopās, un tās ir i) politikas satvars, ii) finansējums un tā izlietojums, iii) kibernoturības veidošana un iv) efektīva reaģēšana uz kiberincidentiem. Augstāka kiberdrošības līmeņa nodrošināšana ES joprojām ir ļoti svarīgs uzdevums. Tāpēc katras nodaļas beigās esam formulējuši vairākus jautājumus, ko politikas veidotāji, likumdevēji un praktiķi varētu padziļināti apsvērt.

Mēs vēlamies izteikt atzinību par konstruktīvo atgriezenisko saiti, kas saņemta no Komisijas dienestiem, Eiropas Ārējās darbības dienesta, Eiropas Savienības Padomes, Eiropas Savienības Tīklu un informācijas drošības aģentūras (*ENISA*), Eiropola, Eiropas Kiberdrošības organizācijas un dalībvalstu revīzijas iestādēm.

Saturs

Kopsavilkums

I Tehnoloģijas paver vārtus uz pilnīgi jaunu iespēju pasauli, un jauni produkti un pakalpojumi kļūst par daļu no mūsu ikdienas dzīves. Taču pieaug arī risks kļūt par kibernoziedzības vai kiberuzbrukuma upuri, un šā riska radītā sociālā un ekonomiskā ietekme turpina palielināties. Tādēļ Eiropas Savienības nesenā (2017. gada) ierosme paātrināt centienus kiberdrošības un tās digitālās autonomijas stiprināšanā tika pausta izšķirīgā brīdī.

II Šis informatīvais apskats nav revīzijas ziņojums un tas pamatots uz publiski pieejamo informāciju; tā mērķis ir sniegt pārskatu par sarežģīto un nevienādo situāciju šajā politikas jomā un noteikt galvenās problēmas, kas traucē efektīvi īstenot politiku. Mūsu apskats aptver ES kiberdrošības politiku, kibernoziedzību un kiberaizsardzību, kā arī dezinformācijas apkarošanas centienus. Konstatētās problēmas ir sagrupētas četrās plašās kopās, un tās ir: i) politikas satvars un regulējums, ii) finansējums un tā izlietojums, iii) kibernoturības veidošana un iv) efektīva reaģēšana uz kiberincidentiem. Katrā nodaļā iekļauti vairāki jautājumi pārdomām par minētajām problēmām.

Politikas satvars un tiesiskais regulējums

III Darbību izstrāde atbilstīgi ES kiberdrošības stratēģijas vērienīgajam mērķim kļūt par pasaulē drošāko digitālo vidi ir grūts uzdevums, jo nav noteikti izmērāmi mērķi un trūkst uzticamu datu. Rezultātus nosaka reti, un izvērtētas ir tikai dažas politikas jomas. Tādēļ būtisks uzdevums ir **nodrošināt jēgpilnu pārskatatbildību un izvērtēšanu**, ieviešot uz rezultātiem vērstu pieeju ar integrētu izvērtēšanas praksi.

IV Tiesiskais regulējums joprojām ir nepilnīgs. **ES tiesību aktu nepilnības un to nekonsekventa transponēšana** var apgrūtināt tiesību aktu potenciāla pilnvērtīgu izmantošanu.

Finansējums un tā izlietojums

V **Ieguldījumu līmeņa pielāgošana mērķiem** ir sarežģīts uzdevums — lai to veiktu, ir jāpalielina ne tikai kopējie ieguldījumi kiberdrošības jomā, kuri ES ir bijuši nelieli un sadrumstaloti, bet arī to ietekme, it īpaši, labāk izmantojot pētniecības izdevumu sniegtos rezultātus un nodrošinot efektīvu atbalstu un finansējumu jaunuzņēmumiem.

VI Ir būtiski, lai ES un tās dalībvalstis **gūtu skaidru priekšstatu par ES finansējuma izlietojumu** — tādējādi tās varētu apzināt trūkumus, kas traucē sasniegt to noteiktos

mērķus. Tā kā nav paredzēts īpašs ES finansējums kiberdrošības stratēģijas finansēšanai, nav iespējams gūt skaidru priekšstatu par finansējuma izlietojumu.

VII Laikā, kad lielāka vērība tiek pievērsta ar drošību saistītām politikas prioritātēm, **ES kiberjomas aģentūru resursu nepietiekamība** var liegt iespēju sasniegt ES mērķus. Viens no šīs problēmas risinājumiem ir rast veidus, kā piesaistīt un saglabāt talantīgus darbiniekus.

Kibernoturības veidošana

VIII Kiberdrošības pārvaldības trūkumi publiskajā un privātajā sektorā ir bieži sastopami ne tikai ES, bet arī starptautiskā līmenī. Tie mazina pasaules sabiedrības spēju reaģēt uz kiberuzbrukumiem un ierobežot tos, kā arī apdraud saskaņotas ES mēroga pieejas izmantošanu. Tādēļ uzdevums ir **uzlabot kiberdrošības pārvaldību**.

IX **Prasmju un izpratnes vairošanai** visās nozarēs un sabiedrības līmeņos ir izšķiroša nozīme, ņemot vērā arvien pieaugošo kiberdrošības prasmju trūkumu pasaulē. ES mēroga standarti apmācības, sertifikācijas vai kiberriska izvērtēšanas jomā patlaban ir ierobežoti.

X Lai stiprinātu vispārējo kibernoturību, ir svarīgi veidot uzticību. Komisija ir konstatējusi, ka koordinācija kopumā joprojām ir nepietiekama. **Informācijas apmaiņas un koordinēšanas uzlabošana** publiskā un privātā sektora starpā joprojām ir aktuāls uzdevums.

Efektīva reaģēšana uz kiberincidentiem

XI Digitālās sistēmas ir kļuvušas tik sarežģītas, ka visus uzbrukumus novērst nav iespējams. Šīs problēmas risinājums ir **ātra atklāšana un reaģēšana**. Taču kiberdrošība joprojām nav pilnībā integrēta pašreizējos ES līmeņa krīzes reakcijas koordinācijas mehānismos, un tādējādi, iespējams, tiek ierobežota Savienības spēja reaģēt uz plaša mēroga pārrobežu kiberincidentiem.

XII Ļoti svarīga nozīme ir **kritiskās infrastruktūras un sabiedrības funkciju aizsardzībai**. Būtiskas problēmas rada iespējamā iejaukšanās vēlēšanu procesos un dezinformācijas kampaņas.

XIII Kiberdraudu radītās aktuālās problēmas ES un plašākā globālajā vidē nosaka nepieciešamību pastāvīgi uzņemties saistības un nelokāmi ievērot ES pamatvērtības.

Ievads

01 Tehnoloģijas paver vārtus uz pilnīgi jaunu iespēju pasauli. Jauni produkti un pakalpojumi, kas tiek ieviesti, kļūst par daļu no mūsu ikdienas dzīves. Taču līdz ar katru jauno atklājumu palielinās mūsu tehnoloģiskā atkarība un attiecīgi arī kiberdrošības nozīme. Jo vairāk personas datu mēs publiskojam tiešsaistē un jo ciešāk esam savienoti tīklā, jo vairāk palielinās iespēja kļūt par kibernozieguma vai kiberuzbrukuma upuriem.

Kas ir kiberdrošība?

02 Nav standarta vispārpieņemtas kiberdrošības definīcijas[1]. Plašākā nozīmē kiberdrošība ir visas garantijas un pasākumi, kas pieņemti, lai aizsargātu informācijas sistēmas un to lietotājus pret neatļautu piekļuvi, uzbrukumiem un bojājumiem, lai nodrošinātu to konfidencialitāti, integritāti un pieejamību.

03 Kiberdrošība ietver kiberincidentu novēršanu un atklāšanu, reaģēšanu uz tiem un to seku pārvarēšanu. Incidenti var būt tīši vai netīši, un tie var būt dažādi, piemēram, gan informācijas nejauša izpaušana, gan arī uzbrukumi uzņēmumiem un kritiskai infrastruktūrai, personas datu zādzība un pat iejaukšanās demokrātiskos procesos. Visiem šiem incidentiem var būt plaša negatīva ietekme uz personām, organizācijām un kopienām.

04 Kiberdrošība kā termins, ko lieto ES politikas veidotāju aprindās, neattiecas tikai uz tīklu un informācijas drošību. Kiberdrošība attiecas uz visām nelikumīgām darbībām, kas saistītas ar digitālo tehnoloģiju izmantošanu kibertelpā. Tādējādi kiberdrošība var attiekties arī uz tādiem kibernoziegumiem kā uzbrukumu organizēšana, izmantojot datorvīrusus, un ar bezskaidras naudas maksājumiem saistīta krāpšana, un kiberdrošība var aptvert dažādas sistēmas un saturu, piemēram, kā gadījumā, ja tiešsaistē tiek izplatīti materiāli par bērnu seksuālo izmantošanu. Kiberdrošība var attiekties arī uz dezinformācijas kampaņām ar mērķi ietekmēt debates tiešsaistē un iespējamu iejaukšanos vēlēšanu norisē. Turklāt Eiropols uzskata, ka pastāv saistība starp kibernoziedzību un terorismu[2].

05 Dažādi spēki, tostarp valstis, noziedzīgi grupējumi un hakeraktīvisti, izraisa kiberincidentus dažādu apsvērumu dēļ. Šādu incidentu sekas jūtamas valsts, Eiropas un pat pasaules līmenī. Taču, ņemot vērā to, ka internetam lielākoties nav robežu un tajā tiek izmantoti nemateriāli līdzekļi un taktika, bieži vien ir ļoti grūti atklāt uzbrukuma rīkotāju (tā dēvētā attiecinājuma problēma).

06 Kiberdrošības draudu dažādos veidus var klasificēt, pamatojoties uz to, kā tiek izmantoti dati, proti, izpaušana, sagrozīšana, iznīcināšana vai piekļuves liegšana, vai arī, ņemot vērā to, kādi informācijas aizsardzības pamatprincipi tiek pārkāpti, — sk. ***1. attēlu***. Daži uzbrukumu piemēri aprakstīti ***1. izcēlumā***. Tā kā uzbrukumi informācijas sistēmām kļūst arvien rafinētāki, mūsu aizsardzības mehānismu efektivitāte samazinās[3].

1. attēls. Draudu veidi un drošības principi, ko tie apdraud

Avots: ERP pielāgota informācija, pamatojoties uz Eiropas Parlamenta pētījumu[4]. Slēdzene = drošība nav apdraudēta; Izsaukuma zīme =drošība apdraudēta.

1. izcēlums

Kiberuzbrukumu veidi

Katru reizi, kad jauna ierīce tiek pieslēgta internetam vai savienota ar citām ierīcēm, palielinās tā dēvētais kiberdrošības uzbrukumu apmērs. Lietu interneta, mākoņdatošanas, lielo datu un rūpniecības digitalizācijas eksponenciāla attīstība palielina neaizsargātības risku un dod iespēju ļaunprātīgiem spēkiem uzbrukt arvien lielākam skaitam upuru. Ņemot vērā uzbrukumu daudzveidību un to arvien pieaugošo rafinētību, ir patiešām grūti iet kopsolī ar pārmaiņām[5].

Ļaunatūra (ļaunprogrammatūra) ir izstrādāta, lai kaitētu ierīcēm vai tīkliem. Tā var ietvert vīrusus, Trojas zirgus, izspiedējprogrammatūru, datortārpus, reklāmprogrammatūru un spiegprogrammatūru. **Izspiedējprogrammatūra** šifrē datus, liedzot lietotājiem piekļūt savām datnēm, līdz tiek samaksāta izpirkuma maksa — parasti kriptovalūtā — vai veikta darbība. Saskaņā ar Eiropola sniegto informāciju uzbrukumi, izmantojot izspiedējprogrammatūru, tiek veikti visbiežāk, turklāt pēdējos dažos gados būtiski ir palielinājies izspiedējprogrammatūras veidu skaits. Palielinās **izkliedētā pakalpojumu atteikuma** uzbrukumu (*DDoS*) skaits — šādos gadījumos pakalpojumi vai resursi kļūst nepieejami, jo tos ir pārpludinājuši vairāk pieprasījumu, nekā iespējams apstrādāt; 2017. gadā šādi uzbrukumi bija vērsti pret vienu trešo daļu organizāciju[6].

Lietotājus var ietekmēt, liekot viņiem neapzināti veikt kādu darbību vai izpaust konfidenciālu informāciju. Šo viltīgo paņēmienu var izmantot, lai veiktu datu zādzību vai datorspiegošanu, un šādas darbības sauc par **sociālo inženieriju**. Tiek izmantotas dažādas metodes, lai to panāktu, — plaši izmantota metode ir **pikšķerēšana**, ko īsteno tā, ka lietotāji saņem e-pasta vēstules no šķietami uzticamiem avotiem ar aicinājumu izpaust informāciju vai atvērt saites, kas inficē ierīces ar lejuplādētu ļaunatūru. Vairāk nekā puse dalībvalstu ziņoja par to, ka veikušas izmeklēšanas par uzbrukumiem tīkliem[7].

Iespējams, nekrietnākais draudu veids ir **attīstīts pastāvīgs apdraudējums** (APA). To rada pieredzējuši uzbrucēji, kas veic ilgtermiņa uzraudzību un zog datus, un reizēm ir iecerējuši sasniegt postošus mērķus. Šādu darbību nolūks ir pēc iespējas ilgāk palikt nepamanītam. APA nereti ir saistīts ar valsts darbību un vērsts uz īpaši jutīgām nozarēm, piemēram, tehnoloģijām, aizsardzību un kritisko infrastruktūru. Tiek uzskatīts, ka datorspiegošana veido vismaz vienu ceturtdaļu visu kiberincidentu un rada lielāko daļu izmaksu[8].

Problēmas apmērs

07 Ir sarežģīti izvērtēt ietekmi, ko rada nepietiekama sagatavotība kiberuzbrukumiem, jo trūkst uzticamu datu. Laikposmā no 2013. līdz 2017. gadam kibernoziedzības ekonomiskā ietekme palielinājās piecas reizes[9], radot zaudējumus

valdībām un uzņēmumiem — gan lieliem, gan arī maziem. Kiberapdrošināšanas prēmiju prognozētais pieaugums no 3 miljardiem EUR 2018. gadā līdz 8,9 miljardiem EUR 2020. gadā apstiprina šo tendenci.

08 Kiberuzbrukumu finansiālā ietekme turpina palielināties, turklāt pastāv satraucošas atšķirības starp izmaksām, kas rodas saistībā ar uzbrukuma organizēšanu, un novēršanas, izmeklēšanas un seku mazināšanas izmaksām. Piemēram, izkliedētā pakalpojumu atteikuma uzbrukuma veikšanas izmaksas var būt tikai 15 EUR mēnesī, savukārt uzņēmumam, kuram veikts uzbrukums, radītie zaudējumi, tostarp kaitējums reputācijai, ir ievērojami lielāki[10].

09 Lai gan 80 % ES uzņēmumu 2016. gadā piedzīvoja vismaz vienu kiberdrošības incidentu[11], risku apzināšanas līmenis joprojām ir satraucoši zems. No visiem ES uzņēmumiem 69 % nav zināšanu vai ir tikai pamatzināšanas par to, cik lielā mērā tie pakļauti kiberdraudiem[12], un 60 % uzņēmumu nekad nav aprēķinājuši iespējamos finansiālos zaudējumus[13]. Turklāt pasaules mēroga apsekojuma rezultāti rāda, ka viena trešdaļa organizāciju drīzāk maksātu hakera pieprasītu maksu, nevis veiktu ieguldījumus informācijas drošības jomā[14].

10 *Wannacry* izspiedējprogrammatūras un *NotPetya* iznīcinātājļaunatūras pasaules mēroga uzbrukumi 2017. gadā ietekmēja vairāk nekā 320 000 lietotājus aptuveni 150 valstīs[15]. Šie incidenti zināmā mērā pievērsa visas pasaules uzmanību kiberuzbrukumu radītajiem draudiem, dodot jaunu impulsu kiberdrošību integrēt galveno politikas virzienu veidošanā. Turklāt 86 % ES iedzīvotāju patlaban uzskata, ka risks kļūt par kibernoziedzības upuri palielinās[16].

ES darbība kiberdrošības jomā

11 ES 2001. gadā kļuva par Eiropas Padomes Konvencijas par kibernoziegumiem (Budapeštas konvencijas) komitejas novērotājorganizāciju[17]. Kopš tā laika ES ir izmantojusi politiku, tiesību aktus un finansējumu, lai uzlabotu savu kibernoturību. Ņemot vērā to, ka vērienīgi kiberuzbrukumi un incidenti notiek arvien biežāk, kopš 2013. gada procesi noris ātrāk, kā redzams ***2. attēlā***. Vienlaikus dalībvalstis ir pieņēmušas (dažos gadījumos pat jau atjauninājušas) savas kiberdrošības sākotnējās stratēģijas.

12 Galvenie ES dalībnieki, kas atbildīgi par kiberdrošību, ir minēti ***2. zcēlumā*** un ***I pielikumā***.

2. izcēlums

Iesaistītās puses

Eiropas Komisijas mērķis ir uzlabot spējas un sadarbību kiberdrošības jomā, stiprināt ES kā kiberdrošības veicinātāju un integrēt kiberdrošību citās ES politikas jomās. Galvenie ģenerāldirektorāti, kas ir atbildīgi par kiberdrošības politiku, ir **Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts (CNECT ĢD)** (kiberdrošība) un **Migrācijas un iekšlietu ģenerāldirektorāts (HOME ĢD)** (kibernoziedzība) — tie ir atbildīgi attiecīgi par digitālo vienoto tirgu un drošības savienību. **Informātikas ģenerāldirektorāts (DIGIT ĢD)** ir atbildīgs par Komisijas sistēmu informācijas un tehnoloģiju drošību.

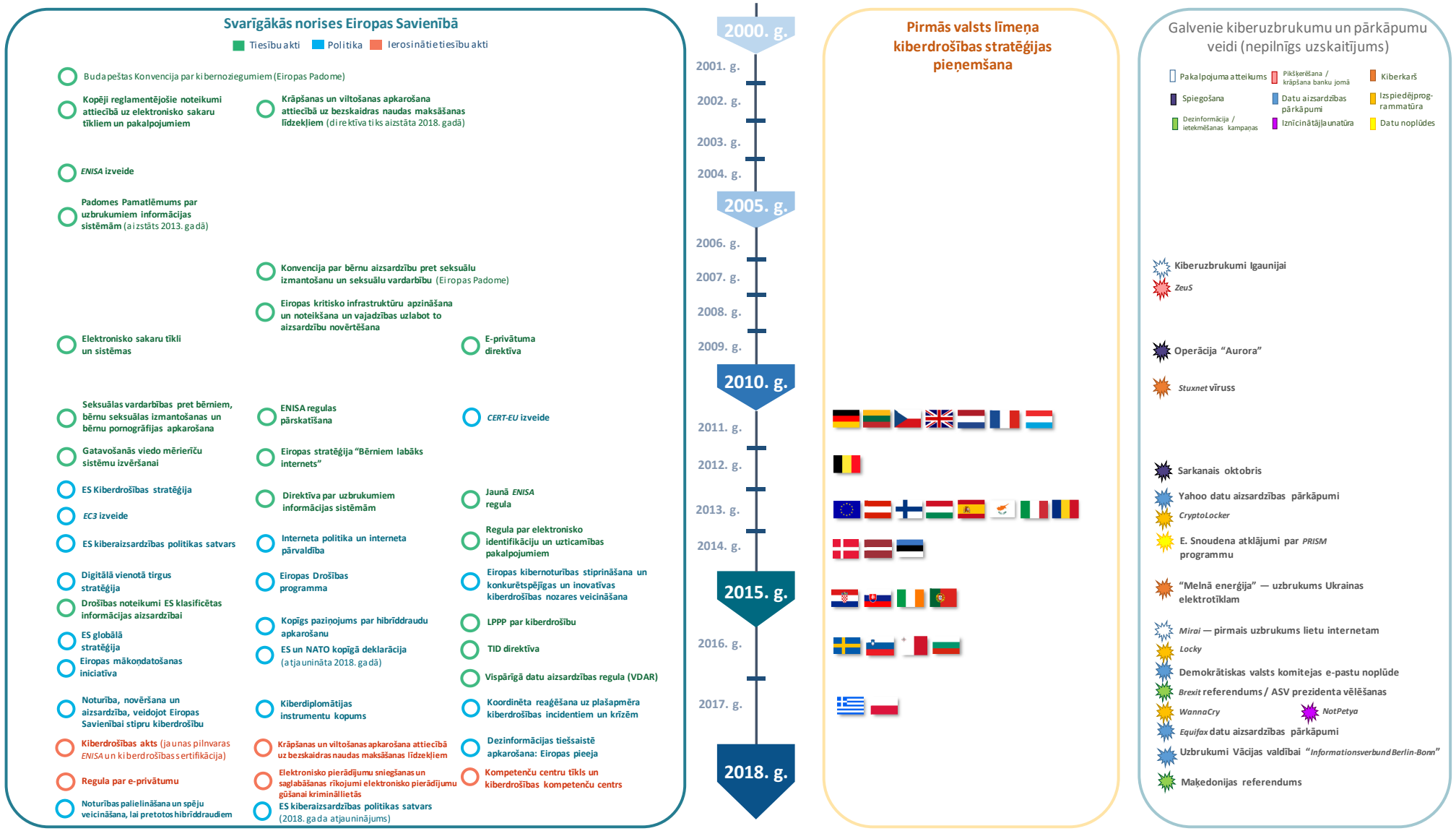
Liela daļa ES aģentūru atbalsta Komisiju, it īpaši ***ENISA*** (Eiropas Savienības Tīklu un informācijas drošības aģentūra) un ES Kiberdrošības aģentūra —galvenokārt padomdevēja struktūra, kas sniedz atbalstu politikas izstrādē, kā arī spēju un izpratnes veidošanā. Eiropola Eiropas Kibernoziedzības apkarošanas centru (***EC3***) izveidoja, lai uzlabotu ES tiesībaizsardzības iestāžu spēju reaģēt uz kibernoziedzību. Datorapdraudējumu reaģēšanas vienība (***CERT-EU***), kas sniedz atbalstu visām Savienības iestādēm, struktūrām un aģentūrām, veic darbu Komisijas telpās.

Eiropas Ārējās darbības dienests (EĀDD) vada darbu kiberaizsardzības, kiberdiplomātijas un stratēģiskās komunikācijas jomā, un tā pakļautībā strādā izlūkošanas un analīzes centri. **Eiropas Aizsardzības aģentūras** (EAA) mērķis ir veidot kiberaizsardzības spējas.

Dalībvalstis galvenokārt ir atbildīgas par savu kiberdrošību un ES līmenī rīkojas ar **Padomes** starpniecību, kurai pakļautas vairākas koordinēšanas un informācijas apmaiņas struktūras (cita starpā Kiberjautājumu horizontālā darba grupa). **Eiropas Parlaments** ir viens no likumdevējiem.

Privātā sektora organizācijas, tostarp nozares pārstāvji, interneta pārvaldības struktūras un akadēmiskās aprindas ir gan partneri, gan arī piedalās politikas veidošanā un īstenošanā, tostarp izmantojot līgumisku publiskā un privātā sektora partnerību (**LPPP**).

2. attēls. Politikas veidošanas un likumdošanas ātrāka norise (situācija 2018. gada 31. decembrī)



Avots: Eiropas Revīzijas palāta.

Politika

13 ES kibertelpas ekosistēma ir sarežģīta, un to veido vairāki līmeņi, turklāt uz to attiecas vairākas iekšpolitikas jomas, piemēram, tieslietas un iekšlietas, kā arī digitālā satura vienotā tirgus un pētniecības politika. Ārpolitikā kiberdrošība tiek ņemta vērā diplomātijā, un tai ir arvien būtiskāka nozīme ES jaunajā aizsardzības politikā.

14 ES politikas stūrakmens ir **2013. gada Kiberdrošības stratēģija**[18]. Stratēģijas mērķis ir panākt, lai ES digitālā vide kļūtu par drošāko pasaulē, vienlaikus aizsargājot pamatvērtības un brīvības. Stratēģijas pieci galvenie mērķi ir šādi: i) stiprināt kibernoturību; ii) mazināt kibernoziedzību; iii) veidot kiberaizsardzības politiku un spējas; iv) palielināt rūpnieciskos un tehnoloģiskos kiberdrošības resursus, kā arī v) veidot starptautisku kibertelpas politiku atbilstīgi ES pamatvērtībām.

15 Kiberdrošības stratēģija ir savstarpēji saistīta ar trim vēlāk pieņemtām stratēģijām, un tās ir:

— **Eiropas Drošības programma** (2015. gads) — tās mērķis ir uzlabot tiesībaizsardzību un tiesisko reaģēšanu uz kibernoziegumiem, galvenokārt atjauninot esošos politikas dokumentus un tiesību aktus[19]. Tās uzdevumi ir arī konstatēt šķēršļus kibernoziegumu kriminālizmeklēšanai un veicināt spēju veidošanu kiberaizsardzības jomā;

— **Digitālā vienotā tirgus stratēģija**[20] (2015. gads) — tās mērķis ir nodrošināt labāku piekļuvi digitālajām precēm un pakalpojumiem, nodrošinot piemērotus apstākļus, lai pēc iespējas palielinātu digitālās ekonomikas izaugsmes potenciālu. Šai sakarā būtiska nozīme ir drošības, uzticēšanās un iekļautības veicināšanai tiešsaistē;

— ES 2016. gada **globālā stratēģija**[21] — tās mērķis ir palielināt ES ietekmi pasaulē; kiberdrošība ir viens no pamatuzdevumiem, ko veic, atjaunojot apņemšanos risināt kiberjautājumus, īstenojot sadarbību ar nozīmīgiem partneriem un apņemoties risināt kiberjautājumus visās politikas jomās, tostarp atspēkot dezinformāciju, izmantojot stratēģisku komunikāciju.

