IETEIKUMI

KOMISIJAS IETEIKUMS (ES) 2017/1584

(2017. gada 13. septembris)

par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 292. pantu,

tā kā:

(1) Informācijas un komunikācijas tehnoloģiju lietošana un paļaušanās uz tām visās saimnieciskās dzīves nozarēs ir kļuvušas par fundamentāliem aspektiem laikā, kad mūsu uzņēmumi un pilsoņi ir cits ar citu pāri nozarēm un robežām saistīti un savstarpēji atkarīgi vairāk nekā jebkad agrāk. Kiberdrošības incidents, kas ietekmē organizācijas vairāk nekā vienā dalībvalstī vai pat visā Savienībā un kam ir potenciāls nopietni traucēt iekšējo tirgu un plašākā nozīmē tīklu un informācijas sistēmas, kurās balstās Savienības ekonomika, demokrātija un sabiedrība, ir scenārijs, kam dalībvalstīm un ES iestādēm jābūt gatavām.

(2) Kiberdrošības incidentu var uzskatīt par Savienības mēroga krīzi tad, ja izraisītais traucējums ir tik plašs, ka tā skartā dalībvalsts nespēj viena ar to tikt galā, vai skar divas vai vairāk dalībvalstis tik plašā apmērā un ar tādu tehnisku un politisku nozīmi, ka prasa laicīgu koordinēšanu un reaģēšanu Savienības politiskajā līmenī.

(3) Kiberdrošības incidenti var izraisīt plašāku krīzi, skarot plašākas darbības nozares, ne tīklu un informācijas sistēmas un sakaru tīklus vien; pienācīgai reaģēšanai ir jābalstās gan uz kiberdrošības apdraudējuma, gan visāda citāda apdraudējuma novēršanas pasākumiem.

(4) Kiberdrošības incidenti nav prognozējami, mēdz rasties un attīstīties īsā laika sprīdī, un to skartajām struktūrām un atbildīgajiem par pretdarbību un incidenta seku mazināšanu reaģēšana ir jākoordinē ātri. Kiberdrošības incidenti arī neaprobežojas ar tikai vienu ģeogrāfisku apgabalu, bet var vienlaicīgi rasties un acumirklī izplatīties daudzās zemēs.

(5) Efektīvai atbildei uz plaša mēroga kiberdrošības incidentiem un krīzēm ES līmenī ir vajadzīga ātra un efektīva sadarbība starp visām attiecīgajām ieinteresētajām personām, un tā balstās uz atsevišķo dalībvalstu gatavību un jaudām, kā arī koordinētu vienotu rīcību ar atbalstu no Savienības jaudām. Tātad laicīga un efektīva reaģēšana uz incidentiem ir atkarīga no iepriekš izveidotām un iespēju robežās ietrenētām sadarbības procedūrām un mehānismiem, kur valsts un Savienības līmenī skaidri noteikta katra galvenā izpildītāja loma un pienākumi.

(6) 2011. gada 27. maija secinājumos ([1]) par informācijas kritiskās infrastruktūras aizsardzību Padome mudināja ES dalībvalstis "stiprināt sadarbību starp dalībvalstīm un, pamatojoties uz valstu gūto pieredzi un rezultātiem krīžu pārvarēšanas jomā un sadarbojoties ar *ENISA*, kiberincidentu jomā veicināt Eiropas sadarbības mehānismu izstrādi, kurus iecerēts izmēģināt 2012. gadā saistībā ar nākamajām mācībām *CyberEurope*".

(7) 2016. gada paziņojums "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari" ([2]) mudināja dalībvalstis optimāli izmantot TID direktīvas ([3]) noteiktos sadarbības

([1]) Padomes secinājumi par informācijas kritiskās infrastruktūras aizsardzību "Sasniegumi un turpmākie pasākumi virzībā uz globālu kiberdrošību", dok. 10299/11, Brisele, 2011. gada 27. maijs.
([2]) COM(2016) 410 final, 2016. gada 5. jūlijs.
([3]) 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 (OV L 194, 19.7.2016., 1. lpp.).

mehānismus un stiprināt pārrobežu sadarbību, kas skar gatavību plašapmēra kiberdrošības incidentiem. Tur arī minēts, ka gatavību uzlabotu koordinēta pieeja sadarbībai krīzes brīdī visos kiberdrošības sistēmas elementos, kas būtu izklāstīta "plānā", un ka tādam plānam būtu arī jānodrošina sinerģija un saskanība ar pastāvošajiem krīzes pārvarēšanas mehānismiem.

(8) Padomes secinājumos ([1]) par minēto paziņojumu dalībvalstis aicināja Komisiju tādu plānu iesniegt atbildīgajām struktūrām un attiecīgajām ieinteresētajām personām apsvēršanai. Tomēr TID direktīvā nav paredzēta Savienības sadarbības sistēma plašapmēra kiberdrošības incidentu un krīžu gadījumiem.

(9) Komisija apspriedās ar dalībvalstīm divos atsevišķos konsultatīvos semināros, kas notika Briselē 2017. gada 5. aprīlī un 4. jūlijā, dalībvalstu pārstāvjiem no datordrošības incidentu reaģēšanas vienībām (*CSIRT*), sadarbības grupu, kas izveidota ar TID direktīvu, un Padomes kiberjautājumu horizontālo darba grupu, kā arī pārstāvjiem no Eiropas Ārējās darbības dienesta (EĀDD), *ENISA*, *Europol*/*EC3* un Padomes Ģenerālsekretariāta (PĢS).

(10) Šim ieteikumam pievienotais koordinētas reaģēšanas plāns plašapmēra kiberdrošības incidentu un krīžu risināšanai Savienības līmenī ir tapis pēc minētajām konsultācijām un papildina paziņojumu "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari".

(11) Plānā aprakstīti un noteikti mērķi un veidi dalībvalstu sadarbībai ar ES iestādēm, struktūrām, dienestiem un aģentūrām (tālāk – "ES iestādes") reaģēšanā plašapmēra kiberdrošības incidentos un krīzēs un tas, kā pastāvošie krīzes pārvarēšanas mehānismi var pilnībā izmantot pastāvošās ES līmeņa kiberdrošības struktūras.

(12) Reaģējot uz kiberdrošības krīzi 2. apsvērumā minētajā nozīmē, politiskas reaģēšanas koordinēšanai Savienības līmenī Padome izmantos integrētos krīzes situāciju politiskās reaģēšanas mehānismus (*IPCR*) ([2]); Komisija izmantos krīzes augstlīmeņa starpnozaru koordinācijas procesu *ARGUS* ([3]). Ja krīzei būs nozīmīgs ārējās politikas vai kopīgās drošības un aizsardzības politikas (KDAP) aspekts, tiks iedarbināts Eiropas Ārējās darbības dienesta (EĀDD) mehānisms reaģēšanai krīzes situācijās (*CRM*) ([3]).

(13) Dažās jomās kiberdrošības incidentu vai krīžu gadījumos sadarbību nodrošina ES līmeņa nozaru krīzes pārvarēšanas mehānismi. Piemēram, Eiropas Globālās navigācijas satelītu sistēmā (*GNSS*) Padomes Lēmums 2014/496/KĀDP ([4]) jau nosaka pienākumus attiecīgi Padomei, augstajai pārstāvei, Komisijai, Eiropas *GNSS* aģentūrai un dalībvalstīm operatīvo pienākumu ķēdē, kas izveidota reaģēšanai uz briesmām Savienībai, dalībvalstīm vai *GNSS*, arī kiberuzbrukuma gadījumā. Tādēļ šis ieteikums tādus mehānismus neskar.

(14) Galvenās atbildīgās par reaģēšanu plašapmēra kiberdrošības incidentos vai krīzēs ir dalībvalstis, kuras tie skar. Komisijai, augstajai pārstāvei un citām ES iestādēm vai dienestiem tomēr ir svarīga loma, kas izriet no Savienības tiesībām vai no tā, ka kiberdrošības incidenti un krīzes vienotajā tirgū var ietekmēt visas saimnieciskās dzīves nozares, Savienības drošību un starptautiskās attiecības, kā arī pašas iestādes.

(15) Reaģējot uz kiberdrošības krīzēm, Savienības līmenī galvenie izpildītāji ir TID direktīvas nupat izveidotās struktūras un mehānismi, proti, datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīkls, kā arī attiecīgās aģentūras un struktūras, proti, Eiropas Savienības Tīklu un informācijas drošības aģentūra (*ENISA*), Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*Europol*/*EC3*), ES Izlūkdatu analīzes centrs (*INTCEN*), Eiropas Savienības Militārā štāba Izlūkošanas nodaļa (*EUMS INT*) un Dežūrcentrs (*SITROOM*), kuri kopā īsteno vienoto izlūkdatu analīzes procedūru (*SIAC*), ES Hibrīddraudu analīzes vienība (*INTCEN*), ES Iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība (*CERT-EU*) un Ārkārtas reaģēšanas koordinācijas centrs Eiropas Komisijā.

(16) Reaģēšanai tehniskā līmenī uz kiberdrošības incidentiem dalībvalstu sadarbību nodrošina ar TID direktīvu izveidotais datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīkls. *ENISA* nodrošina sekretariāta pakalpojumus

([1]) Dokuments 14540/16, 2016. gada 15. novembris.
([2]) Sīkāk – pielikuma par krīzes pārvaldību, sadarbības mehānismiem un reaģēšanas izpildītājiem ES līmenī 3.1. punktā.
([3]) Turpat.
([4]) Padomes 2014. gada 22. jūlija Lēmums 2014/496/KĀDP par Eiropas Globālās navigācijas satelītu sistēmas ieviešanas, darbības un izmantošanas aspektiem, kas ietekmē Eiropas Savienības drošību, un ar ko atceļ Vienoto rīcību 2004/552/KĀDP (OV L 219, 25.7.2014., 53. lpp.).

un aktīvi atbalsta *CSIRT* sadarbību. Valstu *CSIRT* un *CERT-EU* sadarbojas un dalās informācijā brīvprātīgi, vajadzības gadījumā – arī reaģējot uz kiberdrošības incidentiem, kas skar vienu vai vairākas dalībvalstis. Pēc dalībvalsts *CSIRT* pārstāvja lūguma tās var apspriest un, ja iespējams, noteikt, kā koordinēti reaģēt uz incidentu, kas identificēts šās dalībvalsts jurisdikcijā. Attiecīgās procedūras tiks aprakstītas *CSIRT* tīkla darbības standartprocedūrās (*SOP*) ([1]).

(17) *CSIRT* tīklam ir arī uzdevums apspriest, izpētīt un formulēt operatīvās sadarbības turpmākos veidus, arī sakarā ar briesmu un incidentu kategorijām, laicīgu brīdināšanu, savstarpējo palīdzību, koordinēšanas principiem un kārtību reizēs, kad dalībvalstis reaģē uz pārrobežu apdraudējumu un incidentiem.

(18) Ar TID direktīvas 11. pantu izveidotās Sadarbības grupas darbs ir dot stratēģiskus norādījumus par *CSIRT* tīkla darbībām, apspriest dalībvalstu spējas un gatavību un brīvprātīgi izvērtēt valstu tīklu un informācijas sistēmu drošības stratēģiju un *CSIRT* darbības efektivitāti un noskaidrot labāko praksi.

(19) Specializēta vienība Sadarbības grupā pašlaik saskaņā ar TID direktīvas 14. panta 7. punktu gatavo vadlīnijas ziņošanai incidenta gadījumā par apstākļiem, kādos pienākums ziņot par incidentiem saskaņā ar 14. panta 3. punktu ir pamatpakalpojumu sniedzējiem, un ziņošanas formu un procedūru ([2]).

(20) Reālā laika situācijas, risku un briesmu apzināšanās un izpratne, kas gūta no ziņojumiem, izvērtējumiem, izpētes, izmeklēšanas un analīzes, ir būtiska, lai varētu pieņemt uz informāciju balstītus lēmumus. Šāda situācijas apzināšanās visās attiecīgajās ieinteresētajās aprindās ir būtiski svarīga, lai varētu efektīvi koordinēt reaģēšanu. Situācijas apzināšanās ietver arī tādus elementus kā incidenta cēloņi, ietekme un izcelsme. Tiek atzīts, ka tas ir atkarīgs no informācijas apmaiņas un kopīgošanas attiecīgo personu starpā piemērotā formā, vienotas incidenta apraksta terminoloģijas un pietiekamas drošības.

