EIROPAS
KOMISIJA

SAVIENĪBAS AUGSTĀ
PĀRSTĀVE ĀRLIETĀS UN
DROŠĪBAS POLITIKAS
JAUTĀJUMOS

Briselē, 6.4.2016.
JOIN(2016) 18 final

KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Kopīgs regulējums hibrīddraudu apkarošanai –

Eiropas Savienības reakcija

1. IEVADS

Pēdējos gados ir būtiski mainījusies drošības situācija Eiropas Savienībā. Būtiski draudi mieram un stabilitātei ES austrumu un dienvidu kaimiņvalstīs joprojām izceļ to, ka Savienībai jāpielāgo un jāpalielina savas spējas būt par drošības garantu, spēcīgu uzsvaru liekot uz ciešām saiknēm starp ārējo un iekšējo drošību. Daudzu pašreizējo miera, drošības un labklājības apdraudējumu iemesls ir nestabilitāte ES tuvākajās kaimiņvalstīs un draudu mainīgie veidi. Savās „Politikas pamatnostādnēs" Eiropas Komisijas priekšsēdētājs Žans Klods Junkers 2014. gadā uzsvēra nepieciešamību „panākt to, ka Eiropa ir spēcīgāka drošības un aizsardzības jautājumos," un efektīvāk nekā līdz šim apvienot Eiropas un valsts līmeņa instrumentus. Turklāt pēc Ārlietu padomes 2015. gada 18. maija aicinājuma Augstā pārstāve ciešā sadarbībā ar Komisijas dienestiem un Eiropas Aizsardzības aģentūru (EEA) un, apspriežoties ar ES dalībvalstīm, uzsāka darbu nolūkā nākt klajā ar šo kopējo satvaru, kurā ietverti īstenojami priekšlikumi, lai palīdzētu novērst hibrīda veida apdraudējumu un veicinātu ES un dalībvalstu, kā arī partneru izturētspēju[1]. Eiropadome 2015. gada jūnijā atgādināja, ka ir jāmobilizē ES instrumenti, lai palīdzētu vērsties pret hibrīddraudiem[2].

Kaut arī hibrīddraudu definīcijas atšķiras un tām arī turpmāk jābūt elastīgām, lai reaģētu uz hibrīddraudu mainīgo raksturu, šāda veida apdraudējums aptver piespiedu un graujošu darbību, tradicionālu un netradicionālu (t. i., diplomātisku, militāru, ekonomisku, tehnoloģisku) metožu apvienojumu, ko koordinēti var izmantot valsts vai nevalstiski dalībnieki, lai panāktu konkrētus mērķus, bet nepārkāpjot oficiāli pieteikta kara robežu. Uzsvars parasti tiek likts uz to, lai izmantotu mērķa objekta vājās vietas un radītu neskaidrību nolūkā kavēt lēmumu pieņemšanas procesus. Mehānismi hibrīddraudu piemērošanai var būt masīvas dezinformācijas kampaņas, kuru ietvaros tiek izmantoti sociālie mediji, lai kontrolētu politikas debates vai radikalizētu, vervētu un virzītu marionetes.

Ciktāl hibrīddraudu novēršana attiecas uz valsts drošību un aizsardzību un likumības un kārtības uzturēšanu, galvenā atbildība gulstas uz dalībvalstīm, jo vairums valsts līmeņa neaizsargātības faktoru ir katrai valstij atšķirīgi. Tomēr daudzas ES dalībvalstis sastopas ar kopējiem draudiem, kas var skart arī pārrobežu tīklus vai infrastruktūru. Šādus draudus var efektīvāk novērst ar ES līmenī koordinētu rīcību, izmantojot ES politikas jomas un instrumentus, kam jābalstās uz Eiropas solidaritāti, savstarpēju palīdzību un visu Lisabonas līguma sniegto potenciālu. ES politikas jomas un instrumenti var pildīt būtisku, pievienoto vērtību palielinošu lomu informētības uzlabošanā – un ievērojamā apmērā tas notiek jau tagad. Tas palīdz uzlabot dalībvalstu izturētspēju, lai reaģētu uz kopīgiem apdraudējumiem. Savienības ārējās darbības, kas ierosināta saskaņā ar šo satvaru, pamatā ir Līguma par Eiropas Savienību (LES) 21. pantā izklāstītie principi,

[1] Padomes secinājumi par kopējo drošības un aizsardzības politiku (KDAP), 2015. gada maijs [*Consilium* 8971/15].
[2] Eiropadomes secinājumi, 2015. gada jūnijs [*EUCO* 22/15].

tostarp demokrātija, tiesiskums, universāls un nedalāms cilvēktiesību princips, kā arī Apvienoto Nāciju Organizācijas Statūtu un starptautisko tiesību ievērošana[3].

Šā kopīgā paziņojuma mērķis ir atvieglot holistisku pieeju, kas ļaus Eiropas Savienībai sadarbībā ar dalībvalstīm mērķtiecīgi novērst hibrīda veida apdraudējumu, veidojot sinerģiju starp visiem attiecīgajiem instrumentiem un veicinot ciešu sadarbību starp visiem būtiskajiem dalībniekiem[4]. Darbības balstās uz esošajām stratēģijām un nozaru politiku, kas sekmē lielāku drošību. Jo īpaši Eiropas Drošības programma[5], gaidāmā Eiropas Savienības globālā ārpolitikas un drošības politikas stratēģija un Eiropas Aizsardzības rīcības plāns[6], ES kiberdrošības stratēģija[7], enerģētiskās drošības stratēģija[8] un Eiropas Savienības Jūras drošības stratēģija[9] ir instrumenti, kas arī var palīdzēt novērst hibrīddraudus.

Ņemot vērā to, ka arī NATO veic pasākumus hibrīddraudu apkarošanai un Ārlietu padome ierosināja pastiprināt sadarbību un koordināciju šajā jomā, dažu priekšlikumu nolūks ir uzlabot ES un NATO sadarbību hibrīddraudu apkarošanā.

Ierosinātā rīcība koncentrējas uz šādiem elementiem: informētības uzlabošana, izturētspējas veidošana, krīzes nepieļaušana, reaģēšana uz to un atgūšanās no tās.

2. APDRAUDĒJUMA HIBRĪDĀ RAKSTURA ATPAZĪŠANA

Hibrīddraudu mērķis ir izmantot valsts vājās vietas, un bieži ar tiem tiek mēģināts sagraut demokrātijas pamatvērtības un brīvības. Vispirms Augstā pārstāve un Komisija sadarbosies ar dalībvalstīm, lai uzlabotu situācijas apzināšanos, uzraugot un novērtējot riskus, kas varētu apdraudēt ES vājās vietas. Komisija pašlaik izstrādā drošības riska novērtējuma metodes, lai palīdzētu informēt lēmumu pieņēmējus un sekmētu uz riska balstītas politikas veidošanu dažādās jomās, sākot no aviācijas drošības līdz teroristu finansēšanai un nelikumīgi iegūtu līdzekļu legalizācijai. Turklāt dalībvalstīm būtu lietderīgi veikt pētījumu, kurā ir apzinātas pret hibrīddraudiem neaizsargātās jomas. Tā mērķis būtu apzināt hibrīddraudu rādītājus, iekļaut tos agrīnās brīdināšanas un esošajos riska novērtējuma mehānismos un vajadzības gadījumā apmainīties ar tiem.

<u>1. darbība.</u> Dalībvalstis, kurām vajadzības gadījumā atbalstu sniedz Komisija un Augstā pārstāve, tiek aicinātas izstrādāt pētījumu par hibrīda veida riskiem, lai apzinātu būtiskākās vājās vietas (tostarp specifiskus rādītājus saistībā ar hibrīddraudiem), kas varētu ietekmēt valsts un Eiropas mēroga struktūras un tīklus.

[3] ES Pamattiesību harta ir saistoša iestādēm un dalībvalstīm, kad tās īsteno Savienības tiesību aktus.
[4] Uz iespējamiem tiesību aktu priekšlikumiem attieksies Komisijas labāka regulējuma prasības saskaņā ar Komisijas izstrādātajām „Labāka regulējuma pamatnostādnēm", SWD(2015) 111.
[5] COM(2015) 185 *final*.
[6] Jāiesniedz 2016. gadā.
[7] ES kiberaizsardzības politikas satvars [*Consilium* 15585/14] un kopīgs paziņojums „Eiropas Savienības kiberdrošības stratēģija – atvērta un droša kibertelpa", 2013. gada februāris [JOIN(2013) 1].
[8] Kopīgs paziņojums „Eiropas enerģētiskās drošības stratēģija", 2014. gada maijs [SWD(2014) 330].
[9] Kopīgs paziņojums „Atklātai un drošai jūras videi pasaulē: Eiropas Savienības Jūras drošības stratēģijas elementi", 6.3.2014., JOIN(2014) 9 *final*.