16 Tā kā pēdējos gados kibertelpa ir kļuvusi arvien lielākā mērā militarizēta[22] un tiek izmantota kā ierocis[23], to uzskata par piekto karadarbības vidi[24]. Kiberaizsardzība sargā kibertelpas sistēmas, tīklus un kritisko infrastruktūru pret militāriem un cita veida uzbrukumiem. ES **kiberaizsardzības politikas satvaru** pieņēma 2014. gadā un atjaunināja 2018. gadā[25]. Veicot tā atjauninājumu 2018. gadā, tika noteiktas sešas prioritātes, tostarp kiberaizsardzības spēju uzlabošana, kā arī ES kopējās drošības un

aizsardzības politikas (KDAP) komunikācijas un informācijas tīklu aizsardzība. Kiberaizsardzība ir iekļauta arī pastāvīgās strukturētās sadarbības (*PESCO*) satvarā un ES un NATO sadarbībā.

17 ES **kopīgais regulējums hibrīddraudu apkarošanai** (2016. gads) tiek piemērots, lai apkarotu kiberdraudus gan kritiskai infrastruktūrai, gan arī lietotājiem privātajā sektorā, un tajā uzsvērts, ka kiberuzbrukumus var rīkot, īstenojot arī dezinformācijas kampaņas sociālajos plašsaziņas līdzekļos[26]. Šajā regulējumā arī ņemta vērā nepieciešamība vairot izpratni un uzlabot ES un NATO sadarbību, kā tika uzsvērts ES un NATO 2016. un 2018. gada kopīgajās deklarācijās[27].

18 Tā kā arvien aktuālāks kļūst jautājums par aizsardzības nodrošināšanu digitālajā telpā, Komisija 2017. gadā iesniedza jaunu kiberdrošības paketi. Šī pakete ietvēra jaunu Komisijas paziņojumu par 2013. gada kiberdrošības stratēģijas atjaunināšanu[28] un plānu ātrai un koordinētai reaģēšanai uz liela mēroga uzbrukumiem un Tīklu un informācijas drošības direktīvas (TID direktīva)[29] ātrai īstenošanai. Pakete ietvēra arī vairākus tiesību aktu priekšlikumus (sk. ***22.*** punktu).

Tiesību akti

19 Kopš 2002. gada ir pieņemti tiesību akti ar atšķirīgu ietekmi uz kiberdrošību.

20 Galvenais tiesību akts, uz ko balstās 2013. gada kiberdrošības stratēģija, ir 2016. gada **Tīklu un informācijas drošības (TID) direktīva**[30] — pirmais ES mēroga tiesību akts kiberdrošības jomā. Šī direktīva, kuras transponēšanas termiņš bija 2018. gada maijs, tiecas nodrošināt saskaņotu spēju minimālo līmeni, uzliekot pienākumu dalībvalstīm pieņemt valsts TID stratēģijas un izveidot vienotus kontaktpunktus un datordrošības incidentu reaģēšanas komandas (*CSIRT*)[31]. Direktīva paredz arī drošības un paziņošanas prasības pamatpakalpojumu sniedzējiem īpaši svarīgās nozarēs un digitālo pakalpojumu sniedzējiem.

21 Vienlaikus — 2016. gadā — stājās spēkā **Vispārīgā datu aizsardzības regula**[32] (VDAR), ko piemēro no 2018. gada maija. Tās mērķis ir aizsargāt Eiropas iedzīvotāju personas datus, formulējot noteikumus par to apstrādi un izplatīšanu. Regula paredz konkrētas tiesības datu subjektiem un pienākumus datu pārziņiem (digitālo pakalpojumu sniedzējiem) attiecībā uz informācijas izmantošanu un nodošanu. Regula paredz arī prasības ziņot par pārkāpumiem un iespēju dažos gadījumos piemērot sankcijas. ***3. attēlā*** redzams, kā TID direktīva un VDAR papildina viena otru, ņemot vērā to mērķus stiprināt kiberdrošību un nodrošināt datu aizsardzību.

22 Daži no tiesību aktu projektiem, kas patlaban tiek izskatīti, ir ierosinātais Kiberdrošības akts ar mērķi stiprināt *ENISA* un izveidot ES mēroga sertifikācijas mehānismu[33], ierosinātā regula par elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem[34] un ierosinātā direktīva par elektroniskajiem pierādījumiem[35]. 2018. gadā sagatavotais priekšlikums par Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra izveidi un Nacionālo koordinācijas centru tīkla izveidi (turpmāk — "kiberdrošības kompetenču centru tīkls un pētnieciskais kompetenču centrs") ir daļa no 2017. gada kiberdrošības paketes[36].

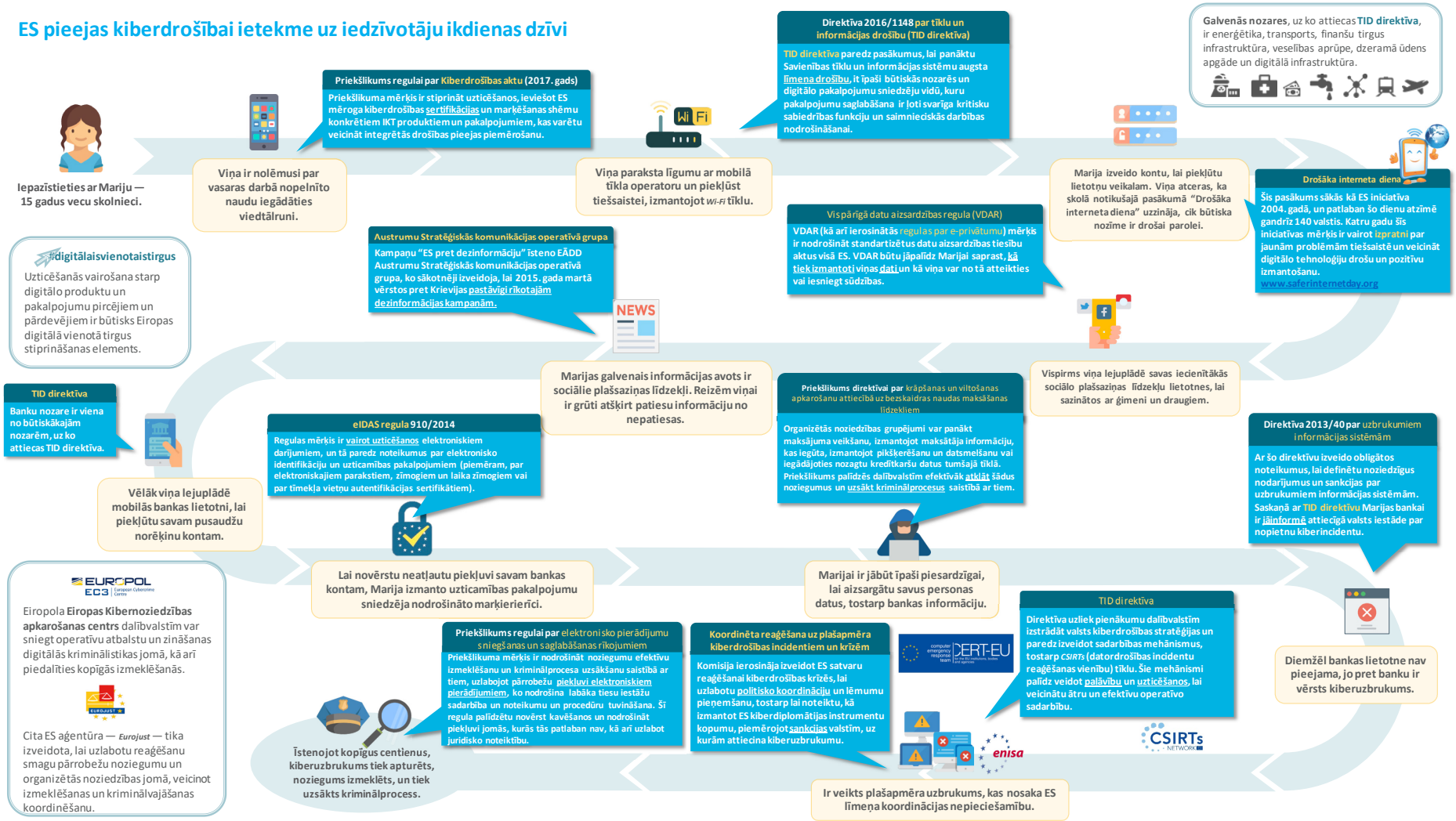
23 Var būt sarežģīti gūt pilnīgu priekšstatu par kiberdrošības politikas satvara un regulējuma tvērumu un par to, kā tas ietekmē mūsu ikdienas dzīvi.

24 Dažādu tiesību aktu un citu darbību ietekme uz iedomāta Eiropas iedzīvotāja dzīvi ir ieskicēta ***4. attēlā***.

3. attēls. VDAR un TID direktīvas savstarpējā papildināmība

Avots: Eiropas Revīzijas palāta.

4. attēls. ES pieejas kiberdrošībai ietekme uz iedzīvotāju ikdienas dzīvi



Avots: Eiropas Revīzijas palāta.

Politikas satvara veidošana un tiesiskā regulējuma izstrāde

25 ES kibertelpas ekosistēma ir sarežģīta vairāklīmeņu struktūra, kurā iesaistītas daudzas ieinteresētās personas (sk. ***I pielikumu***). Visu tās būtiski atšķirīgo elementu apvienošana ir ļoti grūts uzdevums. Kopš 2013. gada tiek veikti vienoti centieni panākt saskaņotību ES kiberdrošības jomā[37].

1. problēma —jēgpilna izvērtēšana un pārskatatbildība

26 Komisija ir konstatējusi, ka ir sarežģīti pierādīt cēloņsakarības starp 2013. gada stratēģiju un notikušajām pārmaiņām. 2013. gada stratēģijas mērķu formulējums bija ļoti vispārīgs, proti, "drīzāk bija noteikts redzējums, nevis izmērāmi mērķi"[38]. Tā kā nav noteikti izmērāmi mērķi, ir sarežģīti plānot šādam plašam redzējumam atbilstīgu darbību. Atjauninātā kiberaizsardzības politikas satvara (2018. gads) uzdevums ir izstrādāt mērķus, lai panāktu minimālo kiberdrošības līmeni un uzticēšanos. Taču tas attieksies tikai uz kiberaizsardzību; mērķi, ar ko paredz vēlamo kopējo ES noturības līmeni, nav noteikti.

27 Rezultātus novērtē reti, un izvērtētas ir tikai dažas politikas jomas[39]. Daļēji šāda situācija radusies tāpēc, ka daudzi pasākumi — likumdošanas vai citi — ir īstenoti nesen un to ietekmes pilnīga izvērtēšana ir apgrūtināta. Būtu jānosaka jēgpilni izvērtēšanas kritēriji, kas var palīdzēt izvērtēt ietekmi. Turklāt rūpīga izvērtēšana kiberdrošības jomā kopumā vēl nav kļuvusi par normu. Tādēļ ir jāmaina pieeja, lai tā būtu vērsta uz rezultātiem, ar integrētu izvērtēšanas praksi un standartizētām ziņošanas prasībām. *ENISA* pašreizējās pilnvaras neietver ES kiberdrošības un gatavības izvērtēšanu un uzraudzību.

28 Uz pierādījumiem balstīta politikas veidošana ir atkarīga no pietiekamu un uzticamu datu un statistikas pieejamības, kas palīdz uzraudzīt un analizēt tendences un vajadzības. Tā kā nav ieviesta obligāti izmantojama un kopēja uzraudzības sistēma, trūkst arī uzticamu datu. Rādītāji bieži vien nav pieejami, un tos ir grūti noteikt[40]. Dažās jomās īpaši rādītāji tomēr ir izstrādāti, piemēram, ES politikas cikls, ko izmanto smagu noziegumu un organizētas noziedzības apkarošanai.

29 Tikai dažas dalībvalstis regulāri vāc oficiālus datus par kiberjomu, un šāda situācija traucē nodrošināt salīdzināmību. ES līdz šim ir reti norādījusi uz nepieciešamību konsolidēt statistiku Eiropas līmenī[41]. Turklāt ir pieejami tikai daži neatkarīgi ES mēroga

pētījumi par būtiskiem jautājumiem, tādiem kā[42] kiberdrošības ekonomika, ietverot rīcības aspektus (stimulu nesaskaņotību, informācijas asimetriju), kiberincidentu un kibernoziedzības ietekmes apzināšana, makrostatistika par tendencēm un gaidāmajām problēmām kiberjomā, kā arī labākie risinājumi draudu mazināšanai.

30 Tā kā nav noteikti konkrēti mērķi un ir pieejami tikai ierobežoti uzticami dati un skaidri noteikti rādītāji, līdz šim stratēģijas īstenošanas rezultātu izvērtēšana ir bijusi galvenokārt kvantitatīva. Progresa ziņojumos bieži aprakstītas veiktās darbības vai sasniegtie starpposma mērķrādītāji, taču nav veikta rezultātu rūpīga izvērtēšana. Arī atsauces scenārijs sistēmu noturības izvērtēšanai joprojām nav noteikts. Turklāt, tā kā nav pieņemta kodificēta kibernoziedzības definīcija, ir gandrīz neiespējami atrast atbilstīgus Eiropas rādītājus, kas būtu noderīgi uzraudzības un izvērtēšanas veikšanai.

31 Kiberdrošības politikas īstenošanas neatkarīga uzraudzība dalībvalstīs atšķiras. Mēs aptaujājām valstu revīzijas iestādes par to pieredzi revīziju veikšanā šajā jomā. Puse respondentu[43] nekad nebija revidējuši šo jomu. Tie respondenti, kuri šādas revīzijas bija veikuši, galvenokārt lika uzsvaru uz informācijas pārvaldību, kritiskās infrastruktūras aizsardzību, informācijas apmaiņu un koordināciju galveno ieinteresēto personu starpā, kā arī uz gatavību incidentiem, informēšanu par tiem un reaģēšanu. Retāk tika veiktas revīzijas saistībā ar tādiem jautājumiem kā izpratnes vairošanas pasākumi un digitālo prasmju trūkums. Šādu revīziju vai izvērtējumu rezultāti ne vienmēr tiek publiskoti ar valsts drošību saistītu apsvērumu dēļ. Valstu revīzijas iestāžu publicēto revīzijas ziņojumu saraksts pievienots ***III pielikumā***.

32 Ar kiberjomu saistīto prasmju ierobežojumi (sk. arī ***82.–90. punktu***) un grūtības kiberdrošības progresa izvērtēšanā tika minētas kā galvenās problēmas, lai veiktu revīziju par valsts īstenotajiem pasākumiem šajā jomā.

2. problēma — ES tiesību aktu nepilnību novēršana un nevienāda transponēšana

33 Jaunu tehnoloģiju ieviešanas un draudu rašanās ātrums krietni pārsniedz ES tiesību aktu izstrādes un īstenošanas tempu. Izstrādājot Savienības procedūras, netika ņemta vērā digitālā laikmeta ietekme — augstākā prioritāte jāpiešķir inovatīvu un elastīgu procedūru izstrādei, lai nodrošinātu tādu politiku un tiesisko regulējumu, kas atbilst mērķim[44] labāk sagatavoties un veidot nākotni[45].

34 Neskatoties uz centieniem panākt lielāku saskaņotību, tiesiskais regulējums kiberdrošības jomā joprojām ir nepilnīgs (vairāki piemēri minēti ***1. tabulā***). Sadrumstalotība un nepilnības traucē sasniegt vispārējos politikas mērķus un mazina efektivitāti. Stratēģijas izvērtēšanas laikā Komisija cita starpā konstatēja nepilnības saistībā ar lietu internetu un atbildības sadalījumu digitālo produktu lietotāju un piedāvātāju starpā, kā arī saistībā ar vairākiem jautājumiem, kuri netika atrisināti, pieņemot TID direktīvu. Ierosinātais Kiberdrošības akts ir mēģinājums novērst šīs nepilnības, veicinot integrētās drošības ieviešanu, ko nodrošinās ES mēroga sertifikācijas shēma. Vairākas ieinteresētās personas uzskata, ka joprojām trūkst skaidri noteiktas kiberaizsardzības rūpniecības politikas un kopīgas pieejas kiberspiegošanai[46].

1. tabula. Tiesiskā regulējuma nepilnības un nevienāda transponēšana (tabula nav pilnīga)

Politikas joma	Piemēri
Digitālais vienotais tirgus	o Spēkā esošās Patēriņa preču pārdošanas direktīvas piemērošanas joma neaptver kiberdrošību. Ierosināto direktīvu par digitālo saturu[47] un tiešsaistes pārdošanu[48] mērķis ir novērst šo nepilnību. o ES dalībvalstu tiesiskais regulējums attiecībā uz rūpības pienākumu ir ierobežots un atšķirīgs, tādējādi vairojot juridisko nenoteiktību un apgrūtinot tiesiskās aizsardzības līdzekļu izmantošanu[49]. o Dalībvalstis savu politiku attiecībā uz informācijas par programmatūras nepilnībām izpaušanu izstrādā atšķirīgā tempā, turklāt nav visaptveroša ES līmeņa tiesiskā regulējuma, kas nodrošinātu saskaņotas pieejas piemērošanu[50].
Tīklu un informācijas drošības stiprināšana	o Dalībvalstis var iekļaut jomas, kuras nav ņemtas vērā TID direktīvā[51]. Izmitināšanas nozare, kas direktīvas piemērošanas jomā nav iekļauta, var būt vārteja citiem noziegumiem, tostarp cilvēku un narkotiku tirdzniecībai un nelikumīgai imigrācijai[52].
Kibernoziedzības apkarošana	o Daudzas dalībvalstis savos tiesību aktos nav definējušas e-pierādījumus[53] (sk. arī ***22. punktu***). o Spēkā esošais pamatlēmums par bezskaidras naudas maksājumiem neparedz skaidrus noteikumus par "netaustāmiem" maksāšanas līdzekļiem, piemēram, virtuālajām valūtām, elektronisko naudu un tā dēvēto mobilo naudu, kā arī neaptver tādas darbības kā pikšķerēšana, datsmelšana un informācijas par maksātājiem turēšana un izplatīšana[54]. o Direktīva par uzbrukumiem informācijas sistēmām tieši nerisina jautājumu par datu nelikumīgu iegūšanu organizācijas iekšienē (proti, kiberspiegošanas jautājumu), tādējādi apgrūtinot tiesību akta izpildi[55]. o Pēc tam, kad tika pieņemts Eiropas Savienības Tiesas nolēmums par datu saglabāšanu[56], tiesiskā regulējuma atšķirīga piemērošana dalībvalstīs ir kavējusi tiesību aktu izpildi, kā rezultātā, iespējams, ir zaudēti izmeklēšanas pavedieni un negatīvi ietekmēta efektīva to personu kriminālvajāšana, kuras veic noziedzīgas darbības tiešsaistē[57].

Avots: Eiropas Revīzijas palāta.

35 Joprojām pastāv iespēja, ka valsts iestādes un privātie uzņēmēji vairākus tiesību aktu aspektus var piemērot pēc brīvprātības principa. Piemēram, sadarbības grupas ietvaros valsts stratēģiju par tīklu un informācijas sistēmu drošību un *CSIRT* efektivitātes izvērtēšana ir brīvprātīga. Arī Kiberdrošības aktā ierosinātā sertifikācijas sistēma paredz, ka sertifikācijas piemērošana IKT produktiem un pakalpojumiem būs brīvprātīga.

36 Eiropas Savienībā kiberdrošība ir dalībvalstu prerogatīva. Tomēr ES ir izšķiroša nozīme tādu apstākļu veidošanā, kas uzlabo dalībvalstu spējas un veicina to sadarbību un savstarpējo uzticību. Taču, ņemot vērā dalībvalstu būtiskās atšķirības spēju un iesaistes ziņā[58], noteikumi par sensitīvas informācijas (saistībā ar valsts drošību) sniegšanu arī turpmāk būs piemērojami pēc brīvprātības principa.

37 ES tiesību aktu nevienādā transponēšana dalībvalstīs var veicināt tiesisko un darbību nesaskaņotību, kā arī liegt iespēju pilnībā izmantot tiesību aktu potenciālu. Piemēram, dalībvalstis atšķirīgi interpretē noteikumus par divējāda lietojuma preču eksporta kontroles pasākumu veikšanu[59], un tādēļ var rasties situācija, ka daži uzņēmumi, kuri darbojas ES, eksportē tehnoloģijas un pakalpojumus, ko var izmantot kibernovērošanas un cilvēktiesību pārkāpumu veikšanai, īstenojot cenzūru vai datu pārtveršanu. Eiropas Parlaments ir paudis bažas par šo jautājumu[60].

38 Turklāt, lai aizsargātu privātumu un vārda brīvību, ir vajadzīgs īpaši pielāgots tiesību akts nolūkā nodrošināt nepieciešamo līdzsvaru starp pamatvērtību aizsardzību un ES drošības mērķu sasniegšanu. Piemēram, kā nodrošināt pilnīgu šifrēšanu, vienlaikus rodot labāko risinājumu, lai atbalstītu tiesībaizsardzību? Vai arī — kā mēs varam sasniegt VDAR mērķus, vienlaikus gūstot izpratni par tās ietekmi uz publiski pieejamu informāciju par personām, kas reģistrējušas domēna nosaukumus, un par IP adrešu bloķētāju turētājiem? Kādu negatīvu ietekmi minētās darbības var radīt uz izmeklēšanu tiesībaizsardzības nolūkā[61]?

39 Tiesību akti vien negarantē noturību. Lai gan TID direktīvas mērķis ir panākt augstu drošības līmeni visā Eiropas Savienībā, tajā skaidrs uzsvars likts uz to, lai tiktu panākta nevis pēc iespējas lielāka, bet minimālā saskaņošana[62]. Kibertelpai attīstoties, taps redzamas arvien jaunas nepilnības.

Jautājumi pārdomām: politikas satvars

- Kādi būtiski pasākumi vajadzīgi, lai rosinātu politikas veidotājus un likumdevējus ieviest stingrāku un uz rezultātiem vērstu pieeju kiberdrošības jomā, tostarp definējot vispārējo noturību?
- Kā pētniecība var labāk veicināt nepieciešamo statistikas datu iegūšanu, lai būtu iespējams veikt jēgpilnu izvērtēšanu?
- Kādos veidos iespējams pielāgot ES likumdošanas procesus, lai tie būtu elastīgāki un vairāk atbilstu tehnoloģiju attīstības un jaunu draudu rašanās tempam?
- Kā rādītāju (indikatoru, mērķu) izstrādes praksi ES politikas ciklā var pielāgot, uzlabot vai izmantot kā paraugu, lai piemērotu visai kiberdrošības jomai?
- Ko valstu revīzijas iestādes var mācīties cita no citas, iepazīstot dažādas pieejas kiberdrošības politikas un pasākumu revīzijai?
- Kuras ES tiesiskā regulējuma transponēšanas un īstenošanas neatbilstības apdraud efektīvāku reakciju uz nepilnībām kiberdrošības jomā un uz kibernoziedzību un kā šo problēmu vislabāk var risināt dalībvalstis un ES iestādes?
- Cik efektīvi ir ES kiberpreču un kiberpakalpojumu eksporta kontroles pasākumi cilvēktiesību pārkāpumu novēršanā ārpus ES?

Finansējums un tā izlietojums

40 ES tiecas kļūt par pasaulē drošāko tiešsaistes vidi. Lai sasniegtu šo vērienīgo mērķi, visām ieinteresētajām personām jāīsteno ievērojami centieni, tostarp nepieciešams drošs un labi pārvaldīts finansiālais pamats.

3. problēma —ieguldījumu līmeņa pielāgošana mērķiem

Ieguldījumu palielināšana

41 Tiek lēsts, ka kopējais finansējums kiberdrošības jomā pasaulē ir aptuveni 0,1 % apmērā no IKP. Amerikas Savienotajās Valstīs[63] finansējuma apmērs ir aptuveni 0,35 % (tostarp privātā sektora finansējums). ASV federālās valdības finansējums 2019. gadā ir aptuveni 0,1 % no IKP jeb aptuveni 21 miljards USD[64].

42 Salīdzinājumam — ES finansējums ir bijis zems, sadrumstalots un bieži vien bez pietiekama atbalsta no saskaņotām valdības virzītām programmām. Datu iegūšana ir sarežģīta, taču tiek lēsts, ka ES publiskais finansējums kiberdrošības jomā ir viens līdz divi miljardi euro gadā[65]. Dažās dalībvalstīs finansējuma īpatsvars procentos no IKP ir viena desmitā vai pat mazāka daļa no ASV finansējuma līmeņa[66]. ES un tās dalībvalstīm ir jānoskaidro, cik liels ir to kopējais ieguldījums, lai zinātu, kādās jomās finansējuma nepietiek.

