EUROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA VANJSKE
POSLOVE I
SIGURNOSNU POLITIKU

Bruxelles, 19.7.2017.
JOIN(2017) 30 final

ZAJEDNIČKO IZVJEŠĆE EUROPSKOM PARLAMENTU I VIJEĆU

o provedbi Zajedničkog okvira za suzbijanje hibridnih prijetnji – odgovor Europske unije

1. UVOD

EU se suočava s jednim od najvećih sigurnosnih izazova u svojoj povijesti. Prijetnje sve više poprimaju nekonvencionalne oblike – neke su fizičke, poput novih oblika terorizma, a kod nekih se digitalni prostor koristi za složene kibernapade. Druge su suptilnije i cilj im je nasilno vršenje pritiska, među ostalim kampanjama dezinformiranja i medijskom manipulacijom. Tako se želi ugroziti temeljne europske vrijednosti, poput ljudskog dostojanstva, slobode i demokracije. Nedavnim koordiniranim kibernapadima u cijelom svijetu, čije je počinitelje teško identificirati, otkrivene su slabe točke naših društava i institucija.

Europska komisija i visoka predstavnica u travnju 2016. donijele su Zajedničku komunikaciju o suzbijanju hibridnih prijetnji[1] (zajednički okvir). U tom se okviru potvrđuje prekogranična i složena priroda hibridnih prijetnji te se predlaže pristup na svim razinama uprave radi jačanja ukupne otpornosti naših društava. Vijeće[2] je pozdravilo inicijativu i predložene mjere te je pozvalo Komisiju i visoku predstavnicu da u srpnju 2017. podnesu izvješće o napretku. Iako EU može pomagati državama članicama u jačanju njihove otpornosti na hibridne prijetnje, glavna je odgovornost i dalje na njima samima jer je suzbijanje hibridnih prijetnji povezano s nacionalnom sigurnošću i obranom.

Taj zajednički okvir za suzbijanje hibridnih prijetnji važan je dio integriranijeg pristupa EU-a sigurnosti i obrani. On pridonosi stvaranju Europe koja štiti, što je zatražio predsjednik Juncker u govoru o stanju Unije iz rujna 2016. Europska unija je 2016. postavila i temelje snažnije europske obrambene politike kao odgovor na činjenicu da građani očekuju bolju zaštitu. U globalnoj strategiji za vanjsku i sigurnosnu politiku EU-a[3] analizirana je potreba za integriranim pristupom radi povezivanja unutarnje otpornosti s vanjskim djelovanjem EU-a te je izražena potreba za sinergijama između obrambene politike i politika koje se odnose na unutarnje tržište, industriju, izvršavanje zakonodavstva te obavještajne službe. Nakon što je u studenome 2016. donesen europski akcijski plan obrane, Komisija je predstavila konkretne inicijative koje će pridonijeti jačanju kapaciteta EU-a za odgovor na hibridne prijetnje povećanjem otpornosti opskrbnih lanaca u sektoru obrane i jačanjem jedinstvenog tržišta za obranu. Konkretno, Komisija je 7. lipnja 2017. uspostavila Europski fond za obranu, za koji je predložena dodjela sredstava u iznosu od 600 milijuna EUR do 2020. te 1,5 milijardi EUR godišnje nakon 2020. U Komunikaciji o sigurnosnoj uniji[4] prepoznala je potrebu za suzbijanjem hibridnih prijetnji i važnost osiguravanja bolje usklađenosti unutarnjeg i vanjskog djelovanja u području sigurnosti.

Čelnici EU-a stavili su sigurnost i obranu u središte rasprave o budućnosti Europe[5]. To je navedeno u **Rimskoj deklaraciji** od 25. ožujka 2017., u kojoj je iznesena vizija sigurne i zaštićene Unije predane jačanju svoje zajedničke sigurnosti i obrane. Predsjednici Europskog vijeća i Europske komisije te glavni tajnik NATO-a potpisali su Zajedničku izjavu u Varšavi

[1] Zajednička komunikacija Europskom parlamentu i Vijeću *Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije*, JOIN(2016) 18 final.
[2] *Zaključci Vijeća o suzbijanju hibridnih prijetnji*, Objava za medije 196/16, 19. travnja 2016.
[3] Visoka predstavnica predstavila ju je Europskom vijeću 28. lipnja 2016.
[4] COM(2016) 230 final, 20.4.2016.
[5] Plan iz Bratislave Europskog vijeća od 16. rujna 2016. te Rimska deklaracija čelnika 27 država članica te Europskog vijeća, Europskog parlamenta i Europske komisije od 25. ožujka 2017.