3. ES REAKCIJAS NODROŠINĀŠANA – INFORMĒTĪBAS UZLABOŠANA

3.1. ES hibrīddraudu analīzes vienība (*EU Hybrid Fusion Cell*)

Ir ļoti būtiski, lai Eiropas Savienība, sadarbojoties ar tās dalībvalstīm, pietiekami augstā līmenī nodrošinātu situācijas apzināšanos nolūkā identificēt jebkuru drošības vides izmaiņu, kas saistīta ar hibrīda veida darbību, kuru veic valsts un/vai nevalstiski dalībnieki. Efektīvai hibrīddraudu apkarošanai ir svarīgi uzlabot informācijas apmaiņu un sekmēt apmainīšanos ar attiecīgajiem izlūkošanas datiem starp nozarēm, kā arī Eiropas Savienības, tās dalībvalstu un partneru vidū.

ES hibrīddraudu analīzes vienības vienotajā fokusā būs to hibrīddraudu analīze, kurus konstatējis Eiropas Ārējās darbības dienesta (EĀDD) ES Izlūkdatu analīzes centrs (ES *INTCEN*). Šī analīzes vienība saņemtu, analizētu un apmainītos ar klasificētu un publiskos avotos atrodamu informāciju, kas konkrēti skar ar hibrīddraudiem saistītus rādītājus un brīdinājumus, kuri saņemti no dažādām ieinteresētajām personām EĀDD paspārnē (tostarp ES delegācijām), Komisijas (un ES aģentūrām[10]) un dalībvalstīm. Saziņā ar līdzīgām struktūrām, kuras jau tagad darbojas ES[11] un valstu līmenī, analīzes vienība izvērtētu ārējos hibrīddraudu aspektus, kas ietekmē ES un tās kaimiņvalstis, lai tādējādi ātri analizētu attiecīgos incidentus un informētu ES stratēģisko lēmumu pieņemšanas procesos iesaistītos dalībniekus, tostarp sniedzot ieguldījumu ES līmenī veiktajos drošības riska novērtējumos. Analīzes vienības analītiskie rezultāti tiktu apstrādāti un izmantoti saskaņā ar Eiropas Savienības klasificētas informācijas un datu aizsardzības noteikumiem[12]. Vienībai būtu jāsazinās ar struktūrām, kas jau tagad darbojas ES un valstu līmenī. Dalībvalstīm būtu jāizveido valsts kontaktpunkti, kas ir saistīti ar ES hibrīddraudu analīzes vienību. Arī personāls, kas strādā Eiropas Savienībā un ārpus tās (tostarp uz ES delegācijām, operācijām un misijām nosūtītie darbinieki), kā arī dalībvalstīs, būtu jāapmāca atpazīt pirmās hibrīddraudu pazīmes.

<u>2. darbība.</u> Esošās ES* INTCEN *struktūras ietvaros izveidot ES hibrīddraudu analīzes vienību, kas ir spējīga saņemt un analizēt klasificētu un publiskos avotos atrodamu informāciju par hibrīddraudiem. Dalībvalstis tiek aicinātas izveidot valsts kontaktpunktus hibrīddraudu jautājumos, lai nodrošinātu sadarbību un drošu saziņu ar ES hibrīddraudu analīzes vienību.

3.2. Stratēģiskā komunikācija

Hibrīddraudu izteicēji var sistemātiski izplatīt dezinformāciju, tostarp ar mērķtiecīgu kampaņu starpniecību sociālajos medijos, tādējādi mēģinot radikalizēt atsevišķas personas, destabilizēt sabiedrību un kontrolēt politiskās debates. Spēja reaģēt uz hibrīddraudiem, piemērojot rūpīgu **stratēģiskās komunikācijas** stratēģiju, ir ļoti būtiska.

[10] Saskaņā ar to pilnvarām.
[11] Piemēram, Eiropola Eiropas Kibernoziedzības centrs un Terorisma apkarošanas centrs, *Frontex*, ES datorapdraudējumu reaģēšanas vienība (*CERT-EU*).
[12] Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK.

Uz faktiem balstītu atbilžu ātra sniegšana un sabiedrības informētības vairošana par hibrīddraudiem ir nozīmīgi faktori sabiedrības izturētspējas palielināšanai.

Stratēģiskajā komunikācijā būtu pilnībā jāizmanto sociālo mediju instrumenti, kā arī tradicionālie audiovizuālie un interneta plašsaziņas līdzekļi. Eiropas Ārējās darbības dienestam, balstoties uz Austrumu un Arābu stratēģiskās komunikācijas operatīvo grupu darbībām, būtu labāk jāizmanto valodnieki, kuri tekoši pārvalda attiecīgās valodas, kas nav ES valodas, un sociālo mediju speciālisti, kuri var pārraudzīt informāciju no trešām valstīm un nodrošināt mērķtiecīgu komunikāciju, lai reaģētu uz dezinformāciju. Turklāt dalībvalstīm būtu jāizstrādā koordinētas stratēģiskās komunikācijas mehānismi, kuru mērķis, lai atmaskotu hibrīddraudus, ir palīdzēt atklāt dezinformācijas avotus un cīnīties pret to.

<u>3. darbība.</u> Augstā pārstāve kopā ar dalībvalstīm izpētīs veidus, kā aktualizēt un koordinēt spējas īstenot proaktīvu stratēģiskās komunikācijas politiku un labāk izmantot plašsaziņas līdzekļu monitoringu un valodniekus.

3.3. Izcilības centrs „hibrīddraudu apkarošanai”

Balstoties uz dažu dalībvalstu un partnerorganizāciju[13] pieredzi, daudznacionāls institūts vai šādu institūtu tīkls varētu darboties kā izcilības centrs hibrīddraudu novēršanai. Šāds centrs varētu koncentrēties uz izpēti par to, kā hibrīdstratēģijas tiek piemērotas, un tas varētu sekmēt jaunu koncepciju un tehnoloģiju izstrādi privātajā sektorā un nozarē, lai tādējādi palīdzētu dalībvalstīm veidot izturētspēju. Minētā izpēte varētu palīdzēt saskaņot ES un valsts līmeņa politiku, doktrīnas un koncepcijas un nodrošināt to, ka lēmumu pieņemšanā var ņemt vērā ar hibrīddraudiem saistīto sarežģītību un neskaidrību. Šādam centram būtu jāizstrādā programmas pētniecības veicināšanai un pasākumi, kas ļautu rast praktiskus risinājumus esošajām problēmām, kuru iemesls ir hibrīddraudi. Šāda centra spēks būtu atkarīgs no speciālajām zināšanām, ko uzkrājuši centra daudznacionālie un starpnozaru dalībnieki, kas pārstāv civilo un militāro, kā arī privāto sektoru un akadēmiskās aprindas.

Šāds centrs varētu cieši sadarboties ar esošajiem ES[14] un NATO[15] izcilības centriem, lai izmantotu tās atziņas par hibrīddraudiem, kuras gūtas kiberaizsardzības, stratēģiskās komunikācijas, civilmilitārās sadarbības, enerģētikas un krīzes situāciju reaģēšanas jomā.

<u>4. darbība.</u> Dalībvalstis tiek aicinātas apsvērt izcilības centra „hibrīddraudu apkarošanai” izveidi.

4. ES REAKCIJAS NODROŠINĀŠANA – IZTURĒTSPĒJAS VEIDOŠANA

Izturētspēja ir spēja izturēt spriedzi un atgūties vēl spēcīgākam. Efektīvai hibrīddraudu apkarošanai ir jānovērš svarīgākās infrastruktūras, piegādes ķēžu un sabiedrības

[13] NATO izcilības centri.

[14] Piemēram, ES Drošības izpētes institūts (*EUISS*), tematiski ES izcilības centri, kas nodarbojas ar ķīmiska, bioloģiska, radioloģiska un kodolmateriālu (*CBRN*) rakstura jautājumiem.

[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

iespējamās vājās vietas. Izmantojot ES instrumentus un politikas jomas, var ES līmenī palielināt infrastruktūras izturētspēju.