43 Ir sarežģīti veidot pilnīgu priekšstatu, ja trūkst skaidru datu, — to trūkuma iemesls ir kiberdrošības transversālais raksturs, kā arī tas, ka finansējumu kiberdrošības jomā un vispārējos izdevumus IT jomā bieži vien nav iespējams nodalīt[67]. Mūsu aptaujas rezultāti apstiprināja, ka ir sarežģīti iegūt uzticamu statistiku par finansējuma izlietojumu publiskajā un privātajā sektorā. Trīs ceturtdaļas valsts revīzijas iestāžu ziņoja, ka netiek veikta ar kiberjomu saistītā valsts finansējuma izlietojuma centralizēta uzraudzība, turklāt nevienā dalībvalstī nebija noteikta prasība valsts struktūrām to finanšu plānos atsevišķi norādīt izdevumus kiberdrošības jomā.

44 Publiskā un privātā sektora ieguldījumu palielināšana Eiropas kiberdrošības nozares uzņēmumos ir īpaši sarežģīts uzdevums. Publiskā sektora kapitāls bieži vien ir pieejams tikai sākotnējos posmos, taču izaugsmes un paplašināšanās posmos tā pieejamība ir ierobežota[68]. Ir pieņemts liels skaits ES finansēšanas iniciatīvu, taču tās netiek izmantotas galvenokārt birokrātijas dēļ[69]. Kopumā ES kiberdrošības uzņēmumi gūst sliktākus rezultātus nekā to starptautiskie konkurenti — lai gan ES šādu

uzņēmumu ir mazāk, vidējais finansējuma apjoms, ko tie piesaista, ir ievērojami mazāks[70]. Tādēļ, lai sasniegtu ES digitālās politikas mērķus, ir ļoti svarīgi nodrošināt efektīvu plānošanu un finansējuma novirzīšanu jaunuzņēmumiem.

Ietekmes palielināšana

45 Ieguldījumu nepietiekamības novēršanai kiberjomā ir jānodrošina lietderīgi rezultāti. Piemēram, lai gan ES pētniecības un inovācijas nozare ir spēcīga, rezultāti netiek pietiekami patentēti, komercializēti vai attīstīti, lai palīdzētu stiprināt noturību, konkurētspēju un digitālo autonomiju[71]. Tas ir īpaši pamanāms, veicot salīdzinājumu ar ES konkurentiem pasaules mērogā. To, ka pienācīgi tiek izmantota tikai neliela daļa gūto rezultātu, ietekmē dažādi faktori[72], tostarp šādi:

- trūkst saskaņotas starpvalstu stratēģijas, kas pilnveidotu pieeju nolūkā panākt tās piemērotību plašākām ES vajadzībām digitālajā jomā, lai nodrošinātu konkurētspēju un lielāku autonomiju;
- garais vērtības veidošanas ķēdes cikls nozīmē to, ka instrumenti ātri zaudē aktualitāti;
- nav ilgtspējas — projekti parasti noslēdzas ar to, ka izjūk projekta īstenotāju komanda un tiek pārtraukts atbalsts, tostarp atjauninājumiem un korekciju veikšanas risinājumiem.

46 Komisijas priekšlikums izveidot kiberdrošības kompetenču centru tīklu un pētniecisko kompetenču centru ir mēģinājums novērst sadrumstalotību kiberdrošības pētniecības jomā un piesaistīt vērienīgus ieguldījumus[73]. Kopumā Eiropas Savienībā ir aptuveni 665 lietpratības centri.

4. problēma — skaidrs pārskats par ES finansējuma izlietojumu

47 Finansējuma izlietojuma centralizētai uzraudzībai ir būtiska nozīme, lai nodrošinātu pārredzamību un uzlabotu koordinēšanu. Ja centralizēta uzraudzība netiek veikta, politikas veidotājiem ir sarežģīti noteikt, kādā mērā finansējums atbilst vajadzībām, lai sasniegtu prioritāros mērķus.

48 Kiberdrošības stratēģijas īstenošanai īpašs budžeta finansējums nav paredzēts. ES līmenī kiberdrošības finansējumu nodrošina ES vispārējais budžets un dalībvalstu līdzfinansējums. Veicot analīzi, konstatējām, ka pastāv sarežģīts vismaz desmit dažādu

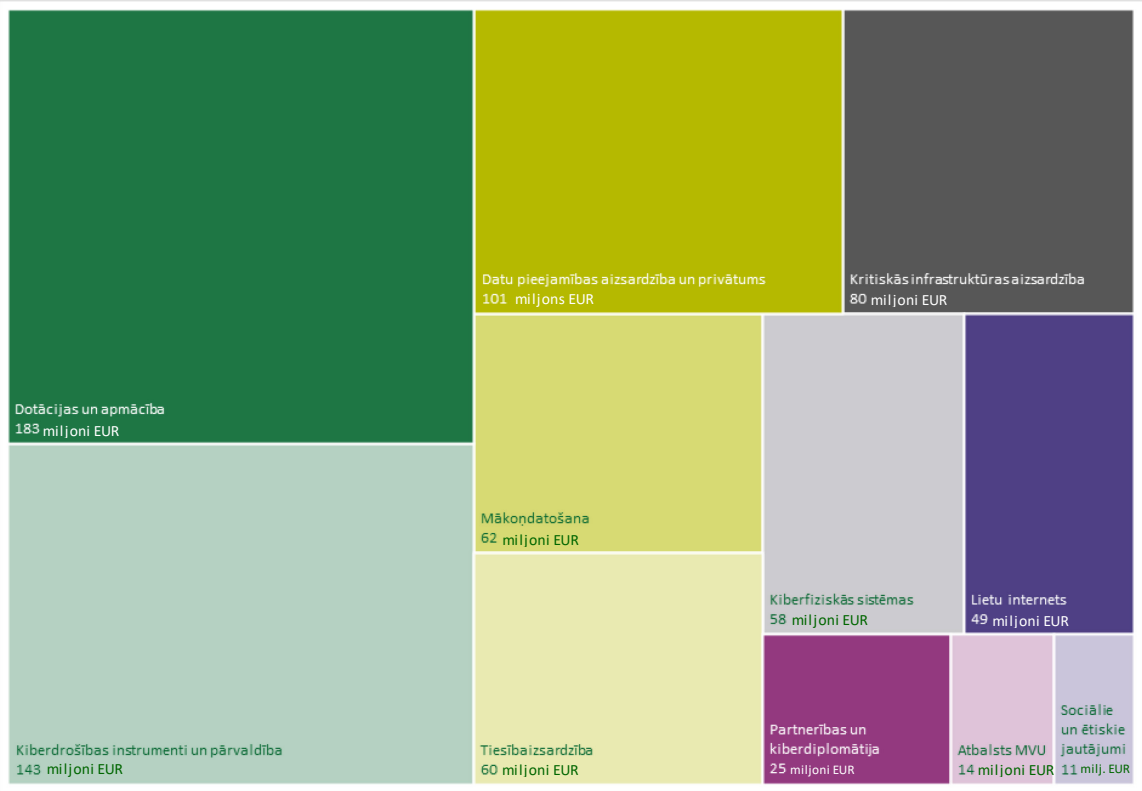
instrumentu kopums, ko finansē no ES vispārējā budžeta, taču nav skaidra priekšstata par finansējuma izlietojumu (sk. ***II pielikumu***).

49 Tāpēc ir ļoti grūti sniegt skaidru pārskatu par finansējuma izlietojumu nozarē, kas skar daudzas politikas jomas. Finansēšanas programmu pārvaldība ir uzticēta dažādām Komisijas struktūrvienībām, un katrai no tām ir savi mērķi, noteikumi un termiņi. Situācija kļūst vēl sarežģītāka, ja tiek ņemts vērā dalībvalstu līdzfinansējums, kā, piemēram, Iekšējās drošības fonda gadījumā (policijas komponents)[74].

Identificējami izdevumi kiberdrošības jomā

50 Komisija 2014.–2018. gada periodā izlietoja vismaz 1,4 miljardus EUR stratēģijas īstenošanai[75], piešķirot lielāko finansējuma daļu pamatprogrammai "Apvārsnis 2020"[76] (turpmāk —"Apvārsnis 2020"). Programmas "Apvārsnis 2020" finansējums galvenokārt tiek novirzīts, īstenojot programmu "Sabiedrības problēmu risināšana — droša sabiedrība" un mērķa "Vadošā loma pamattehnoloģiju un rūpniecisko tehnoloģiju jomā" projektus[77]. Mēs konstatējām, ka līdz 2018. gada septembrim noslēgti līgumi par 279 ar kiberdrošību saistītu projektu īstenošanu, un to kopējais ES finansējuma apmērs ir 786 miljoni EUR[78]. ***5. attēlā*** redzams šo projektu iedalījums, kas veikts, pamatojoties uz šo analīzi.

5. attēls. Saskaņā ar “Apvārsnis 2020” noslēgtie līgumi par kiberdrošības pētniecības projektu īstenošanu (miljoni EUR)



Avots: Eiropas Revīzijas palāta.

51 2016. gadā tika izveidota līgumiska publiskā un privātā partnerība (LPPP), lai veicinātu Eiropas kiberdrošības nozares attīstību. Mērķis bija šai LPPP novirzīt 450 miljonus EUR no programmas “Apvārsnis 2020” finansējuma un līdz 2020. gadam piesaistīt vēl 1,8 miljardus EUR no privātā sektora. Līdz 2017. gada 31. decembrim 18 mēnešu laikā no “Apvārsnis 2020” finansējuma LPPP bija novirzīti 67,5 miljoni EUR, un no privātā sektora bija saņemti ieguldījumi 1 miljarda EUR apmērā[79].

52 Cīņa pret kibernoziedzību tiek atbalstīta, izmantojot arī Iekšējās drošības fonda policijas komponentu (IDF-P). IDF-P sniedz atbalstu pētījumiem, ekspertu sanāksmju organizēšanai un komunikācijas darbībām; laikposmā no 2014. līdz 2017. gadam šo darbību veikšanai atvēlēts finansējums gandrīz 62 miljonu EUR apmērā. Dalībvalstis var saņemt arī dotācijas aprīkojumam, mācībām, pētniecībai un datu vākšanai dalītas pārvaldības jomās. Šādas dotācijas ir izmantojušas 19 dalībvalstis par summu 42 miljonu EUR apmērā.

53 Finansējums tiesu iestāžu sadarbībai un savstarpējas tiesiskās palīdzības nolīgumu īstenošanai ar īpašu uzsvaru uz elektronisku datu un finanšu informācijas apmaiņu

sasniedza 9 miljonus EUR, un to piešķīra no Tiesiskuma un patērētāju ģenerāldirektorāta pārvaldītās programmas "Tiesiskums" līdzekļiem.

54 TID direktīvā skaidri noteikts, ka *CSIRT* jābūt pieejamiem atbilstīgiem resursiem, lai efektīvi veiktu savus uzdevumus[80]. Laikposmā no 2016. līdz 2018. gadam katru gadu bija pieejami 13 miljoni EUR no Eiropas infrastruktūras savienošanas instrumenta līdzekļiem, un dalībvalstis varēja pieteikties šā finansējuma saņemšanai, lai izpildītu direktīvas prasības. Nav veikts neviens pētījums ar mērķi noteikt *CSIRT* tīkla un sadarbības grupas faktiskās finansējuma vajadzības, lai panāktu ietekmi.

55 Vairākas aģentūru darbības izmaksu pozīcijas īpaši paredzētas ar kiberdrošību vai kibernoziedzību saistītām darbībām. Taču, pamatojoties uz publiski pieejamo informāciju, ir grūti noteikt konkrētas summas.

56 Budapeštas konvencija (sk. ***11. punktu***) ir pamats ES ārējo izdevumu izlietojumam kiberdrošības jomā. Laikposmā no 2014. līdz 2018. gadam ES izlietoja aptuveni 50 miljonus EUR, lai stiprinātu kiberdrošību aiz savām robežām. Gandrīz puse šā finansējuma tika izlietota, izmantojot Stabilitātes un miera veicināšanas instrumentu, un viena galvenā projekta *GLACY+* (13,5 miljoni EUR) mērķis bija visā pasaulē stiprināt spējas izstrādāt un īstenot tiesību aktus kibernoziedzības jomā un sekmēt starptautisko sadarbību[81]. Citviet pasaulē citu ES finanšu instrumentu finansējums tika novirzīts galvenokārt Rietumbalkānu reģionam[82], kā arī Eiropas kaimiņvalstīm, piemēram, sadarbībā ar austrumu partnervalstīm īstenotā projekta "*Cybercrime@EaP*" mērķis bija uzlabot starptautisko sadarbību kibernoziedzības un elektronisko pierādījumu jomā.

Citi izdevumi kiberdrošības jomā

57 Ne vienmēr iespējams identificēt tieši ar kiberdrošību saistītus izdevumus ES programmās:

- programmas "Apvārsnis 2020" finansējums ir piešķirts arī ar kopuzņēmuma "Elektroniski komponenti un sistēmas Eiropas vadošās lomas nostiprināšanai" (*ECSEL*) starpniecību kiberfizisku sistēmu izveidei. Tomēr mēs nevarējām noteikt summu, kas laikposmā no 2015. līdz 2016. gadam no 27 projektiem piešķirtajiem 437 miljoniem EUR attiecās tieši uz kiberdrošību.

- No Eiropas strukturālo un investīciju fondu finansējuma līdz pat 400 miljoniem EUR ir pieejami tādu izdevumu segšanai, kas saistīti ar kiberdrošību un uzticamības pakalpojumiem; tas ietver ieguldījumus drošības un datu aizsardzības jomā, lai uzlabotu sadarbspēju un digitālās infrastruktūras

savienojamību, kā arī elektroniskās identifikācijas un privātuma un uzticamības pakalpojumu finansēšanu.

58 Eiropas Investīciju banka savā 2018. gada darbības plānā paziņoja par nodomu triju gadu periodā līdz 6 miljardiem EUR[83] palielināt finansējumu divējāda lietojuma tehnoloģiju, kiberdrošības un civiliedzīvotāju drošības jomā.

Nākotnes perspektīva

59 Ierosinātās jaunās Digitālās Eiropas programmas[84] (DEP) kiberdrošības komponents ar finansējumu 2 miljardu EUR apmērā 2021.–2027. gadam ir izveidots, lai stiprinātu ES kiberdrošības nozari un uzlabotu sabiedrības vispārējo aizsardzību, tostarp palīdzot īstenot TID direktīvu. Sagaidāms, ka ierosinātais kiberdrošības kompetenču centru tīkls un pētniecisko kompetenču centrs, kuru mērķis ir piemērot efektīvāku pieeju, būs galvenais īstenošanas mehānisms attiecībā uz ES DEP finansējumu.

60 Aizsardzības izdevumi no ES budžeta nesen ir palielināti, izveidojot Eiropas aizsardzības rūpniecības attīstības programmu, kam 2019.–2020. gadā tiks piešķirti 500 miljoni EUR[85]. Šo finansējumu novirzīs, lai uzlabotu dalībvalstu aizsardzības izdevumu izlietojuma koordināciju un efektivitāti, izmantojot stimulus saskaņotas attīstības veicināšanai. Mērķis ir rast iespēju pēc 2020. gada veikt kopumā 13 miljardu EUR ieguldījumus aizsardzības spēju veidošanā, izmantojot Eiropas Aizsardzības fondu, un daļa no šā finansējuma ir paredzēta arī kiberaizsardzībai[86].

5. problēma — pienācīgu resursu nodrošināšana ES aģentūrām

61 Laikā, kad lielāks uzsvars tiek likts uz politikas prioritātēm, kas saistītas ar drošību, trīs galvenās struktūras, kuras nodrošina ES kiberdrošības politikas īstenošanu, proti, *ENISA*, Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*EC3*) un Datorapdraudējumu reaģēšanas vienība (*CERT-EU*) (sk. ***2. izcēlumu***), saskaras ar resursu pieejamības problēmu. ES aģentūrām patlaban iedalītie cilvēkresursi un finanšu resursi joprojām nav pietiekami, lai sasniegtu gaidītos rezultātus[87].

62 Aģentūru pieprasījumi piešķirt papildu resursus, lai nodrošinātu arvien pieaugošās vajadzības, nav pilnībā izpildīti, tādējādi, iespējams, apdraudot politikas mērķu (savlaicīgu) sasniegšanu. Skatīt turpmāk izklāstītos piemērus.

- Ierobežotie resursi liedza *ENISA* 2017. gadā pilnībā sasniegt savus mērķus[88]. Lai ņemtu vērā *ENISA* jaunās pilnvaras, 2017. gada paketē tika ierosināta papildu resursu piešķiršana.

- Analītiķu piesaiste un ieguldījumi IKT spēju veidošanā Eiropola *EC3* nav bijuši atbilstīgi pieprasījumam[89]. Eiropola Eiropas Kibernoziedzības apkarošanas centra Kopīgās kibernoziedzības rīcības uzdevumgrupas *(J-CAT*) personāls ir dalībvalstu un trešo valstu eksperti, kas sniedz atbalstu uz izlūkdatiem balstītā izmeklēšanā. Taču lielāko daļu izmaksu sedz nosūtītājas valstis, tādējādi mazinās interese nosūtīt lielāku skaitu ekspertu. Izmantojot Eiropolam vai ES politikas ciklam paredzēto finansējumu, ir organizēta personāla īslaicīga piesaiste konkrētu jautājumu risināšanai, lai nodrošinātu lielāka valstu skaita līdzdalību.

63 Vairāki ierobežojumi ir iestāžu un aģentūru pašu radīti. Liela daļa *CERT-EU* un *ENISA* darbinieku ir līgumdarbinieki, kuru darbā pieņemšanas procedūras parasti ir ilgstošas. Citi ierobežojumi, kas saistīti ar talantīgu darbinieku piesaisti un saglabāšanu, rodas no tā, ka aģentūras nespēj konkurēt ar atalgojumu privātajā sektorā, vai tāpēc, ka netiek piedāvātas pietiekamas karjeras veidošanas iespējas. Tādēļ *ENISA* laikposmā no 2014. līdz 2016. gada lielāko daļu uzdevumu veica, izmantojot ārpakalpojumus[90].

64 Darbinieku un nepieciešamo līdzekļu trūkums var radīt būtiskus riskus, it īpaši vācot izlūkdatus par draudiem. Datu apjoms, ko iegūst no publiski pieejamiem un publiski nepieejamiem datu avotiem, turpina palielināties, un rodas risks pārsniegt analītiķu spēju veikt pienācīgu draudu analīzi. Ja netiks nodrošinātas atbilstīgas spējas un līdzekļi šādu datu veiksmīgai integrēšanai un sasaistei, nebūs iespējams efektīvi sniegt draudu saistībā izmantojamus izlūkdatus, ko var izplatīt un analizēt visā ES[91].

Jautājumi pārdomām: finansējums un tā izlietojums

- Kādā veidā Komisija un likumdevēji var racionalizēt ES kiberdrošības finansējuma izlietojumu un konkrētāk to pielāgot skaidri noteiktiem mērķiem?
- Kā visaptverošā veidā novērst resursu trūkumu ES aģentūrās, ņemot vērā Savienības vajadzības un mērķus?
- Kādi pasākumi pieņemti ES un dalībvalstu līmenī, lai mazinātu šķēršļus MVU, kuri vēlas izmantot ieguldījumu kapitālu savu darbību izvēršanai?
- Kādus konkrētus un ilgstošus rezultātus nodrošina "Apvārsnis 2020" finansējums, kas palīdz rast kiberdrošības risinājumus?
- Kādā veidā ES spēju veidošanas pasākumi stiprina spējas aiz tās robežām atbilstīgi ES vērtībām?

Kibernoturīgas sabiedrības veidošana

65 Kiberdrošības pārvaldības jomā jārisina tādi jautājumi kā draudu un risku pārvaldība, spēju un izpratnes veidošana, kā arī koordinēšana un informācijas apmaiņa, pamatojoties uz uzticības veidošanu.

6. problēma — pārvaldības stiprināšana un standartu uzlabošana

Informācijas drošības pārvaldība

66 Informācijas drošības pārvaldība nozīmē ieviest struktūras un veidot politiku, lai nodrošinātu datu konfidencialitāti, integritāti un pieejamību. Informācijas drošības pārvaldība nav tikai tehnisks uzdevums — lai to veiktu, vajadzīga efektīva vadība, stingras procedūras un stratēģijas, kas pielāgotas organizācijas mērķiem[92]. Informācijas drošības pārvaldībai pakārtots uzdevums ir kiberdrošības pārvaldība, kas risina jautājumus saistībā ar visu veidu kiberdraudiem, tostarp mērķtiecīgiem un sarežģītiem uzbrukumiem, pārkāpumiem vai incidentiem, kurus ir grūti atklāt vai pārvaldīt.

67 Dalībvalstīs izmanto dažādus kiberdrošības pārvaldības modeļus, turklāt nereti šie modeļi paredz, ka atbildība par kiberdrošību tiek sadalīta daudzām struktūrām. Minētās atšķirības var traucēt sadarbībai, kas vajadzīga, lai reaģētu uz plaša mēroga pārrobežu incidentiem un lai apmainītos ar izlūkdatiem par draudiem valstu līmenī, nemaz jau nerunājot par ES līmeni. Mūsu veiktās valsts revīzijas iestāžu aptaujas rezultāti parādīja, ka valsts iestāžu pārvaldības sistēmu un risku pārvaldības nepilnības tika uzskatītas par būtiskākajiem apdraudējumiem.

68 Lai gan sekas privātā sektora organizācijās var būt ļoti smagas, kiberdrošības pārvaldības nepilnības joprojām ir plaši izplatītas. Gandrīz katra devītā no desmit organizācijām uzskata, ka tās kiberdrošības funkcijas pilnībā neatbilst tās vajadzībām[93], un kiberdrošības speciālisti organizatoriskajā struktūrā nereti ir vismaz divus līmeņus zemāk par valdi[94].

69 ES uzņēmējdarbības tiesību direktīvās nav paredzētas īpašas prasības attiecībā uz informācijas par kiberriskiem publiskošanu. Amerikas Savienotajās Valstīs Vērtspapīru un biržas darījumu komisija nesen izdeva nesaistošas pamatnostādnes, lai palīdzētu atklātām akciju sabiedrībām sagatavot publiskojamu informāciju par kiberdrošības riskiem un incidentiem[95]. Eiropas uzraudzības iestāžu apvienotā komiteja[96] brīdināja

par kiberrisku palielināšanos, mudināja finanšu iestādes uzlabot nestabilas IT sistēmas un izvērtēt riskus, kas saistīti ar informācijas drošību, savienojamību un ārpakalpojumu izmantošanu[97].

70 MVU Informācijas drošības pārvaldības stiprināšana ir īpaši sarežģīts uzdevums, jo MVU visbiežāk nespēj ieviest atbilstīgas sistēmas. MVU nav pieejamas piemērotas pamatnostādnes par informācijas drošības un privātuma prasību piemērošanu un ar tehnoloģijām saistīto risku novēršanu[98]. Tādēļ būtisks uzdevums ir labāk apzināt MVU vajadzības un uzlabot vajadzīgos stimulus un atbalstu.

71 Saskaņota starptautiska mēroga kiberdrošības pārvaldības satvara trūkums negatīvi ietekmē starptautiskās sabiedrības spēju reaģēt uz kiberuzbrukumiem un ierobežot tos. Tādēļ ir svarīgi panākt vienprātību par tādu pārvaldības satvaru, kurā pēc iespējas ņemtas vērā ES intereses un vērtības[99]. Centieni noteikt saistošus starptautiska mēroga kibertelpas izmantošanas standartus tiek uztverti arvien negatīvāk — to pierāda vienprātības trūkums ANO Valdību ekspertu grupas darbā 2017. gadā attiecībā uz to, kā starptautiskās tiesības būtu jāpiemēro gadījumos, kad valsts reaģē uz incidentiem.

72 Nolūkā uzlabot savu kibertelpas pārvaldības programmu ES ir arī formāli izveidojusi sešas partnerības kiberdrošības jomā, lai veidotu regulārus politikas dialogus ar mērķi vairot uzticību un attīstīt kopīgas sadarbības jomas[100]. Rezultāti ir dažādi, taču kopumā starptautiskajā telpā Eiropas Savienību vēl nevar uzskatīt par "ietekmīgu rīcībspēku kiberdrošības jomā", lai gan tā savu ietekmi ir palielinājusi[101].

Informācijas drošība ES iestādēs

73 Katrai ES iestādei ir savi informācijas drošības pārvaldības noteikumi. Iestāžu nolīgums paredz, ka Komisija citām iestādēm un aģentūrām sniedz palīdzību informācijas drošības jautājumu risināšanā. ES iestādes un struktūras ir atzinušas, ka to kiberaizsardzības spējas un risku pārvaldības pieejas ir jāveido saskaņoti. Komisijai, Padomei un EĀDD 2020. gadā ir jāiesniedz ziņojums Kiberjautājumu horizontālajai darba grupai par pārvaldību un progresu, kas panākts, apzinot un saskaņojot kiberdrošības pārvaldību ES iestādēs un aģentūrās[102].