(21) Reaģēt uz kiberdrošības incidentiem var daudzējādi: nosakot tehnisko pasākumus, kur divas vai vairākas struktūras kopīgi izpēta incidenta tehniskos cēloņus (piem., analizē ļaunotnes), nosakot, kādos veidos organizācijas var novērtēt, vai ir cietušas (piem., aizskāruma rādītāji), pieņemot operatīvus lēmumus par pretpasākumiem, politiskā līmenī nolemjot izmantot citus instrumentus, kā satvaru vienotai ES reakcijai uz ļaunprātīgām kiberdarbībām ([3]) vai ES operatīvo protokolu hibrīddraudu apkarošanai ([4]), un citādi – kā kurā incidentā.

(22) Plaukstošam digitālajam vienotajam tirgum būtiska ir Eiropas pilsoņu un uzņēmumu uzticēšanās digitālajiem pakalpojumiem. Tādējādi komunikācijai krīzes brīdī ir īpaši svarīga loma kiberdrošības incidentu un krīžu negatīvo seku mazināšanā. Kā līdzekli, kas ietekmē (potenciālo) agresoru no trešām valstīm uzvedību, komunikāciju var izmantot arī vienotas ES diplomātiskās reakcijas satvarā. Lai politiskā reakcija būtu efektīva, ir būtiski līdzsvarot publisko komunikāciju, kas mazina kiberdrošības incidentu un krīžu sekas, ar publisko komunikāciju, kas iespaido agresoru.

(23) Vispārības informēšana par to, kā incidenta sekas mazināt lietotāja un organizācijas līmenī (piem., ar drošības ielāpu vai papildinošiem pasākumiem, kas ļauj izvairīties no apdraudējuma, utt.), var būt efektīvs plašapmēra kiberdrošības incidenta vai krīzes seku mazināšanas līdzeklis.

(24) Izmantojot Eiropas infrastruktūras savienošanas instrumenta (EISI) kiberdrošības digitālo pakalpojumu infrastruktūru, Komisija attīsta ar nosaukumu *MeliCERTes* pazīstamo pamatpakalpojumu platformas sadarbības mehānismu, kas uzlabo tajā piedalošos dalībvalstu *CSIRT* gatavību, sadarbību un reaģēšanu uz jauniem kiberdraudiem un incidentiem. Ar uzaicinājumiem iesniegt priekšlikumus par EISI dotāciju piešķiršanu Komisija līdzfinansē dalībvalstu *CSIRT*, lai uzlabotu to operatīvās spējas valsts līmenī.

([1]) Izstrādē, pieņemt paredzēts 2017. gada beigās.
([2]) Vadlīnijas iecerēts pabeigt līdz 2017. gada beigām.
([3]) Padomes secinājumi par satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām (*Cyber Diplomacy Toolbox*), dok. 9916/17.
([4]) Komisijas dienestu darba dokuments "ES operatīvais protokols hibrīddraudu apkarošanai" (*EU Playbook*), SWD(2016) 227 final, 2016. gada 5. jūlijs.

(25) Būtiskas ir kiberdrošības mācības ES līmenī, jo tās veicina un uzlabo sadarbību starp dalībvalstīm un privāto sektoru. Šim nolūkam *ENISA* kopš 2010. gada rīko regulāras Eiropas kiberdrošības mācības ("Kibereiropa").

(26) Secinājumos par Eiropadomes priekšsēdētāja, Eiropas Komisijas priekšsēdētāja un Ziemeļatlantijas Līguma organizācijas ģenerālsekretāra kopīgās deklarācijas īstenošanu [1] Padome aicina pastiprināt sadarbību kiberdrošības mācībās, personālam savstarpēji piedaloties attiecīgās mācībās, it īpaši kiberdrošības koalīcijā un mācībās "Kibereiropa".

(27) Apdraudējuma aina nepārtraukti mainās, un nesenie kiberdrošības incidenti liecina, ka Savienība sastopas ar augošu risku; dalībvalstīm būtu jārīkojas saskaņā ar šo ieteikumu bez ilgākas kavēšanās, katrā ziņā – pirms 2018. gada beigām,

IR PIEŅĒMUSI ŠO IETEIKUMU.

1. Dalībvalstīm un ES iestādēm būtu jāizveido ES satvars reaģēšanai kiberdrošības krīzēs, kurā būtu aptverti plānā minētie sadarbības mērķi un kārtība un sekots tajā aprakstītajiem vadprincipiem.

2. ES satvarā reaģēšanai kiberdrošības krīzēs būtu jānorāda attiecīgie darbību veicēji, ES iestādes un dalībvalstu iestādes visos nepieciešamajos līmeņos – tehniskā, operatīvā, stratēģiskā/politiskā – un, ja nepieciešams, darbības standartprocedūras, kurās būtu noteikts, kā tie sadarbojas ES krīzes pārvarēšanas mehānismu kontekstā. Galvenajai jābūt informācijas apmaiņas nodrošināšanai bez nepamatotas kavēšanās un reaģēšanas koordinācijai plašapmēra kiberdrošības incidentu un krīžu laikā.

3. Tālab dalībvalstu kompetentajām iestādēm būtu kopīgā darbā sīkāk jāformulē informācijas kopīgošanas un sadarbības protokoli. Sadarbības grupai būtu šajos jautājumos jādalās pieredzē ar attiecīgajām ES iestādēm.

4. Dalībvalstīm būtu jānodrošina, ka to krīzes pārvarēšanas mehānismi adekvāti īsteno reaģēšanu kiberdrošības incidentu gadījumos, kā arī jāievieš nepieciešamās procedūras ES līmeņa sadarbībai ES satvara kontekstā.

5. Attiecībā uz pastāvošajiem ES krīzes pārvarēšanas mehānismiem dalībvalstīm kopā ar Komisijas dienestiem un EĀDD atbilstīgi reaģēšanas plānam būtu jānosaka praktiskas īstenošanas vadlīnijas savas valsts krīzes pārvarēšanas un kiberdrošības struktūru un procedūru integrācijai pastāvošajos ES krīzes pārvarēšanas mehānismos, proti, *IPCR* un EĀDD *CRM*. Dalībvalstīm īpaši būtu jānodrošina, ka pastāv piemērotas struktūras, kas ES krīzes pārvarēšanas mehānismos dara iespējamu efektīvu informācijas apriti starp valsts krīzes pārvaldības iestādēm un to pārstāvjiem ES līmenī.

6. Dalībvalstīm būtu pilnībā jāizmanto iespējas, ko dod Eiropas infrastruktūras savienošanas instrumenta (EISI) kiberdrošības digitālo pakalpojumu infrastruktūras (*DSI*) programma, un jāsadarbojas ar Komisiju, lai nodrošinātu, ka pamatpakalpojumu platformas sadarbības mehānisms, kas patlaban tiek veidots, arī kiberdrošības krīžu laikā nodrošina nepieciešamās funkcijas un atbilst sadarbības prasībām.

7. Dalībvalstīm, saņemot *ENISA* palīdzību un balstoties uz līdzšinējo darbu šajā jomā, būtu jāsadarbojas, izstrādājot un pieņemot vienotu terminoloģiju un formu ziņojumiem par stāvokli, kas ļautu aprakstīt kiberdrošības incidentu tehniskos cēloņus un ietekmi, lai vēl vairāk uzlabotu tehnisko un operatīvo sadarbību krīzes laikā. Šajā sakarā dalībvalstīm būtu jāņem vērā pašlaik notiekošais darbs Sadarbības grupā, kas izstrādā incidentu izziņošanas vadlīnijas, it īpaši aspekti, kas saistīti ar valstu ziņojumu formu.

8. Satvarā izklāstītās procedūras būtu jāizmēģina un vajadzības gadījumā jāpārskata atbilstoši pieredzei, ko dalībvalsts gūst no dalības valsts, reģiona un Savienības, kā arī kiberdiplomātijas un NATO kiberdrošības mācībās. Pirmām kārtām tās būtu jāizmēģina *ENISA* rīkotajās mācībās *CyberEurope*. *CyberEurope 2018* ir pirmā tāda iespēja.

[1] ST 15283/16, 2016. gada 6. decembris.

9. Dalībvalstīm un ES iestādēm būtu regulāri jāvingrinās reaģēt uz plašapmēra kiberdrošības incidentiem un krīzēm valsts un Eiropas līmenī, ieskaitot politisko reaģēšanu, ja nepieciešams, un piemērotā veidā iesaistot privātā sektora struktūras.

Briselē, 2017. gada 13. septembrī

Komisijas vārdā –
Komisijas locekle
Mariya GABRIEL

PIELIKUMS

Plāns, kā koordinēti reaģēt uz plašapmēra pārrobežu kiberdrošības incidentiem un krīzēm

IEVADS

Šis plāns attiecas uz kiberdrošības incidentiem, kuru izraisītie traucējumi ir pārāk plaši, lai skartā dalībvalsts varētu tos pārvarēt viena pati, vai kuri skar divas vai vairākas dalībvalstis vai ES iestādes un kuru ietekme tehniskajā vai politiskajā ziņā ir tik plaša un nozīmīga, ka ir vajadzīga savlaicīga rīcībpolitikas koordinācija un reakcija Savienības politiskajā līmenī.

Šādus plašapmēra kiberdrošības incidentus uzskata par kiberdrošības krīzi.

Iestājoties ES mēroga krīzei ar kiberelementiem, reakciju Savienības politiskajā līmenī koordinē Padome, tālab izmantojot integrētos krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismus.

Komisijā koordinācija notiek saskaņā ar ātrās brīdināšanas sistēmu *ARGUS*.

Ja krīzei ir nozīmīga ārējā vai kopējās drošības un aizsardzības politikas (KDAP) dimensija, aktivizē EĀDD mehānisms reaģēšanai krīzes situācijās.

Plānā ir aprakstīts, kā šajos sekmīgi izveidotajos krīzes pārvarēšanas mehānismos būtu pilnā mērā izmantojamas esošās ES mēroga kiberdrošības struktūrvienības, kā arī sadarbības mehānismi starp dalībvalstīm.

Šajā sakarā plānā ir izklāstīti pamatprincipi (proporcionalitāte, subsidiaritāte, papildināmība un informācijas konfidencialitāte) un galvenie sadarbības mērķi (reakcijas efektivitāte, kopīga situācijas apzināšanās, publisko paziņojumu vēstījums) trīs līmeņos (stratēģiskais/politiskais, tehniskais un operatīvais), mehānismi un iesaistītie aktori, kā arī minēto galveno mērķu sasniegšanai veicamās darbības.

Plāns neaptver visu krīzes pārvarēšanas ciklu (prevencija / seku mazināšana, gatavība, reaģēšana un atgūšanās) un koncentrējas tikai uz reaģēšanas posmu. Tomēr cita starpā ir pievērsta uzmanība dažām tādām darbībām, kas attiecas uz to, kā panākt kopīgu situācijas apzināšanos.

Papildus jāuzsver, ka kiberdrošības incidenti var būt daļa no plašākas krīzes vai tie var šādu krīzi izraisīt un ietekmēt citas nozares. Tā kā sagaidāms, ka lielākajai daļai kiberdrošības krīžu būs fiziski sajūtama ietekme, visiem attiecīgajiem reaģēšanas pasākumiem jāietver gan kiberietekmes, gan nekiberietekmes mazināšanas darbības. Darbības, ar kurām reaģē uz kiberkrīzēm, būtu jākoordinē ar citiem krīzes pārvarēšanas mehānismiem ES, valstu vai nozaru līmenī.

Visbeidzot, jānorāda, ka šis plāns neaizstāj un tam nebūtu jāskar esošie nozarēm vai rīcībpolitikām specifiskie mehānismi, pasākumi vai instrumenti, piemēram, Eiropas Globālās navigācijas satelītu sistēmas (*GNSS*) programmas vajadzībām izveidotais mehānisms ([1]).

Pamatprincipi

Izstrādājot mērķus, apzinot vajadzīgās darbības un uzticot lomas un pienākumus attiecīgajiem dalībniekiem vai mehānismiem, tika piemēroti turpmāk uzskaitītie pamatprincipi, kuri jāievēro arī nākotnē, gatavojot īstenošanas vadlīnijas.