4.1. Kritiskās infrastruktūras aizsardzība

Ir svarīgi aizsargāt kritisko infrastruktūru (piemēram, energoapgādes ķēdes, transportu), jo netradicionāls hibrīddraudu izteicēju uzbrukums jebkuram viegli pieejamam mērķim varētu nopietni satricināt ekonomiku vai sabiedrību. Lai nodrošinātu kritiskās infrastruktūras aizsardzību, Eiropas programmā kritiskās infrastruktūras aizsardzībai[16] (*EPCIP*) ir paredzēta visa veida apdraudējumus aptveroša starpnozaru sistēmiska pieeja, kura pievēršas savstarpējai atkarībai un kuras pamatā ir pasākumu īstenošana novēršanas, sagatavotības un reaģēšanas darbplūsmās. Ar direktīvu par Eiropas kritisko infrastruktūru[17] tiek izveidota procedūra Eiropas kritiskās infrastruktūras (EKI) apzināšanai un noteikšanai un paredzēta kopīga pieeja, kā novērtēt vajadzību uzlabot šīs infrastruktūras aizsardzību. Jo īpaši būtu jāatsāk darbs saskaņā ar minēto direktīvu, lai stiprinātu tās kritiskās infrastruktūras izturētspēju, kas saistīta ar transportu (piemēram, ES galvenās lidostas un tirdzniecības ostas). Komisija izvērtēs, vai jāizstrādā kopīgi instrumenti (tostarp rādītāji), ar kuriem visās attiecīgajās nozarēs uzlabo kritiskās infrastruktūras izturētspēju hibrīddraudu gadījumā.

<u>5. darbība.</u> Komisija sadarbībā dalībvalstīm un ieinteresētajām personām apzinās kopīgus instrumentus, tostarp rādītājus, lai attiecīgajās nozarēs uzlabotu kritiskās infrastruktūras aizsardzību un izturētspēju hibrīddraudu gadījumā.

4.1.1. Enerģētikas tīkli

Netraucēta elektroenerģijas ražošana un piegāde ir ļoti svarīga Eiropas Savienībai, un ievērojami elektroapgādes pārtraukumi varētu nodarīt kaitējumu. Būtisks hibrīddraudu apkarošanas elements ir turpmāka ES enerģijas avotu, piegādātāju un maršrutu dažādošana nolūkā panākt drošāku un noturīgāku enerģijas piegādi. Komisija arī veic ES spēkstaciju riska un drošības novērtējumus („noturības testi”). Lai nodrošinātu enerģijas piegādes dažādošanu, norit intensīvāks darbs Enerģētikas savienības stratēģijas kontekstā, piemēram, gāze no Kaspijas jūras reģiona var sasniegt Eiropu pa Dienvidu gāzes koridoru, un Ziemeļeiropā tiek veidoti sašķidrinātas gāzes mezgli ar vairākiem piegādātājiem. Šim piemēram vajadzētu sekot Centrāleiropā un Austrumeiropā, kā arī Vidusjūras reģionā, kur tiek projektēts gāzes mezgls[18]. Pozitīva ietekme šā mērķa sasniegšanā būs arī augošajam sašķidrinātas dabasgāzes tirgum.

Attiecībā uz kodolmateriāliem un kodoliekārtām Komisija atbalsta visaugstāko drošības standartu izstrādi un pieņemšanu, tādējādi stiprinot izturētspēju. Komisija mudina

[16] Komisijas paziņojums par Eiropas programmu kritisko infrastruktūru aizsardzībai, 12.12.2006., COM(2006) 786 galīgā redakcija.
[17] Padomes Direktīva 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību, OV L 345, 23.12.2008.
[18] Līdz šim gūtajam progresam skatīt Enerģētikas savienības 2015. gada stāvokļa apskatu, COM(2015) 572 *final*.

konsekventi transponēt un īstenot Kodoldrošības direktīvu[19], kurā izklāstīti noteikumi par avāriju novēršanu un avāriju seku mazināšanu, un Drošības pamatstandartu direktīvā[20] paredzētos noteikumus par starptautisko sadarbību (jo īpaši starp kaimiņos esošām dalībvalstīm un ar kaimiņvalstīm) attiecībā uz gatavību avārijas situācijām un reaģēšanu uz tām.

6. darbība. Komisija sadarbībā ar dalībvalstīm atbalstīs centienus dažādot enerģijas avotus un veicināt drošības un drošuma standartus, lai palielinātu kodolinfrastruktūras izturētspēju.

4.1.2. Transporta un piegādes ķēžu drošība

Transports ir ļoti būtisks Savienības darbībai. Hibrīduzbrukumiem transporta infrastruktūrai (piemēram, lidostām, ceļu infrastruktūrai, ostām un dzelzceļam) var būt nopietnas sekas, kas izraisa traucējumus transporta un piegādes ķēdēs. Īstenojot tiesību aktus attiecībā uz aviācijas un jūras satiksmes drošību[21], Komisija veic regulāras pārbaudes[22], un Komisijas darba sauszemes transporta drošības jomā mērķis ir novērst jaunos hibrīddraudus. Šajā kontekstā tiek apspriests ES regulējums saskaņā ar pārskatīto Aviācijas drošības regulu[23], kas ir daļa no Aviācijas stratēģijas Eiropai[24]. Turklāt jūras drošības apdraudējumiem pievēršas Eiropas Savienības Jūras drošības stratēģija un tās rīcības plāns[25]. Šis rīcības plāns ļauj Eiropas Savienībai un tās dalībvalstīm visaptveroši risināt jūras drošības problēmas, tostarp apkarot hibrīddraudus, īstenojot starpnozaru sadarbību starp civilajiem un militārajiem dalībniekiem ar mērķi aizsargāt kuģniecībai svarīgo infrastruktūru, globālo piegādes ķēdi, jūras tirdzniecību, kā arī dabas un enerģijas

[19] Padomes Direktīva 2009/71/Euratom (2009. gada 25. jūnijs), ar ko izveido Kopienas kodoliekārtu kodoldrošības pamatstruktūru, kurā grozījumi izdarīti ar Padomes 2014. gada 8. jūlija Direktīvu 2014/87/Euratom.

[20] Padomes Direktīva 2013/59/Euratom (2013. gada 5. decembris), ar ko nosaka drošības pamatstandartus aizsardzībai pret jonizējošā starojuma radītajiem draudiem un atceļ Direktīvu 89/618/Euratom, Direktīvu 90/641/Euratom, Direktīvu 96/29/Euratom, Direktīvu 97/43/Euratom un Direktīvu 2003/122/Euratom.

[21] Eiropas Parlamenta un Padomes Regula (EK) Nr. 300/2008 (2008. gada 11. marts) par kopīgiem noteikumiem civilās aviācijas drošības jomā un ar ko atceļ Regulu (EK) Nr. 2320/2002; Komisijas Īstenošanas regula (ES) Nr. 2015/1998 (2015. gada 5. novembris), ar ko nosaka sīki izstrādātus pasākumus kopīgu pamatstandartu īstenošanai aviācijas drošības jomā; Eiropas Parlamenta un Padomes Direktīva 2005/65/EK (2005. gada 26. oktobris) par ostu drošības pastiprināšanu; Eiropas Parlamenta un Padomes Regula (EK) Nr. 725/2004 (2004. gada 31. maijs) par kuģu un ostas iekārtu drošības pastiprināšanu.

[22] Saskaņā ar ES tiesību aktiem Komisijai ir jāveic pārbaudes, lai nodrošinātu aviācijas un jūras satiksmes drošības prasību pareizu īstenošanu dalībvalstīs. Šādas pārbaudes cita starpā tiek veiktas attiecīgajā dalībvalsts iestādē, kā arī lidostās, ostās, gaisa pārvadātājos, kuģos un struktūrās, kas īsteno drošības pasākumus. Komisijas pārbaužu mērķis ir nodrošināt to, ka dalībvalstis pilnībā ievēro ES standartus.

[23] Komisijas Regula (ES) 2016/4 (2016. gada 5. janvāris), ar ko attiecībā uz vides aizsardzības pamatprasībām groza Eiropas Parlamenta un Padomes Regulu (EK) Nr. 216/2008; Eiropas Parlamenta un Padomes Regula (EK) Nr. 216/2008 (2008. gada 20. februāris) par kopīgiem noteikumiem civilās aviācijas jomā un par Eiropas Aviācijas drošības aģentūras izveidi.

[24] Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai „Aviācijas stratēģija Eiropai", COM(2015) 598 *final*, 7.12.2015.

[25] Padome 2014. gada decembrī pieņēma rīcības plānu Eiropas Savienības Jūras drošības stratēģijas īstenošanai; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf.

jūras resursus. Starptautiskās piegādes ķēdes drošībai pievēršas arī Eiropas Savienības muitas riska pārvaldības stratēģija un rīcības plāns[26].