74 Komisijā par IT infrastruktūras un pakalpojumu drošību ir atbildīgs Informātikas ģenerāldirektorāts (DIGIT ĢD) (sk. ***3. izcēlumu***). Komisijas Digitālās stratēģijas galvenie mērķi attiecībā uz IT drošību ir integrēt IT drošību pārvaldības procesos, nodrošināt izmaksu ziņā efektīvu infrastruktūru un noturību, paplašināt incidentu atklāšanas un

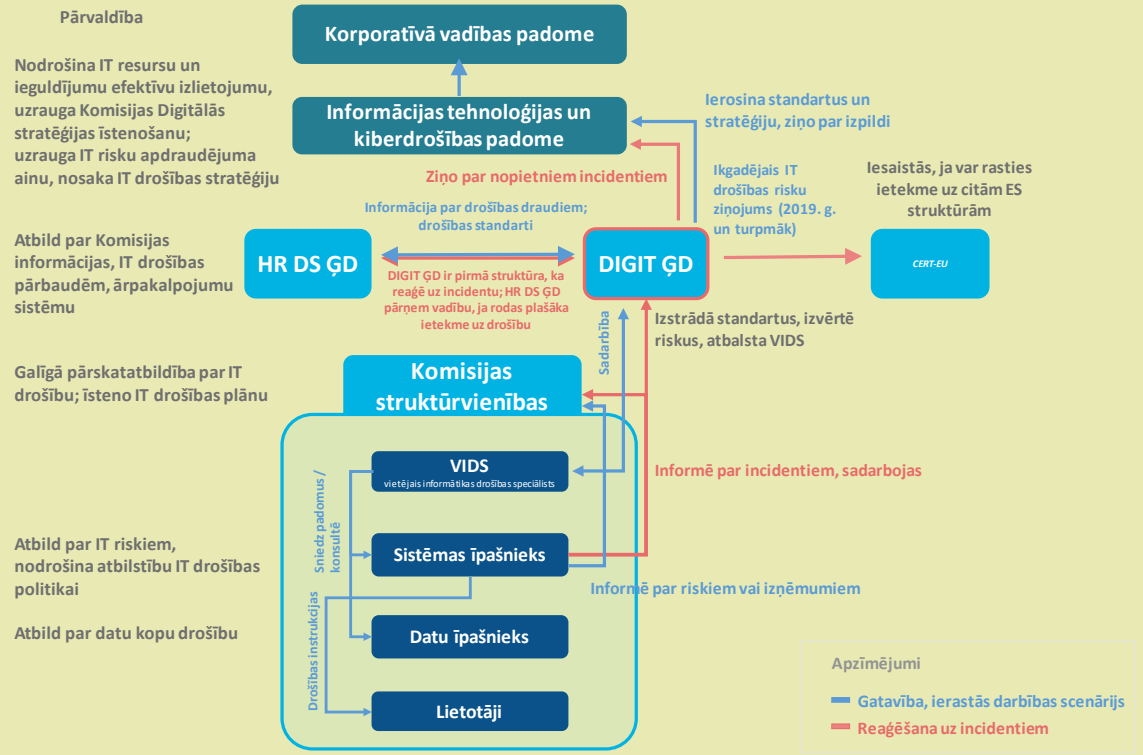
reaģēšanas tvērumu un integrēt IT un drošības pārvaldību[103]. Komisija saskaņā ar savu pakalpojumu sniedzēja līgumu nodrošina gandrīz visas programmatūras aktīvu uzturēšanu un tikai pārdevēja atbalstītas programmatūras izmantošanu[104].

75 Iestāžu aizsardzības būtiskā nozīme attiecas arī uz Eiropas Savienības KDAP misijām un struktūrām visā pasaulē. Viena no ES kiberaizsardzības politikas satvara prioritātēm (atjauninātas 2018. gadā) ir uzlabot ES struktūru izmantoto KDAP komunikācijas un informācijas sistēmu aizsardzību. Ir izveidota EĀDD Kiberpārvaldības padome, un tā pirmo reizi tikās 2017. gada jūnijā[105].

3. izcēlums

Komisijas informācijas sistēmu aizsardzība

Pret Komisijas aptuveni 1300 sistēmām un 50 000 ierīcēm pastāvīgi ir vērsti kiberuzbrukumi. Kā redzams attēlā turpmāk, atbildība par IT ir decentralizēta. Informācijas un IT drošības pamatā ir vienots IT drošības plāns, ko izstrādājis DIGIT ĢD. Informācijas tehnoloģijas un kiberdrošības valde faktiski veic Komisijas galvenā informācijas drošības speciālista funkcijas un IT drošības operatīvos aspektus sasaista ar Komisijas augstākā līmeņa vadītājiem, ko pārstāv korporatīvā vadības padome.



Avots: ERP, pamatojoties uz Komisijas lēmumiem[106].

Cilvēkresursu un drošības ģenerāldirektorāta (HR ĢD) galvenais uzdevums ir aizsargāt Komisijas personālu, informāciju un aktīvus. Tas veic arī tādu drošības incidentu

izmeklēšanu, kuriem ir plašāka ietekme uz drošību nekā IT incidentiem, tādējādi paplašinot pretizlūkošanas un pretterorisma darbību tvērumu.

DIGIT ĢD ir atbildīgs par IT drošību, un tā telpās darbu veic *CERT-EU* (ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība). 2011. gadā izveidotās *CERT-EU* gada budžets ir 2,5 miljoni EUR, un tajā ir aptuveni 30 darbinieki. *CERT-EU* ir pirmā struktūra, kas reaģē uz ikvienu informācijas drošības incidentu, kurš ietekmē vairākas iestādes, taču tā neveic darbību 24 stundas diennaktī. *CERT-EU* uztur informācijas apmaiņas platformu. *CERT-EU* 2018. gadā parakstīja nesaistošu saprašanās memorandu ar *ENISA, EC3* un Eiropas Aizsardzības aģentūru par sadarbības un koordinēšanas stiprināšanu. *CERT-EU* ir noslēgusi arī tehnisku vienošanos ar NATO Datorincidentu reaģēšanas spēju centru.

Draudu un riska novērtējumi

76 Labi pamatoti un pastāvīgi sagatavoti draudu un riska novērtējumi ir svarīgi instrumenti gan publiskā, gan arī privātā sektora organizācijām. Taču nav standarta pieejas kiberdraudu vai riska novērtējumu klasificēšanai un plānošanai, un tas nozīmē, ka novērtējumu saturs būtiski atšķiras, tādējādi apgrūtinot saskaņotas ES mēroga pieejas piemērošanu kiberdrošības jomā[107]. Turklāt minētie novērtējumi nereti ir balstīti uz līdzīgiem avotiem vai pat citiem draudu novērtējumiem, tādēļ tajos tikai atkārtojas vieni un tie paši konstatējumi[108], un šāda situācija rada risku, ka citiem draudiem netiek pievērsta pietiekama uzmanība. Situāciju vēl vairāk pasliktina pastāvīgi novērotā nevēlēšanās apmainīties ar informāciju un neziņošana par incidentiem.

77 ES Hibrīddraudu analīzes vienība[109], kas darbojas EĀDD ietvaros, tika izveidota, lai efektīvāk apzinātu situāciju un sniegtu atbalstu lēmumu pieņemšanā, veicot analīzes datu apmaiņu, taču tai jāpaplašina sava kompetences joma, iekļaujot tajā arī kiberdrošību. Paralēli *CERT-EU* sniedz ES iestādēm, struktūrām un aģentūrām ziņojumus un informatīvus dokumentus par kiberdraudiem, kas vērsti pret tām.

78 *ENISA* iepriekš ir norādījusi, ka daudzās dalībvalstīs ir laba izpratne par draudiem un ka jāveic vairāk kiberdraudu modelēšanas pasākumu[110]. Uzraudzības spējas, ko izmanto stratēģiskās analīzes veikšanai, uzlabos vispārējo izpratni. Taču draudu novērtējumos varētu iekļaut ne tikai tehnoloģiskos draudus, bet arī sociāli politiskos un ekonomiskos draudus, lai nodrošinātu plašāku priekšstatu par situāciju, kā arī draudu avotiem un rīcībspēku motīviem.

Stimuli

79 Joprojām ir pārāk maz tiesisko un ekonomisko stimulu organizācijām ziņot par incidentiem un apmainīties ar informāciju par tiem. Baidoties, ka tiks nodarīts kaitējums reputācijai, daudzas organizācijas vēl arvien dod priekšroku diskrētai kiberuzbukumu seku likvidēšanai vai maksā uzbrukumu veicējiem. Vēl nav zināms, cik efektīvi TID direktīva paaugstinās ziņošanas līmeni. Komisija prognozē, ka uzlabojumi būs jūtami galvenokārt valsts līmenī, savukārt Kiberdrošības akts sekmēs plašāku ES mēroga ietekmi.[111]

80 Publiskā sektora iestādes, kas savās iepirkuma procedūrās integrē konkrētus standartus, kā digitālo produktu un pakalpojumu pircējas ar publiskā iepirkuma procedūru palīdzību var būtiski ietekmēt piegādātājus, kā arī pētniecības un programmu finansējumu (proti, tās var pieprasīt pieņemt konkrētus tehniskos standartus, piemēram, interneta protokolu IPv6, kas palīdz cīnīties pret kibernoziedzību). Tomēr patlaban nav vienota iepirkuma regulējuma attiecībā uz kiberdrošības infrastruktūru[112]. Šai sakarā Komisija var paveikt ļoti daudz. Ierosinātās Digitālās Eiropas programmas nākamajai daudzgadu finanšu shēmai mērķis ir risināt jautājumu par līdz šim ierobežotajiem publiskā sektora ieguldījumiem jaunāko kiberdrošības tehnoloģiju iegādē.

81 Komisija, izmantojot savas regulatīvās spējas, var nodrošināt atbilstīgu standartu izstrādi, lai tos drošības uzlabošanas nolūkā pieņemtu plašā mērogā. Komisija un Eiropols sadarbojas ar interneta pārvaldības struktūrām, piemēram, ar *ICANN* (sk. ***38. punktu***) un *RIPE-NCC*[113], un tas ir ļoti svarīgi, lai izveidotu piemērotu kibernoziedzības apkarošanas sistēmu nolūkā sniegt atbalstu tiesībaizsardzības un tiesu iestādēm.

7. problēma — prasmju un izpratnes vairošana

82 *ENISA* ir norādījusi, ka lietotājiem ir izšķiroša loma cīņā pret kiberuzbrukumiem un ka prasmju, zināšanu un izpratnes uzlabošanai ir būtiska nozīme kibernoturīgas sabiedrības veidošanā[114]. Personas, kuras darbā vai mājās ir pietiekami zinošas, lai pamanītu brīdinājuma signālus, un kuru rīcībā ir atbilstīgi līdzekļi, var palēnināt vai novērst uzbrukumus.

83 Īpašas bažas rada arvien pieaugošā neatbilstība starp zināšanām, kas vajadzīgas, lai veiktu kibernoziegumu vai kiberuzbrukumu, un prasmēm, kas vajadzīgas, lai aizsargātos pret tiem. Modelis “noziegums kā pakalpojums” ir mazinājis šķēršļus, lai iekļūtu kibernoziedzības tīklā, — personas bez tehniskām zināšanām par to, kā izveidot

robottīklus, mūķu komplektus vai izspiedējprogrammatūras paketes, tagad var tos iznomāt.

Apmācības, prasmju un spēju attīstīšana

84 Pasaulē ir vērojams arvien pieaugošs kiberdrošības prasmju trūkums; kopš 2015. gada darbaspēka trūkums ir palielinājies par 20 %[115]. Tradicionālie personāla atlases ceļi nenodrošina pieprasījumu, tostarp vadošiem un starpdisciplīnu kategorijas amatiem[116]. Gandrīz 90 % kiberdrošības jomas darbinieku visā pasaulē ir vīrieši; pastāvīgi novērotais dzimumu dažādības trūkums vēl vairāk ierobežo talantīgu darbinieku pieejamību[117]. Turklāt universitāšu netehniskajās programmās ir pārāk maz ar kiberdrošību saistītu mācību priekšmetu.

85 Apmācība un izglītošanās ir vajadzīga visiem — gan ierēdņiem, tiesībaizsardzības amatpersonām un tiesu iestādēm, gan arī bruņotajiem spēkiem un mācībspēkiem. Piemēram, tiesām ir jāspēj izprast kibernoziedzības un kibernoziegumos cietušo strauji mainīgos tehniskos aspektus[118]; patlaban nav ES mēroga standartu apmācības un sertifikācijas jomā[119]. ES iestādēs būtiska nozīme ir atbilstīgam prasmju kopumam. Ja iestādēm nav atbilstīga prasmju kopuma, var rasties situācija, ka tās nevar pienācīgi noteikt darbības jomu, piemērotus partnerus un drošības vajadzības vai arī tām trūkst programmu pārvaldības spēju. Savukārt šāda situācija var apdraudēt ES programmu vai politikas veidošanas efektivitāti.

86 Lai gan par izglītības politikas īstenošanu ES līmenī ir atbildīgas dalībvalstis, daudzas ar apmācību saistītas darbības (sk. ***2. tabulu***) un pasākumi (sk. ***4. izcēlumu***) jau tiek īstenoti. ES var palīdzēt ES mēroga standartus iekļaut mācību programmās visās attiecīgajās zinību nozarēs[120]. Piemēram, digitālās kriminālistikas jomā kopēji apmācību standarti ir vajadzīgi, lai veicinātu virzību uz pierādījumu pieņemamību dalībvalstīs. Kibernoziedzības pārrobežu rakstura dēļ var tikt iesaistītas vairākas jurisdikcijas, tādēļ jānodrošina ES līmeņa apmācība. Taču *CEPOL* — Eiropas Savienības Tiesībaizsardzības apmācības aģentūra — ir norādījusi, ka vairāk nekā divas trešdaļas dalībvalstu tiesībaizsardzības amatpersonām nenodrošina regulāru apmācību kiberdrošības jomā[121]. ES var arī noteikt veidus, kā panākt civilās un militārās jomas sinerģiju izglītībā un apmācībā[122]. Ņemot to vērā, *ENISA* ir konstatējusi, ka, lai gan pašreizējās apmācību iespējas svarīgākajās nozarēs ir plašas, tās nav pietiekami vērstas uz kritiskās infrastruktūras noturības veidošanu[123].

2. tabula. Ar kiberdrošību saistītas apmācības ierosmes ES

Eiropas Aizsardzības aģentūras projekti, piemēram, atbalsts privātā sektora dalībnieku mācībām un projekts "Kiberpoligons"	Eiropas Drošības un aizsardzības koledžas tīkls (nodrošina civilo un militāro apmācību), tostarp kiberjomas izglītības, apmācības, izvērtēšanas un mācību platforma	*ENISA* piedāvātā apmācība — mācību programmas jomās, kurās komerciālā tirgus dalībnieki tās nenodrošina
Eiropola, *CEPOL* un *ECTEG*[124] mācību programmas, tostarp apmācības pārvaldības modelis un apmācības kompetenču satvars (arī sertifikācija)	Kompetenču centru tīkls un pētniecisko kompetenču centrs (ierosināts)	Pasākumi šifrēšanas jomā, kas ierosināti 11. progresa ziņojumā par drošības savienību
ES un NATO sadarbība kiberaizsardzības apmācības un izglītības jomā	Militārā *Erasmus* programma	Eiropas Tiesiskās apmācības tīkls

Avots: Eiropas Revīzijas palāta.

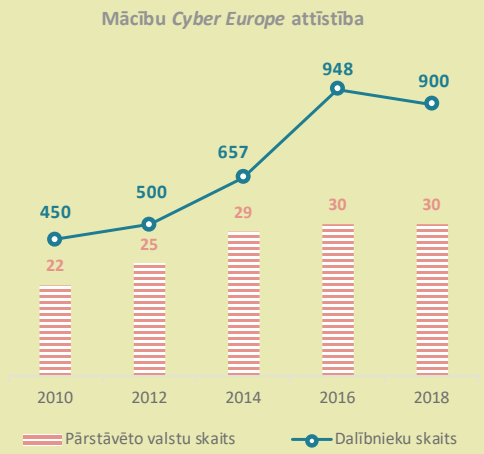
87 ES ir norīkojusi pretterorisma un drošības ekspertus darbā 17 delegācijās, lai stiprinātu saikni starp ES iekšējo un ārējo drošību[125]. Kaut gan resursi ir ierobežoti, plašākas zināšanas kiberjomā varētu palīdzēt īstenot atbilstīgus projektus, kā arī noteikt sinerģiju ar citām programmām vai finansējuma avotiem[126]. Šādas zināšanas arī palielinātu kiberdrošības jautājuma nozīmi politiskajā dialogā, lai gan tam būtu jākonkurē ar daudzām citām prioritātēm, piemēram, migrāciju, organizēto noziedzību vai ārvalstu kaujinieku atgriešanu.

4. izcēlums

Mācības

Mācības ir būtisks kiberjomas izglītības un apmācības elements, kas nodrošina būtiskas iespējas uzlabot gatavību, pārbaudot spējas, dodot iespēju reaģēt uz reālās dzīves situācijām un veidojot sadarbības tīklus. Kopš 2010. gada mācības tiek organizētas ievērojami biežāk.

Dalībnieki piedalās mācībās uz vietas vai attālināti. Pēc mācībām tiek veikta izvērtēšana, lai apzinātu gūto pieredzi, kas tomēr pilnībā var neattiekties uz stratēģisko/politisko, darbības un tehnisko līmeni[127].



Avots: ERP, pamatojoties uz *ENISA* dokumentiem.

ES un NATO paraugmācībās — operatīvajās mācībās "Kibereiropa", kas notiek reizi divos gados, un ikgadējās tehniskajās mācībās "*Locked Shields*" – piedalās vairāk nekā 1000 dalībnieku no 30 iesaistītajām valstīm. Abas mācības ir vērstas uz kritiskās infrastruktūras aizsardzību un saglabāšanu imitētu uzbrukumu scenārijos. Mācības ir kļuvušas ievērojami sarežģītākas, un patlaban tajās tiek iekļauti plašsaziņas līdzekļi, tiesiskie un finanšu politikas elementi, lai uzlabotu dalībnieku situatīvo izpratni. Vienlaikus notiekošās un koordinētās stratēģiskās mācības, ko nodrošina Eiropas Padomes Parlamentārā asambleja *(PACE),* pārbauda ES un NATO sadarbību hibrīdkrīzes gadījumā.

Tās nav vienīgās starptautiskās mācības. *ENISA* organizē ikgadējas sacensības kiberjomā, kuru laikā komandas sacenšas, risinot ar drošību saistītus uzdevumus, piemēram, tīkla un viedierīču drošības uzdevumus, kriptomīklas, reversās inženierijas uzdevumus, kā arī uzdevumus ētikas un kriminālistikas jomā. Pirmās ministru līmeņa mācības *EU CYBRID* notika 2017. gada septembrī, un tajās uzmanība tika pievērsta stratēģisku lēmumu pieņemšanai. 2018. gadā NATO rīkoja mācības "*Crossed Swords*", lai uzlabotu tās mācību "*Locked Shields*" uzbrukuma elementus. NATO organizē arī mācības "Kiberkoalīcija".

Būtisks uzdevums ir nodrošināt visu galveno ieinteresēto personu aktīvu iesaisti un visu mācību koordināciju, lai izvairītos no dublēšanās un efektīvi apmainītos ar gūto pieredzi.

Izpratne

88 Uzbrukumu un dezinformācijas izplatīšanas darbību mērķis bieži vien ir iedzīvotāji — viņi parasti, pašiem to neapzinoties, ir neaizsargāti, jo izmanto lētas un plaši pieejamas ierīces un programmatūru vai kļūst par sociālās inženierijas upuriem. Tādēļ izpratnes veidošanai ir būtiska nozīme, lai veidotu efektīvu kibernoturību, taču tas nebūt nav viegls uzdevums, jo nespeciālistiem ir grūti izprast kiberdrošības sarežģītību un ar to saistītos riskus.

89 Ikgadējās iniciatīvas "Eiropas kiberdrošības izpratnes mēnesis" un "Drošāka interneta diena" ir izpratnes veidošanas iniciatīvu piemēri. Līdz šim iniciatīvā "Eiropas kiberdrošības izpratnes mēnesis" ir iesaistījušās septiņas trešās valstis[128]. Eiropola kampaņas "Saki nē!" mērķis ir mazināt risku, ka bērni var tikt pakļauti seksuālai izmantošanai un izspiešanai tiešsaistē. Ir svarīgi mazināt šo risku, jo patlaban tikai daži uzbrukumos cietušie ziņo par šiem noziegumiem policijai[129]. Komisija atzīst, ka kiberdrošības stratēģija iedzīvotāju un uzņēmumu izpratnes veidošanā ir bijusi tikai "daļēji efektīva"[130]. Šāda iznākuma iemesls ir uzdevumu vērienīgums, ierobežotie resursi, dalībvalstu nevienādā iesaiste un zinātnisku pierādījumu trūkums attiecībā uz to, kā efektīvāk veidot un izvērtēt izpratni.

90 Komisijas un attiecīgo aģentūru uzdevums ir nodrošināt, lai izpratnes veidošanas pasākumi būtu mērķtiecīgi un plaši popularizēti, iekļaujoši, atbilstīgi draudiem, pēc iespējas nerada nevēlamu ietekmi, piemēram, pārmērīgas drošības slogu[131], kā arī izstrādāt vērtēšanas metodes un rādītājus minēto pasākumu izvērtēšanai. Šādi pasākumi jāveic arī ES iestādēs, jo arī tajās izpratnes kultūra ir jāuzlabo[132].

8. problēma — labāka informācijas apmaiņa un koordinēšana

91 Lai panāktu kiberdrošību, ir jāveido publiskā un privātā sektora sadarbība, turklāt galvenokārt informācijas un paraugprakses apmaiņas veidā. Uzticībai ir izšķiroša nozīme visos līmeņos, lai izveidotu atbilstīgu vidi jutīgas informācijas apmaiņai pāri robežām. Slikta koordinācija veicina sadrumstalotību, centienu dublēšanos un vērtīgu zināšanu izkliedētību. Efektīva koordinācija var nodrošināt reālu pozitīvu ietekmi, piemēram, šifrēto tirdzniecības vietu darbības pārtraukšanu[133]. Neskatoties uz pēdējo gadu sasniegumiem, uzticības līmenis joprojām ir "nepietiekams"[134] gan ES mērogā, gan arī vairākās dalībvalstīs[135].

ES iestāžu un dalībvalstu darbību koordinācija

92 Viens no Kiberdrošības stratēģijas un saskaņā ar TID direktīvu ieviesto sadarbības struktūru mērķiem ir vairot uzticību ieinteresēto personu starpā. Izvērtējot stratēģiju, tika atzīts, ka ir izveidots pamats stratēģiskai un operatīvai sadarbībai ES līmenī[136]. Tomēr koordinācija kopumā joprojām ir "nepietiekama"[137]. Ir jānodrošina, lai informācijas apmaiņa būtu ne tikai jēgpilna, bet arī sniegtu pilnīgu priekšstatu par situāciju kopumā. Šai sakarā ļoti svarīgi ir panākt vienotu izpratni, pamatojoties uz saskaņotu terminoloģiju (sk. ***5. izcēlumu***).

93 Taču *ENISA* savā novērtējumā norādīja, ka ES pieeja kiberdrošībai nebija pietiekami koordinēta un tas neļāva panākt *ENISA* darbību sinerģiju ar citu ieinteresēto personu darbībām. Sadarbības mehānismi joprojām ir salīdzinoši jauni[138]; Kiberdrošības akta mērķis ir risināt šo jautājumu, stiprinot *ENISA* koordinācijas funkcijas. Vēlme uzlabot sadarbību bija iemesls tam, ka *ENISA*, Eiropas Aizsardzības aģentūra (EAA), Eiropola Eiropas Kibernoziedzības apkarošanas centrs un *CERT-EU* 2018. gadā parakstīja sapratnes memorandu[139]. Komisijas prioritāte turpmākajos gados būs nodrošināt politikas iniciatīvu, vajadzību un ieguldījumu programmu pienācīgu saskaņošanu, lai novērstu sadrumstalotību un veidotu sinerģiju[140].

94 Dažādas institucionālas struktūras veic koordinācijas funkcijas. Drošības savienības darba grupa tika izveidota, lai uzņemtos vadošo lomu Komisijas dažādo ģenerāldirektorātu koordinēšanā nolūkā sniegt atbalstu drošības savienības programmas īstenošanā[141]. CNECT ĢD vada darba grupas apakšgrupu kiberdrošības jautājumos.

95 Padomē kiberdrošības jautājumus risina Kiberjautājumu horizontālā darba grupa, kas koordinē stratēģiskos un horizontālos kiberjautājumus un palīdz sagatavot mācības un izvērtēt to rezultātus. Tā cieši sadarbojas ar Politikas un drošības komiteju, kas ir galvenā lēmumu pieņēmēja attiecībā uz visiem ar kiberjomu saistītiem diplomātiskajiem pasākumiem (sk. ***6. izcēlumu*** nākamajā nodaļā). Tā kā kiberdrošība ir transversāla joma, visu attiecīgo interešu koordinēšana nav vienkāršs uzdevums — ar kiberjomu saistītos jautājumus pēdējā laikā risina vismaz 24 darba grupas un sagatavošanas struktūras[142].

96 Divi pēdējie tiesību aktu priekšlikumi par *ENISA* stiprināšanu (2017. gads) un par kiberdrošības kompetenču centru tīkla un pētniecisko kompetenču centra izveidi (2018. gads) ir īpaši izstrādāti, lai mazinātu sadrumstalotību un centienu dublēšanos. Kiberdrošības kompetenču centru tīkla un pētniecisko kompetenču centra izveides

iemesls ir nepieciešamība novērst nepilnības, ar ko nenodarbojas saskaņā ar TID direktīvu izveidotās sadarbības struktūras, jo to uzdevums nav atbalstīt inovatīvu risinājumu attīstību.