Proporcionalitāte. Lielākā daļa kiberdrošības incidentu, kuri skar dalībvalstis, ir tādi, kuri ne tuvu nav uzskatāmi par valsts mēroga krīzi un vēl jo mazāk par Eiropas mēroga krīzi. Pamatu dalībvalstu sadarbībai, kad tām jāreaģē uz šādiem starpgadījumiem, sniedz datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīkls, ko izveidoja ar TID direktīvu ([2]). Atbilstoši *CSIRT* tīkla darbības standartprocedūrām (*SOP*) valstu *CSIRT* ikdienā sadarbojas un apmainās ar informāciju brīvprātīgi, tostarp vajadzības gadījumā reaģējot uz kibedrošības incidentiem, kas skar vienu vai vairākas dalībvalstis. Tāpēc plānā šīs darbības standartprocedūras būtu jāizmanto pilnā mērā, un tajās vajadzētu atspoguļot visus papildu uzdevumus, kas attiecas uz kiberdrošības krīzi.

([1]) Lēmums 2014/496/KĀDP.
([2]) Direktīva (ES) 2016/1148.

Subsidiaritāte. Šis ir ļoti svarīgs princips. Iestājoties plašapmēra kiberdrošības incidentam vai krīzei, atbildība par reaģēšanu primāri jāuzņemas skartajām dalībvalstīm. Tomēr nozīmīga loma ir arī Komisijai, Eiropas Ārējās darbības dienestam un citām ES iestādēm, birojiem, aģentūrām un struktūrām. Šī loma ir skaidri izklāstīta *IPCR* mehānismos, taču to paredz arī Savienības tiesību akti, kā arī vienkārši tas, ka kiberdrošības incidenti un krīzes var ietekmēt visas saimnieciskās darbības nozares vienotajā tirgū, drošību un Savienības starptautiskās attiecības, kā arī pašas ES iestādes.

Papildināmība. Plānā ir pilnā mērā ņemti vērā esošie krīzes pārvarēšanas mehānismi ES līmenī, proti, integrētie krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismi, *ARGUS* un EĀDD mehānisms reaģēšanai krīzes situācijās, un tas šajos mehānismos integrē jaunās TID direktīvas struktūras un mehānismus, proti, *CSIRT* tīklu, kā arī attiecīgās aģentūras un struktūras, proti, Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*), Eiropola Eiropas Kibernoziedzības centru (*Europol/EC3*), ES Izlūkdatu analīzes centru (*INTCEN*), ES Militārā štāba Izlūkošanas nodaļu (*EUMS INT*), *INTCEN* Dežūrcentru (*SITROOM*), kuri kopā darbojas vienotajā izlūkdatu analīzes procedūrā (*SIAC*); ES Hibrīddraudu analīzes vienību (kura bāzēta *INTCEN*) un ES iestāžu un aģentūru datordrošības incidentu reaģēšanas vienību (*CERT-EU*). Šajā sakarībā plānam būtu arī jānodrošina, ka, minētajiem mehānismiem un struktūrvienībām mijiedarbojoties un sadarbojoties, tie cits citu maksimāli papildina, un vienlaikus jāraugās, lai tie pēc iespējas mazāk pārklātos.

Informācijas konfidencialitāte. Visa informācijas apmaiņa, kas notiek šā plāna kontekstā, jāveic saskaņā ar piemērojamajiem noteikumiem par drošību ([1]) un par personas datu aizsardzību, kā arī saskaņā ar Gaismas signālu protokolu ([2]). Neatkarīgi no tā, pēc kādas klasifikācijas shēmas informācija ir klasificēta, klasificētās informācijas apmaiņai izmanto pieejamos akreditētos rīkus ([3]). Personas datu apstrādē jāievēro piemērojamie ES noteikumi, jo īpaši Vispārīgā datu aizsardzības regula ([4]), E-privātuma direktīva ([5]), kā arī Regula par personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un šādu datu brīvu apriti ([6]).

Galvenie mērķi

Šajā plānā aprakstītā sadarbība tiek īstenota, izmantojot minēto trīs līmeņu (politiskais, operatīvais un tehniskais) pieeju. Katrā līmenī sadarbība var ietvert informācijas apmaiņu, kā arī kopīgu rīcību, un tai ir šādi galvenie mērķi:

— nodrošināt reakcijas efektivitāti: reakcijas var būt dažādas, proti, atkarībā no konkrētā incidenta reaģēšana var izpausties kā tehnisko pasākumu apzināšana, kad divas vai vairākas struktūrvienības kopīgi izmeklē incidenta tehniskos iemeslus (piem., analizē ļaunprogrammatūru), vai tādu paņēmienu apzināšana, kas ļautu organizācijām (piem., ar aizskāruma rādītāju palīdzību) novērtēt, vai incidents tās ir ietekmējis, taču tikpat labi tie var būt operatīvi lēmumi par šādu tehnisko pasākumu piemērošanu un – politiskajā līmenī – lēmumi izmantot citus instrumentus, piem., ES diplomātisko reakciju uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopums") vai ES operatīvo protokolu hibrīddraudu apkarošanai,

— kopīgi apzināties situāciju: lai reakcija būtu koordinēta, ir ārkārtīgi svarīgi, ka visām attiecīgajām ieinteresētajām personām visos trīs līmeņos (tehniskajā, operatīvajā, politiskajā) ir pietiekami laba izpratne par notikumu attīstību. Situācijas apzināšanās nozīmē, ka ieinteresētās personas cita starpā ir lietas kursā par incidenta cēloņu, ietekmes un izcelsmes tehnoloģiskajiem elementiem. Tā kā kiberdrošības incidenti var skart visdažādākās nozares (finanses, enerģētika, transports, veselības aprūpe u. c.), ir kritiski svarīgi, ka attiecīgā informācija atbilstošā formātā savlaicīgi sasniedz visas attiecīgās ieinteresētās personas,

([1]) Komisijas 2015. gada 13. marta Lēmums (ES, Euratom) 2015/443 par drošību Komisijā (OV L 72, 17.3.2015., 41. lpp.) un Komisijas 2015. gada 13. marta Lēmums (ES, Euratom) 2015/444 par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.); Augstā pārstāvja 2013. gada 19. aprīļa Lēmums par Eiropas Ārējās darbības dienesta drošības noteikumiem (OV C 190, 29.6.2013., 1. lpp.); Padomes 2013. gada 23. septembra Lēmums 2013/488/ES par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 274, 15.10.2013., 1. lpp.).

([2]) https://www.first.org/tlp/

([3]) 2016. gada jūnijā šie informācijas pārsūtīšanas kanāli ietvēra *CIMS* (klasificētas informācijas pārvaldības sistēma), *ACID* (šifrēšanas algoritms), *RUE* (droša sistēma *RESTREINT UE/EU RESTRICTED* statusā esošo dokumentu izveidei, apmaiņai un glabāšanai) un *SOLAN*. Citi klasificētas informācijas pārsūtīšanas līdzekļi ir, piemēram, *PGP* vai *S/MIME*.

([4]) Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (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.).

([5]) Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

([6]) Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.) – pašlaik tiek caurskatīta.

— vienoties par svarīgākajiem publisko paziņojumu vēstījumiem ([1]): saziņai krīzes gaitā ir ļoti svarīga loma kiberdrošības incidentu un krīžu negatīvo seku mazināšanā, taču to var arī izmantot kā līdzekli (potenciālo) agresoru uzvedības ietekmēšanai. Ar atbilstošu vēstījumu ir iespējams dot skaidru signālu par to, kādas sekas varētu būt diplomātiskajai atbildes reakcijai, un tādējādi ietekmēt agresoru uzvedību. Lai politiskā līmeņa reakcija būtu sekmīga, ir ļoti svarīgi panākt, ka publiskie paziņojumi nolūkā mazināt kiberdrošības incidentu un krīžu negatīvās sekas un publiskie paziņojumi nolūkā ietekmēt agresoru ir savstarpēji pārdomāti. Kiberdrošības aspektā ir ļoti svarīgi izplatīt precīzu informāciju par to, kā iedzīvotājiem rīkoties, lai mazinātu incidenta sekas (piem., instalēt "ielāpu", veikt papildpasākumus, lai izvairītos no apdraudējuma utt.).

SADARBĪBA DALĪBVALSTU STARPĀ UN STARP DALĪBVALSTĪM UN ES AKTORIEM TEHNISKĀ, OPERATĪVĀ UN STRATĒĢISKĀ/POLITISKĀ LĪMENĪ

Efektīva reakcija uz plašapmēra kiberdrošības incidentiem vai krīzēm ES līmenī ir atkarīga no efektīvas tehniskas, operatīvas un stratēģiskas/politiskas sadarbības.

Katrā sadarbības līmenī iesaistītajiem aktoriem jāveic īpašas darbības attiecībā uz trīs galvenajiem mērķiem:

— koordinēta reakcija,

— kopīga situācijas apzināšanās,

— publiski paziņojumi.

Incidenta vai krīzes laikā sadarbības zemākie līmeņi brīdinās, informēs un atbalstīs augstākos līmeņus, savukārt augstākie līmeņi attiecīgi dos norādes ([2]) un pieņems zemākiem līmeņiem adresētus lēmumus.

Sadarbība tehniskajā līmenī

Darbību tvērums:

— incidenta risināšana ([3]) kiberdrošības krīzes laikā,

— incidenta uzraudzība un pārraudzība, tostarp apdraudējumu un risku pastāvīga analīze.

Potenciālie aktori

Tehniskajā līmenī plāna centrālais sadarbības mehānisms ir *CSIRT* tīkls, ko vada Padomes prezidentvalsts kopā ar sekretariātu, kuru nodrošina *ENISA*.

— Dalībvalstis

  — Kompetentās iestādes un ar TID direktīvu izveidotie vienotie kontaktpunkti

  — CSIRT

— ES struktūras/biroji/aģentūras

  — ENISA

  — Eiropols/*EC3*

  — CERT-EU

([1]) Jāatzīmē, ka publiskie paziņojumi var izpausties gan kā visas sabiedrības apziņošana par incidentu, gan kā paziņojumi, kuri satur tehnisku vai operatīvu informāciju un kuri paredzēti kritiski svarīgajiem sektoriem un/vai skartajām personām. Tas nozīmē, ka varētu rasties vajadzība izmantot konfidenciālus informācijas izplatīšanas kanālus un specifiskus tehniskus rīkus/platformas. Jebkurā gadījumā saziņa ar operatoriem un plašākas sabiedrības apziņošana dalībvalstīs ir katras dalībvalsts prerogatīva un atbildība. Tāpēc saskaņā ar iepriekš minēto subsidiaritātes principu galīgā atbildība par informāciju, kas tiek izplatīta dalībvalstu teritorijā un paziņota abonentiem, ir jāuzņemas attiecīgi dalībvalstīm un valstu *CSIRT*.

([2]) "Atļauja rīkoties" – kiberdrošības krīzes gadījumā ir būtiski reaģēt īsā laikā, lai noteiktu atbilstīgus ietekmes mazināšanas pasākumus. Lai nodrošinātu ātru reakciju, viena dalībvalsts otrai dalībvalstij var izdot "atļauju rīkoties", ar kuru dalībvalstij tiek piešķirta atļauja rīkoties nekavējoties bez vajadzības apspriesties ar augstākiem līmeņiem vai ES iestādēm, ievērot visas standartprasības un izmantot oficiālos kanālus, ja vien konkrētā incidenta gadījumā tas netiek prasīts (piem., *CSIRT* nebūtu jāapspriežas ar augstākiem līmeņiem pirms vērtīgas informācijas nosūtīšanas *CSIRT* citā dalībvalstī).

([3]) "Incidenta risināšana" ir visas procedūras, kas ļauj atklāt incidentu, veikt tā analīzi, to ierobežot un reaģēt uz to.

— Eiropas Komisija

  — *ERCC* (diennakts operatīvais dienests, kurš atrodas *ECHO* ĢD) un izraudzītais vadošais dienests (*CNECT* ĢD vai *HOME* ĢD atkarībā no incidenta rakstura), Ģenerālsekretariāts (*ARGUS* sekretariāts), Cilvēkresursu un drošības ĢD (Drošības direktorāts), *DIGIT* ĢD (IT drošības operācijas)

  — Attiecībā uz citām ES aģentūrām ([1]): atbildīgais Komisijas ĢD vai EĀDD (pirmais kontaktpunkts)

— EĀDD

  — *SIAC* (vienotā izlūkdatu analīzes procedūra – ES *INTCEN* un *EUMS INT*)

  — ES Dežūrcentrs un izraudzītais ģeogrāfiskais vai tematiskais dienests

  — ES Hibrīddraudu analīzes vienība (ES *INTCEN* – kiberdrošība hibrīddraudu kontekstā)

Kopīga situācijas apzināšanās

— Lai regulāras tehniskās sadarbības ietvaros veicinātu situācijas apzināšanos Savienībā, *ENISA* ir regulāri jāsagatavo ES kiberdrošības tehniskās situācijas ziņojums par incidentiem un apdraudējumiem, kurš balstīts uz publiski pieejamo informāciju, *ENISA* veikto analīzi un ziņojumiem, ko tai snieguši dalībvalstu *CSIRT* (brīvprātīgi) vai ar TID direktīvu izveidotie vienotie kontaktpunkti, Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), *CERT-EU* un – attiecīgā gadījumā – Eiropas Ārējās darbības dienesta (EĀDD) ES Izlūkdatu analīzes centrs (*INTCEN*). Ziņojums būtu jādara pieejams attiecīgajām Padomes un Komisijas struktūrām, Augstajam pārstāvim un priekšsēdētāja vietniekam (AP/PV) un *CSIRT* tīklam.