<u>7. darbība.</u> Komisija uzraudzīs jaunos apdraudējumus visā transporta nozarē un vajadzības gadījumā atjauninās tiesību aktus. Īstenojot ES Jūras drošības stratēģiju un ES Muitas riska pārvaldības stratēģiju un rīcības plānu, Komisija un Augstā pārstāve (to attiecīgās kompetences ietvaros) sadarbībā ar dalībvalstīm izvērtēs veidus, kā reaģēt uz hibrīddraudiem, jo īpaši tiem, kuri skar kritisko infrastruktūru transporta jomā.

4.1.3. Kosmoss

Hibrīddraudu mērķis varētu būt kosmosa infrastruktūra, izraisot sekas daudzās nozarēs. Eiropas Savienība ir izstrādājusi kosmisko objektu novērošanas un uzraudzības atbalsta sistēmu[27], lai izveidotu dalībvalstīm piederošo resursu tīklu ar nolūku sniegt identificētiem lietotājiem (dalībvalstīm, ES iestādēm, kosmosa kuģu īpašniekiem un operatoriem un civilās aizsardzības iestādēm) kosmisko objektu novērošanas un uzraudzības pakalpojumus[28]. Saistībā ar gaidāmo Eiropas kosmosa stratēģiju Komisija izpētīs minētās sistēmas turpmāku izstrādi, lai pārraudzītu hibrīddraudus kosmosa infrastruktūrai.

Satelītsakari (*SatComs*) ir ļoti būtiski resursi krīžu pārvarēšanas, reaģēšanas uz katastrofām, policijas, robežuzraudzības un krasta apsardzes jomā. Tie ir pamats liela mēroga infrastruktūrai, piemēram, transporta, kosmosa vai tālvadības gaisa kuģu sistēmām. Atbilstīgi Eiropadomes aicinājumam sagatavot nākamās paaudzes valdības satelītsakarus (*GovSatCom*) Komisija sadarbībā ar Eiropas Aizsardzības aģentūru gaidāmās kosmosa stratēģijas un Eiropas aizsardzības rīcības plāna kontekstā izvērtē veidus, kā apvienot pieprasījumu.

Daudzos gadījumos kritiskā infrastruktūra ir atkarīga no informācijas par precīzu laiku, lai sinhronizētu savus tīklus (piemēram, enerģētikā un telekomunikāciju jomā) vai laika zīmoga darījumus (piemēram, finanšu tirgos). Atkarība no viena vienīga laika sinhronizācijas signāla, ko sniedz globālā navigācijas satelītu sistēma, nenodrošina hibrīddraudu apkarošanai vajadzīgo izturētspēju. Eiropas Globālā navigācijas satelītu sistēma *Galileo* piedāvātu otru uzticamu precīza laika avotu.

<u>8. darbība.</u> Gaidāmās kosmosa stratēģijas un Eiropas aizsardzības rīcības plāna kontekstā Komisija ierosinās palielināt kosmosa infrastruktūras izturētspēju pret hibrīddraudiem, jo īpaši, iespējams, paplašinot kosmisko objektu novērošanas un uzraudzības sistēmas darbības jomu, lai aptvertu hibrīddraudus, Eiropas līmenī

[26] Komisijas Paziņojums Eiropas Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai par ES muitas riska pārvaldības stratēģiju un rīcības plānu: risku novēršana, piegādes ķēdes drošības uzlabošana un tirdzniecības vienkāršošana, COM(2014) 527 *final*.
[27] Skatīt Eiropas Parlamenta un Padomes Lēmumu Nr. 541/2014.
[28] Piemēram, tādus kā brīdināšana sadursmju novēršanai orbītā, brīdināšana par kosmisko objektu sabrukumu vai sadursmēm un riskantu atgriešanos Zemes atmosfērā.

sagatavojot nākamās paaudzes GovSatCom un ieviešot kritiskajā infrastruktūrā, kas ir atkarīga no laika sinhronizācijas, Galileo sistēmu.

4.2. Aizsardzības spējas

Aizsardzības spējas ir jāpastiprina, lai uzlabotu ES izturētspēju hibrīddraudu gadījumā. Būtiski ir apzināt konkrētās galvenās spēju jomas, piemēram, novērošanas un izlūkošanas spējas. Eiropas Aizsardzības aģentūra varētu būt katalizators ar hibrīddraudiem saistītu militāro spēju attīstīšanai (piemēram, saīsinot aizsardzības spēju veidošanas ciklus, veicot ieguldījumus tehnoloģijā, sistēmās un prototipos, atverot aizsardzības nozares uzņēmumus inovatīvām komerciālām tehnoloģijām). Iespējamos pasākumus varētu izvērtēt gaidāmā Eiropas aizsardzības rīcības plāna ietvaros.

<u>9. darbība.</u> Augstā pārstāve, kuru vajadzības gadījumā atbalsta dalībvalstis, saziņā ar Komisiju ierosinās projektus par to, kā pielāgot aizsardzības spējas un attīstīt aizsardzības spējas ar ES mēroga nozīmīgumu, lai konkrēti apkarotu hibrīddraudus pret vienu vai vairākām dalībvalstīm.

4.3. Sabiedrības veselības un pārtikas nodrošinājuma aizsardzība

Iedzīvotāju veselība varētu tikt apdraudēta infekcijas slimību manipulācijas rezultātā vai, piesārņojot pārtiku, augsni, gaisu un dzeramo ūdeni ar ķīmiskiem, bioloģiskiem, radioloģiskiem un kodolmateriāliem (*CBRN*). Turklāt tīša dzīvnieku vai augu slimību izplatīšana varētu nopietni skart pārtikas nodrošinājumu Savienībā, un tai būtu liela ekonomiskā un sociālā ietekme uz ļoti svarīgām ES pārtikas ķēdes jomām. Lai reaģētu uz hibrīddraudiem gadījumos, kad tiek pielietotas šīs metodes, var izmantot esošās ES struktūras, kas darbojas veselības drošības, vides aizsardzības un pārtikas nekaitīguma jomā.

Atbilstīgi ES tiesību aktiem, kas attiecas uz pārrobežu veselības apdraudējumiem[29], ar esošajiem mehānismiem tiek koordinēta sagatavotība nopietniem pārrobežu veselības apdraudējumiem, ar agrīnās brīdināšanas un reaģēšanas sistēmas starpniecību savienojot dalībvalstis, ES aģentūras un zinātniskās komitejas[30]. Veselības drošības komiteja, kas koordinē dalībvalstu reakciju uz apdraudējumiem, var darboties kā kontaktpunkts jautājumos par vājajām vietām sabiedrības veselības jomā[31], lai iekļautu hibrīddraudu (jo īpaši bioterorisma) aspektus krīzes komunikācijas vadlīnijās un (krīžu simulācijai paredzētajos) spēju veidošanas pasākumos ar dalībvalstīm. Pārtikas nekaitīguma jomā kompetentās iestādes, izmantojot ātrās brīdināšanas sistēmu pārtikas un barības jomā (*RASFF*) un kopējo muitas apdraudējumu pārvaldības sistēmu (*CRMS*), apmainās ar riska

[29] Eiropas Parlamenta un Padomes Lēmums Nr. 1082/2013/ES (2013. gada 22. oktobris) par nopietniem pārrobežu veselības apdraudējumiem un ar ko atceļ Lēmumu Nr. 2119/98/EK, OV L 293, 5.11.2013., 1. lpp.

[30] Komisijas Lēmums C(2015) 5383 (2015. gada 7. augusts), ar ko izveido zinātniskas komitejas sabiedrības veselības, patērētāju drošības un vides jomā.

[31] Saskaņā ar Eiropas Parlamenta un Padomes 2013. gada 22. oktobra Lēmumu Nr. 1082/2013/ES par nopietniem pārrobežu veselības apdraudējumiem un ar ko atceļ Lēmumu Nr. 2119/98/EK, OV L 293, 1. lpp.

analīzes informāciju, lai uzraudzītu piesārņotas pārtikas izraisītos veselības apdraudējumus. Attiecībā uz dzīvnieku un augu veselību jāatzīmē, ka ES tiesiskā regulējuma[32] pārskatīšanas rezultātā esošais instrumentu kopums [33] tiks papildināts ar jauniem elementiem, lai panāktu labāku sagatavotību arī hibrīddraudu gadījumā.

<u>10. darbība.</u> Esošo sagatavotības un koordinācijas mehānismu, jo īpaši Veselības drošības komitejas, ietvaros Komisija sadarbībā ar dalībvalstīm uzlabos informētību par hibrīddraudiem un izturētspēju pret tiem.