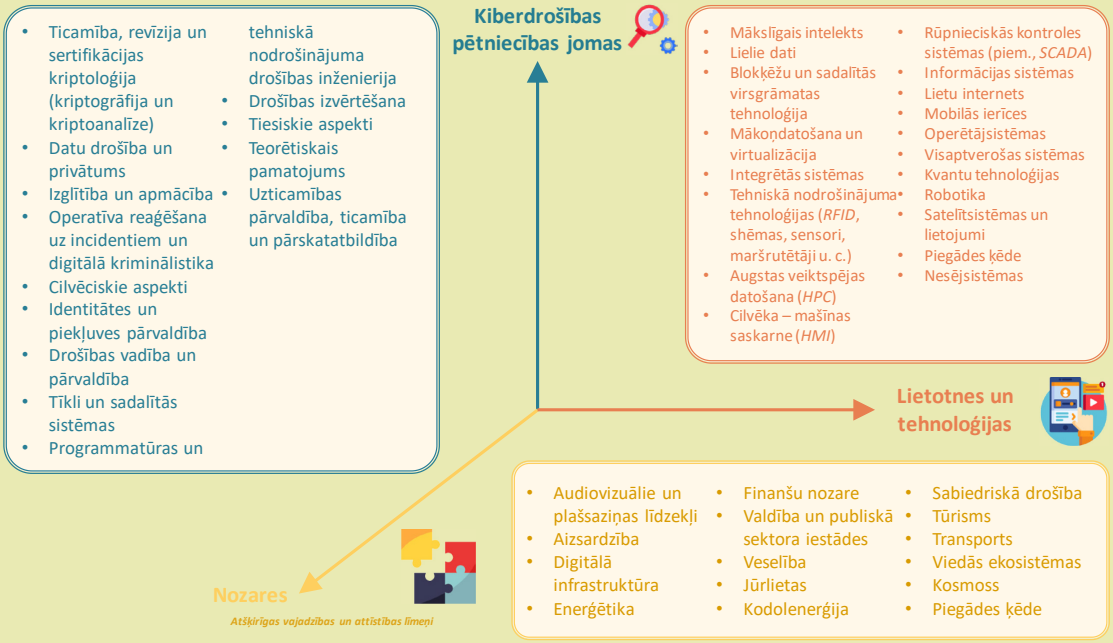
5. izcēlums

Centieni runāt vienā kibervalodā — *tehnoloģiju saskaņotība*

Terminoloģijas skaidrība vairo izpratni par situāciju un uzlabo koordināciju[143], kā arī palīdz precizēt, kas ir draudi un risks.

Komisijas Kopīgais pētniecības centrs (*JRC*), pamatojoties uz dažādiem starptautiskiem standartiem, nesen ir izveidojis pārskatītu pētniecības taksonomiju[144]. Paredzēts, ka tā kļūs par atsauces materiālu un katalogu pētniecības struktūrām visā Eiropā.

Kiberdrošības taksonomija



Avots: ERP, pamatojoties uz Eiropas Komisijas datiem.

Vēl nesen ES iestādes un aģentūras neizmantoja vienotas definīcijas. Situācija mainās. Atbilstīgi plānam sadarbības grupa izstrādāja incidentu taksonomiju ar mērķi veicināt efektīvu pārrobežu sadarbību.

Sadarbība un informācijas apmaiņa ar privātā sektora dalībniekiem

97 Publiskā sektora iestāžu un privātā sektora dalībnieku sadarbībai ir būtiska nozīme, lai uzlabotu vispārējo kiberdrošības līmeni. Tomēr Komisija savā 2017. gadā veiktajā Kiberdrošības stratēģijas novērtējumā konstatēja, ka informācijas apmaiņa privātā sektora ieinteresēto personu starpā un publiskā un privātā sektora dalībnieku starpā "joprojām nav optimāla", jo "trūkst uzticamu ziņošanas mehānismu un stimulu informācijas apmaiņai"[145], un tas traucē sasniegt stratēģiskos mērķus. Komisija ir arī norādījusi, ka trūkst efektīva sadarbības mehānisma, ko dalībvalstis varētu kopīgi izmantot, lai stratēģiski uzlabotu ilglaicīgas plaša mēroga nozares spējas[146].

98 Informācijas apmaiņas un analīzes centri (*ISACs*) ir organizācijas, kas izveidotas, lai nodrošinātu platformas un resursus informācijas apmaiņas veicināšanai publiskā un privātā sektora starpā, kā arī lai vāktu informāciju par kiberdraudiem. Mērķis ir radīt uzticību, apmainoties ar pieredzi, zināšanām un analīzes rezultātiem, it īpaši par pamatcēloņiem, incidentiem un draudiem. Valsts un nozaru informācijas apmaiņas un analīzes centri jau ir izveidoti daudzās valstīs, tomēr Eiropas līmenī to skaits joprojām ir salīdzinoši neliels[147]. Taču šie centri saskaras ar vairākām problēmām (resursu ierobežojumi, grūtības izvērtēt to panākumus, atbilstīgu struktūru nodrošināšana, lai iesaistītu gan publiskā, gan arī privātā sektora dalībniekus, tiesībaizsardzības iestāžu iesaistes nodrošināšana), kas būs jārisina, lai šie centri varētu palīdzēt īstenot TID direktīvu un veidot drošības spējas Eiropas līmenī[148].

99 Ciešai sadarbībai ar privāto sektoru ir īpaši svarīga nozīme, lai cīnītos pret sarežģītiem kibernoziegumiem, taču šādas sadarbības efektivitāte dalībvalstīs nav vienāda un ir atkarīga no uzticības līmeņa[149]. Tomēr Eiropola Eiropas Kibernoziedzības apkarošanas centrs ir izveidojis vairākas padomdevējas grupas, kurās piedalās privātā sektora dalībnieki, ES iestādes un aģentūras un citas starptautiskās organizācijas, lai uzlabotu sadarbību, veidojot tīklus, apmainoties ar stratēģiskiem izlūkdatiem un īstenojot sadarbību. Tās darbojas atbilstīgi plāniem, kas pielāgoti ES politikas cikla mērķiem[150]. Šifrēšanas izmantošana noziedzīgiem nolūkiem ir vēl viena joma, kas rada problēmas, kuru risināšanai vajadzīga ciešāka sadarbība ar privāto sektoru. Eiropola Eiropas Kibernoziedzības apkarošanas centrs patlaban izvērtē iespējas īpašos gadījumos Kopīgās kibernoziedzības rīcības uzdevumgrupā (sk. ***62. punktu***) īslaicīgi iesaistīt ekspertus no privātā sektora un akadēmiskajām aprindām.

100 Efektīvu sadarbības mehānismu trūkums negatīvi ietekmē civilo sabiedrību un aizsardzības kopienas gan publiskajā, gan arī privātajā sektorā. Kopīgas problemātiskās jomas cita starpā ir kriptogrāfija, drošas integrētās sistēmas, ļaunprogrammatūras

atklāšana, imitācijas metodes, tīklu un sistēmu komunikācijas aizsardzība un autentifikācijas tehnoloģijas. Civilās un militārās sadarbības veicināšana un atbalsts pētniecībai un tehnoloģiju attīstībai (it īpaši atbalsts MVU) ir divas no prioritātēm atjaunotajā ES kiberaizsardzības politikas satvarā (2018. gada atjauninājums).

Jautājumi pārdomām: noturības veidošana

- Kā ES līmenī panākt atbilstīgu līdzsvaru starp nepieciešamību racionalizēt kiberdrošības politiku un nodrošināt efektīvu koordināciju dažādo dalībnieku starpā, un kā sadalīt atbildību?
- Cik labi ES iestādes un aģentūras ir sagatavojušās nākamajam vērienīgam un tieši pret tām vērstam uzbrukumam?
- Kā ES kiberjomas aģentūras padarīt par pievilcīgākām darbvietām talantīgiem darbiniekiem?
- Kādi turpmākie pasākumi jāveic, lai nodrošinātu atbilstīgas spējas ES iestādēs un aģentūrās nolūkā izveidot saskaņotu risku un draudu novērtēšanas satvaru?
- Kā Eiropas uzraudzības iestādes (Eiropas banku iestāde, Eiropas Vērtspapīru un tirgu iestāde un Eiropas Apdrošināšanas un aroda pensiju iestāde) novērš kiberjomas nepilnības finanšu nozarē un kādu to pieredzi var izmantot citās nozarēs?
- Ņemot vērā īpašo zināšanu vispārējo trūkumu, kā pēc iespējas labāk izmantot ES tehnisko palīdzību publiskā sektora iestādēm, lai panāktu pēc iespējas lielāku kopējo ietekmi uz kibernoturības uzlabošanu?
- Kā ES un dalībvalstis var nodrošināt jēgpilnu klātbūtni starptautiskās diskusijās, lai veidotu kibertelpas pārvaldību un izstrādātu standartus, kā arī lai popularizētu ES vērtības?
- Kuri ES un dalībvalstu līmeņa izpratnes veidošanas pasākumi (tostarp preventīvie pasākumi) patiešām nodrošina pārmaiņas, un ko var darīt ES, lai palielinātu to ietekmi?
- Kāda ir ES loma, lai palīdzētu nodrošināt dzimumu dažādību kiberdrošības jomā?
- Kā ES un dalībvalstis var veicināt civilās sabiedrības un aizsardzības kopienas sinerģiju atbilstīgi kiberaizsardzības politikas satvaram (2018. gada atjauninājums)?

Efektīva reaģēšana uz kiberincidentiem

101 Efektīvas atbildes reakcijas uz kiberuzbrukumiem plānošanai ir būtiska nozīme, lai pēc iespējas savlaicīgāk apturētu šādu uzbrukumu veikšanu. Ir īpaši svarīgi, lai kritiskās nozares, dalībvalstis un ES iestādes spētu reaģēt ātri un saskaņoti. Šai sakarā būtiska nozīme ir savlaicīgai atklāšanai.

9. problēma — efektīva atklāšana un reaģēšana

Atklāšana un ziņošana

102 Kopēji atklāšanas mehānismi ik dienu palīdz apturēt lielāko daļu uzbrukumu[151]. Taču digitālās sistēmas ir kļuvušas tik sarežģītas, ka visus uzbrukumus novērst nav iespējams. Rafinētu līdzekļu izmantošana nodrošina to, ka uzbrukumi bieži netiek atklāti ilgu laiku. Tādēļ eksperti uzskata, ka uzsvars jāliek uz ātru atklāšanu un aizsardzību[152]. Taču daži atklāšanas paņēmieni, piemēram, automatizācija, mašīnmācīšanās un rīcības analīze, ko izmanto risku mazināšanai, kā arī sistēmas uzvedības analīze un mācīšanās no tās, uzņēmumos tiek izmantoti maz[153]. Daļēji iemesls ir maldīgi pozitīvu rezultātu ieguve, kuru dēļ darbības, kas nerada draudus, kļūdaini tiek uzskatītas par ļaunprātīgām.

103 Pēc pārkāpuma atklāšanas un analīzes ir jāveic ātra informēšana un ziņošana, lai citas publiskā un privātā sektora struktūras varētu veikt preventīvas darbības un attiecīgās iestādes varētu sniegt atbalstu tiem, kurus incidents ietekmējis. Daudzas organizācijas nevēlas atzīt kiberincidentus un ziņot par tiem[154]. Būtiska nozīme ir arī tiesībaizsardzības iestāžu agrīnai iesaistei sākotnējās darbībās, reaģējot uz iespējamiem kibernoziegumiem, un proaktīvai informācijas apmaiņai ar *CSIRT*.

104 Tā kā iepriekš nebija noteiktas vienotas ES prasības attiecībā uz ziņošanu par incidentiem, pastāvēja risks, ka var tikt aizkavēta informācijas par pārkāpumiem sniegšana un traucēta reaģēšana, — TID direktīva tika pieņemta, lai risinātu šos jautājumus (sk. ***20. punktu***). Pēc *Wannacry* uzbrukumiem 2017. gadā Komisija secināja, ka *CSIRT* tīkla sistēma "vēl nebija pilnībā funkcionāla"[155]. Turpinot īstenot direktīvu, joprojām atklāts ir jautājums, vai sadarbības grupas izstrādātās pamatnostādnes efektīvi palīdzēs pārvarēt nevēlēšanos ziņot par incidentiem[156].

105 Spēkā esošie ES noteikumi paredz, ka pamatpakalpojumu sniedzējiem konkrētās nozarēs ir dažādi informēšanas pienākumi (tostarp pienākums informēt

patērētājus), un tas var negatīvi ietekmēt procesa efektivitāti. Piemēram, uz pakalpojumu sniedzējiem finanšu un banku nozarē attiecas dažādi informēšanas kritēriji, standarti, robežvērtības un termiņi, ko paredz VDAR, TID direktīva, Maksājumu pakalpojumu direktīva, ECB un VUM, *TARGET2* un *eIDAS* regula[157]. Tādēļ ir svarīgi saskaņot šos pienākumus, jo šāds neviendabīgs regulējums ne tikai rada nevajadzīgu administratīvo slogu, bet arī var veicināt sadrumstalotību ziņošanas pienākumu izpildē.

Saskaņota reaģēšana

106 Eiropas sadarbības sistēma reaģēšanai uz kiberdrošības krīzēm joprojām tiek veidota. Tādēļ tika ieviests attiecīgais plāns[158] (sk. ***18. punktu***), lai kiberperspektīvu iekļautu Integrētajā krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismā, uzlabotu izpratni par situāciju un nodrošinātu labāku integrāciju citos ES krīzes pārvaldības mehānismos[159]. Plāna īstenošanā piedalās ES iestādes, aģentūras un dalībvalstis. Visu šo krīzes situāciju reaģēšanas mehānismu vienmērīga integrācija ir sarežģīts uzdevums[160]. Būtisks traucēklis ir arī tas, ka patlaban trūkst vienota un droša ES iestāžu komunikācijas tīkla[161].

107 ES spējas operatīvi un politiski reaģēt uz kiberuzbrukumiem plašapmēra pārrobežu incidentu gadījumā ir atzītas par "ierobežotām", un iemesls daļēji ir tas, ka kiberdrošība vēl nav integrēta pašreizējos ES līmeņa krīzes reakcijas koordinācijas mehānismos[162]. TID direktīva šo jautājumu nerisina.

108 Nesen ierosināto *ENISA* reformu, kas paredzēja plašākas operatīvās funkcijas, reaģējot uz plašapmēra kiberdrošības incidentiem, neatbalstīja dalībvalstis — tās uzskatīja, ka aģentūrai būtu jāatbalsta un jāpapildina to operatīvās darbības[163]. Dalībvalstu līmenī jau ir izveidotas daudzas*CERT*/*CSIRT*, taču to spējas būtiski atšķiras. Tas rada šķēršļus efektīvai pārrobežu sadarbībai, kas vajadzīga, lai reaģētu uz plašapmēra incidentiem[164].

109 Mēs mēģinājām noteikt atšķirīgās funkcijas, kas uzticētas dažādiem plānā minētajiem dalībniekiem, taču konstatējām nepilnības, kas būs jānovērš, turpinot plāna īstenošanu. Viens no sākotnēji nepietiekami risinātiem jautājumiem bija tiesībaizsardzība, lai gan ES tiesībaizsardzības ārkārtas reaģēšanas protokols stājās spējā 2018. gada decembrī[165]. Lai plānu sekmīgi īstenotu, ir svarīgi nodrošināt tā praktisku izpildi, nosakot visu pušu pienākumus; turpmākajos gados šai sakarā būs jāveic rūpīgas pārbaudes.

110 Efektīva reaģēšana nav tikai kaitējuma apzināšana; ļoti svarīgi ir arī noteikt atbildīgos par uzbrukumu veikšanu. Uzbrukumu veicēju izsekošana un identificēšana, it īpaši hibrīduzbrukuma gadījumā, var būt ļoti sarežģīta, jo arvien biežāk ļaunprātīgi tiek izmantotas anonimizācijas metodes, kriptovalūtas un šifrēšana. Šī problēma ir zināma kā attiecinājuma problēma. Tās risināšana nav tikai tehnisks jautājums — tas ir arī krimināls tiesvedības uzdevums. Juridiskās un procesuālās atšķirības valstīs var traucēt krimināllizmeklēšanā un kavēt aizdomās turēto saukšanu pie atbildības. Lai risinātu attiecinājuma problēmu, būs vajadzīga formālāka operatīvā informācijas apmaiņa, piemēram, ar Eiropolu vai *Eurojust* Eiropas Tiesu iestāžu tīklu kibernoziedzības jautājumos, izmantojot skaidrākas procedūras.

111 Politiskā līmenī ir izveidots kiberdiplomātijas instrumentu kopums (sk. ***6. izcēlumu***), lai sniegtu atbalstu starptautisku strīdu kibertelpā mierīgā izšķiršanā. Kiberdrošības ātrās reaģēšanas vienību izveide un iniciatīva savstarpējās palīdzības sniegšanai kiberdrošības jomā ir divi projekti, kas veicina efektīvāku informācijas apmaiņu, un tos izstrādā saskaņā ar *PESCO* satvaru[166].

6. izcēlums

Kiberdiplomātijas instrumentu kopums

ES satvars vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām[167] vai tā dēvētais kiberdiplomātijas instrumentu kopums tika izveidots, pamatojoties uz Padomes 2015. gada secinājumiem par kiberdiplomātiju[168]. Kiberdiplomātijas mērķis ir izveidot un īstenot vienotu un visaptverošu pieeju kibertelpai, pamatojoties uz ES vērtībām, tiesiskumu, spēju veidošanu un partnerībām, interneta pārvaldības veicināšanu, izmantojot vairāku ieinteresēto personu iesaistes modeli, kā arī kiberdrošības draudu novēršanu un starptautisko attiecību stabilitātes veicināšanu.

Instrumentu kopums dod iespēju ES un tās dalībvalstīm vienoti reaģēt uz ļaunprātīgām kiberdarbībām, pilnībā izmantojot pasākumus, ko paredz kopējā ārpolitika un drošības politika. Cita starpā tie var būt preventīvi pasākumi (piemēram, izpratnes vairošana, spēju veidošana), uz sadarbību un stabilitāti vērsti pasākumi un ierobežojoši pasākumi (piemēram, ceļošanas aizliegums, ieroču embargo, aktīvu iesaldēšana) vai atbalsts dalībvalstu reakcijai[169]. Pamatojums ir tāds, ka turpmāka sadarbība ar mērķi novērst draudus un dot skaidru signālu par vienotas reakcijas iespējamajām sekām var atturēt no (potenciāli) agresīvas rīcības.

Vienota ES reakcija uz ļaunprātīgām kiberdarbībām būtu samērīga ar attiecīgās kiberdarbības jomu, mērogu, ilgumu, intensitāti, sarežģītību, rafinētību un ietekmi.

Lai nodrošinātu instrumentu kopuma sekmīgu izmantošanu, būtiska nozīme būs tam, cik labi minētais kopums tiks iekļauts plānā un *IPCR* (sk. ***106.*** punktu), cik efektīvi tiks

apzināta situācija, veicot informācijas (tostarp attiecinājuma elementu) ātru un pastāvīgu apmaiņu[170], un, visbeidzot, vai tiks īstenota efektīva sadarbība. Instrumentu kopuma sekmīgas izmantošanas nodrošināšanā būtiska nozīme būs arī efektīvai un koordinētai komunikācijai. Līdz šim instrumentu kopums ir izmantots divas reizes, proti, lai sāktu dialogu ar Amerikas Savienotajām Valstīm pēc *Wannacry* uzbrukuma[171] un lai sagatavotu Padomes secinājumus ar mērķi paust nosodījumu par IKT ļaunprātīgu izmantošanu[172]. Patlaban notiek instrumentu kopuma izmantošanas iespēju apzināšana; vēl nav skaidrs, cik efektīvi tas darbosies, lai sasniegtu noteiktos mērķus.

10. problēma — kritiskās infrastruktūras un sabiedrības funkciju aizsardzība

Infrastruktūras aizsardzība

112 Lielu daļu ES kritiskās infrastruktūras ekspluatē, izmantojot rūpnieciskās kontroles sistēmas (RKS)[173]. Daudzas no šīm sistēmām tika izveidotas kā patstāvīgas sistēmas ar ierobežotu savienojamību ar pārējo pasauli. Kopš RKS komponenti ir pievienoti internetam, sistēmas kļuvušas neaizsargātākas pret ārēju iejaukšanos. Pastāvošo sistēmu uzturēšana un ielāpošana reizēm nav iespējama, taču to atjaunināšana nav ātrs process, turklāt rada izmaksas. Tādēļ centieniem uzlabot kritiskās infrastruktūras drošību ir jāietver RKS atjaunināšana.

113 Tā kā rūpniecībā turpinās digitalizācija (plašāk zināma kā ceturtā rūpniecības revolūcija), plašapmēra incidenta ietekmei vienā rūpniecības nozarē var būt plašāka ietekme uz citām nozarēm. *ENISA* ir norādījusi, ka ir svarīgi prognozēt kritisko nozaru savstarpējās atkarības ietekmi[174]. Šādām prognozēm ir būtiska nozīme, lai apzinātu incidenta seku iespējamo izplatību un attiecīgi izstrādātu efektīvi koordinētus atbildes pasākumus.

114 TID direktīvas mērķis ir uzlabot gatavību galvenajās nozarēs, kuras atbildīgas par kritisko infrastruktūru. Taču minētās direktīvas piemērošanas jomā nav iekļautas visas nozares (sk. ***1. tabulu***)[175], un šāda situācija "mazina stratēģijas efektivitāti"[176] — šai sakarā ir īpaši svarīgi aizsargāt vēlēšanu demokrātisko integritāti no iejaukšanās vēlēšanu infrastruktūrā un no dezinformācijas (sk. ***7. izcēlumu***). Tādēļ būtisks uzdevums būs ne tikai pārskatīt spēkā esošos tiesību aktus, bet arī apzināt, kā šīs nozares iesaistīt efektīvos pasākumos, lai reaģētu uz plašapmēra incidentiem.

115 Kritiskā infrastruktūra nav aizsargāta ne tikai Eiropā. Komisijas īpaši svarīgs uzdevums ir aicināt kandidātvalstis pieņemt tādus pašus standartus, kādus īsteno dalībvalstis, piemēram, attiecībā uz tiesību aktiem kiberjomā vai kritiskās infrastruktūras aizsardzību.

7. izcēlums

Kritisku sabiedrības funkciju aizsardzība: *cīņa pret iejaukšanos vēlēšanu norisē*

2019. gada maijā aptuveni 400 miljoni vēlētāju dosies balsot Eiropas Parlamenta vēlēšanās — tās būs pirmās vēlēšanas, kas notiks saskaņā ar VDAR. Tuvojoties vēlēšanām, ir jāņem vērā notikušie skandāli saistībā ar personas datu ļaunprātīgu izmantošanu politiskai mazapmēra ietekmēšanai, kā arī nepieredzēti efektīvi koordinētās dezinformācijas kampaņas (viltus ziņas). Komisija ir brīdinājusi par iespējamu kiberiejaukšanos arī šajās vēlēšanās[177]; lai to novērstu, būs vajadzīga visu valdību un visas sabiedrības kopēja pieeja.

Vēlēšanu infrastruktūra

Vēlēšanu organizēšana ir sarežģīta, un par to aizsardzības un integritātes nodrošināšanu ir atbildīgas dalībvalstis. Iejaukšanās vēlēšanās un vēlēšanu infrastruktūrā mērķis var būt ietekmēt vēlētāju izvēli, vēlēšanu iznākumu vai vēlēšanu norisi, tostarp balsošanas procesu, balsu skaitīšanu un rezultātu paziņošanu. Eiropas Parlamenta vēlēšanās tā dēvētās pēdējās jūdzes (rezultātu paziņošana no valstu galvaspilsētām Briselei) aizsardzība ir īpaši svarīgs uzdevums, ņemot vērā to, ka nav vienota drošības risinājuma vai ka šāds risinājums nav pārbaudīts[178].

Komisijas nesen pieņemtajā ar vēlēšanām saistītajā dokumentu kopumā bija iekļauti elektorāta kiberdrošības stiprināšanas pasākumi, piemēram, to valstu kontaktpunktu noteikšana, kuri koordinēs informāciju un nodrošinās informācijas apmaiņu, gatavojoties vēlēšanām. Īpaši būtiska nozīme ir paraugprakses un gūtās pieredzes apmaiņai[179].

Vēlēšanu sistēmas neuzskata par kritiskās infrastruktūras daļu[180], un uz tām neattiecas TID direktīva. Tomēr sadarbības grupa ir izstrādājusi praktiskas pamatnostādnes par vēlēšanās izmantoto tehnoloģiju drošību, lai sniegtu atbalstu publiskā sektora iestādēm. Tiek plānots, ka valstu kontaktpunktu pārstāvji tiksies 2019. gada sākumā[181]. Dalībvalstis tiek arī aicinātas veikt riska novērtējumus attiecībā uz kiberdraudiem, kas vērsti pret to vēlēšanu procesiem.

Dezinformācija

Dezinformācija kļūst par arvien būtiskāku elementu hibrīduzbrukumos, kas ietver kiberuzbrukumus un tīklu uzlaušanu. Dezinformāciju var izmantot, lai šķeltu sabiedrību, vairotu neuzticēšanos un apdraudētu ticību demokrātiskiem procesiem vai citiem jautājumiem (piemēram, dezinformācija par vakcinācijas kaitīgumu vai klimata pārmaiņām). Ir palielinājies dezinformācijas kampaņu apmērs, tās izplatīšanas ātrums un tvērums, un dezinformācija ir reāls Eiropas Savienības drošības apdraudējums.