— Nopietna incidenta gadījumā *CSIRT* tīkla priekšsēdētājs ar *ENISA* palīdzību sagatavo ziņojumu par ES kiberdrošības incidenta situāciju ([2]), kuru ar rotējošās prezidentvalsts *CSIRT* starpniecību iesniedz Padomes prezidentvalstij, Komisijai un AP/PV.

— *Visas pārējās ES aģentūras* ziņo saviem attiecīgajiem atbildīgajiem ĢD, kuri savukārt ziņo Komisijas vadošajam dienestam.

— *CERT-EU* sniedz tehniskus ziņojumus *CSIRT* tīklam, ES iestādēm un aģentūrām (pēc vajadzības) un *ARGUS* (ja sistēma aktivizēta).

— *Eiropols/EC3* ([3]) *un CERT-EU* sniedz tehnisko artefaktu kriminālistisko ekspertīzi un citu tehnisko informāciju *CSIRT* tīklam.

— EĀDD *SIAC* – ES Hibrīddraudu analīzes vienība *INTCEN* vārdā ziņo attiecīgajām EĀDD struktūrvienībām.

Reakcija

— *CSIRT* tīkls apmainās ar incidenta tehnisko informāciju un analīzi, piemēram, IP adresēm, aizskāruma rādītājiem ([4]) u. c. Šāda informācija bez nepamatotas kavēšanās un ne vēlāk kā 24 stundu laikā no incidenta konstatēšanas brīža ir jāsaņem *ENISA*.

— Saskaņā ar *CSIRT* tīkla darbības standartprocedūrām tīkla dalībnieki, analizējot pieejamos tehniskos artefaktus un citu ar incidentu saistīto informāciju, sadarbojas, lai noteiktu cēloņus un iespējamos tehniskos pasākumus ietekmes mazināšanai.

— *ENISA*, balstoties uz savām speciālajām zināšanām un ievērojot savas pilnvaras, palīdz *CSIRT* veikt tehniskos pasākumus ([5]).

([1]) Atkarībā no incidenta rakstura un ietekmes uz dažādām darbības nozarēm (finanses, transports, enerģētika, veselības aprūpe u. c.) tiks piesaistītas attiecīgās ES aģentūras vai struktūras.

([2]) Ziņojumā par ES kiberdrošības incidenta situāciju ir apkopoti ziņojumi, ko sniegušas valstu *CSIRT*. Ziņojuma formāts ir jāapraksta, izmantojot *CSIRT* tīkla *SOP*.

([3]) Saskaņā ar *EC3* tiesiskajā regulējumā noteiktajām procedūrām un nosacījumiem.

([4]) Aizskāruma rādītājs (*Indicator of compromise – IOC*) datorkriminālistikā ir tīklā vai operētājsistēmā konstatēts artefakts, kurš ar augstu ticamības pakāpi norāda uz ielaušanos datorā. Parastākie *IOC* ir vīrusa kodi un IP adreses, ļaunprogrammatūras datņu MD5 jaucējkodi vai robottīklu komandserveru un kontrolserveru adreses vai domēna vārdi.

([5]) Priekšlikums regulai par *ENISA*, Eiropas Kiberdrošības aģentūru un ar kuru atceļ Regulu (ES) Nr. 526/2013, un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju ("Kiberdrošības akts"), 2017. gada 13. septembris.

— Dalībvalstu *CSIRT* ar *ENISA* un Komisijas palīdzību koordinē tehniskos reaģēšanas pasākumus.

— EĀDD *SIAC – INTCEN* vārdā ES Hibrīddraudu analīzes vienība nosaka informācijas vākšanas procesu ar mērķi apkopot sākotnējos pierādījumus.

Publiski paziņojumi

— *CSIRT* sagatavo tehniskus ieteikumus ([1]) un brīdinājumus par neaizsargātību ([2]) un tos izplata attiecīgajām kopienām un sabiedrībai, ievērojot katrā konkrētajā gadījumā piemērojamās atļaujas procedūras.

— *ENISA* palīdz sagatavot un izplatīt kopīgus *CSIRT* tīkla paziņojumus.

— *ENISA* savas publiskās komunikācijas darbības koordinē ar *CSIRT* tīklu un Komisijas preses dienestu.

— *ENISA* un *EC3* savas publiskās komunikācijas darbības koordinē, balstoties uz kopīgo situācijas apzināšanos, par ko vienojušās dalībvalstis. Abas minētās struktūras savas publiskās komunikācijas darbības koordinē ar Komisijas preses dienestu.

— Ja krīzei ir ārēja vai kopējās drošības un aizsardzības politikas (KDAP) dimensija, publiskā komunikācija ir jākoordinē ar EĀDD un AP/PV preses dienestu.

Sadarbība operatīvā līmenī

Darbību tvērums:

— sagatavoties lēmumu pieņemšanai politiskā līmenī,

— koordinēt kiberdrošības krīzes pārvarēšanu (attiecīgā gadījumā),

— novērtēt sekas un ietekmi ES līmenī, un ierosināt iespējamus ietekmes mazināšanas pasākumus.

Potenciālie aktori

— Dalībvalstis

  — Kompetentās iestādes un ar TID direktīvu izveidotie vienotie kontaktpunkti

  — *CSIRT*, kiberdrošības aģentūras

  — Citu nozaru valsts iestādes (tāda incidenta vai krīzes gadījumā, kas skar vairākas nozares)

— ES struktūras/biroji/aģentūras

  — ENISA

  — Eiropols/*EC3*

  — CERT-EU

— Eiropas Komisija

  — Ģenerālsekretārs (tā vietnieks) (*ARGUS* process)

  — *CNECT*/*HOME* ĢD

  — Komisijas Drošības iestāde

  — Citi ĢD (tāda incidenta vai krīzes gadījumā, kas skar vairākas nozares)

([1]) Tehniska rakstura ieteikums par incidenta cēloņiem un iespējamiem ietekmes mazināšanas pasākumiem.
([2]) Informācija par tehnisko neaizsargātību, kas tiek ļaunprātīgi izmantota IT sistēmu ietekmēšanas nolūkā.

— EĀDD

  — Ģenerālsekretārs (tā vietnieks) jautājumos, kas skar reaģēšanu uz krīzēm un *SIAC* (ES *INTCEN* un *EUMS INT*)

  — ES Hibrīddraudu analīzes vienība

— Padome

  — Padomes prezidentvalsts (Kiberjautājumu horizontālās darba grupas vai *Coreper* ([1]) vadītāja) ar PĢS vai PDK ([2]) palīdzību un *IPCR* mehānismu (ja aktivizēti) atbalstu

Situācijas apzināšanās

— Atbalsta sniegšana politisku/stratēģisku situācijas ziņojumu sagatavošanā (piem., *ISAA IPCR* aktivizēšanas gadījumā).

— *Padomes Kiberjautājumu horizontālā darba grupa* sagatavo attiecīgi *Coreper* vai PDK sanāksmi.

— *IPCR* aktivizēšanas gadījumā:

  — lai palīdzētu sagatavoties *Coreper* vai PDK sanāksmei, prezidentvalsts var sasaukt apaļā galda sanāksmes, kurās piedalās attiecīgās ieinteresētās personas no dalībvalstīm, kā arī iestādes, aģentūras un trešās puses, piemēram, trešās valstis un starptautiskās organizācijas. Tās ir krīzes sanāksmes, kuru mērķis ir identificēt trūkumus un sagatavot priekšlikumus rīcībai attiecībā uz transversāliem jautājumiem;

  — *Komisijas vadošais dienests vai EĀDD*, kas vada *ISAA*, sagatavo *ISAA* ziņojumu, kurā ņemta vērā *ENISA*, *CSIRT* tīkla, Eiropola/*EC3*, *EUMS INT*, *INTCEN* un citu attiecīgo aktoru sniegtā informācija. *ISAA* ziņojums ir ES mēroga novērtējums, kurš ir balstīts uz korelāciju starp tehniskiem incidentiem un krīzes novērtējumu (apdraudējuma analīze, riska novērtējums, netehniska rakstura sekas un ietekme, ar kiberdrošību nesaistīti incidenta vai krīzes aspekti u. c.) un ir pielāgots operatīvā un politiskā līmeņa vajadzībām.

— *ARGUS* aktivizēšanas gadījumā:

  — *CERT-EU* un *EC3* ([3]) tiešā veidā dod ieguldījumu informācijas apmaiņā Komisijā.

— Ja ir aktivizēts EĀDD mehānisms reaģēšanai krīzes situācijās:

  — *SIAC* pastiprinās informācijas vākšanu un apkopos informāciju no visiem avotiem, kā arī sagatavos incidenta analīzi un novērtējumu.

Reakcija (pēc politiska līmeņa pieprasījuma)

— Pārrobežu sadarbība ar vienoto kontaktpunktu un valstu kompetentajām iestādēm (TID direktīva) ar mērķi mazināt sekas un ietekmi.

— Visu to tehnisko ietekmes mazināšanas pasākumu aktivizēšana un tehnisko spēju koordinēšana, kas nepieciešamas, lai apturētu vai mazinātu uzbrukumu ietekmi uz skartajām informācijas sistēmām.

— Sadarbība un, ja tā ir nolemts, tehnisko spēju koordinācija ar mērķi nodrošināt kopīgu vai sadarbīgu reakciju saskaņā ar ***CSIRT tīkla* SOP**.

— Izvērtējuma veikšana par to, vai ir nepieciešams sadarboties ar attiecīgajām trešajām pusēm.

— Lēmumu pieņemšana *ARGUS* procesā (ja aktivizēts).

— Lēmumu sagatavošana un koordinācijas īstenošana saskaņā ar *IPCR* mehānismiem (ja aktivizēti).

— Atbalsta sniegšana EĀDD lēmumu pieņemšanā, izmantojot EĀDD mehānismu reaģēšanai krīzes situācijās (ja aktivizēts), tostarp attiecībā uz sakariem ar trešām valstīm un starptautiskajām organizācijām, kā arī jebkuru pasākumu, kura mērķis ir aizsargāt KDAP misijas un operācijas un ES delegācijas.

([1]) Pastāvīgo pārstāvju komiteja jeb *Coreper* (Līguma par Eiropas Savienības darbību (LESD) 240. pants) ir atbildīga par Eiropas Savienības Padomes darba sagatavošanu.

([2]) Politikas un drošības komiteja ir Eiropas Savienības Padomes komiteja, kuras pārziņā ir Līguma par Eiropas Savienību 38. pantā minētā kopējā ārpolitika un drošības politika (KĀDP).

([3]) Saskaņā ar *EC3* tiesiskajā regulējumā noteiktajām procedūrām un nosacījumiem.

Publiski paziņojumi

— Vienoties par publiskiem vēstījumiem, kas saistīti ar incidentu.

— Ja krīzei ir ārēja vai kopējās drošības un aizsardzības politikas (KDAP) dimensija, publiskā komunikācija ir jākoordinē ar EĀDD un AP/PV preses dienestu.

Sadarbība stratēģiskā/politiskā līmenī

Potenciālie aktori

— Dalībvalstīs – par kiberdrošību atbildīgie ministri

— Eiropadomē – priekšsēdētājs

— Padomē – valsts, kura rotācijas kārtībā pilda prezidentvalsts pienākumus

— Ja pasākumi ietilpst "Kiberdiplomātijas instrumentu kopumā", PDK un horizontālā darba grupa

— Eiropas Komisijā – priekšsēdētājs vai deleģēts priekšsēdētāja vietnieks / Komisijas loceklis

— Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos / Komisijas priekšsēdētāja vietniece

Darbību tvērums. Gan kiberdrošības, gan ar to nesaistītu krīzes aspektu stratēģiska un politiska vadība, tostarp pasākumi saskaņā ar satvaru vienotai ES diplomātiskai reakcijai uz ļaunprātīgām kiberdarbībām.

Kopīga situācijas apzināšanās

— Apzināt ietekmi, ko Savienības darbībā rada krīzes izraisīti traucējumi.