4.4. Kiberdrošība

Eiropas Savienība gūst ievērojamu labumu no savas savstarpēji savienotās un digitalizētās sabiedrības. Kiberuzbrukumi varētu pārtraukt digitālos pakalpojumus visā ES, un šādus uzbrukumus varētu izmantot hibrīddraudu izteicēji. Komunikācijas un informācijas sistēmu izturētspējas uzlabošana Eiropā ir būtiska digitālā vienotā tirgus atbalstam. ES kiberdrošības stratēģijā un Eiropas Drošības programmā ir paredzēts vispārējais stratēģiskais satvars ES iniciatīvām kiberdrošības un kibernoziedzības jomā. Eiropas Savienība ir aktīvi darbojusies, lai veidotu informētību, izstrādātu sadarbības mehānismus un nodrošinātu reaģēšanas pasākumus atbilstoši kiberdrošības stratēģijā paredzētajiem rezultātiem. Konkrēti – ierosinātā Tīklu un informācijas drošības (TID) direktīva[34] pievēršas kiberdrošības riskiem, ar kuriem saskaras dažādi būtisku pakalpojumu sniedzēji enerģētikas, transporta, finanšu un veselības jomā. Šiem pakalpojumu sniedzējiem, kā arī svarīgāko digitālo pakalpojumu (piemēram, mākoņdatošanas) sniedzējiem būtu jāveic pienācīgi drošības pasākumi un jāziņo valsts iestādēm par nopietniem incidentiem, norādot uz visām hibrīda rakstura pazīmēm. Kad likumdevēji pieņems minēto direktīvu, tās efektīva transponēšana un īstenošana uzlabotu kiberdrošības spējas visās dalībvalstīs, hibrīddraudu apkarošanai veltītās informācijas un paraugprakses apmaiņas rezultātā pastiprinot to sadarbību kiberdrošības jomā. Konkrēti – saskaņā ar direktīvu ir jāizveido valstu līmenī strādājošo 28 datordrošības incidentu reaģēšanas vienību (*CSIRT*) un *CERT-EU*[35] tīkls, lai brīvprātīgi īstenotu operatīvo sadarbību.

Lai sekmētu publiskā un privātā sektora sadarbību un ES mēroga pieeju kiberdrošības jautājumos, Komisija izveidoja tīklu un informācijas drošības (TID) platformu, kas sniedz paraugprakses norādījumus par riska pārvaldību. Kaut arī dalībvalstis pašas

[32] Eiropas Parlamenta un Padomes Regula 2016/429 par pārnēsājamām dzīvnieku slimībām un ar ko groza un atceļ konkrētus aktus dzīvnieku veselības jomā („Dzīvnieku veselības tiesību akts"), OV L 84, 31.3.2016. Attiecībā uz Eiropas Parlamenta un Padomes regulu par aizsardzības pasākumiem pret augiem kaitīgajiem organismiem („Augu veselības tiesību akts") jāatzīmē, ka Eiropas Parlaments un Padome 2015. gada 16. decembrī panāca politisku vienošanos par regulas tekstu.

[33] Piemēram, ES vakcīnu bankas, moderna, elektroniska dzīvnieku slimību informācijas sistēma, paaugstinātas saistības ievērot atbilstošus pasākumus, kuras atteicas uz laboratorijām un citām vienībām, kas strādā ar patogēniem.

[34] Komisijas priekšlikums Eiropas Parlamenta un Padomes direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā, COM(2013) 48 *final*, 7.2.2013. ES Padome un Eiropas Parlaments ir panākuši politisku vienošanos par šo ierosināto direktīvu, un direktīva drīz tiks oficiāli pieņemta.

[35] ES iestāžu datorapdraudējumu reaģēšanas vienība (*CERT-EU*).

nosaka drošības prasības un kārtību ziņošanai par valsts mēroga incidentiem, Komisija mudina panākt augstu konverģences līmeni riska pārvaldības pieejās, balstoties jo īpaši uz Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*).

<u>11. darbība.</u> Komisija mudina dalībvalstis prioritārā kārtā izveidot un pilnībā izmantot 28* CSIRT *un* CERT-EU *tīklu, kā arī stratēģiskās sadarbības regulējumu. Komisijai sadarbībā ar dalībvalstīm būtu jānodrošina, ka ar hibrīddraudiem saistītās nozaru iniciatīvas (piemēram, aviācijas, enerģētikas, jūrlietu jomā) atbilst TID direktīvā paredzētajām starpnozaru spējām apkopot informāciju un zināšanas un ātri reaģēt.

4.4.1. Rūpniecība

Aizvien lielākā atkarība no mākoņdatošanas un „lielo datu" tehnoloģijas ir palielinājusi neaizsargātību pret hibrīddraudiem. Saskaņā ar digitālā vienotā tirgus stratēģiju ir paredzēts izveidot līgumisku publiskā un privātā sektora partnerību[36], kas koncentrēsies uz pētniecību un inovāciju un palīdzēs Savienībai saglabāt šajā jomā augsta līmeņa tehnoloģiskās spējas. Līgumiskā publiskā un privātā sektora partnerība radīs uzticību dažādu tirgus dalībnieku vidū un veidos sinerģiju starp pieprasījumu un piedāvājumu. Kaut arī līgumiskā publiskā un privātā sektora partnerība un papildinošie pasākumi galvenokārt koncentrēsies uz civiliem kiberdrošības produktiem un pakalpojumiem, tomēr šo iniciatīvu rezultātā tehnoloģiju lietotājiem vajadzētu būt labāk aizsargātiem arī pret hibrīddraudiem.

<u>12. darbība.</u> Komisija saziņā ar dalībvalstīm līgumiskas publiskā un privātā sektora partnerības ietvaros kiberdrošības jomā sadarbosies ar rūpniecību, lai izstrādātu un izmēģinātu tehnoloģijas labākai lietotāju un infrastruktūras aizsardzībai pret hibrīddraudiem kiberdrošības jomā.

4.4.2. Enerģētika

Arī viedo mājokļu un iekārtu rašanās un viedtīkla izveide, kā rezultātā pieaug enerģētikas sistēmas digitalizācija, palielina neaizsargātību pret kiberuzbrukumiem. Ar Eiropas enerģētiskās drošības stratēģiju[37] un Enerģētikas savienības stratēģiju[38] tiek atbalstīta visus riskus aptveroša pieeja, kurā ir integrēta izturētspēja pret hibrīddraudiem. Tematiskais tīkls kritiskās energoinfrastruktūras aizsardzībai sekmē sadarbību starp operatoriem enerģētikas nozarē (naftas, gāzes un elektroenerģijas jomā). Komisija ieviesa tīmekļa vidē izveidotu platformu, lai analizētu un apmainītos ar informāciju par draudiem un incidentiem[39]. Kopā ar ieinteresētajām personām[40] Komisija arī izstrādā visaptverošu, neaizsargātības samazināšanai paredzētu enerģētikas nozares stratēģiju par kiberdrošību viedtīkla darbībā. Kaut arī elektroenerģijas tirgi ir aizvien ciešāk integrēti, noteikumiem

[36] Jāuzsāk 2016. gada vidū.
[37] Komisijas paziņojums Eiropas Parlamentam un Padomei „Eiropas enerģētiskās drošības stratēģija", COM(2014) 330 *final*.
[38] Paziņojums „Pamatstratēģija spēcīgai Enerģētikas savienībai ar tālredzīgu klimata pārmaiņu politiku", COM(2015) 80 *final*.
[39] ES Centrs informācijas apmaiņai par incidentiem un draudiem (*ITIS*).
[40] Proti, Enerģētikas ekspertu platformu kiberdrošības jautājumos (*EECSP*).

un procedūrām par reaģēšanu krīzes situācijās vēl joprojām ir valsts mērogs. Mums jānodrošina, ka valdības savstarpēji sadarbojas attiecībā uz sagatavotību riskiem un to novēršanu un mazināšanu un ka visi nozīmīgie dalībnieki rīkojas uz vienota noteikumu kopuma pamata.

<u>13. darbība.</u> Komisija sniegs norādes viedtīkla resursu īpašniekiem, lai uzlabotu viņu iekārtu kiberdrošību. Elektroenerģijas tirgus modeļa iniciatīvas kontekstā Komisija apsvērs iespēju ierosināt „riska sagatavotības plānus" un procesuālus noteikumus informācijas apmaiņai un solidaritātes nodrošināšanai starp dalībvalstīm krīzes laikā, tostarp noteikumus par to, kā novērst kiberuzbrukumus un mazināt to sekas.