ES ir veikusi vairākus pasākumus dezinformācijas apkarošanai. 2015. gadā EĀDD pakļautībā tika izveidota Austrumu Stratēģiskās komunikācijas operatīvā grupa ar mērķi vērsties pret Krievijas dezinformācijas kampaņām[182]. Eksperti ir atzinīgi novērtējuši tās darbu saistībā ar ES politikas veicināšanu, atbalstu neatkarīgiem plašsaziņas līdzekļiem kaimiņvalstīs un dezinformācijas prognozēšanu, izsekošanu un apkarošanu[183]. Taču, ņemot vērā dezinformācijas kampaņu apmēru un sarežģītību, operatīvās grupas resursi ir ierobežoti[184]. Ir vajadzīga sistemātiska mijiedarbība ar pašreizējām ES struktūrām un ciešāka sadarbība stratēģiskās komunikācijas jomā[185]. Eiropadome 2018. gada decembrī apstiprināja jaunu rīcības plānu[186].

Komisija, ņemot vērā tās 2018. gada aprīļa paziņojumu par dezinformācijas apkarošanu tiešsaistē[187], nesen ir izstrādājusi brīvprātīgi piemērojamu un pašregulatīvu prakses kodeksu[188], kas balstīts uz spēkā esošajiem politikas instrumentiem un ko tiešsaistes platformas un reklāmas nozares pārstāvji apņēmušies ievērot[189]. Paredzētie pasākumi cita starpā ir vairot satura uzticamību un atbalstīt centienus uzlabot medijpratību un spēju izvērtēt ziņu patiesumu. Ir izveidots arī neatkarīgs Eiropas faktu pārbaudītāju tīkls.

Komisija ir paziņojusi, ka, ja prakses kodekss netiks ievērots, var tikt pieņemti vēl citi regulatīvi pasākumi. Pasākumu efektivitātes izvērtēšanai būs izšķiroša nozīme, un it īpaši būs jāpieņem lēmums par to, kā izvērtēt uzlabojumus uzticības veidošanas, pārredzamības un pārskatatbildības jomā.

Vēl viens uzdevums būs rast risinājumus, kā uzlabot dezinformācijas atklāšanu, analīzi un atmaskošanu[190]. Ir jāveic arī publiski pieejamo datu avotu aktīva un stratēģiska uzraudzība un analīze[191]. Īstenojot centienus gūt labāku izpratni par draudu vidi, būtu jāņem vērā arī jaunās tendences, tādas kā satura dziļviltošana (viltus video materiālu sagatavošana, izmantojot mākslīgo intelektu un dziļo mašīnmācīšanos), kā arī instrumenti, kas vajadzīgi to atklāšanai.

Autonomijas palielināšana

116 ES ir kiberdrošības produktu un pakalpojumu neto importētāja, un tādēļ palielinās tehnoloģiskās atkarības no trešām valstīm risks, kā arī neaizsargātība pret

trešo valstu uzņēmumiem[192]. Šāda situācija īpaši apdraud ES kritiskās infrastruktūras drošību, jo šādas infrastruktūras izveidē piedalās arī sarežģītas globālās piegādes ķēdes. Risks vēl vairāk palielinās tad, ja Eiropas kiberdrošības uzņēmumus pārņem trešo valstu uzņēmumi. Dalībvalstis ir atbildīgas par ārvalstu tiešo ieguldījumu (ĀTI) pārbaudi, un patlaban nav ES mēroga pārbaudes mehānisma[193].

117 Lielāka stratēģiskā autonomija ir mērķis, kas noteikts ES globālajā stratēģijā un 2017. gada paziņojumā "*Noturība, novēršana un aizsardzība*"[194]. Šajā ziņojumā izklāstīto daudzo problēmu risināšana palīdzēs panākt autonomiju, uz ko tiecamies. To nevar nodrošināt ar vienu atsevišķu pasākumu.

Jautājumi pārdomām: efektīva reaģēšana

- Kā TID direktīva ir uzlabojusi situāciju ziņošanā par kiberincidentiem kritiskās nozarēs un citās nozarēs?
- Cik efektīvi ES iestādes internalizē krīzes reakcijas koordināciju plaša mēroga kiberincidentu gadījumā?
- Kā iespējams palielināt kiberdiplomātijas nozīmi ES ārējās darbībās?
- Vai pastāvošās ES struktūras un to darbības dezinformācijas apkarošanai ir samērīgas ar problēmas apmēru un sarežģītību?

Noslēguma piezīmes

118 Pēdējos gados Eiropas Savienība un tās dalībvalstis ir aktualizējušas kiberdrošības jautājumu, lai uzlabotu vispārējo kibernoturību. Taču augstāka kiberdrošības līmeņa nodrošināšana Savienībā joprojām ir ļoti vērienīgs uzdevums. Šajā informatīvajā apskatā esam uzsvēruši vairākas būtiskas problēmas, kas traucē ES sasniegt mērķi kļūt par pasaulē drošāko digitālo vidi.

119 Mūsu pārskats liecina, ka ir jāmaina pieeja un tai jābūt vērstai uz rezultātiem, kā arī jābalstās uz novērtēšanas praksi, lai nodrošinātu jēgpilnu **pārskatatbildību un izvērtēšanu**. **Spēkā esošajos tiesību aktos joprojām ir nepilnības, un dalībvalstis tos netransponē saskaņoti.** Šāda situācija var apgrūtināt tiesību aktu potenciāla pilnvērtīgu izmantošanu. Vēl viena konstatētā problēma ir saistīta ar **ieguldījumu līmeņa pielāgošanu stratēģiskajiem mērķiem**, kas nosaka nepieciešamību paaugstināt ieguldījumu līmeni un ietekmi. Situāciju sarežģī tas, ka ES un tās dalībvalstīm nav **skaidra priekšstata par ES finansējuma izlietojumu** kiberdrošības jomā. Tiek ziņots arī par **ES kiberjomas aģentūru ierobežotajiem resursiem,** tostarp par grūtībām piesaistīt un saglabāt talantīgus darbiniekus.

120 Pieejamajos pētījumos secināts, ka **kiberdrošības pārvaldību iespējams stiprināt**, lai uzlabotu pasaules sabiedrības spēju reaģēt uz kiberuzbrukumiem un incidentiem. Vienlaikus visus uzbrukumus novērst nav iespējams. Tādēļ **ātra atklāšana un reaģēšana,** kā arī **kritiskās infrastruktūras un sabiedrības funkciju aizsardzība** un labāka **informācijas apmaiņa un koordinācija** publiskā un privātā sektora starpā ir būtiskas problēmas, kas jārisina. Visbeidzot, arvien pieaugošais kiberdrošības prasmju trūkums visā pasaulē norāda uz to, ka būtiska problēma ir arī **prasmju uzlabošana un izpratnes vairošana** visās nozarēs un visos sabiedrības slāņos.

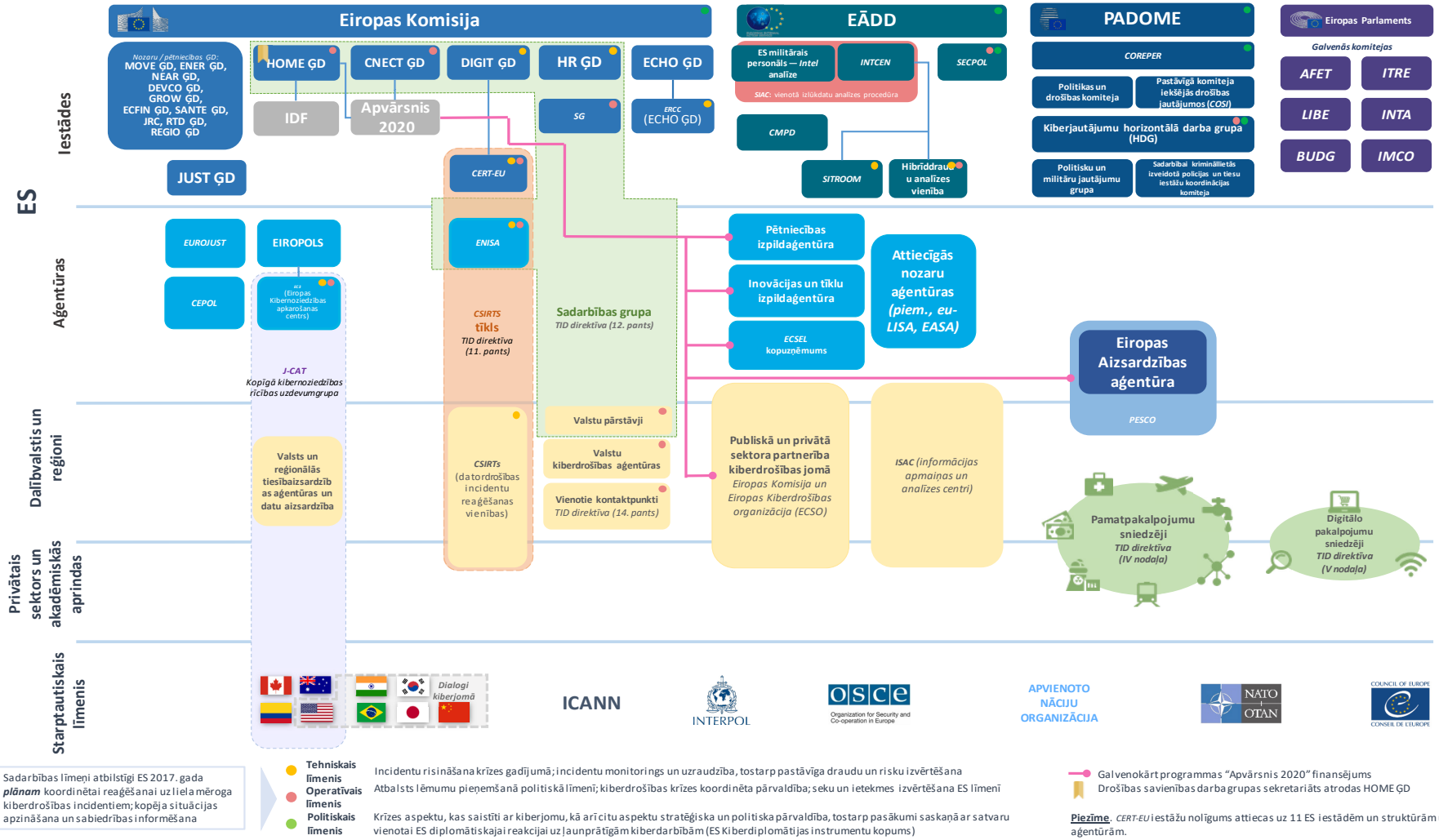
121 Šīs problēmas, ko rada kiberdraudi ES un plašākā globālā vidē, nosaka nepieciešamību arī turpmāk paust apņēmību un nelokāmi ievērot ES vērtības.

Šo informatīvo apskatu 2019. gada 14. februāra sēdē pieņēma Revīzijas palātas III apakšpalāta.

Revīzijas palātas vārdā –

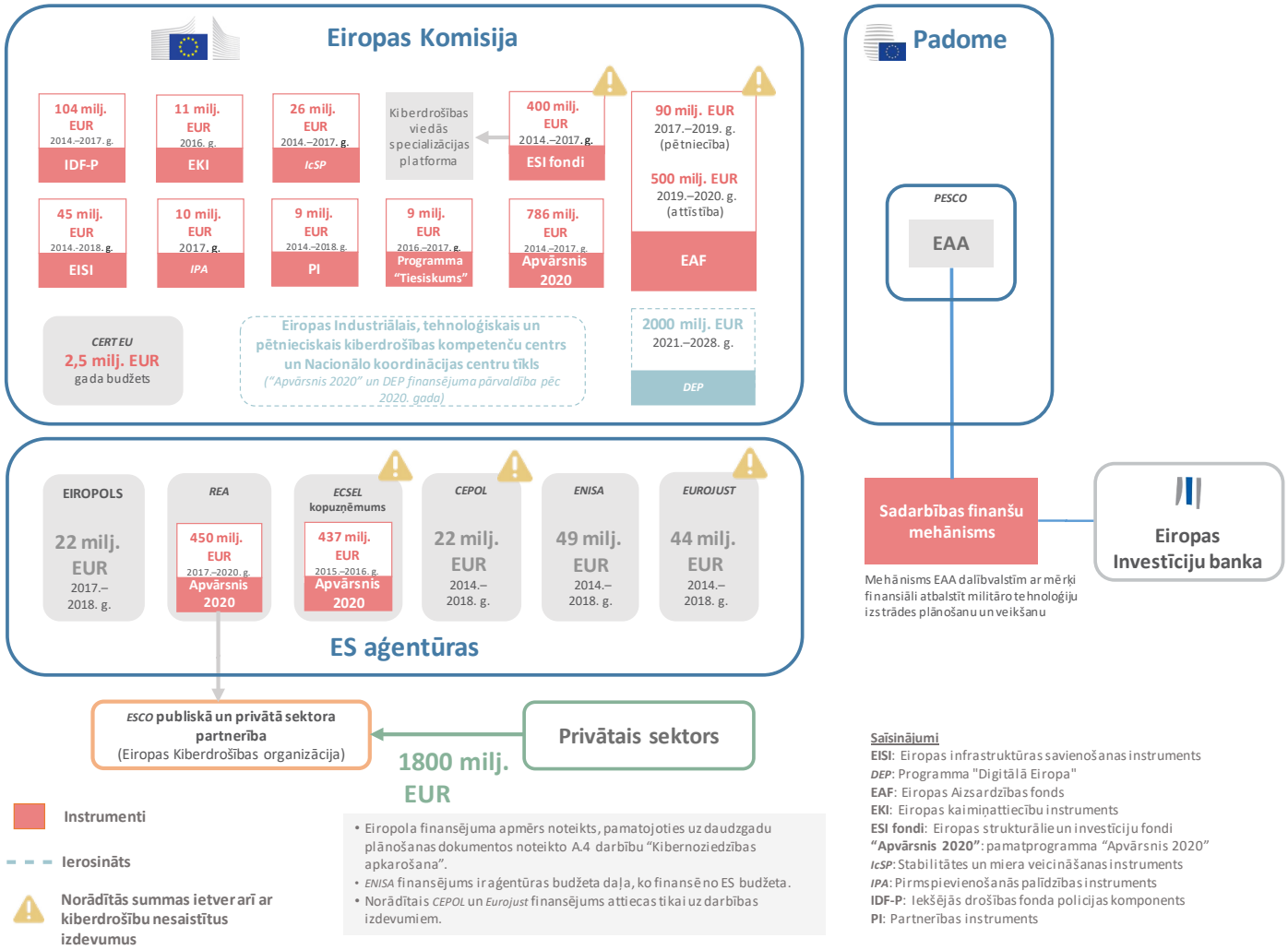
priekšsēdētājs
Klaus-Heiner Lehne

I pielikums. Sarežģīta vairāklīmeņu vide ar daudziem dalībniekiem



Avots: Eiropas Revīzijas palāta.

II pielikums. ES finansējuma izlietojums kiberdrošības jomā kopš 2014. gada



Avots: ERP, pamatojoties uz Eiropas Komisijas un ES aģentūru dokumentiem.

III pielikums. ES dalībvalstu revīzijas iestāžu ziņojumi

Veids	Nosaukums (ar hipersaiti)	Gads	Dalībvalsts
Atbilstības revīzijas	Iekšējās kontroles novērtējuma ziņojums	2014. g.	FR
	Apliecinājuma ziņojums par vispārējās sociālā nodrošinājuma sistēmas pārskatiem (aizsardzība, ārlietas)	2016. g.	FR
	Valsts pārskatu apliecinājums	2016. g.	FR
	Igaunijas valsts kritiski svarīgu datubāžu drošības un saglabāšanas nodrošināšana	2018. g. beigas / ziņojums vēl nav publicēts	EE
	Iekšējo kontroles pasākumu efektivitāte valsts datubāzēs esošo personas datu aizsardzībā	2008. g.	EE
Lietderības / ieguldīto līdzekļu atdeves revīzijas	Ziņojums par kiberuzbrukumu novēršanu	2013. g.	DK
	RiR 2014:23 Informācijas drošība civildienestā un valsts pārvaldē	2014. g.	SE
	Ziņojums par to, kā valdība apstrādā konfidenciālus datus par personām un uzņēmumiem	2014. g.	DK
	Valsts kiberdrošības programma	2014. g.	UK
	Vācijas Federālā Parlamenta ziņojums Budžeta komitejai saskaņā ar Federālā Budžeta kodeksa (*BHO*) 88. panta 2. punktu — IT konsolidācija, federālā valdība	2015. g.	DE
	Ziņojums par piekļuvi IT sistēmām, kas atbalsta pamatpakalpojumu sniegšanu Dānijas sabiedrībai	2015. g.	DK
	Francijas līdzenuma zemes izmantošanas plānošanas iestāde	2015. g.	FR
	Kiberdrošības vide Lietuvā teksts lietuviešu valodā kopsavilkums tulkots angļu valodā	2015. g.	LT
	Valsts iestāžu darbības rezultāti, veicot uzdevumus kiberdrošības jomā Polijā (poļu val.)	2015. g.	PL
	RiR 2015:21 Kibernoziedzība: policija un prokuratūra var strādāt efektīvāk	2015. g.	SE
	Digitālo prasmju trūkums valsts sektorā (apsekojums)	2015. g.	Apvienotā Karaliste
	Ziņojums federālajam parlamentam: "Federālās finanses: mantojuma nodokļa iekasēšana"	2016. g.	BE
	Ziņojums par IT drošības pārvaldību sistēmās, kuras nodrošina ārēji piegādātāji	2016. g.	DK
	Revīzijas ziņojums par Valsts kreditēšanas institūta aizdevumu darbībām 2016. gadā	2016. g.	ES
	Valsts drošības tīkla pārvaldība	2016. g.	FI
	Publiskā sektora uzdevumu veikšanai izmantoto IT sistēmu drošība	2016. g.	PL
	Aizskaršanas tiešsaistē novēršana un apkarošana bērnu un jauniešu vidū	2016. g.	PL
	Informācijas drošība deviņās aģentūrās	2016. g.	SE

Veids	Nosaukums (ar hipersaiti)	Gads	Dalībvalsts
	Revīzija par situāciju informācijas drošības jomā valstī RiR 2016:8		
	Informācijas aizsardzība valdībā	2016. g.	Apvienotā Karaliste
	Ziņojums par IT sistēmu un veselības datu aizsardzību trijos Dānijas reģionos	2017. g.	DK
	Piezīmes par starptautiskas paralēlās revīzijas "Iekšējo kontroles pasākumu efektivitāte valsts datubāzēs esošo personas datu aizsardzībā" rezultātiem	2017. g.	EE
	Kiberaizsardzības sistēma	2017. g.	FI
	Elektronisko pakalpojumu sniegšanas uzticamības pārvaldība	2017. g.	FI
	Lauksaimniecības kameru tīkls (kopsavilkums)	2017. g.	FR
	Voklīzes Tirdzniecības un rūpniecības kamera (Provansas-Alpu-Kotdazīras reģionālā revīzijas iestāde)	2017. g.	FR
	Igaunijas valsts kritiski svarīgu datubāžu drošības un saglabāšanas nodrošināšana	Pabeigta 2018. g. / ziņojums vēl nav publicēts	EE
	"Valsts elektroniskās komunikācijas infrastruktūras attīstība" teksts lietuviešu valodā kopsavilkums tulkots angļu valodā	2017. g.	LT
	IT revīzija: kiberdrošība valdības struktūrās	2017. g.	MT
	Valsts reģistru sistēma: drošība, darbības rezultāti un lietderība	2017. g.	PL
	WannaCry incidents	2017. g.	UK
	Krāpšana tiešsaistē	2017. g.	UK
	Ziņojums par aizsardzību pret uzbrukumiem, izmantojot izspiedējprogrammatūru	2018. g.	DK
	Arpažonas slimnīca (Ildefransas reģionālā revīzijas iestāde)	2018. g.	FR
	"Kritiskas valsts informācijas resursu pārvaldība"	2018. g.	LT
	"Elektroniskā noziedzība"	2019. g.	LT
	Informācijas drošība Polijā	2019. g.	PL
Cits	Valsts sektora struktūru datubāze	Neattiecas	BE
	Apsekojums par drošību un risku analīzes politiku (patlaban tiek veikts)	Neattiecas	BE

Akronīmi un abreviatūras

ĀTI: ārvalstu tiešie ieguldījumi

***CERT- EU*:** ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība

CNECT ĢD: Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts

***CSIRT*:** datordrošības incidentu reaģēšanas vienība

***DDoS*:** izkliedētais pakalpojuma atteikums

***DEP*:** programma "Digitālā Eiropa"

DIGIT ĢD: Informātikas ģenerāldirektorāts

EAA: Eiropas Aizsardzības aģentūra

EĀDD: Eiropas Ārējās darbības dienests

***EC3*:** Eiropola Eiropas Kibernoziedzības apkarošanas centrs

***ECSEL*:** Elektroniskie komponenti un sistēmas Eiropas vadošās lomas nostiprināšanai

***ECSM*:** Eiropas kiberdrošības izpratnes mēnesis

***ECSO*:** Eiropas Kiberdrošības organizācija

***ENISA*:** Eiropas Savienības Tīklu un informācijas drošības aģentūra

ERP: Eiropas Revīzijas palāta

ES: Eiropas Savienība

ESI fondi: Eiropas strukturālie un investīciju fondi

EUI: Eiropas Uzraudzības iestāde

HOME ĢD: Migrācijas un iekšlietu ģenerāldirektorāts

***HWPCI*:** kiberjautājumu horizontālā darba grupa

IDF - P: Iekšējās drošības fonda policijas komponents

IDKP: Informācijas drošības koordinācijas padome

***JRC*:** Kopīgais pētniecības centrs

JUST ĢD: Tiesiskuma un patērētāju ģenerāldirektorāts

KDAP: kopējā drošības un aizsardzības politika

LPPP: līgumiskā publiskā un privātā sektora partnerība

MVU: mazie un vidējie uzņēmumi

***NCIRC*:** NATO Datorincidentu reaģēšanas spējas

***PESCO*:** pastāvīgā strukturētā sadarbība

RKS: rūpnieciskās kontroles sistēmas

TID direktīva: Tīklu un informācijas drošības direktīva

VDAR: Vispārīgā datu aizsardzības regula

VIDS: vietējais informātikas drošības speciālists

VRI: valsts revīzijas iestāde

Glosārijs

Ar kibervidi saistīts noziegums: noziegums, ko var izdarīt, tikai izmantojot IT ierīces.

Datsmelšana: kredītkartes vai debetkartes datu zādzība, kad datus ievada tiešsaistē.

Dezinformācija: pārbaudāmi nepatiesa vai maldinoša informācija, kas tiek sagatavota, publiskota un izplatīta, lai gūtu ekonomisku labumu vai tīši maldinātu sabiedrību, un var radīt kaitējumu sabiedrībai.

Digitālais saturs: visi dati, piemēram, teksts, skaņas, attēli vai video, kas tiek glabāti digitālā formātā.

Hakeraktīvists: privātpersona vai grupa, kas nesankcionēti piekļūst informācijas sistēmām vai tīkliem, lai veicinātu sociālu vai politisku mērķu sasniegšanu.

Hibrīddraudi: pretinieku naidīga nodoma izpausme, izmantojot tradicionālu un netradicionālu karadarbības metožu apvienojumu (t. i., militārās, politiskās, ekonomiskās un tehnoloģiskās metodes) nolūkā nepiekāpīgi panākt savus mērķus.

Ielāpošana: izmaiņu kopums, ko ievieš programmatūrā, vai tās atjaunināšana, labošana vai uzlabošana, tostarp novēršot drošības apdraudējumus.

Informācijas drošība: tādu procesu un rīku kopums, kas aizsargā fiziskus un digitālus datus pret neatļautu piekļuvi, izmantošanu, izpaušanu, pārtraukšanu, grozīšanu, ierakstīšanu vai iznīcināšanu.

Integritāte: informācijas nepareizas pārveidošanas vai iznīcināšanas nepieļaušana un tās autentiskuma garantēšana.

Izkliedētais pakalpojuma atteikums (*DDoS*): kiberuzbrukums, kas liedz likumīgiem lietotājiem piekļūt tiešsaistes pakalpojumam vai resursam, to pārpludinot ar lielāku skaitu pieprasījumu, nekā tas spēj apstrādāt.

Iznīcinātājļaunatūra: ļaunprogrammatūras veids, kuras nolūks ir iznīcināt tā datora cietā diska saturu, ko tas inficē.

Izspiedējprogrammatūra: ļaunprātīga programmatūra, kas liedz cietušajiem piekļuvi datorsistēmai vai padara datnes nelasāmas, parasti izmantojot šifrēšanu. Tad uzbrucējs parasti šantažē cietušo un atsakās atjaunot piekļuvi, kamēr nav samaksāta izpirkuma maksa.

Kiberaizsardzība: kiberdrošības apakškopa, kuras mērķis ir aizsargāt kibertelpu ar militāriem un citiem piemērotiem līdzekļiem, lai sasniegtu militāri stratēģiskos mērķus.

Kiberdrošība: visas garantijas un pasākumi, kas pieņemti, lai aizsargātu IT sistēmas un to datus pret neatļautu piekļuvi, uzbrukumiem un bojājumiem nolūkā nodrošināt to pieejamību, konfidencialitāti un integritāti.

Kiberdrošības ekosistēma: ierīces, dati, tīkli, cilvēki, procesi un organizācijas, kas mijiedarbojas komplicētā kopienā, kā arī procesu un tehnoloģiju vide, kas ietekmē un atbalsta šo mijiedarbību.