Reakcija

— Aktivizēt papildu krīzes pārvarēšanas mehānismus/instrumentus atkarībā no incidenta veida un ietekmes. Šie pasākumi var ietvert, piemēram, civilās aizsardzības mehānismu.

— Veikt pasākumus, kas ietilpst satvarā vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām.

— Darīt pieejamu ārkārtas atbalstu cietušajām dalībvalstīm, piemēram, aktivizējot kiberdrošības ātrās reaģēšanas fondu ārkārtas situācijās ([1]), kad tas būs pieejams.

— Ja tas ir lietderīgi, sadarbība un koordinācija ar starptautiskām organizācijām, piemēram, Apvienoto Nāciju Organizāciju (ANO), Eiropas Drošības un sadarbības organizāciju (EDSO) un jo īpaši – NATO.

— Novērtēt valsts drošības un aizsardzības aspektus.

Publiskā komunikācija

Lemt par kopēju publiskās komunikācijas stratēģiju.

KOORDINĒTA DALĪBVALSTU REAKCIJA ES LĪMENĪ *IPCR* MEHĀNISMU IETVAROS

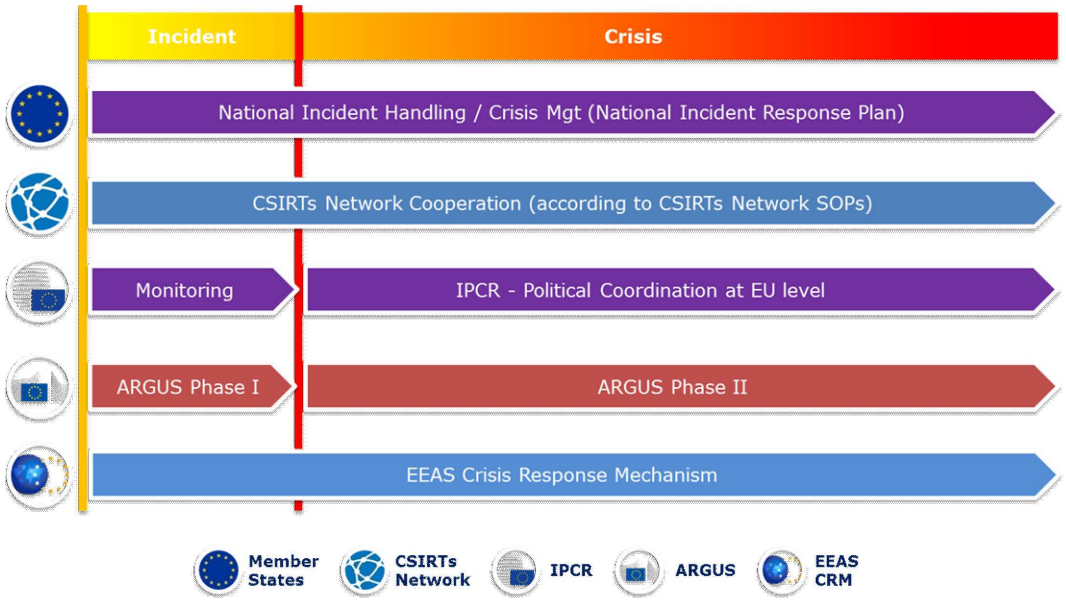
Atbilstoši papildināmības principam ES līmenī šajā iedaļā aplūkoti un jo īpaši uzmanība vērsta uz galveno mērķi un pienākumiem un pasākumiem, kas *IPCR* procesa ietvaros ir dalībvalstu iestādēm, *CSIRT* tīklam, *ENISA*, *CERT-EU*, *Europol/EC3*, *INTCEN*, ES Hibrīddraudu analīzes vienībai un Padomes kiberjautājumu horizontālajai darba grupai. Tiek pieņemts, ka aktori rīkojas saskaņā ar noteiktajām procedūrām ES vai valsts līmenī.

Ir svarīgi atzīmēt, ka, kā redzams 1. attēlā, neatkarīgi no ES krīzes pārvarēšanas mehānismu aktivizēšanas rīcība valsts līmenī, kā arī sadarbība *CSIRT* tīklā (vajadzības gadījumā) notiek jebkura incidenta/krīzes laikā, ievērojot subsidiaritātes un proporcionalitātes principus.

([1]) Kiberdrošības ātrās reaģēšanas fonds ārkārtas situācijās ir ierosinātā rīcība saskaņā ar kopīgo paziņojumu "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" (*Resilience, Deterrence and Defence*: *Building strong cybersecurity for the EU*, JOIN(2017) 450/1.

1. attēls

Kiberdrošības incidents/reaģēšana krīzes situācijā ES līmenī



Visas turpmāk aprakstītās darbības jāveic saskaņā ar un ievērojot sekojošas darbības standartprocedūras/sadarbības mehānismu noteikumus, un tām jāatbilst atsevišķu aktoru un iestāžu noteiktajām pilnvarām un kompetencēm. Lai panāktu vislabāko iespējamo sadarbību un efektīvu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm, šīm procedūrām/noteikumiem var būt vajadzīgi daži papildinājumi vai grozījumi.

Jebkurā konkrētā incidentā ne vienmēr var būt nepieciešama visu turpmāk minēto aktoru rīcība. Tomēr plānā un sadarbības mehānismu attiecīgajās darbības standartprocedūrās vajadzētu paredzēt to iespējamo līdzdalību.

Ņemot vērā kiberdrošības incidenta vai krīzes iespējamo atšķirīgo ietekmi uz sabiedrību, nozaru aktoru izteikti elastīgu līdzdalību visos līmeņos un jebkādu atbilstošu reaģēšanu nodrošināt palīdzēs gan ar kiberdrošību saistīti, gan ar to nesaistīti draudu mazināšanas pasākumi.

Kiberdrošības krīzes pārvarēšana – kiberdrošības integrēšana *IPCR* procesā

IPCR mehānismi, kas aprakstīti *IPCR* darbības standartprocedūrās ([1]), secīgi norit atbilstoši turpmāk aprakstītajiem posmiem (dažu posmu izmantošana būs atkarīga no situācijas).

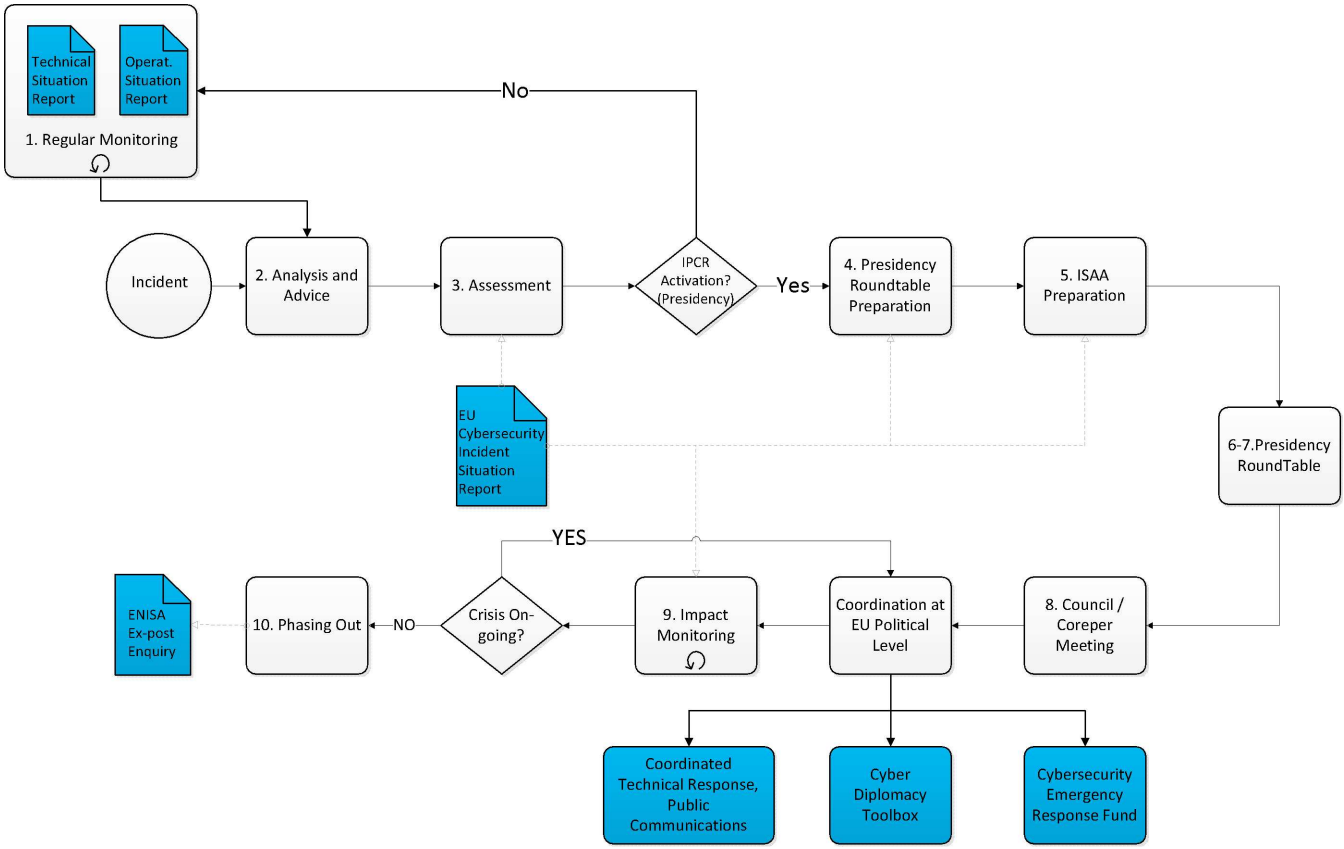
Katrā posmā tiek precizētas ar kiberdrošību saistītas darbības un aktori. Lasītāju ērtībai katrā posmā vispirms ir teksts no *IPCR SOP* un tad izklāstītas ar plānu saistītās darbības. Šī pakāpeniskā pieeja ļauj arī skaidri identificēt esošos **trūkumus** vajadzīgajās spējās un procedūrās, kuri kavē efektīvu reakciju uz kiberdrošības krīzēm.

Tālāk 2. attēlā ([2]) ir grafisks *IPCR* process, kurā ieviestie jaunie elementi izcelti ar zilu krāsu.

([1]) No dokumenta Nr. 12607/15 "*IPCR* darbības standartprocedūras", par ko vienojusies Prezidentvalsts draugu grupa un 2015. gada oktobrī pieņēmusi zināšanai Pastāvīgo pārstāvju komiteja.
([2]) Šis attēls lielākā izmērā ir pieejams pielikumā.

2. attēls

Ar kiberdrošību saistītie *IPCR* elementi



Piezīme. Ņemot vērā kiberjomā esošo hibrīddraudu īpašības (tie ir izstrādāti tā, lai nepārsniegtu atpazīstamas krīzes slieksni), ES nepieciešams veikt preventīvus un gatavības pasākumus. ES hibrīddraudu analīzes vienībai ir uzdots ātri analizēt attiecīgos incidentus un informēt attiecīgās koordinācijas struktūras. Regulāri ziņojumi no analīzes vienības var palīdzēt informēt nozaru politikas izstrādātājus un tādējādi paaugstināt gatavības līmeni.

— **1. posms – regulāra nozaru uzraudzība un brīdināšana.** Esošie, regulārie ziņojumi par nozaru stāvokli un brīdinājumi sniedz Padomes prezidentvalstij norādes par potenciālu krīzi un tās iespējamo attīstību.

— **Konstatētais trūkums.** Patlaban attiecībā uz kiberdrošības incidentiem (un draudiem) ES līmenī nav regulāru un saskaņotu kiberdrošības situācijas ziņojumu un brīdinājumu.

— **Plāns: ES kiberdrošības situācijas pārraudzība/ziņošana**

— *ENISA* regulāri sagatavos **ES kiberdrošības tehniskās situācijas ziņojumu** par incidentiem un draudiem, kurš balstīts uz publiski pieejamo informāciju, *ENISA* veikto analīzi un ziņojumiem, ko tai snieguši dalībvalstu *CSIRT* (brīvprātīgi) vai ar TID direktīvu izveidotie vienotie kontaktpunkti, Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), *CERT-EU* un Eiropas Ārējās darbības dienesta (EĀDD) ES Izlūkdatu analīzes centrs (*INTCEN*). Ziņojums būtu jādara pieejams attiecīgajām Padomes un Komisijas struktūrām un *CSIRT* tīklam.