4.4.3. Stabilu finanšu sistēmu nodrošināšana

ES ekonomikas darbībai ir vajadzīga droša finanšu un maksājumu sistēma. Finanšu sistēmas un tās infrastruktūras aizsardzība pret kiberuzbrukumiem – neatkarīgi no uzbrucēja motīviem vai rakstura – ir ļoti būtiska. Lai tiktu galā ar hibrīddraudiem, kas vērsti pret ES finanšu pakalpojumiem, nozarei ir jāizprot draudi, tās aizsardzības mehānismiem ir jābūt pārbaudītiem un tai ir jābūt vajadzīgajai tehnoloģijai nozares aizsardzībai pret uzbrukumu. Tāpēc informācijas apmaiņa finanšu tirgus dalībnieku vidū, kā arī ar attiecīgajām iestādēm un galvenajiem pakalpojumu sniedzējiem vai klientiem ir svarīga, taču tai jābūt arī drošai un jāatbilst datu aizsardzības prasībām. Atbilstīgi darbam, kas tiek veikts starptautiskos forumos, tostarp G7 ietvaros šajā nozarē, Komisija centīsies apzināt faktorus, kas kavē pienācīgu informācijas apmaiņu par draudiem, un ierosināt atbilstošus risinājumus. Ir svarīgi nodrošināt, ka uzņēmējdarbības un attiecīgās infrastruktūras aizsardzības nolūkā protokoli tiek regulāri pārbaudīti un pilnveidoti, tostarp pastāvīgi modernizējot drošību uzlabojošās tehnoloģijas.

<u>14. darbība.</u> Komisija sadarbībā ar* ENISA[41]*, dalībvalstīm, attiecīgām starptautiskām, Eiropas un valsts līmeņa iestādēm un finanšu iestādēm sekmēs un atvieglos ar draudiem saistītās informācijas apmaiņas platformu un tīklu darbību un novērsīs šķēršļus šādas informācijas apmaiņai.

4.4.4. Transports

Modernas transporta (dzelzceļa transporta, autotransporta, gaisa transporta, jūras transporta) sistēmas ir atkarīgas no informācijas sistēmām, kas ir neaizsargātas pret kiberuzbrukumiem. Ņemot vērā pārrobežu dimensiju, Eiropas Savienībai jāpilda īpaša loma šajā jautājumā. Komisija sadarbībā ar dalībvalstīm turpinās analizēt kiberdraudus un riskus, kas saistīti ar nelikumīgu iejaukšanos transporta sistēmās. Komisija sadarbībā ar Eiropas Aviācijas drošības aģentūru (*EASA*)[42] izstrādā kiberdrošības rīcības plānu

[41] Eiropas Savienības Tīklu un informācijas drošības aģentūra.

[42] Pēc tam, kad Komisija 2015. gada decembrī iesniedza priekšlikumu, Eiropas Parlaments un Padome pašlaik apspriež jauno *EASA* regulu. Priekšlikums Eiropas Parlamenta un Padomes regulai par kopīgiem noteikumiem civilās aviācijas jomā, par Eiropas Savienības Aviācijas drošības aģentūras izveidi un par Eiropas Parlamenta un Padomes Regulas (EK) Nr. 216/2008 atcelšanu, COM(2015) 613 *final*, 2015/0277 (COD).

aviācijas jomā. Jūras drošības apdraudējumiem, kuru iemesls ir kiberdraudi, pievēršas arī Eiropas Savienības Jūras drošības stratēģija un tās rīcības plāns.

<u>15. darbība.</u> Komisija un Augstā pārstāve (to attiecīgās kompetences ietvaros) sadarbībā ar dalībvalstīm izvērtēs veidus, kā reaģēt uz hibrīddraudiem, jo īpaši tiem, kuri attiecas uz kiberuzbrukumiem transporta nozarei.

4.5. Hibrīddraudu finansēšanas apkarošana

Hibrīddraudu izteicējiem ir vajadzīgs finansējums to darbību veikšanai. Finansējumu var izmantot, lai atbalstītu teroristu grupas vai slēptākus destabilizācijas veidus, piemēram, sabiedriskās domas ietekmēšanas grupas un mazsvarīgas politiskās partijas. Kā izklāstīts Eiropas Drošības programmā[43] un jo īpaši tai pievienotajā rīcības plānā, Eiropas Savienība ir pastiprinājusi centienus cīņā pret noziedzību un teroristu finansēšanu. Šajā kontekstā jo īpaši ar Eiropas regulējumu nelikumīgi iegūtu līdzekļu legalizācijas novēršanai tiek pastiprināta cīņa pret teroristu finansēšanu un nelikumīgi iegūtu līdzekļu legalizāciju, atvieglots valsts finanšu izlūkošanas vienību (*FIU*) darbs nolūkā apzināt un izsekot aizdomīgus naudas pārskaitījumus un informācijas plūsmas, vienlaikus nodrošinot līdzekļu pārskaitījumu izsekojamību Eiropas Savienībā. Tāpēc minētais regulējums varētu arī palīdzēt apkarot hibrīddraudus. KĀDP instrumentu kontekstā varētu apsvērt iespēju izmantot mērķtiecīgus un efektīvus ierobežojošus pasākumus hibrīddraudu apkarošanai.

<u>16. darbība.</u> Rīcības plāna par teroristu finansēšanas apkarošanu īstenošanas gaitā Komisija ņems vērā arī hibrīddraudu apkarošanu.

4.6. Izturētspējas veidošana pret radikalizāciju un vardarbīgu ekstrēmismu

Kaut arī terora aktiem un vardarbīgam ekstrēmismam pašam par sevi nav hibrīda rakstura, tomēr hibrīddraudu izteicēji var mērķtiecīgi uzrunāt un vervēt neaizsargātus sabiedrības locekļus, radikalizējot viņus ar modernu komunikācijas kanālu starpniecību (tostarp internetā, izmantojot sociālos medijus un līdzīgi domājošo grupas) un ar propagandas palīdzību.

Lai vērstos pret ekstrēmistisku saturu internetā, Komisija digitālā vienotā tirgus stratēģijas kontekstā analizē vajadzību pēc iespējamiem jauniem pasākumiem, pienācīgi ņemot vērā šādu pasākumu ietekmi uz vārda un informācijas brīvības pamattiesībām. Šādi pasākumi varētu izpausties kā stingras procedūras nelikumīga satura izņemšanai, vienlaikus nepieļaujot likumīga satura ierobežošanu („paziņošana un rīcība"), kā arī tas, ka starpniekiem būtu lielāka atbildība un viņiem būtu jāveic pienācīga pārbaude attiecībā uz savu tīklu un sistēmu pārvaldību. Tas papildinātu pašreizējo brīvprātīgo pieeju, saskaņā ar kuru interneta un sociālo mediju uzņēmumi (jo īpaši ES interneta foruma

[43] Komisijas paziņojums Eiropas Parlamentam un Padomei par rīcības plānu par pastiprinātu cīņu pret teroristu finansēšanu, COM(2016) 50 *final*.

ietvaros) sadarbībā ar Eiropola ES vienību ziņošanai par interneta saturu ātri izņem teroristu propagandu.

Eiropas Drošības programmas kontekstā radikalizācija tiek apkarota, apmainoties ar pieredzi un izstrādājot paraugpraksi, tostarp īstenojot sadarbību trešās valstīs. Sīrijas Stratēģiskās komunikācijas konsultatīvā grupas mērķis ir pastiprināt alternatīvu vēstījumu izstrādi un izplatīšanu, lai apkarotu teroristu propagandu. Radikalizācijas izpratnes tīkls atbalsta dalībvalstis un speciālistus, kam jānodarbojas ar radikalizētām personām (tostarp ārvalstu kaujiniekiem teroristiem) vai cilvēkiem, kurus uzskata par neaizsargātiem pret radikalizāciju. Radikalizācijas izpratnes tīkls nodrošina apmācības pasākumus un konsultācijas un piedāvās atbalstu prioritārām trešām valstīm, ja tajās pastāv gatavība sadarboties. Turklāt Komisija veicina tiesu iestāžu sadarbību starp krimināltiesību jomas dalībniekiem (tostarp *Eurojust*), lai visās dalībvalstīs apkarotu terorismu un radikalizāciju, tostarp jautājumos par attieksmi pret ārvalstu kaujiniekiem teroristiem un personām, kuras atgriežas.

Papildus iepriekš minētajām pieejām, ko ES īsteno savā **ārējā darbībā**, tā sniedz ieguldījumu vardarbīga ekstrēmisma apkarošanā, tostarp ar ārēju iesaistīšanos un informēšanu, novēršanas darbībām (radikalizācijas un teroristu finansēšanas apkarošana), kā arī veicot pasākumus, kuru mērķis ir vērsties pret ekonomiskiem, politiskiem un sociāliem pamatfaktoriem, kas ļauj uzplaukt teroristu grupām.