Kiberincidents: notikums, kas tieši vai netieši kaitē IT sistēmas un tās apstrādāto, uzglabāto vai pārraidīto datu noturībai un drošībai vai arī tos apdraud.

Kibernoturība: spēja novērst un izturēt kiberuzbrukumus un incidentus, kā arī sagatavoties tiem un no tiem atgūties.

Kibernoziegumi: dažādas noziedzīgas darbības, kurās datori un IT sistēmas ir galvenais līdzeklis vai galvenais mērķis. Šīs darbības ietver: tradicionālus pārkāpumus (piemēram, krāpšana, viltošana un identitātes zādzība), ar saturu saistītus pārkāpumus (piemēram, bērnu pornogrāfijas izplatīšana tiešsaistē vai kūdīšana uz rasu naidu) un pārkāpumus, kas saistīti tikai ar datoriem un informācijas sistēmām (piemēram, uzbrukumi informācijas sistēmām, pakalpojumatteice un ļaunprātīga programmatūra).

Kibertelpa: nemateriāla globālā vide, kurā tiešsaistes saziņa notiek starp cilvēkiem, programmatūru un pakalpojumiem, izmantojot datortīklus un tehnoloģiskas ierīces.

Kiberuzbrukums: mēģinājums kibertelpā apdraudēt vai iznīcināt datu vai datorsistēmas konfidencialitāti, integritāti un pieejamību.

Konfidencialitāte: informācijas, datu vai aktīvu aizsardzība pret neatļautu piekļuvi vai izpaušanu.

Kriptovalūta: digitālais aktīvs, ko emitē un ar ko apmainās, izmantojot šifrēšanas metodes, neatkarīgi no centrālās bankas. Virtuālas kopienas locekļi to pieņem kā maksāšanas līdzekli.

Kritiskās infrastruktūras: fiziskie resursi, pakalpojumi un iekārtas, kuru darbības traucējumi vai iznīcināšana būtiski ietekmētu ekonomikas un sabiedrības darbību.

Lietu internets: tādu ikdienā lietojamu priekšmetu tīkls, kas aprīkoti ar elektroniku, programmatūru un sensoriem, lai tie varētu sazināties un apmainīties ar datiem internetā.

Ļaunatūra: ļaunprogrammatūra. Datorprogramma, kas paredzēta, lai nodarītu kaitējumu datoram, serverim vai tīklam.

Mantotā sistēma: mūsdienu prasībām neatbilstoša vai novecojusi datorsistēma, lietotne vai programmēšanas valoda, kas joprojām tiek izmantota, bet kurai, iespējams, vairs nav pieejami jauninājumi un pārdevēju atbalsts, tostarp drošības atbalsts.

Mākoņdatošana: IT resursu — piemēram, glabāšanas, datošanas jaudas vai datu koplietošanas jaudas — piegāde pēc pieprasījuma internetā, izmantojot izmitināšanu attālas piekļuves serveros.

Mūķu komplekts: instrumentu kopums, ko kibernoziedznieki izmanto, lai uzbruktu tīklu un informācijas sistēmu vājajām vietām nolūkā izplatīt ļaunprogrammatūru vai veikt citas ļaunprātīgas darbības.

Neaizsargātības pārvaldība: datordrošības un tīklu drošības neatņemama daļa, kuras nolūks ir proaktīvi mazināt vai novērst sistēmas un programmatūras vājo vietu ekspluatāciju, izmantojot to identifikāciju, klasifikāciju un koriģēšanu.

Noziegums, kas iespējams kibertelpā: tradicionāls noziegums, kas veikts plašākā mērogā, izmantojot IT sistēmas.

Personas dati: informācija, kas attiecas uz identificējamu personu.

Pieejamība: savlaicīgas un uzticamas piekļuves informācijai un tās izmantošanai nodrošināšana.

Piekļuves dati: informācija par lietotāja pieteikšanās un atteikšanās darbību, lai piekļūtu pakalpojumam, piemēram, laiks, datums un IP adrese.

Pikšķerēšana: tādu e-pasta vēstuļu nosūtīšana, kuru izcelsme atdarina uzticamu avotu, lai maldinātu saņēmējus un aicinātu tos klikšķināt uz ļaunprātīgām saitēm vai paziņot personisku informāciju.

Reklāmprogrammatūra: ļaunprātīga programmatūra, kas parāda reklāmkarogus vai uznirstošos logus un kas ietver kodu, lai izsekotu cietušo uzvedību tiešsaistē.

Robottīkls: ar ļaunprogrammatūru inficētu datoru tīkls, kurš tiek kontrolēts attālināti un kuru, lietotājam nezinot, izmanto, lai nosūtītu surogātpastu, nozagtu informāciju vai uzsāktu koordinētus kiberuzbrukumus.

Sociālā inženierija: attiecībā uz informācijas drošību — psiholoģiskas manipulācijas, lai maldinātu cilvēkus un tiem liktu veikt kādas darbības vai izpaust konfidenciālu informāciju.

Šifrēšana: nolasāmas informācijas pārveidošana nesalasāmā tās aizsardzības nolūkā. Lai izlasītu informāciju, lietotājam jābūt pieejamai slepenai atslēgai vai parolei.

Tekstu vektorizēšana: vārdu, teikumu vai visa dokumenta pārvēršana cipariskā vektorā, ko var izmantot mašīnmācīšanās algoritmi.

Tīkla drošība: kiberdrošības apakškopa, kas aizsargā datus, kuri nosūtīti ar viena un tā paša tīkla ierīcēm, lai nodrošinātu, ka informācija netiek pārtverta vai mainīta.

Uzņēmējdarbības modelis "noziegums kā pakalpojuma veids" (*Caas*): noziedzīgs uzņēmējdarbības modelis, kurš ir digitālās ēnu ekonomikas virzītājspēks, nodrošinot plašu komerciālo pakalpojumu un rīku klāstu, kas ļauj nekvalificētiem, iesācēja līmeņa kibernoziedzniekiem veikt kibernoziegumus.

Uzticamības pakalpojumi: pakalpojumi, kas uzlabo elektroniska darījuma juridisko spēku, piemēram, elektroniskie paraksti, zīmogi, laika zīmogi, reģistrēta piegāde un tīmekļa vietņu autentifikācija.

Vēlēšanu infrastruktūra: tā ietver informācijas kampaņā izmantotās IT sistēmas un datubāzes, sensitīvu informāciju par kandidātiem, vēlētāju reģistrācijas un pārvaldības sistēmas.

[1] ES Kiberdrošības akta projekt kiberdrošība definēta kā "visas darbības, kas jāveic, lai tīklu un informācijas sistēmas, to lietotājus un iesaistītās personas aizsargātu pret kiberdraudiem". Tiek plānots, ka Eiropas Parlaments un Padome aktu pieņems 2019. gada sākumā.

[2] Eiropols, *Internet Organised Crime Threat Assessment 2017* [Interneta organizētās noziedzības draudu novērtējums 2017. gadā].

[3] Eiropas Kiberdrošības organizācija (*ECSO*), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* [Eiropas kiberdrošības nozares priekšlikums par līgumiskas publiskā un privātā sektora partnerības izveidi], 2016. gada jūnijs.

[4] Eiropas Parlaments, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* [Kiberdrošība Eiropas Savienībā un aiz tās robežām: draudu un politikas risinājumu izpēte], pētījums Pilsoņu brīvību, tieslietu un iekšlietu komitejai (*LIBE*) komitejai, 2015. gada septembris.

[5] *ENISA*, *ENISA Threat Landscape Report 2017* [*ENISA* 2017. gada ziņojums par draudiem], 2018. gada 18. janvāris.

[6] Eiropols, *Internet Organised Crime Threat Assessment 2018* [Interneta organizētās noziedzības draudu novērtējums 2018. gadā].

[7] Eiropols, *turpat*, 2018. gads.

[8] Eiropas Politekonomikas centrs, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* [Intelektuālā īpašuma zādzība: vai pieļausim, ka datorspiegošana kavē Eiropu pasaules sacensībās par rūpniecības konkurētspēju?], Īpašais dokuments Nr. 2/18, 2018. gada februāris.

[9] Eiropas Komisija, priekšsēdētāja runa par stāvokli Savienībā 2017. gadā.

[10] Eiropols, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down* [Novērsti *DDoS* uzbrukumi, kas paralizēja pasaulē lielāko tiešsaistes tirgu], paziņojums presei, 2018. gada 25. aprīlis.

[11] Eiropols, *Internet Organised Crime Threat Assessment 2017* [Interneta organizētās noziedzības draudu novērtējums 2017. gadā].

[12] Eiropas Komisija, faktu lapa par kiberdrošību, 2017. gada septembris.

[13] Izmaksas var ietvert: zaudētos ieņēmumus, izmaksas saistībā ar bojāto sistēmu labošanu un iespējamo atbildību par nozagtiem aktīviem vai informāciju, izmaksas saistībā ar klientu saglabāšanas pasākumiem, lielākas apdrošināšanas prēmijas, palielinātas aizsardzības izmaksas (jaunas sistēmas, darbinieki, apmācība), iespējamās atbilstības nodrošināšanas izmaksas vai tiesvedības izmaksas.

[14] *NTT Security*, *Risk:Value 2018 Report* [Riska cena — 2018. gada ziņojums].

[15] *Wannacry* izspiedējprogrammatūra izmantoja nepilnības *Microsoft Windows* protokolā, kuras deva iespēju attālināti iegūt kontroli pār ikvienu datoru. Pēc nepilnību konstatācijas *Microsoft* izlaida atjauninājumu. Taču vairākiem simtiem tūkstošu datoru programmatūra nebija atjaunināta, un daudzi no šiem datoriem tika inficēti. *Avots*: *Greenberg, A.*, *Hold*

North Korea Accountable For Wannacry—and the NSA, too [Atbildība par *Wannacry* jāprasa Ziemeļkorejai un arī *NSA*], *WIRED*, 2017. gada 19. decembris.

[16] Eiropas Komisija, *Europeans' attitudes towards cybersecurity* [Eiropiešu attieksme pret kiberdrošību], Eirobarometra speciālaptauja 464a, 2017. gada septembris. Papildu aptauju plānots publicēt 2019. gada sākumā.

[17] Budapeštas konvencija ietver saistošas starptautiskas pamatnostādnes valstīm, kuras izstrādā tiesību aktus cīņā pret kibernoziedzību. Tā nodrošina satvaru starptautiskai sadarbībai starp valstīm, kas ir konvencijas puses. ES patlaban pārstāv Komisija, Eiropas Savienības Padome, Eiropols, *ENISA* un *Eurojust*.

[18] Eiropas Komisija, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* [Eiropas Savienības kiberdrošības stratēģija — atvērta un droša kibertelpa], JOIN (2013) 1 final, 2013. gada 7. februāris.

[19] Eiropas Komisija, *Eiropas Drošības programma*, COM(2015) 185 final, 28.4.2015.

[20] Eiropas Komisija, *Digitālā vienotā tirgus stratēģija Eiropai*, COM(2015) 192 final, 6.5.2015.

[21] EĀDD, *Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy* [Kopīga rīcība — spēcīgāka Eiropa. Globāla Eiropas Savienības ārpolitikas un drošības politikas stratēģija], 2016. gada jūnijs.

[22] Eiropas politikas pētījumu centrs, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* [ES kiberaizsardzības spēju stiprināšana: *CEPS* darba grupas ziņojums], 2018. gada novembris.

[23] Ļaunatūru, ko izmantoja *Wannacry* uzbrukumā, kura organizēšanā Amerikas Savienotās Valstis, Apvienotā Karaliste un Austrālija vainoja Ziemeļkoreju, sākotnēji izstrādāja un glabāja ASV Valsts drošības aģentūra, lai pētītu *Windows* nepilnības. *Avots*: *Greenberg, A.*, *turpat*, *WIRED*, 2017. gada 19. decembris. Pēc uzbrukumiem *Microsoft* pauda nosodījumu par to, ka valdības glabāja informāciju par programmatūras nepilnībām un vairākkārt aicināja noslēgt Ženēvas digitālo konvenciju.

[24] Tāpat kā sauszemi, jūru, gaisa telpu un kosmosu.

[25] ES kiberaizsardzības politikas satvars (2018. gada atjauninājums), 14413/18, 2018. gada 19. novembris.

[26] Eiropas Komisija, Eiropas Ārējās darbības dienests, *Kopīgs regulējums hibrīddraudu apkarošanai — Eiropas Savienības reakcija*, JOIN(2016) 18 final, 6.4.2016.

[27] Eiropadomes priekšsēdētāja, Eiropas Komisijas priekšsēdētāja un Ziemeļatlantijas līguma organizācijas ģenerālsekretāra 2016. gada 8. jūlija un 2018. gada 10. jūlija kopīgā deklarācija.

[28] Eiropas Komisija, Eiropas Ārējās darbības dienests, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* [Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību], JOIN (2017) 450 final, 13.9.2017.

[29] Eiropas Parlamenta un Padomes 2016. gada 6. jūlijaDirektīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

[30] Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

[31] Tās ir integrētas saskaņā ar direktīvu izveidotās sadarbības struktūrās, proti, *CSIRT* tīklā (tīkls, ko veido ES dalībvalstu izraudzītas *CSIRT* un *CERT-EU*; sekretariāts atrodas *ENISA* telpās) un sadarbības grupā (kas atbalsta un veicina stratēģisko sadarbību un informācijas apmaiņu dalībvalstu starpā; sekretariāts atrodas Komisijas telpās).

[32] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļaRegula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

[33] Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes regulai par ENISA – ES Kiberdrošības aģentūru – un Regulas (ES) Nr. 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju (''Kiberdrošības akts''),* COM (2017) 477 final, 13.9.2017.

[34] Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes regulai par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu gūšanai krimināllietās,* COM (2018) 225 final, 17.4.2018.

[35] Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes direktīvai, ar ko paredz saskaņotus noteikumus juridisko pārstāvju iecelšanai ar mērķi iegūt pierādījumus kriminālprocesā*, COM (2018) 226 final, 17.4.2018.

[36] Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes regulai, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu*, COM (2018) 630 final, 12.9.2018.

[37] *Carrapico, H*. un *Barrinha, A*., *The EU as a Coherent (Cyber)Security Actor?* [Vai ES ir vienots rīcībspēks (kiber)drošības jomā?], Kopējā tirgus pētījumu žurnāls, 55. sējums, Nr. 6, 2017. gads.

[38] Eiropas Komisija, turpat, SWD (2017) 295 final, 13.9.2017.

[39] Eiropas Parlamenta Izpētes dienests, *Transatlantic cyber-insecurity and cybercrime Economic impact and future prospects* [Transatlantiskā kibernedrošība un kibernoziedzība. Ekonomiskā ietekme un nākotnes prognozes], PE 603.948, 2017. gada decembris.

[40] *ENISA*, *An evaluation framework for Cyber Security Strategies* [Kiberdrošības stratēģiju izvērtēšanas satvars], 2014. gada 27. novembris.

[41] Izņēmums ir 14. pants (Uzraudzība un statistika) Eiropas Parlamenta un Padomes 2013. gada 12. augusta Direktīvā 2013/40/ES par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI.

[42] Eiropas Ekonomikas un sociālo lietu komiteja, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* [Kiberdrošība: Eiropas privātā sektora informētības un noturības nodrošināšana, ņemot vērā arvien pieaugošos kiberdrošības riskus], 2018. gada marts; *CEPS-ECRI* darba grupa, *Cybersecurity in Finance*: *Getting the policy mix right*! [Kiberdrošība finanšu jomā: atbilstīga politikas pasākumu kopuma pieņemšana], 2018. gada jūnijs.

[43] Uz mūsu aptaujas jautājumiem atbildēja 24 no 28 valsts revīzijas iestādēm.

[44] Tas nozīmē, ka politikai un regulējumam jābalstās uz principiem un tehnoloģiju ziņā jābūt pēc iespējas neitrālākiem.

[45] Eiropas Komisijas zinātnisko konsultāciju mehānisms, zinātniskais atzinums Nr. 2/2017, 2017. gada 24. marts.

[46] *Rebuffi, L.*, *EU Digital Autonomy: A possible approach* [ES digitālā autonomija — iespējamā pieeja], *Digma Zeitschrift für Datenrecht und Informationssicherheit*, 2018. gada septembris. Eiropas Politekonomikas centrs, turpat, Īpašais dokuments Nr. 2/18, 2018. gada februāris.

[47] Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes direktīvai par dažiem digitālā satura piegādes līgumu aspektiem*, COM(2015) 634 final, 9.12.2015.

[48] Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes direktīvai par dažiem preču tiešsaistes un cita veida distances pārdošanas līgumu aspektiem*, COM(2015) 635 final, 9.12.2015.

[49] Nīderlandes Kiberdrošības padome, *Eiropas 2016. gada sanāksme par prognozēm kiberdrošības jomā, Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care* [Publiskā un privātā sektora akadēmisko aprindu ieteikumi Eiropas Komisijai par lietu internetu un rūpības pienākumu saskaņošanu], 2016. gads.

[50] Eiropas politikas pētījumu centrs, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* [Informācijas par programmatūras nepilnībām izpaušana Eiropā: tehnoloģija, politika un juridiskie šķēršļi. *CEPS* darba grupas ziņojums], 2018. gada jūnijs.

[51] Eiropas Komisija, *TID direktīvas potenciāla maksimāla izmantošana – kā efektīvi īstenot Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā*, COM(2017) 476 final/2, 4.10.2017.

[52] Eiropols, turpat, 2017. gads.

[53] Eiropas Savienības Padome, *Gala ziņojums par septīto savstarpējo izvērtējumu kārtu par "Eiropas politikas nostādņu attiecībā uz kibernoziedzības novēršanu un apkarošanu praktisko īstenošanu un darbību"*, 12711/1/17 REV 1, 2017. gada 9. oktobris.

[54] Eiropas Komisija, *Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment* [Ietekmes novērtējums, kas pievienots direktīvas priekšlikumam par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem], SWD/2017/0298 final, 13.9.2017. Politiska vienošanās par jauno tiesību aktu tika panākta 2018. gada decembrī, un sagaidāms, ka tas tiks pieņemts 2019. gada sākumā.

[55] Eiropols, turpat, 2017. gads.

[56] Lieta C-362/14, *Maximillian Schrems* pret datu aizsardzības komisāru (Īrija), 2015. gada 6. oktobris.

[57] Eiropols, *Eurojust*, *Common challenges in combating cybercrime* [Kopīgas problēmas kibernoziedzības apkarošanā], 7021/17, 2017. gada 13. marts.

[58] Eiropas Komisija, *Assessment of the EU 2013 Cybersecurity Strategy* [ES 2013. gada kiberdrošības stratēģijas izvērtējums], SWD (2017) 295 final, 13.9.2017.

[59] Eiropas Parlamenta Izpētes dienests, *Briefing: EU Legislation in Progress – Review of dual-use export controls* [Informatīvs dokuments: ES tiesību akti izstrādes procesā — divējāda lietojuma preču eksporta kontroles pasākumu pārskatīšana], *PE 589.832*.

[60] Eiropas Parlamenta rezolūcija, *"Cilvēktiesības un tehnoloģijas — ielaušanās un uzraudzības sistēmu ietekme uz cilvēktiesībām trešās valstīs"*, (2014/2232(INI)), 2015. gada 8. septembris. Divējāda lietojuma preces un pakalpojumus, kas ietver programmatūru un tehnoloģiju, var izmantot gan civilām, gan arī militārām vajadzībām.

[61] Publiski pieejama informācija tiek glabāta *WHOIS* datubāzē, ko pārvalda *ICANN* (Piešķirto nosaukumu un numuru interneta korporācija). *ICANN* uztur domēna nosaukumu sistēmu. Domēna nosaukumu neatbilstīga izmantošana veicina kibernoziedzību.

[62] TID direktīvas 3. pants, turpat.

[63] Ziemeļatlantijas Padome, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* [Risku apburtais loks: vai kiberriski gūst pārsvaru? Dažādu kiberjomas nākotnes scenāriju ekonomiskie ieguvumi un izmaksas], 2015. gada 10. septembris.

[64] Baltais Nams, *Cybersecurity spending fiscal year 2019* [Finansējums kiberdrošības jomā 2019. fiskālajā gadā].

[65] Eiropas Komisija, *Commission Staff Working Document: Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'* [Komisijas dienestu darba dokuments "Ietekmes novērtējums, kas pievienots priekšlikumam Eiropas Parlamenta un Padomes regulai, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu"], SWD(2018) 305 final, 6.6.2018.

[66] Hāgas Stratēģisko pētījumu centrs, *Dutch investments in ICT and cybersecurity: putting it in perspective* [Nīderlandes ieguldījumi IKT un kiberdrošības jomā: plašāka perspektīva], 2016. gada decembris.

[67] Eiropas Komisija, turpat, COM (2018) 630 final, 12.9.2018.

[68] Eiropas Parlamenta Izpētes dienesta Zinātniskās perspektīvikas nodaļa, *Achieving a sovereign and trustworthy ICT industry in the EU* [Suverēnas un uzticamas IKT nozares izveide ES], 2017. gada decembris.

[69] Eiropas digitālās nozares MVU alianse, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* [Nostājas dokuments par Eiropas kiberdrošības stratēģiju: MVU ekosistēmas veidošana], 2017. gada 31. jūlijs.

[70] Eiropas Parlamenta Izpētes dienesta Zinātniskās perspektīvikas nodaļa, turpat, 2017. gada decembris.

[71] Turpat.

[72] Eiropas Komisija, *Ietekmes novērtējums par priekšlikumu regulai, ar ko izveido pētniecisko kompetenču centru un Nacionālo koordinācijas centru tīklu*, SWD(2018) 403 final (1. daļa no 4), 12.9.2018.

[73] Eiropas Komisija, turpat, COM (2018) 630 final, 12.9.2018.

[74] ERP Īpašais ziņojums Nr. 13/2018 "Vēršanās pret radikalizāciju, kas ved uz terorismu".

[75] Šajā iedaļā norādītās summas ir minētas publiski pieejamos Komisijas dokumentos, izņemot ***51. punktā*** minēto summu 42 miljoni EUR, par ko Komisija mūs informēja tieši.

[76] Pamatprogramma "Apvārsnis 2020" ir ES 80 miljardus EUR vērta pētniecības un inovācijas programma, kas nodrošina atbalstu Inovācijas savienības izveidei ar mērķi nodrošināt ES konkurētspēju pasaulē.

[77] Pamatprogrammas "Apvārsnis 2020" 7. sabiedrības problēma: "Drošas un inovatīvas sabiedrības izveide Eiropas un tās iedzīvotāju brīvības un drošības aizsardzībai".

[78] Mēs analizējām "Apvārsnis 2020" projektus, izmantojot *CORDIS* datu kopu. Mēs veicām katra projekta apraksta teksta vektorizēšanu, izmantojot Kopīgā pētniecības centra kiberdrošības taksonomiju (sk. ***5. izcēlumu*** nākamajā nodaļā), lai noteiktu projektus, kuri varēja būt saistīti ar kiberdrošību. Pēc tam mēs manuāli pārbaudījām un analizējām rezultātus.

[79] Eiropas Kiberdrošības organizācija, *ECS cPPP Progress Monitoring Report 2016-2017* [Eiropas kiberdrošības LPPP 2016.–2017. gada progresa uzraudzības ziņojums], 2018. gada 29. oktobris.

[80] TID direktīva, 9. panta 2. punkts, turpat.

[81] Projekts *GLACY+* (Kopīga rīcība kibernoziedzības jomā plus) ir kopējs projekts, ko īsteno sadarbībā ar Eiropas Padomi. Īstenojot šo projektu, tiek sniegts atbalsts divpadsmit valstīm Āfrikā, Āzijas un Klusā okeāna reģionā un Latīņamerikas un Karību jūras reģionā, kas var kļūt par centriem, kuri dalās ar iegūto pieredzi attiecīgajos reģionos.

[82] Eiropas Politiskās stratēģijas centrs (EPSC) — Komisijas domnīca — ir norādījis, ka, ja turpinās palielināties ES un tās Rietumbalkānu reģiona kaimiņvalstu atšķirības, pastāv risks, ka var izveidoties tā dēvētais digitālais vakuums. Tādas valstis kā Ķīna un Krievija veic

ievērojamus ieguldījumus šajā reģionā, un tas var radīt risku, ka ES kļūs par atstumtu kibertelpas rīcībspēku šajā reģionā. *Avots*: EPSC, *Engaging with the Western Balkans: an investment in Europe's security* [Sadarbība ar Rietumbalkānu reģionu — ieguldījums Eiropas drošībā], 2018. gada 17. maijs.

[83] Eiropas Investīciju banka, *The EIB Group Operating Framework and Operational Plan 2018* [EIB grupas darbības programma un darbības plāns 2018. gadam], 2017. gada 12. decembris. Šā dokumenta sagatavošanas laikā papildu informācija nebija pieejama.

[84] Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes regulai, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu*, COM(2018) 434 final, 6.6.2018.

[85] Eiropas Komisija, *Eiropas Parlamenta un Padomes 2018. gada 18. jūlija Regula (ES) 2018/1092, ar ko izveido Eiropas aizsardzības rūpniecības attīstības programmu, lai atbalstītu Savienības aizsardzības rūpniecības konkurētspēju un inovētspēju* (OV L 200, 7.8.2018, 30. lpp.). Turklāt 2017. gadā tika veiktas darbības, lai sagatavotos pētniecībai aizsardzības jomā, 2017.–2019. gada periodam paredzot finansējumu 90 miljonu EUR apmērā, kas tiks atvēlēts no programmas "Apvārsnis 2020" līdzekļiem. Nav skaidrs, vai šī summa ietver arī ar kiberdrošību saistītus izdevumus.