— *SIAC* vārdā ES hibrīddraudu analīzes vienībai būtu jāizveido **ES kiberdrošības darbības situācijas ziņojums**. Ziņojums arī atbalstīs satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām.

— Abi ziņojumi tiek izplatīti ES un valstu ieinteresētajām personām, lai veicinātu to izpratni par situāciju, informētu lēmumu pieņēmējus un veicinātu pārrobežu reģionālo sadarbību.

Pēc incidenta konstatēšanas

— **2. posms – analīze un ieteikumi.** Balstoties uz pieejamo pārraudzību un brīdināšanu, Komisijas dienesti, EĀDD un PĢS cits citu informē par iespējamo notikumu attīstību, lai būtu gatavi sniegt ieteikumus prezidentvalstij par iespējamo *IPCR* aktivizēšanu (pilnībā vai informācijas apmaiņas režīmā).

— **Plāns:**

— Komisijā – *CNECT* ĢD, *HOME* ĢD, Cilvēkresursu un drošības ĢD (Drošības direktorāts) un *DIGIT* ĢD, ko atbalsta *ENISA*, *EC3* un *CERT-EU*.

— EĀDD. Pamatojoties uz *SITROOM* veikto darbu un informācijas avotiem, ES hibrīddraudu analīzes vienība sniedz informāciju par situāciju un potenciālajiem hibrīddraudiem, tostarp kiberddraudiem, kas skar ES un tās partnerus. Tādēļ, ja ES hibrīddraudu analīzes vienības analīze un novērtējums norāda uz iespējamiem draudiem, kas vērsti pret kādu dalībvalsti, partnervalsti vai organizāciju, *INTCEN* saskaņā ar noteiktajām procedūrām informāciju sniedz (pirmkārt) operatīvajā līmenī. Tad operatīvajā līmenī tiek sagatavoti ieteikumi politiski stratēģiskajam līmenim, tostarp par krīzes pārvarēšanas mehānismu iespējamo aktivizēšanu uzraudzības režīmā (piemēram, EĀDD mehānisms reaģēšanai krīzes situācijās vai *IPCR* uzraudzības lapa).

— *CSIRT* tīkla priekšsēdētājs ar *ENISA* palīdzību sagatavo ziņojumu par ES kiberdrošības incidenta situāciju ([1]), kuru ar rotējošās prezidentvalsts *CSIRT* starpniecību iesniedz Padomes prezidentvalstij, Komisijai un AP/PV.

— **3. posms – novērtējums/lēmums par *IPCR* aktivizēšanu.** Prezidentvalsts izvērtē, vai ir vajadzīga politikas koordinācija, informācijas apmaiņa vai lēmumu pieņemšana ES līmenī. Lai to panāktu, prezidentvalsts var sasaukt neoficiālu apaļā galda sanāksmi. Prezidentvalsts sākotnēji nosaka jomas, kur vajadzīga *Coreper* vai Padomes iesaistīšanās. Tas veidos pamatu Integrēto situācijas apzināšanās un analīzes (*ISAA*) ziņojumu izveides vadlīnijām. Ņemot vērā krīzes raksturojumu, tās iespējamās sekas un ar to saistītās politiskās vajadzības, prezidentvalsts lems par attiecīgo Padomes darba grupu un/vai *Coreper*, un/vai PDK sanāksmju sasaukšanas lietderību.

— **Plāns:**

— apaļā galda dalībnieki:

— Komisijas dienesti un EĀDD, kas konsultēs prezidentvalsti savās attiecīgajās kompetences jomās

— Dalībvalstu pārstāvji kiberjautājumu horizontālajās darba grupās ar ekspertiem no galvaspilsētām (*CSIRT*, kiberdrošības kompetentās iestādes u. c.)

— Politiskās/stratēģiskās vadlīnijas *ISAA* ziņojumiem, kas sagatavotas, balstoties uz jaunāko ziņojumu par ES kiberdrošības incidenta situāciju un apaļā galda dalībnieku sniegto papildu informāciju

— Attiecīgās darba grupas un komitejas:

— kiberjautājumu horizontālā darba grupa

Komisija, EĀDD un PĢS, pilnībā vienojoties un saistoties ar prezidentvalsti, var arī pieņemt lēmumu *IPCR* aktivizēt informācijas apmaiņas režīmā, ģenerējot krīzes lapu, lai sagatavotos iespējamai pilnīgai aktivizēšanai.

— **4. posms – *IPCR* aktivēšana/informācijas vākšana un apmaiņa.** Pēc aktivizēšanas (pilnībā vai informācijas apmaiņas režīmā) *IPCR* tīmekļa platformā ģenerē krīzes lapu, kas ļauj veikt konkrētas informācijas apmaiņu, galveno uzmanību pievēršot aspektiem, kas sekmēs *ISAA* izstrādi un sagatavošanos diskusijai politiskā līmenī. To, kurš (kāds no Komisijas dienestiem vai EĀDD) kļūs par *ISAA* vadošos dienestu, noteiks konkrētā gadījuma apstākļi.

— **5. posms – *ISAA* izstrāde.** Tiks uzsākta *ISAA* ziņojumu izstrāde. Komisija/EĀDD izdos *ISAA* ziņojumus, kā izklāstīts *ISAA SOP*, un var turpmāk veicināt informācijas apmaiņu *IPCR* tīmekļa platformā vai izdot konkrētus

([1]) Ziņojumā par ES kiberdrošības incidenta situāciju ir apkopoti ziņojumi, ko sniegušas valstu *CSIRT*. Ziņojuma formāts ir jāapraksta, izmantojot *CSIRT* tīkla *SOP*.

informācijas pieprasījumus. *ISAA* ziņojumi tiks izstrādāti atbilstoši politiskā līmeņa (t. i., *Coreper* vai Padomes) vajadzībām, kā noteikusi prezidentvalsts un norādīts tās vadlīnijās, tādējādi sniedzot stratēģisku pārskatu par situāciju un ļaujot sarīkot uz informāciju balstītas debates par prezidentvalsts noteiktiem darba kārtības jautājumiem. Saskaņā ar *ISAA SOP* kiberdrošības krīzes veids noteiks, vai *ISAA* ziņojumu sagatavo kāds no Komisijas dienestiem (*CNECT* ĢD, *HOME* ĢD) vai EĀDD.

Pēc *IPCR* aktivizēšanas prezidentvalsts izklāstīs konkrētās jomas, uz ko *ISAA* koncentrēties, lai atbalstītu politikas koordinācijas un/vai lēmumu pieņemšanas procesu Padomē. Pēc apspriešanās ar Komisijas dienestiem/EĀDD prezidentvalsts konkretizēs arī ziņojuma termiņu.

— **Plāns:**

— *ISAA* ziņojumā ir ietverts attiecīgu dienestu ieguldījums, tostarp no:

— *CSIRT* tīkla – ziņojums par ES kiberdrošības incidenta situāciju;

— *EC3*, *SITROOM*, ES hibrīddraudu analīzes vienības, *CERT-EU*. ES hibrīddraudu analīzes vienība pēc vajadzības atbalstīs un sniegs ieguldījumu *ISAA* vadošajam dienestam un *IPCR* apaļajam galdam;

— ES nozaru aģentūrām un struktūrām atkarībā no skartajām nozarēm;

— dalībvalstu iestādēm (izņemot *CSIRT*).

— *ISAA* devuma apkopošana ([1]):

— Komisija un ES aģentūras. *ARGUS* IT sistēma nodrošinās *ISAA* iekšējo pamattīklu. ES aģentūras nosūta savus ieguldījumus saviem attiecīgajiem ĢD, kuri savukārt ievadīs attiecīgo informāciju *ARGUS* sistēmā. Komisijas dienesti un aģentūras vāks informāciju no esošajiem nozaru tīkliem ar dalībvalstīm un starptautiskām organizācijām un no citiem attiecīgiem avotiem.

— Attiecībā uz EĀDD. ES Dežūrcentrs, ko atbalsta pārējās attiecīgās EĀDD struktūrvienības, nodrošinās iekšējo pamattīklu un vienotu kontaktpunktu *ISAA*. EĀDD vāks informāciju no trešām valstīm un attiecīgām starptautiskajām organizācijām.

— **6. posms – prezidentvalsts neformālā apaļā galda sagatavošana**. Prezidentvalsts, kam palīdz Padomes Ģenerālsekretariāts, noteiks prezidentvalsts neformālā apaļā galda sanāksmes laiku, darba kārtību, dalībniekus un sagaidāmo rezultātu (iespējamos nodevumus). Padomes Ģenerālsekretariāts prezidentūras vārdā nodos attiecīgu informāciju *IPRC* tīmekļa platformai un izdos paziņojumu par sanāksmi.

— **7. posms – prezidentūras apaļais galds/sagatavošanas pasākumi ES politiskajai koordinācijai/lēmumu pieņemšanai**. Prezidentvalsts rīkos neformālu apaļo galdu, lai pārskatītu situāciju un sagatavotu un pārskatītu jautājumus, kas iesniedzami izskatīšanai *Coreper* vai Padomei. Neformālais prezidentvalsts apaļais galds būs arī forums visu *Coreper*/Padomei iesniedzamo rīcības priekšlikumu izstrādāšanai, pārskatīšanai un apspriešanai.

— **Plāns:**

— Padomes Kiberjautājumu horizontālajai darba grupai būtu jāsagatavo PDK vai *Coreper* sanāksme.

— **8. posms – Politiskā koordinācija un lēmumu pieņemšana *Coreper*/Padomē**. *Coreper*/Padomes sanāksmju rezultāti attiecas uz reaģēšanas pasākumu koordinēšanu visos līmeņos, lēmumiem par ārkārtas pasākumiem, politiskām deklarācijām utt. Šie lēmumi veido arī atjauninātus politiskos/stratēģiskos norādījumus turpmākai *ISAA* ziņojumu sagatavošanai.

— **Plāns:**

— politisko lēmumu koordinēt reaģēšanu uz kiberdrošības krīzi īsteno ar pasākumiem (kurus veic attiecīgie dalībnieki), kas iepriekš 1. iedaļā "Sadarbība stratēģiskā/politiskā, operatīvajā un tehniskajā līmenī" aprakstīti attiecībā uz **reaģēšanu** un **sabiedrības informēšanu**,

— *ISAA* sagatavošanu turpina, pamatojoties uz sadarbību tehniskajā, operatīvajā un politiskajā/stratēģiskajā līmenī attiecībā uz **situācijas apzināšanos**, kas arī aprakstīts iepriekš 1. iedaļā.

([1]) *ISAA SOP*.

— **9. posms – ietekmes monitorings**. *ISAA* vadošais dienests ar *ISAA* ieguldījumu sniedzēju atbalstu informēs par krīzes attīstību un par pieņemto politisko lēmumu ietekmi. Šī atgriezeniskā saite veicinās procesa nepārtrauktību un atbalstīs prezidentvalsts lēmumu, turpinot ES politiskā līmeņa iesaisti vai pakāpeniski izbeidzot *IPCR*.

— **10. posms – pakāpeniska izbeigšana**. Ievērojot to pašu procesu, ko izmanto aktivācijai, prezidentvalsts drīkst sasaukt neformālu apaļā galda sanāksmi, lai izvērtētu, vai saglabāt *IPCR* aktīvā stāvoklī. Prezidentvalsts var nolemt izbeigt vai pazemināt aktivāciju.

— **Plāns:**

— Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*) drīkst uzaicināt dot ieguldījumu vai veikt incidenta *ex post* tehnisko izmeklēšanu saskaņā ar tās pilnvarojumu.

PAPILDINĀJUMS

1. KRĪZES PĀRVARĒŠANA, SADARBĪBAS MEHĀNISMI UN AKTORI ES LĪMENĪ

Krīzes pārvarēšanas mehānismi

Integrētie krīzes situāciju politiskās reaģēšanas mehānismi (IPRC). Integrētie krīzes situāciju politiskās reaģēšanas mehānismi (*IPRC*), ko Padome apstiprināja 2013. gada 25. jūnijā ([1]), ir paredzēti, lai veicinātu savlaicīgu sadarbību un reaģēšanu ES politiskajā līmenī smagas krīzes gadījumā. *IPCR* atbalsta arī reaģēšanas uz solidaritātes klauzulas piemērošanu (LESD 222. pants) koordināciju politiskā līmenī, kā noteikts Padomes 2014. gada 24. jūnijā pieņemtajā Lēmumā 2014/415/ES par kārtību, kādā Savienība īsteno solidaritātes klauzulu. *ICPR* darbības standartprocedūrās ([2]) (*SOP*) ir noteikts aktivācijas process un turpmākās veicamās darbības.