<u>17. darbība.</u> Komisija īsteno Eiropas Drošības programmā izklāstītos pasākumus pret radikalizāciju un analizē nepieciešamību pastiprināt procedūras nelikumīga satura izņemšanai, vienlaikus aicinot starpniekus nodrošināt pienācīgu rūpību tīklu un sistēmu pārvaldībā.

4.7. Ciešāka sadarbība ar trešām valstīm

Kā uzsvērts Eiropas Drošības programmā, Eiropas Savienība ir pastiprināti pievērsusies spēju veidošanai ***partnervalstīs*** drošības sektorā, cita starpā balstoties uz saikni starp drošību un attīstību un izstrādājot pārskatītās Eiropas kaimiņattiecību politikas[44] drošības dimensiju. Šie pasākumi var arī sekmēt partnervalstu izturētspēju pret hibrīda rakstura darbībām.

Komisija plāno vēl vairāk pastiprināt operatīvas un stratēģiskas informācijas apmaiņu ar paplašināšanās procesā iesaistītajām valstīm, kā arī Austrumu partnerības ietvaros un dienvidu kaimiņreģionā, lai atbilstoši palīdzētu apkarot organizēto noziedzību, terorismu, neatbilstīgu migrāciju un vieglo ieroču nelikumīgu tirdzniecību. Terorisma apkarošanas jomā Eiropas Savienība pastiprina sadarbību ar trešām valstīm, izveidojot atjauninātus drošības dialogus un rīcības plānus.

[44] Kopīgs paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai „Eiropas kaimiņattiecību politikas pārskatīšana", 18.11.2015., JOIN(2015) 50 *final*.

ES ārējās finansēšanas instrumentu mērķis ir veidot trešās valstīs funkcionējošas un atbildīgas iestādes[45], kas ir priekšnoteikums efektīvai reaģēšanai uz drošības apdraudējumiem un izturētspējas uzlabošanai. Šajā saistībā būtiski instrumenti ir drošības sektora reforma un spēju veidošana drošības un attīstības atbalstam[46]. Stabilitātes un miera veicināšanas instrumenta[47] ietvaros Komisija ir izstrādājusi pasākumus, kuru mērķis ir stiprināt kibernoturību un uzlabot partneru spējas atklāt kiberuzbrukumus un kibernoziegumus un reaģēt uz tiem, kā rezultātā hibrīddraudus var apkarot trešās valstīs. Eiropas Savienība finansē partnervalstīs spēju veidošanas pasākumus, lai mazinātu drošības riskus, kas saistīti ar *CBRN* jautājumiem[48].

Visbeidzot, ņemot vērā visaptverošo pieeju krīžu pārvarēšanā, dalībvalstis varētu izmantot kopējās drošības un aizsardzības politikas (KDAP) instrumentus un misijas, pielietojot tos atsevišķi vai papildus citiem ES instrumentiem, lai palīdzētu partneriem palielināt to spējas. Varētu apsvērt šādas darbības: i) atbalsts stratēģiskajai komunikācijai, ii) konsultatīvs atbalsts svarīgākajām ministrijām, kas ir pakļautas hibrīddraudiem, iii) papildu atbalsts robežu pārvaldībai ārkārtas situācijā. Turklāt varētu izpētīt, vai ir iespējama papildu sinerģija starp KDAP instrumentiem un drošības, muitas un tieslietu jomas dalībniekiem, tostarp attiecīgajām ES aģentūrām[49], Interpolu un Eiropas Žandarmērijas spēkiem atbilstīgi to pilnvarām.

<u>18. darbība.</u> Augstā pārstāve sadarbībā ar Komisiju sāks pētījumu par hibrīda veida riskiem kaimiņreģionos.

Augstā pārstāve, Komisija un dalībvalstis izmantos to rīcībā esošos instrumentus, lai veidotu partneru spējas un stiprinātu to izturētspēju pret hibrīddraudiem. Varētu nosūtīt KDAP misijas (atsevišķi vai papildus citiem ES instrumentiem), lai palīdzētu partneriem palielināt to spējas.

5. KRĪZES NEPIEĻAUŠANA, REAĢĒŠANA UZ TO UN ATGŪŠANĀS NO TĀS

Kā izklāstīts 3.1. iedaļā, ierosinātās ES hibrīddraudu analīzes vienības mērķis ir analizēt attiecīgos rādītājus, lai nepieļautu hibrīddraudus, reaģētu uz tiem un informētu ES lēmumu pieņēmējus. Kaut arī neaizsargātību var mazināt ar valstu un ES līmenī veiktiem ilgtermiņa politikas pasākumiem, tomēr īstermiņā joprojām ir svarīgi stiprināt dalībvalstu

[45] Turpat; Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai „ES paplašināšanās stratēģija", 10.11.2015., COM(2015) 611 *final*. Komisijas Paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai „ES attīstības politikas ietekmes palielināšana: Pārmaiņu programma", 13.10.2011., COM(2011) 637 galīgā redakcija.

[46] Kopīgs Paziņojums „Spēju veidošana drošības un attīstības atbalstam – palīdzība partneriem krīžu novēršanai un pārvaldībai" (JOIN(2015) 17 *final*).

[47] Eiropas Parlamenta un Padomes Regula (ES) Nr. 230/2014 (2014. gada 11. marts), ar ko izveido stabilitātes un miera veicināšanas instrumentu, OV L 77, 15.3.2014., 1. lpp.

[48] Aptvertās jomas cita starpā ir šādas: robežu uzraudzība, krīžu pārvarēšana, pirmā reaģēšana, nelikumīga tirdzniecība, divējāda lietojuma preču eksporta kontrole, slimību uzraudzība un slimību kontrole, kodolkriminālistika, atgūšanās pēc incidentiem un augsta riska objektu aizsardzība. Ar trešām valstīm var dalīties paraugpraksē, kas gūta no ES *CBRN* rīcības plāna ietvaros izstrādātajiem instrumentiem, piemēram, Eiropas Kodoldrošības mācību centrs un ES līdzdalība starptautiskajā Robežuzraudzības jautājumu darba grupā.

[49] Eiropolu, *Frontex, CEPOL, Eurojust*.

un Savienības spēju ātri un koordinēti nepieļaut hibrīddraudus, reaģēt uz tiem un atgūties no tiem.

Ātra reaģēšana uz hibrīddraudu izraisītiem notikumiem ir ļoti būtiska. Šajā saistībā efektīvs mehānisms reaģēšanai uz hibrīddraudu aspektiem, kuru gadījumā ir vajadzīgi civilās aizsardzības reaģēšanas pasākumi, varētu izpausties tādējādi, ka Eiropas Ārkārtas reaģēšanas koordinācijas centrs[50] veicina valsts līmeņa civilās aizsardzības darbības un spējas. Tas varētu notikt sadarbībā ar citiem ES reaģēšanas mehānismiem un agrīnās brīdināšanas sistēmām, jo īpaši ar EĀDD Dežūrcentru saistībā ar ārējiem drošības aspektiem un Stratēģiskās analīzes un reaģēšanas centru iekšējās drošības jautājumos.

Solidaritātes klauzula (LESD 222. pants) ļauj Savienībai un dalībvalstīm darboties kopīgi, ja dalībvalsts ir teroristu uzbrukuma vai arī dabas vai cilvēku izraisītas katastrofas upuris. Savienības darbība nolūkā atbalstīt dalībvalsti tiek īstenota, piemērojot Padomes Lēmumu 2014/415/ES[51]. Koordinēšanas kārtībai Padomē būtu jābalstās uz ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem[52]. Saskaņā ar šo kārtību Komisija un Augstā pārstāve (to attiecīgās kompetences ietvaros) nosaka attiecīgos Savienības instrumentus un iesniedz Padomei priekšlikumus lēmumiem par izņēmuma pasākumiem.

LESD 222. pants attiecas arī uz situācijām, kad viena vai vairākas dalībvalstis sniedz tiešu palīdzību dalībvalstij, kas kļūst par teroristu uzbrukuma vai katastrofas upuri. Šajā gadījumā Padomes Lēmumu 2014/415/ES nepiemēro. Ņemot vērā ar hibrīda rakstura darbībām saistīto nenoteiktību, Komisijai un Augstajai pārstāvei (to attiecīgās kompetences ietvaros) vajadzētu izvērtēt, vai tad, ja kāda ES dalībvalsts ir pakļauta būtiskiem hibrīddraudiem, kā galējais līdzeklis, iespējams, būtu jāpiemēro solidaritātes klauzula.

Turpretī tādu vairākveidu nopietnu hibrīddraudu gadījumā, kas ir bruņota agresija pret kādu ES dalībvalsti, lai pienācīgi un laicīgi reaģētu, LESD 222. panta vietā varētu piemērot LES 42. panta 7. punktu. Liela mēroga un nopietnu hibrīddraudu gadījumā varētu būt nepieciešama arī pastiprināta sadarbība un koordinācija ar NATO.