[86] ERP ir paredzējusi 2019. gadā publicēt atsevišķu informatīvo apskatu par ES aizsardzības jomu.

[87] Eiropola *EC3*, *ENISA*, EĀDD, Eiropas Aizsardzības aģentūras un *CERT-EU* kopējais darbinieku skaits ir 159. Tas neietver kiberdrošības jomā iesaistītos darbiniekus Eiropas Komisijā vai dalībvalstīs. *Avots*: Eiropas Politikas pētījumu centrs, turpat, 2018. gada novembris.

[88] *ENISA novērtējums*, 2017. gads.

[89] Eiropols savā 2018.–2020. gada daudzgadu plānā pieprasīja katru gadu palielināt darbinieku skaitu par 70 pagaidu darbiniekiem, taču 2018. gadā apstiprinātais darbinieku skaita pieaugums bija tikai 26 darbinieki. Nākamā daudzgadu plāna projektā 2019.–2021. gadam Eiropols norādīja mērenāku darbinieku skaita pieaugumu, "pieņemot, ka lielāks resursu pieprasījums netiks izpildīts". *Avots*: apspriežu dokuments par daudzgadu plāna projektu 2019.–2021. gadam, kas iesniegts Kopīgajai parlamentārās uzraudzības grupai, A 000834, 2018. gada 1. februāris.

[90] *ENISA novērtējums*, 2017. gads. Laikposmā no 2014. līdz 2016. gadam aptuveni 80 % *ENISA* darbības budžeta tika izlietoti pētījumu pasūtīšanai.

[91] *ENISA*, *Exploring the opportunities and limitations of current Threat Intelligence Platforms* [Draudu izlūkdatu pašreizējo platformu iespējas un ierobežojumi], 2017. gada decembris.

[92] *ISACA* (iepriekš zināma kā Informācijas sistēmu revīzijas un kontroles asociācija), *Information Security Governance: Guidance for Boards of Directors and Executive Management* [Informācijas drošības pārvaldība: pamatnostādnes vadības struktūrām un vadošajiem darbiniekiem], 2. izdevums, 2006. gads.

[93] *EY*, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* [Kiberdrošība atjaunota — gatavojoties pārvarēt kiberuzbrukumus. Divdesmitais globāla mēroga apsekojums par informācijas drošību 2017. gadā], 16. lpp.

[94] *McKinsey* (*Choi, J., Kaplan, J., Krishnamurthy, C. un Lung, H.*), *Hit or myth? Understanding the true costs and impact of cybersecurity programs* [Panākums vai mīts? Kiberdrošības programmu patiesās izmaksas un ietekme], 2017. gada jūlijs.

[95] Vērtspapīru un biržas darījumu komisija, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* [Paziņojums un skaidrojošas pamatnostādnes par kiberdrošības informāciju, ko publisko atklātas akciju sabiedrības], 2018. gada 21. februāris.

[96] Sadarbības forums, kurā piedalās Eiropas Banku iestāde, Eiropas Vērtspapīru un tirgu iestāde un Eiropas Apdrošināšanas un aroda pensiju iestāde.

[97] Eiropas Vērtspapīru un tirgu iestāde, *Joint Committee report on risks and vulnerabilities in the EU financial system* [Apvienotās komitejas ziņojums par ES finanšu sistēmas riskiem un nepilnībām], 2018. gada aprīlis.

[98] *ENISA*, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs* [Informācijas drošības un privātuma standarti MVU: ieteikumi informācijas drošības un privātuma standartu efektīvākai piemērošanai MVU], 2015. gada decembris.

[99] Komisijas zinātnisko konsultāciju mehānisms, atsaucoties uz ES dalībvalstīm, ir norādījis, ka ir panākts "ievērojams un unikāls vienprātības līmenis par pamatprincipiem un vērtībām, kā arī ir paustas vienotas stratēģiskās intereses, kas var veidot pamatu efektīvai ES kiberdrošības pārvaldībai". *Avots*: zinātniskais atzinums Nr. 2/2017, 2017. gada 24. marts.

[100] ASV, Ķīna, Japāna, Dienvidkoreja, Indija un Brazīlija.

[101] Eiropas Drošības un aizsardzības koledža (*Renard, T., Barrinha, A.*), *Handbook on cyber security* [Kiberdrošības rokasgrāmata], 3.4. nodaļa "ES kā partnere kiberdiplomātijas un aizsardzības jomā", 2018. gada 23. novembris.

[102] Eiropas Savienības Padome, *Rīcības plāns, lai īstenotu Padomes secinājumus par kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību"*, 15748/17, 2017. gada 12. decembris.

[103] Eiropas Komisija, *Eiropas Komisijas Digitālā stratēģija:digitāli pārveidota, uz lietotāju vērsta un uz datiem balstīta Komisija*, C(2018) 7118 final, 21.11.2018.

[104] Komisāres *M. Gabriel* atbilde uz Parlamenta rakstisko jautājumu (E-004294-17), 2017. gada 28. jūnijs.

[105] Eiropas Savienības Padome, *Annual Report on the Implementation of the Cyber Defence Policy Framework* [Gada ziņojums par kiberaizsardzības politikas satvara īstenošanu], 15870/17, 2017. gada 19. decembris.

[106] Lēmumi 2015/443, 2015/444 un 2017/46 reglamentē Komisijas komunikācijas un informācijas sistēmu drošību. Ar Komisijas 2018. gada 21. novembra Lēmumu C(2018) 7706

ir izveidota Informācijas tehnoloģijas un kiberdrošības valde, kas apvieno iepriekšējās IT padomes un Informācijas drošības koordinācijas valdes funkcijas.

[107] Eiropas Ekonomikas un sociālo lietu komiteja, turpat, 2018. gada marts.

[108] Eiropas Parlaments, turpat, 2015. gada septembris.

[109] Hibrīddraudu analīzes vienību izveidoja 2016. gadā EĀDD ES Izlūkošanas un situāciju centrā. Tā saņem klasificētu un publiskos avotos pieejamu informāciju no dažādām ieinteresētajām personām par hibrīddraudiem un analizē to.

[110] *ENISA*, *National-level Risk Assessments: An Analysis Report* [Valsts līmeņa riska novērtējumi: analīzes ziņojums], 2013. gada novembris.

[111] Eiropas Komisija, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act* [ES Kiberdrošības aģentūras un Kiberdrošības akta ietekmes novērtējums], SWD(2017) 500 final (1. daļa no 6), 13.9.2017.

[112] Eiropas Komisija, turpat, SWD(2018) 403 final, 12.9.2018.

[113] *Résaux IP Européens* tīkla koordinācijas centrs — Eiropas reģionālais interneta reģistrs, kas uzrauga interneta reģistrācijas numuru resursu piešķiršanu un reģistrāciju.

[114] *ENISA*, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* [*EISAS* plaša mēroga izmēģinājuma un kopdarbības projekts ES iedzīvotāju un MVU izpratnes vairošanai], 2012. gada novembris.

[115] Kiberdrošības un izglītības centrs partnerībā ar *Booz Allen Hamilton*, *Alta Associates* un *Frost & Sullivan, 2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* [2017. gada globāla mēroga apsekojums par darbaspēku informācijas drošības jomā: darbaspēka spēju un reaģēšanas uz kiberriskiem salīdzinoša novērtēšana].

[116] Eiropas Ekonomikas un sociālo lietu komiteja, turpat, 2018. gada marts.

[117] Lordu palātas un *Pārstāvju palātas Apvienotā komiteja jautājumos par valsts drošības stratēģiju, kiberdrošības prasmēm un Apvienotās Karalistes valsts kritisko infrastruktūru, 2017.–2019. gada sesijas otrais ziņojums*, 2018. gada 16. jūlijs.

[118] Eiropols, *Eurojust*, *Common challenges in combating cybercrime* [Kopīgas problēmas kibernoziedzības apkarošanā], 7021/17, 2017. gada 13. marts.

[119] Eiropols, *Eurojust*, turpat, 7021/17, 2017. gada 13. marts.

[120] Eiropas Komisija, turpat, SWD(2018) 403 final, 12.9.2018.

[121] *CEPOL*, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022* [Valdes Lēmums Nr. 33/2018/MB par *CEPOL* vienoto programmdokumentu 2020.–2022. gadam], 2018. gada 20. novembris.

[122] Piemēram, sadarbība starp EĀDD, dalībvalstīm, aģentūrām un tādām struktūrām kā *CEPOL*, *ECTEG* vai *ESDC*.

[123] *ENISA*, *Stock-taking of information security training needs in critical sectors* [Novērtējums par apmācības vajadzībām informācijas drošības jomā svarīgākajās nozarēs], 2017. gada decembris.

[124] Eiropas Kibernoziedzības apkarošanas apmācības un izglītības grupa.

[125] Eiropas Komisija, Trīspadsmitais progresa ziņojums virzībā uz efektīvu un patiesu drošības savienību, COM(2018) 46 final, 24.1.2018.

[126] Konstatējums izdarīts, pamatojoties uz apsvērumiem Īpašajā ziņojumā Nr. 14/2018, turpat.

[127] Eiropas Parlamenta 2018. gada 13. jūnija rezolūcija par kiberaizsardzību (2018/2004(INI)). Eiropas Savienības Padome, turpat, 15870/17, 2017. gada 19. decembris.

[128] Šveice, bijusī Dienvidslāvijas Maķedonijas Republika, Ukraina, Bosnija un Hercegovina, Kosova (šis nosaukums neskar nostāju par statusu un atbilst ANO Drošības padomes rezolūcijai Nr. 1244/1999 un Starptautiskās Tiesas atzinumam par Kosovas neatkarības deklarāciju), Turcija un ASV.

[129] Eiropols, *Internet Organised Crime Threat Assessment 2018* [Interneta organizētās noziedzības draudu novērtējums 2017. gadā].

[130] Eiropas Komisija, turpat, SWD (2017) 295 final, 13.9.2017.

[131] *Stanton, B., Theofanos, M. F., Prettyman, S. S. un Furman, S.*, *Security Fatigue* [Pārmērīgas drošības slogs], *IT Professional*, 18. izdevums, Nr. 5, 2016. gads, 26.–32. lpp. Sk. arī *NIST*.

[132] Eiropas Komisija un Eiropas Ārējās darbības dienests, *Noturības un spēju palielināšana cīņā ar hibrīddraudiem*, JOIN (2018) 16 final, 13.6.2018.

[133] Piemēram, tirdzniecības vietu *AlphaBay* un *Hansa* slēgšana, īstenojot kopīgas operācijas, ko ar Eiropola atbalstu vadīja FIB un Nīderlandes Valsts policija. Tās bija divas no lielākajām tirdzniecības vietām, kurās notika tirdzniecība ar nelikumīgām precēm, tādām kā narkotikas, ieroči un kibernoziedzības instrumenti, piemēram, ļaunatūra. *Avots*: Eiropols, *Crime on the Dark Web: Law Enforcement coordination is the only cure* [Noziedzība tumšajā tīklā: vienīgais risinājums ir tiesībaizsardzības koordinācija], paziņojums presei, 2018. gada 29. maijs.

[134] Eiropas Komisija, turpat, SWD(2018) 403 final, 12.9.2018.

[135] Eiropas Savienības Padome, turpat, 12711/1/17 REV 1, 2017. gada 9. oktobris.

[136] Eiropas Komisija, turpat, SWD (2017) 295 final, 13.9.2017.

[137] Eiropas Komisija, Eiropas Ārējās darbības dienests, turpat, JOIN(2018) 16, 2018. gada 13. jūnijs.

[138] Eiropas Komisija, SWD (2017) 500 final, 13.9.2017.

[139] *ENISA, EAA, Eiropola Eiropas Kibernoziedzības apkarošanas centra un CERT-EU saprašanās memorands*, 2018. gada 23. maijs.

[140] Eiropas Komisija, uzaicinājums iesniegt piedāvājumus *"Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap"* [Izmēģinājuma projekta izstrāde un īstenošana ar mērķi izveidot kiberdrošības kompetenču centru tīklu, lai izstrādātu un īstenotu kopēju kiberdrošības pētniecības un inovācijas ceļvedi], 2017. gada 27. oktobris.

[141] *Jean-Claude Juncker*, *Mission letter for the Commissioner for the Security Union* [Pilnvarojuma vēstule drošības savienības komisāram], 2016. gada 2. augusts. Aizsardzība nav darba grupas darbības jomā.

[142] Eiropas Savienības Padome, *EU cybersecurity roadmap* [ES kiberdrošības ceļvedis], 8901/17, 2017. gada 11. maijs.

[143] Organizācija *Friends of Europe*, *Debating Security Plus: Crowdsourcing solutions to the world's security issues* [Debates par drošību un citiem jautājumiem: pasaules drošības problēmu kolektīvie risinājumi], *5. izdevums*, 2017. gada novembris.

[144] *JRC* tehniskie ziņojumi, Eiropas kiberdrošības lietpratības centru karte: *definīcijas un taksonomija.* Ietekmes novērtējums par priekšlikumu regulai, ar ko izveido pētniecisko kompetenču centru un Nacionālo koordinācijas centru tīklu, SWD(2018) 403 final, 12.9.2018.

[145] Eiropas Komisija, turpat, SWD (2017) 295 final, 13.9.2017.

[146] Eiropas Komisija, turpat, SWD(2018) 403 final, 12.9.2018.

[147] Piemēram, Eiropas finanšu iestāžu *ISAC* darbībā piedalās finanšu nozaru pārstāvji, valstu datorapdraudējumu reaģēšanas vienības, tiesībaizsardzības aģentūras, *ENISA*, Eiropols, Eiropas Centrālā banka, Eiropas Maksājumu padome un Eiropas Komisija.

[148] *ENISA*, *Information Sharing and Analysis Centres (ISACs) Cooperative models* [Informācijas apmaiņas un analīzes centru (*ISACs*) sadarbības modeļi], 2018. gada 14. februāris.

[149] Eiropas Savienības Padome, turpat, 12711/1/17 REV 1, 2017. gada 9. oktobris.

[150] https://www.europol.europa.eu/empact.

[151] *Accenture* 2018. gadā 15 valstīs veikta pētījuma rezultāti parādīja, ka 87 % mērķtiecīgu kiberuzbrukumu tika novērsti, — *2018 State of Cyber Resilience* [Situācija kibernoturības jomā 2018. gadā], 2018. gada 10. aprīlis.

[152] *Timmers, P.*, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* ([Kiberdrošība liek pārdomāt stratēģisko autonomiju], Oksfordas Universitātes politikas blogs, 2018. gada 14. septembris.

[153] *Caroline Preece*, *Three reasons why cyber threat detection is still ineffective* [Trīs iemesli, kādēļ kiberdraudu atklāšana joprojām ir neefektīva], *IT Pro*, 2017. gada 14. jūlijs.

[154] Eiropas Ekonomikas un sociālo lietu komiteja, *turpat*, 2018. gada marts.

[155] Eiropas Komisija, *Astotais progresa ziņojums virzībā uz efektīvu un patiesu drošības savienību*, COM(2017) 354 final, 29.6.2017.

[156] Sk. dažādas TID sadarbības grupas publikācijas.

[157] *PSD2* — otrā Maksājumu pakalpojumu direktīva; ECB un VUM — Eiropas Centrālā banka un vienotais uzraudzības mehānisms; *TARGET2* — Eiropas Vienotā automatizētā reālā laika bruto norēķinu sistēma (2. paaudze); Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū. *Avots*: *CEPS-ECRI* darba grupa, turpat, 2018. gada jūnijs.

[158] Eiropas Komisija, *Ieteikums par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm*, C(2017) 6100 final, 13.9.2017.

[159] Eiropas Komisija, turpat, SWD (2017) 295 final, 13.9.2017. Ir izveidoti vairāki krīžu pārvarēšanas mehānismi, tostarp Integrētais krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānisms, *Argus* (Komisijas krīzes situāciju reaģēšanas mehānisms), EĀDD krīzes situāciju reaģēšanas mehānisms, Savienības civilās aizsardzības mehānisms un ES tiesībaizsardzības ārkārtas situāciju reaģēšanas protokols.

[160] Turklāt tas var būt iemesls, lai piemērotu Līguma par Eiropas Savienību 42. panta 7. punktu (savstarpējās palīdzības klauzula) vai Līguma par Eiropas Savienības darbību 222. pantu (solidaritātes klauzula).

[161] Eiropas Komisija, Eiropas Ārējās darbības dienests, turpat, JOIN(2018) 16, 2018. gada 13. jūnijs. 2018. gada decembrī plašsaziņas līdzekļos tika ziņots par iespējamiem uzbrukumiem EĀDD diplomātiskās komunikācijas tīklam *COREU* (avots: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran* [Uzbrukumi Eiropas tīkliem atklāj satraukumu saistībā ar Trampu, Krieviju un Irānu], 2018. gada 18. decembris). Lieta patlaban tiek izmeklēta.

[162] Ir jāturpina attīstīt arī sadarbību agrīnās brīdināšanas un savstarpējās palīdzības jomā: *Padomes secinājumi par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm*, 10086/18, 2018. gada 26. jūnijs.

[163] Eiropas Parlamenta Izpētes dienests, *Informatīvs dokuments "EU Legislation in Progress: ENISA and a new cybersecurity act"* [ES tiesību aktu izstrāde: *ENISA* un jaunais Kiberdrošības akts], PE 614.643, 2018. gada septembris.

[164] Eiropas Ekonomikas un sociālo lietu komiteja, turpat, 2018. gada marts.

[165] Eiropas Savienības Padome, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks* [ES tiesībaizsardzības ārkārtas reaģēšanas protokols (*LE ERP)* plašapjoma pārrobežu kiberuzbrukumiem], 14893/18, 2018. gada decembris.

[166] Kiberdrošības ātrās reaģēšanas vienības un savstarpēja palīdzība kiberdrošības jomā; kiberdraudu un kiberincidentu reaģēšanas informācijas apmaiņas platforma. *Avots*: Eiropas Savienības Padome, *Pastāvīgā strukturētā sadarbība (PESCO), PESCO projektu atjaunināts saraksts: pārskats*, 2018. gada 19. novembris.

[167] Eiropas Savienības Padome, *Secinājumi par ES satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām*, 9916/17, 2017. gada 7. jūnijs.

[168] Eiropas Savienības Padome, *Secinājumi par kiberdiplomātiju*, 6122/15, 2015. gada 11. februāris.

[169] Eiropas Savienības Padome, *Satvara vienotai diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām īstenošanas pamatnostādņu projekts*, 13007/17.

[170] Atbildību par incidentu joprojām attiecina dalībvalstis, pieņemot suverēnu politisku lēmumu, turklāt ne visi instrumentu kopuma pasākumi nosaka attiecinājuma nepieciešamību.

[171] Instrumentu kopuma izmantošana neveicināja vienotu rīcību; atsevišķas dalībvalstis pieņēma ASV nostāju.

[172] Eiropas Savienības Padome, *Secinājumi par ļaunprātīgām kiberdarbībām*, 7925/18, 2018. gada 16. aprīlis.

[173] Datorizētas sistēmas, ko izmanto, lai kontrolētu procesus dažādās nozarēs, piemēram, sabiedrisko pakalpojumu nozarē, ķīmijas un rūpnieciskajā ražošanā, pārtikas pārstrādē, transporta sistēmās un centros, kā arī loģistikas pakalpojumu nozarē.

[174] *ENISA*, turpat, 2017. gada decembris.

[175] Piemēram, valsts pārvalde, ķīmiskā un kodolrūpniecība, ražošana, pārtikas pārstrāde, tūrisms, loģistika un civilā aizsardzība.

[176] Eiropas Komisija, turpat, SWD (2017) 295 final, 13.9.2017.

[177] Komisāres *Věra Jourová* runa Eiropas Parlamenta plenārsesijā *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign* [Jāpalielina ES noturība pret ārvalstu rīcībspēku ietekmi uz gaidāmo EP vēlēšanu kampaņu], 2018. gada 14. novembris.

[178] Kārnegi Starptautiskā miera fonds, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* [Krievijas iejaukšanās vēlēšanās: Eiropa cīnās pret viltus ziņām un kiberuzbrukumiem], 2018. gada 23. maijs.

[179] Eiropas Politiskās stratēģijas centrs (*Past, L.*), *Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses* [Vēlēšanās izmantoto tehnoloģiju kiberdrošība: neizbēgami uzbrukumi un atšķirīga reakcija], publicēts: "*Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts*" [Iejaukšanās vēlēšanās digitālajā laikmetā — noturības pret kiberdraudiem veidošana: 35 vadošo praktiķu un ekspertu pārdomu dokumenti], 2018. gads.

[180] Saskaņā ar Padomes Direktīvu 2008/114/EK par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību.

[181] Eiropas Komisija, Ieteikums par vēlēšanu sadarbības tīkliem, tiešsaistes pārredzamību, aizsardzību pret kiberdrošības incidentiem un cīņu pret dezinformācijas kampaņām saistībā ar Eiropas Parlamenta vēlēšanām, C(2018) 5949 final, 12.9.2018.

[182] Eiropadomes secinājumi, EUCO 11/15, 2015. gada 20. marts. Kopš tā laika ir izveidotas vēl divas operatīvās grupas darbībām, kas saistītas ar Rietumbalkānu reģionu un dienvidu kaimiņreģioniem.

[183] Ziemeļatlantijas Padomes ziņojumā ES tika aicināta pieprasīt visām dalībvalstīm norīkot valsts ekspertus darbā operatīvajā grupā. Sk. *Fried, D*. un *Polyakova, A*., *Democratic Defense Against Disinformation* [Demokrātiska aizsardzība pret dezinformāciju], 2018. gada 5. marts.

[184] Operatīvajai grupai sākotnēji nebija sava budžeta; 2018. gadā Eiropas Parlaments tai piešķīra 1,1 miljonu EUR sagatavošanās darbības "*StratCom Plus*" veikšanai.

[185] Kārnegi Starptautiskā miera fonds (*Brattberg, E., Maurer, T*.), turpat, 2018. gada 23. maijs.

[186] Eiropas Komisija, Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos, *Rīcības plāns dezinformācijas apkarošanai*, JOIN(2018) 36 final. Plānā uzsvars likts uz šādiem jautājumiem: jāuzlabo ES iestāžu spēja atklāt, analizēt un atmaskot dezinformāciju, jāpastiprina koordinēta un kopēja reakcija, jāmobilizē privātais sektors, kā arī jāvairo izpratne un jāpastiprina sabiedrības noturība.

[187] Eiropas Komisija, *Vēršanās pret dezinformāciju tiešsaistē: Eiropas pieeja*, COM(2018) 236 final, 26.4.2018.

[188] Nejaukt ar rīcības kodeksu nelikumīgas naida runas apkarošanai tiešsaistē.

[189] *JRC*, *The digital transformation of news media and the rise of disinformation and fake news* [Ziņu mediju digitālā pārveide un dezinformācijas un viltus ziņu izplatība], *JRC* tehniskie ziņojumi, *JRC* digitālās ekonomikas darba dokuments Nr. 2018-02, 2018. gada aprīlis.

[190] *ENISA*, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")* [Tīklu un informācijas drošības stiprināšana un aizsardzība pret dezinformāciju (viltus ziņām) tiešsaistē], 2018. gada aprīlis.

[191] Eiropas Politiskās stratēģijas centrs (*Frutos López, C*.), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* [Atbildība par atbalsta nodrošināšanu vēlēšanu administrēšanas iestādēm, lai tās varētu sagatavoties kiberdraudiem un novērst tos], turpat, 2018. gads.

[192] Eiropas Komisija, turpat, SWD(2018) 403 final, 12.9.2018.

[193] Attiecībā uz 2017. gada septembrī iesniegto priekšlikumu regulai par ĀTI izvērtēšanu (COM(2017) 487 final, 13.9.2017.) patlaban tiek īstenota likumdošanas procedūra. Tajā īpaša vērība pievērsta kritiskām tehnoloģijām, kas ietver mākslīgo intelektu, kiberdrošību un divējāda lietojuma tehnoloģijas.

[194] Eiropas Komisija, Eiropas Ārējās darbības dienests, turpat, JOIN(2017) 450, 13.9.2017.

ERP darbinieku grupa

Informatīvo apskatu *"Problēmas, kas traucē īstenot efektīvu ES kiberdrošības politiku"* pieņēma ERP locekles *Bettina Jakobsen* vadītā III apakšpalāta, kuras pārziņā ir ārējo darbību un drošības un tiesiskuma izdevumu jomu revīzija. Darbu vadīja ERP loceklis *Baudilio Tomé Muguruza*, un viņam palīdzēja locekļa biroja vadītājs *Daniel Costa de Magalhaes* un locekļa biroja atašejs *Ignacio Garcia de Parada*, atbildīgais vadītājs *Alejandro Ballester-Gallardo*, darbuzdevuma vadītājs *Michiel Sweerts*, revidenti *Simon Dennett*, *Aurelia Petliza*, *Mirko Iaconisi*, *Michele Scardone*, *Silvia Monteiro Da Cunha* un praktikants *Johannes Bolkart*. Lingvistisko atbalstu sniedza *Hannah Critoph*.

No kreisās uz labo: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

EIROPAS REVĪZIJAS PALĀTA

Publikāciju birojs

EIROPAS REVĪZIJAS PALĀTA
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tālrunis: +352 4398-1

Uzziņām: eca.europa.eu/lv/Pages/ContactForm.aspx
Tīmekļa vietne: eca.europa.eu
Twitter: @EUAuditors