ARGUS. Krīzes koordinācijas sistēma, ko Eiropas Komisija 2005. gadā izveidoja, lai nodrošinātu īpašu koordinācijas procesu smagas daudznozaru krīzes gadījumā. To atbalsta tāda paša nosaukuma vispārēja agrīnās brīdināšanas sistēma (IT rīks). *ARGUS* paredz divus posmus; II posms (smagas daudznozaru krīzes gadījumā) paredz Krīzes koordinācijas komitejas sanāksmju sasaukšanu Komisijas priekšsēdētāja vai atbildīgā Komisijas locekļa pakļautībā. Krīzes koordinācijas komitejā tiekas attiecīgo ĢD, biroju un citu ES dienestu pārstāvji, lai vadītu un koordinētu Komisijas reakciju uz krīzi. Krīzes koordinācijas komiteja, kuru vada ģenerālsekretāra vietnieks, izvērtē situāciju, apsver variantus un pieņem īstenojamus lēmumus attiecībā uz Komisijas atbildībā esošiem ES rīkiem un instrumentiem, kā arī nodrošina lēmumu īstenošanu ([3]), ([4]).

EĀDD mehānisms reaģēšanai krīzes situācijās. EĀDD mehānisms reaģēšanai krīzes situācijās ir strukturēta sistēma EĀDD reaģēšanai uz tādām ārēja rakstura krīzēm un ārkārtas situācijām vai krīzēm un ārkārtas situācijām ar svarīgu ārēju dimensiju, tostarp hibrīddraudiem, kuras potenciāli vai faktiski ietekmē ES vai to dalībvalstu intereses. Nodrošinot attiecīgu Komisijas, kā arī Padomes Sekretariāta ierēdņu dalību tā sanāksmēs, mehānisms reaģēšanai uz krīzēm veicina sinerģiju starp diplomātiskiem, drošības un aizsardzības centieniem un Komisijas pārvaldītiem sadarbības instrumentiem. Krīzes vienību var aktivizēt uz krīzes laiku.

Sadarbības mehānismi

CSIRT tīkls. Datordrošības incidentu reaģēšanas vienības tīkls apvieno visu valstu un valdību *CSIRT* un *CERT-EU*. Šā tīkla mērķis ir nodrošināt un uzlabot informācijas apmaiņu starp *CSIRT* par draudiem un kiberdrošības incidentiem, kā arī sadarboties, reaģējot uz kiberdrošības incidentiem un krīzēm.

Padomes kiberjautājumu horizontālā darba grupa. Šī darba grupa tika izveidota, lai Padomē nodrošinātu kiberpolitikas jautājumu stratēģisko un horizontālo koordināciju, un to var iesaistīt gan leģislatīvās, gan neleģislatīvās darbībās.

Aktori

ENISA. Eiropas Savienības Tīklu un informācijas drošības aģentūra tika izveidota 2004. gadā. Šī aģentūra cieši sadarbojas ar dalībvalstīm un privāto sektoru, lai sniegtu padomus un piedāvātu risinājumus tādos jautājumos kā Eiropas mēroga kiberdrošības mācības, valstu kiberdrošības stratēģiju izstrāde, *CSIRT* sadarbība un spēju veidošana. *ENISA* sadarbojas tieši ar *CSIRT* visā ES un ir *CSIRT* tīkla sekretariāts.

ERCC. Ārkārtas reaģēšanas koordinācijas centrs Komisijā (Eiropas Civilās aizsardzības un humānās palīdzības operāciju ģenerāldirektorāta (ECHO ĢD pakļautībā) diennakts režīmā atbalsta un koordinē dažādas novēršanas, gatavības un reaģēšanas darbības. Tas tika atklāts 2013. gadā un darbojas kā Komisijas krīžu reaģēšanas centrmezgls (sadarbojoties ar citiem ES krīžu centriem), tostarp kā centrālais *IPCR* 24/7 kontaktpunkts.

([1]) 10708/13 "*CCA* pārskatīšanas procesa pabeigšana: ES integrētie krīzes situāciju politiskās reaģēšanas mehānismi", ko Padome apstiprināja 2013. gada 24. jūnijā.

([2]) 12607/15 "*IPCR* darbības standartprocedūras", par ko vienojusies Prezidentvalsts draugu grupa un 2015. gada oktobrī pieņēmusi zināšanai *Coreper*.

([3]) Komisijas noteikumi par vispārējās ātrās trauksmes izziņošanas sistēmu *ARGUS*, COM(2005) 662 galīgā redakcija, 2005. gada 23. decembris.

([4]) Komisijas 2005. gada 23. decembra Lēmums 2006/25/EK, Euratom, ar ko groza tās Iekšējo reglamentu (OV L 19, 24.1.2006., 20. lpp.), par vispārējās ātrās trauksmes izziņošanas sistēmas *ARGUS* izveidi.

Eiropols/EC3. Eiropolā 2013. gadā izveidotais Eiropas Kibernoziedzības apkarošanas centrs (*EC3*) atbalsta tiesībaizsardzības iestāžu reaģēšanu uz kibernoziegumiem ES. *EC3* nodrošina operatīvo un analītisko atbalstu dalībvalstu veiktām izmeklēšanām un darbojas kā kriminālās informācijas un izlūkošanas centrmezgls, kas dalībvalstu operācijas un izmeklēšanas atbalsta ar operatīvo analīzi, koordināciju un zinātību, kā arī ar augsti specializētām tehniskās un digitālās kriminālistikas atbalsta spējām.

CERT-EU. ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība ir pilnvarota uzlabot ES iestāžu, struktūru un aģentūru aizsardzību pret kiberdraudiem. Tā ir *CSIRT* tīkla dalībnieks. *CERT-EU* ir tehniskie nolīgumi par informācijas par kiberdraudiem koplietošanu ar NATO *CIRC*, dažām trešām valstīm un svarīgākajiem komerciālajiem aktoriem kiberdrošības jomā.

ES izlūkošanas kopiena ietver ES izlūkdatu analīzes centru (***INTCEN***) un ES Militārā štāba (*EUMS*) Izlūkošanas nodaļu (*EUMS INT*) saskaņā ar **vienoto izlūkdatu analīzes procedūras** (*SIAC*) *SIAC* kārtību. *SIAC* uzdevums ir nodrošināt izlūkošanas analīzes, agrīnu brīdināšanu un situācijas apzināšanos Savienības Augstajam pārstāvim ārlietās un drošības politikas jautājumos un Eiropas Ārējās darbības dienestam (EĀDD). *SIAC* piedāvā savus pakalpojumus dažādām ES lēmumu pieņemšanas struktūrām kopējās ārpolitikas un drošības politikas (KĀDP), kopējās drošības un aizsardzības politikas (KDAP) un pretterorisma jomā, kā arī dalībvalstīm. *EU INTCEN* un *EUMS INT* nav operatīvās aģentūras, un tām nav nekādu izlūkdatu vākšanas spēju. Par izlūkošanas operatīvo līmeni ir atbildīgas dalībvalstis. *SIAC* nodarbojas tikai ar stratēģisko analīzi.

ES Hibrīddraudu analīzes vienība. Kopīgajā paziņojumā par hibrīddraudu apkarošanu, kas pieņemts 2016. gada aprīlī, ES Hibrīddraudu analīzes vienība (*EU HFC*) ir noteikta kā galvenā struktūra visu avotu analīzei par hibrīddraudiem ES: tās pilnvaras Komisija apstiprināja 2016. gada decembrī, izmantojot starpdienestu konsultācijas. ES Hibrīddraudu analīzes vienība ietilpst *INTCEN*, ir daļa no *SIAC* un tādējādi darbojas kopā ar *EUMS INT*, un tajā darbojas pastāvīgi norīkota militārpersona. Hibrīddraudi ir valsts vai nevalstiska darbības veicēja apzināti izmantota daudzu slepenu/atklātu un militāru/civilu rīku un ietekmēšanas līdzekļu, piemēram, kiberuzbrukumu, dezinformācijas kampaņu, spiegošanas, ekonomiskā spiediena, sabiedroto spēku vai citu graujošu darbību, izmantošana. *EU HFC* sadarbojas ar plašu kontaktpunktu (*PoCs*) tīklu gan Komisijā, gan dalībvalstīs, lai nodrošinātu integrētu reaģēšanu/visas valdības pieeju, kas nepieciešama dažādu problēmu pārvarēšanai.

ES Dežūrcentrs. ES Dežūrcentrs ir daļa no ES Izlūkdatu analīzes centra (*EU INTCEN*) un pārstāv EĀDD operatīvās spējas, kas vajadzīgas, lai nodrošinātu tūlītēju un iedarbīgu reaģēšanu uz krīzēm. Tā ir pastāvīga civilmilitāra dežūrstruktūra ar diennakts režīma (24/7) spējām, kas nodrošina vispasaules monitoringu un situācijas apzināšanos.

Attiecīgie instrumenti

Satvars vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām. Vienošanās par šo satvaru tika panākta 2017. gada jūnijā, un tas ir daļa no ES pieejas kiberdiplomātijai, kas sekmē konfliktu novēršanu, kiberdrošības draudu mazināšanu un lielāku stabilitāti starptautiskajās attiecībās. Satvarā pilnībā izmanto kopējās ārpolitikas un drošības politikas pasākumus, tostarp, ja vajadzīgs, ierobežojošus pasākumus. Pasākumu izmantošanai šajā satvarā būtu jāveicina sadarbība, jāsekmē tūlītēju un ilgtermiņa apdraudējumu mazināšana un ilgtermiņā jāietekmē par pārkāpumu atbildīgā nodarītāja un potenciālo agresoru rīcība.

2. KIBERDROŠĪBAS KRĪZES KOORDINĒŠANA *IPCR* MEHĀNISMU IETVAROS – HORIZONTĀLĀ KOORDINĀCIJA UN POLITISKĀ AKTIVIZĀCIJA

IPCR mehānismus var izmantot (un tie ir izmantoti), lai novērstu tehniska un operatīva rakstura problēmas, taču vienmēr no politiska/stratēģiska skatu punkta.

IPCR var aktivizēt atbilstoši krīzes līmenim, no "uzraudzības režīma" pārejot uz "informācijas apmaiņas režīmu", kas ir pirmais *IPCR* aktivizēšanas līmenis, un uz "*IPCR* pilnīgas aktivizēšanas" režīmu.

Lēmumu par pilnīgu aktivizēšanu pieņem ES Padomes rotējošā prezidentvalsts. Komisija, EĀDD un PĢS var *IPCR* aktivizēt informācijas apmaiņas režīmā. Uzraudzības un informācijas apmaiņas režīmā tiek izmantota dažāda līmeņa

informācijas apmaiņa, un informācijas apmaiņas režīmā tiek aktivizēts pieprasījums sagatavot *ISAA* ziņojumus. Pilnīgas aktivizēšanas režīmā pieejamie rīki tiek papildināti ar *IPCR* apaļā galda sanāksmēm, iesaistot prezidentvalsti (parasti *Coreper* II priekšsēdētāju vai attiecīgās jomas ekspertu pastāvīgās pārstāvniecības padomnieku līmenī, taču apaļā galda sanāksmes izņēmuma kārtā ir notikušas ministru līmenī).

Aktori

Rotējošā prezidentvalsts (parasti *Coreper* priekšsēdētājs) – vadošais dienests

Eiropadomē – priekšsēdētāja kabinets

Eiropas Komisijā – ĢSV/ģenerāldirektora līmeņa un/vai jomas eksperti

EĀDD – ĢSV/izpilddirektora līmenis un/vai jomas eksperti

PĢS – ĢS kabinets, *IPCR* komanda un atbildīgie ģenerāldirektorāti

Darbību tvērums. Radīt kopīgu integrētu situācijas pārskatu un palielināt informētību par trūkumiem vai nepilnībām katrā no trim līmeņiem, lai tās risinātu politiskā līmenī, pieņemt lēmumus, ja tie ir dalībnieku kompetences jomā vai sagatavot rīcības priekšlikumus, ko tālāk nosūta *Coreper* II un Padomei.

Kopīga situācijas apzināšanās

(*IPCR* nav aktivizēti): var ģenerēt *IPCR* uzraudzības lapas, lai izsekotu progresējošām situācijām, kas varētu izvērsties par krīzi, kura radītu sekas ES.

(*IPCR* informācijas apmaiņa): *ISAA* vadošais dienests sagatavos *ISAA* ziņojumus, pamatojoties uz Komisijas dienestu, EĀDD un dalībvalstu sniegto informāciju un izmantojot *IPCR* aptaujas lapas.