Dalībvalstis tiek mudinātas savu bruņoto spēku sagatavošanā ņemt vērā arī iespējamos hibrīddraudus. Lai hibrīduzbrukuma gadījumā dalībvalstis būtu gatavas pieņemt lēmumus ātri un efektīvi, tām darba un politiskajā līmenī jārīko regulāras mācības ar nolūku pārbaudīt valsts un daudznacionāla mēroga lēmumu pieņemšanas spējas. Mērķis būtu dalībvalstu, Komisijas un Augstās pārstāves kopīgs operatīvs protokols, kurā izklāstītas efektīvas procedūras, kas jāievēro hibrīddraudu gadījumā – sākot ar pirmo identifikācijas posmu līdz pat pēdējam uzbrukuma posmam; minētajā protokolā arī būtu noteikti katras Savienības iestādes un dalībnieka uzdevumi šajā procesā.

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] Padomes Lēmums 2014/415/ES par kārtību, kādā Savienība īsteno solidaritātes klauzulu, OV L 192, 1.7.2014., 53. lpp.
[52] http://www.consilium.europa.eu/lv/documents-publications/publications/2014/eu-ipcr/.

Kā svarīgs KDAP iesaistes elements šāda pieeja varētu nodrošināt a) civilo un militāro apmācību, b) padomdevēju un konsultāciju misijas, kuru mērķis ir uzlabot apdraudētās valsts spējas drošības un aizsardzības jomā, c) ārkārtas situatīvo plānošanu ar nolūku apzināt hibrīddraudu pazīmes un stiprināt agrīnās brīdināšanas spējas, d) atbalstu robežkontroles pārvaldībai ārkārtas situācijā, e) atbalstu specializētās jomās, piemēram, *CBRN* riska mazināšanā un karadarbībā neiesaistīto personu evakuācijā.

19. darbība. ***Augstā pārstāve un Komisija sadarbībā ar dalībvalstīm izstrādās kopīgu operatīvu protokolu un rīkos regulāras mācības ar nolūku uzlabot stratēģisku lēmumu pieņemšanas spējas sarežģītu hibrīddraudu gadījumā, balstoties uz procedūrām krīžu pārvarēšanai un integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem.***

20. darbība. ***Komisija un Augstā pārstāve (to attiecīgās kompetences ietvaros) pārbaudīs, kādas ir iespējas plaša un nopietna hibrīduzbrukuma gadījumā piemērot LESD 222. pantu un LES 42. panta 7. punktu un kādas tam varētu būt praktiskās sekas***.

21. darbība. ***Augstā pārstāve sadarbībā ar dalībvalstīm nodrošinās militāro spēju integrāciju, izmantošanu un koordināciju hibrīddraudu apkarošanā kopējās drošības un aizsardzības politikas ietvaros.***

6. SADARBĪBAS PASTIPRINĀŠANA AR NATO

Hibrīddraudi ir izaicinājums ne tikai Eiropas Savienībai, bet arī citām lielām partnerorganizācijām, tostarp Apvienoto Nāciju Organizācijai (ANO), Eiropas Drošības un sadarbības organizācijai (EDSO) un jo īpaši – NATO. Efektīvai reaģēšanai ir nepieciešams dialogs un koordinācija starp organizācijām gan politiskajā, gan operatīvajā līmenī. Ciešākas mijiedarbības rezultātā starp ES un NATO abas organizācijas būtu labāk sagatavotas hibrīddraudiem un spētu efektīvi reaģēt uz tiem, savstarpēji papildinot un atbalstot viena otru un balstoties uz integrācijas principu, vienlaikus ievērojot katras organizācijas lēmumu pieņemšanas autonomiju un datu aizsardzības noteikumus.

Abām organizācijām ir kopīgas vērtības, un tās saskaras ar līdzīgiem izaicinājumiem. Gan ES dalībvalstis, gan NATO sabiedrotie sagaida no savām attiecīgajām organizācijām atbalstu, krīzes gadījumā ātri, izlēmīgi un saskaņoti rīkojoties, vai – ideālā variantā – krīzes nepieļaušanu. Ir apzinātas vairākas jomas ciešākai sadarbībai un koordinācijai starp ES un NATO, tostarp situācijas apzināšanās, stratēģiskā komunikācija, kiberdrošība, kā arī krīžu nepieļaušana un reaģēšana uz tām. Pašreizējais neformālais ES un NATO dialogs par hibrīddraudiem būtu jāpastiprina, lai saskaņotu abu organizāciju darbības šajā jomā.

Lai nodrošinātu savstarpēji papildinošu ES un NATO reakciju, ir svarīgi, ka abas organizācijas pirms krīzes un krīzes laikā vienādi apzinās situāciju. To varētu panākt, regulāri apmainoties ar analītisko informāciju un gūto pieredzi, kā arī nodrošinot tiešu saziņu starp ES hibrīddraudu analīzes vienību un atbilstošo NATO struktūru. Lai nodrošinātu ātru un efektīvu reaģēšanu, vienlīdz svarīgi ir panākt savstarpējo informētību par otras organizācijas attiecīgajām krīžu pārvarēšanas procedūrām. Izturētspēju varētu

stiprināt, nodrošinot papildināmību kritēriju noteikšanā attiecībā uz kritiskajām savas infrastruktūras daļām, kā arī cieši sadarbojoties stratēģiskās komunikācijas un kiberaizsardzības jomā. Pilnībā iekļaujošas kopīgas mācības, kas tiek rīkotas gan politiskajā, gan tehniskajā līmenī, palielinātu lēmumu pieņemšanas spēju efektivitāti abās organizācijās. Turpmāku risinājumu izpētīšana attiecībā uz apmācību pasākumiem palīdzētu panākt salīdzināmu zinātības līmeni problemātiskajās jomās.

<u>22. darbība.</u> Augstā pārstāve sadarbībā ar Komisiju hibrīddraudu apkarošanas nolūkā turpinās neoficiālu dialogu un pastiprinātu sadarbību un koordināciju ar NATO par situācijas apzināšanos, stratēģisko komunikāciju, kiberdrošību, kā arī „krīžu nepieļaušanu un reaģēšanu uz tām", ievērojot integrācijas un autonomijas principu katras organizācijas lēmumu pieņemšanas procesā.

7. SECINĀJUMI

Šajā kopīgajā paziņojumā ir izklāstītas darbības, kuru mērķis ir palīdzēt apkarot hibrīddraudus un stiprināt ES un tās dalībvalstu, kā arī partnervalstu izturētspēju. Tā kā galvenā uzmanība tiek veltīta **informētības uzlabošanai**, tiek ierosināts izveidot īpašus mehānismus informācijas apmaiņai ar dalībvalstīm un koordinēt ES spējas nodrošināt stratēģisko saziņu. Ir izklāstītas arī darbības **izturētspējas veidošanai** tādās jomās kā kiberdrošība, kritiskā infrastruktūra, finanšu sistēmas aizsardzība pret nelikumīgu izmantošanu un centieni cīņā pret vardarbīgu ekstrēmismu un radikalizāciju. Katrā no šīm jomām pirmais svarīgais solis būs to stratēģiju īstenošana, par kurām ir vienojušās ES un dalībvalstis, kā arī esošo tiesību aktu pilnīga īstenošana dalībvalstīs; vienlaikus ir ierosinātas dažas konkrētākas darbības, lai vēl vairāk pastiprinātu šos centienus.

Attiecībā uz **hibrīddraudu nepieļaušanu, reaģēšanu un tiem un atgūšanos no tiem** tiek ierosināts pārbaudīt, kādas ir iespējas plaša un nopietna hibrīduzbrukuma gadījumā piemērot LESD 222. pantā paredzēto solidaritātes klauzulu (kā norādīts attiecīgajā lēmumā) un LES 42. panta 7. punktu. Varētu uzlabot stratēģisku lēmumu pieņemšanas spējas, izstrādājot kopīgu operatīvu protokolu.

Visbeidzot, tiek ierosināts **pastiprināt sadarbību un koordināciju starp ES un NATO**, kopīgi vēršoties pret hibrīddraudiem.

Šā kopīgā regulējuma īstenošanā Augstā pārstāve un Komisija ir apņēmušās izmantot to rīcībā esošos attiecīgos ES instrumentus. Ir svarīgi, ka Eiropas Savienība kopā ar dalībvalstīm rīkojas, lai samazinātu riskus, kas ir saistīti ar iespējamiem hibrīddraudiem no valsts un nevalstisku dalībnieku puses.