(*IPCR* pilnīga aktivizēšana): papildus *ISAA* ziņojumiem dažādi dalībvalstu aktori, Komisija, EĀDD, attiecīgās aģentūras u. c. tiekas neformālās *IPCR* apaļā galda sanāksmēs, lai apspriestu nepilnības un trūkumus.

Sadarbība un reaģēšana

Aktivizēt/sinhronizēt papildu krīzes pārvarēšanas mehānismus/instrumentus atkarībā no incidenta veida un ietekmes. Tie var ietvert, piemēram, civilās aizsardzības mehānismu, satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām vai kopīgu regulējumu hibrīddraudu apkarošanai.

Komunikācija krīzes brīdī

Prezidentvalsts pēc apspriešanās ar attiecīgajiem Komisijas dienestiem, PĢS un EĀDD*IPCR* var aktivizēt krīzes saziņas tīklu, lai sniegtu atbalstu kopīgu paziņojumu sagatavošanā vai labāk izmantotu visefektīvākos saziņas rīkus.

3. KIBERDROŠĪBAS KRĪZES PĀRVARĒŠANA AR *ARGUS* – INFORMĀCIJAS APMAIŅA EIROPAS KOMISIJĀ

Saskārusies ar negaidītām krīzēm, kam bija nepieciešama rīcība Eiropas līmenī, proti., ar teroristu uzbrukumiem Madridē (2004. gada marts), Dienvidaustrumāzijas cunami (2004. gada decembris) un teroristu uzbrukumiem Londonā (2005. gada jūlijs), Komisija 2005. gadā izveidoja *ARGUS* koordinācijas sistēmu, ko papildina tāda paša nosaukuma vispārējās ātrās trauksmes izziņošanas sistēma ([1]), ([2]). Tās mērķis ir nodrošināt īpašu **krīzes koordinācijas procesu** smagas daudznozaru krīzes gadījumā, lai reāllaikā varētu dalīties ar informāciju, kas saistīta ar krīzi, un nodrošinātu ātru lēmumu pieņemšanu.

ARGUS paredz divus posmus atkarībā no tā, cik nopietns ir notikums.

I posmu izmanto informācijas apmaiņai par ierobežota apmēra krīzi.

([1]) Eiropas Kopienu Komisija, Komisijas 2005. gada 23. decembra paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Komisijas noteikumi par vispārējās ātrās trauksmes izziņošanas sistēmu *ARGUS*", COM(2005) 662 galīgā redakcija.

([2]) Lēmums 2006/25/EK, Euratom.

Kā piemēru neseniem ziņotajiem I posma notikumiem var minēt meža ugunsgrēkus Portugālē un Izraēlā, uzbrukumu Berlīnē 2016. gadā, plūdus Albānijā, viesuļvētru "Metjū" Haiti un sausumu Bolīvijā. Ikviens ĢD var "atvērt" I posma notikumu, ja uzskata, ka situācija tā kompetences jomā ir pietiekami nopietna, lai attaisnotu informācijas apmaiņu vai gūtu no tās labumu. Piemēram, *HOME* ĢD, *CNECT* ĢD var "atvērt" I posma notikumu, ja uzskata, ka ar kiberdrošību saistītā situācija tā kompetences jomā ir pietiekami nopietna, lai attaisnotu informācijas apmaiņu vai gūtu no tās labumu.

II posmu izmanto smagas daudznozaru krīzes gadījumā vai ja pastāv paredzami vai nenovēršami draudi Savienībai.

II posmā iedarbina īpašu koordinācijas procesu, kas ļauj Komisijai pieņemt lēmumus un pārvaldīt ātru, koordinētu un saskaņotu reaģēšanu augstākajā līmenī savā kompetences jomā un sadarbībā ar citām iestādēm. II posms ir paredzēts smagas daudznozaru krīzes gadījumam vai tās radītiem paredzamiem vai nenovēršamiem draudiem. Reāli II posma notikumu piemēri ir migrācijas/bēgļu krīze (no 2015. gada līdz šim brīdim), Fukušimas trīskāršā katastrofa (2011. gadā) un Islandes vulkāna *Eyjafjallajökull* izvirdums (2010. gadā).

II posmu aktivizē priekšsēdētājs pēc savas iniciatīvas vai pēc Komisijas locekļa pieprasījuma. Politisko atbildību par Komisijas reakciju priekšsēdētājs var uzņemties pats vai piešķirt Komisijas loceklim, kas ir atbildīgs par dienestu, kuru attiecīgā krīze skar visvairāk.

Šajā posmā paredzētas Krīzes koordinācijas komitejas (KKK) ārkārtas sanāksmes. Tās sasauc priekšsēdētāja vai atbildīgā Komisijas locekļa pakļautībā. Sanāksmes sasauc ģenerālsekretārs, izmantojot *ARGUS* IT rīku. Krīzes koordinācijas komiteja ir īpaša operatīva krīzes vadības struktūra, ko izveido Komisijas krīzes risinājuma vadībai un koordinācijai un kurā apvienojas pārstāvji no attiecīgajiem Komisijas ģenerāldirektorātiem, kabinetiem un citiem ES dienestiem. **Krīzes koordinācijas komiteja**, kuru vada ģenerālsekretāra vietnieks, **izvērtē situāciju, apsver risinājumus un pieņem lēmumus, kā arī nodrošina lēmumu un rīcību īstenošanu**, vienlaikus arī nodrošinot risinājuma saskanību un konsekvenci. Krīzes koordinācijas komiteju atbalsta ģenerālsekretariāts.

4. EĀDD MEHĀNISMS REAĢĒŠANAI KRĪZES SITUĀCIJĀS

EĀDD mehānismu reaģēšanai krīzes situācijās (*CRM*) aktivizē, ja ir radusies ar ES ārējo dimensiju saistīta nopietna vai ārkārtas situācija. *CRM* aktivizē ģenerālsekretāra vietnieks jautājumos, kas skar reaģēšanu uz krīzēm, apspriežoties ar AP/PV vai ģenerālsekretāru. AP/PV vai ģenerālsekretārs, vai cits ģenerālsekretāra vietnieks vai izpilddirektors arī var pieprasīt ģenerālsekretāra vietniekam jautājumos, kas skar reaģēšanu uz krīzēm, iedarbināt mehānismu reaģēšanai krīzes situācijās.

CRM palīdz nodrošināt to, ka, reaģējot krīzes situācijās, ES rīcība ir saskaņā ar drošības stratēģiju. Jo īpaši *CRM* veicina sinerģiju starp diplomātiskiem, drošības un aizsardzības centieniem un Komisijas pārvaldītiem finanšu, tirdzniecības un sadarbības instrumentiem.

CRM ir saistīts ar Komisijas vispārējo ātrās reaģēšanas sistēmu (*ARGUS*) un ES integrētiem krīzes situāciju politiskās reaģēšanas mehānismiem (*IPCR*) nolūkā izmantot sinerģijas, ja notiek vienlaicīga aktivizēšana. EĀDD Dežūrcentrs darbojas kā saziņas centrs starp EĀDD un Padomes un Komisijas ārkārtas reaģēšanas sistēmām.

Krīzes sanāksmes sasaukšana parasti ir pirmā darbība saistībā ar *CRM* aktivizēšanu, un tajā piedalās EĀDD, Komisijas un Padomes augstākā līmeņa vadītāji, kurus tieši skar attiecīgā krīze. Krīzes sanāksmē izvērtē krīzes īstermiņa ietekmi, un tajā var vienoties par tūlītējo rīcību, Krīzes vienības aktivizēšanu vai Krīzes platformas sasaukšanu. Šīs darbības var veikt jebkādā secībā.

Krīzes vienība ir neliela dežūrtelpa, kurā krīzes risināšanā iesaistīto EĀDD, Komisijas un Padomes dienestu pārstāvji tiekas, lai pastāvīgi uzraudzītu situāciju un sniegtu atbalstu lēmuma pieņēmējiem EĀDD galvenajā birojā. Pēc aktivizēšanas Krīzes vienība darbojas 24 stundas diennaktī, septiņas dienas nedēļā.

Krīzes platformā attiecīgie EĀDD, Komisijas un Padomes dienesti tiekas, lai izvērtētu krīzes vidēja termiņa un ilgtermiņa ietekmi un vienotos par turpmākajām darbībām. To vada AP/PV vai ģenerālsekretārs, vai ģenerālsekretāra vietnieks jautājumos, kas skar reaģēšanu uz krīzēm. Krīzes platforma novērtē, cik efektīva ir ES rīcība krīzes valstī vai reģionā, lemj par papildu pasākumu grozījumiem un apspriež Padomes rīcības priekšlikumus. Krīzes platforma ir *ad hoc* sanāksme, tāpēc tā nav pastāvīgi aktivizēta.

Uzdevumgrupas sastāvā ir pārstāvji no dienestiem, kas ir iesaistīti krīzes risināšanā, un to var aktivizēt, lai sekotu ES reaģēšanas gaitai un sekmētu to. Tā izvērtē ES rīcības ietekmi, sagatavo politikas un risinājumu dokumentus, palīdz sagatavot politikas sistēmu krīzes risināšanai (*PFCAs*), sekmē saziņas stratēģiju un pieņem jebkādus citus pasākumus, kas var sekmēt ES reaģēšanas gaitu.

5. ATSAUCES DOKUMENTI

Turpmāk norādīti atsauces dokumenti, kuri ņemti vērā plāna sagatavošanā.

— Eiropas kiberdrošības krīzes sadarbības sistēma, 2012. gada 17. oktobris, 1. versija.

— *Report on Cyber Crisis Cooperation and Management*, *ENISA*, 2014.

— *Actionable Information for Security Incident Response*, *ENISA*, 2014.

— *Common practices of EU-level crisis management and applicability to cyber crises*, *ENISA*, 2015.

— *Strategies for Incident Response and Cyber Crisis Cooperation*, *ENISA*, 2016.

— *EU Cyber Standard Operating Procedures*, *ENISA*, 2016.

— *A good practice guide of using taxonomies in incident prevention and detection*, *ENISA*, 2017.

— Kā nostiprināt Eiropas Kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari, COM(2016) 410 final, 2016. gada 5. jūlijs.

— Padomes secinājumi "Kā nostiprināt Eiropas kiberizturētspējas sistēmu un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari" – Padomes secinājumi (2016. gada 15. novembris), 14540/16.

— Padomes 2014. gada 24. jūnija Lēmums 2014/415/ES par kārtību, kādā Savienība īsteno solidaritātes klauzulu (OV L 192, 1.7.2014., 53. lpp.).

— *CCA* pārskatīšanas procesa pabeigšana: ES integrēti krīzes situāciju politiskās reaģēšanas mehānismi (*IPCR*), 10708/13, 2013. gada 7. jūnijs.

— Integrētā situācijas apzināšanās un analīze (*ISAA*) – darbības standartprocedūras, DS 1570/15, 2015. gada 22. oktobris.

— Komisijas noteikumi par vispārējās ātrās trauksmes izziņošanas sistēmu *ARGUS*, COM(2005) 662 galīgā redakcija, 2005. gada 23. decembris.

— Komisijas 2005. gada 23. decembra Lēmums 2006/25/EK, Euratom, ar ko groza tās Iekšējo reglamentu (OV L 19, 24.1.2006., 20. lpp.).

— *ARGUS Modus Operandi*, Eiropas Komisija, 2013. gada 23. oktobris.

— Padomes secinājumi par satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām (*Cyber Diplomacy Toolbox*), dok. 9916/17.

— ES operatīvais protokols hibrīddraudu apkarošanai (*EU Playbook*), dok. SWD(2016) 227.

— EĀDD mehānisms reaģēšanai krīzes situācijās, 2016. gada 8. novembris [Ares(2017)880661]. Komisijas dienestu darba dokuments "ES operatīvais protokols hibrīddraudu apkarošanai" (*EU Playbook*), SWD(2016) 227 final, 2016. gada 5. jūlijs.

— Kopīgs paziņojums Eiropas Parlamentam un Padomei: Kopīgs regulējums hibrīddraudu apkarošanai – Eiropas Savienības reakcija JOIN/2016/018 final, 2016. gada 6. aprīlis.

— EEAS(2016) 1674, Eiropas Ārējās darbības dienesta darba dokuments "ES Hibrīddraudu analīzes vienība – pilnvaras".

6. AR KIBERDROŠĪBU SAISTĪTIE *IPCR* PROCESA ELEMENTI