8. srpnja 2016. kako bi se strateškom partnerstvu EU-a i NATO-a dao novi zamah i novi sadržaj. U zajedničkoj izjavi navedeno je sedam konkretnih područja, uključujući suzbijanje hibridnih prijetnji, u kojima bi trebalo pojačati suradnju tih dviju organizacija. Zajednički skup 42 prijedloga za provedbu kasnije su prihvatila vijeća EU-a i NATO-a, a prvo izvješće, iz kojeg je vidljiv znatan napredak, objavljeno je u lipnju 2017.[6]

U Komisijinu dokumentu za razmatranje o budućnosti europske obrane[7], predstavljenom u lipnju 2017., navode se različiti scenariji o tome kako riješiti problem sve većih sigurnosnih i obrambenih prijetnji s kojima se Europa suočava te kako poboljšati obrambene sposobnosti Europe do 2025. U sva se tri scenarija sigurnost i obrana smatraju sastavnim dijelovima europskog projekta kako bi se zaštitili i promicali naši interesi unutar i izvan naših granica. Europa mora postati pružatelj sigurnosti i postupno osigurati vlastitu sigurnost. Ni jedna država članica ne može se sama suočiti s budućim izazovima, pogotovo onima koji se odnose na suzbijanje hibridnih prijetnji. Stoga suradnja u području obrane i sigurnosti nije stvar izbora, već je nužna za ostvarenje Europe koja štiti.

Cilj je ovog izvješća analizirati napredak i daljnje korake u provedbi mjera u četiri područja predložena u zajedničkom okviru: stjecanju boljeg uvida u stanje, jačanju otpornosti, jačanju sposobnosti država članica i Unije za sprečavanje krize i odgovor na nju te za usklađeni oporavak, te poboljšanju suradnje s NATO-om radi osiguravanja komplementarnosti mjera. Ovo izvješće treba čitati u kombinaciji s mjesečnim izvješćima o napretku u postizanju učinkovite i istinske sigurnosne unije.

2. PREPOZNAVANJE HIBRIDNE PRIRODE PRIJETNJE

Hibridne aktivnosti postaju česta značajka europskog sigurnosnog okruženja. Te su aktivnosti sve intenzivnije te raste zabrinutost zbog ometanja izbora, kampanja dezinformiranja, zlonamjernih kiberaktivnosti te počinitelja hibridnih djela koji žele radikalizirati osjetljive članove društva kako bi postali njihovim zamjenskim akterima. Osjetljivost na hibridne prijetnje nije ograničena nacionalnim granicama. Za suzbijanje hibridnih prijetnji potreban je usklađen odgovor na razini EU-a i NATO-a. Razvoj događaja od travnja 2016. pokazuje da, iako se prijetnje često još uvijek procjenjuju izolirano, u Uniji se sve više priznaje i shvaća hibridna priroda nekih od zamijećenih aktivnosti te potreba za usklađenim djelovanjem. EU će i dalje nastojati poboljšati suradnju i uvid u stanje.

1. mjera: države članice, koje prema potrebi podupiru Komisija i visoka predstavnica, pozivaju se da provedu istraživanje o hibridnom riziku radi utvrđivanja ključnih slabih točaka, uključujući specifične pokazatelje hibridnih prijetnji, koje mogu utjecati na nacionalne i paneuropske strukture i mreže.

Vijeće je osnovalo Skupinu prijatelja predsjedništva, u kojoj su okupljeni stručnjaci iz država članica kako bi sastavili generički upitnik koji bi im omogućio da bolje utvrde ključne pokazatelje hibridnih prijetnji, uklope ih u mehanizme ranog upozoravanja i procjene postojećih rizika te ih prema potrebi prosljeđuju. Opis poslova je dogovoren i Skupina je već počela s radom. Spomenuti generički upitnik trebao bi biti dovršen do kraja 2017., nakon čega

[6] http://www.consilium.europa.eu/hr/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation/
[7] Dokument za razmatranje o budućnosti europske obrane, 7.6.2017., https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_hr.pdf

bi se trebalo početi s konkretnim istraživanjima. Zaštita od hibridnih prijetnji trebala bi dovesti do uzajamnog jačanja. Stoga se države članice potiču da što prije provedu ta istraživanja jer će ona poslužiti kao izvor vrijednih informacija o razini osjetljivosti i pripravnosti u cijeloj Europi.

a. PODIZANJE SVIJESTI

Razmjena obavještajnih analiza i procjena ključni je alat za smanjenje nesigurnosti i poboljšanje uvida u stanje. Tijekom prošle godine ostvaren je znatan napredak. Uspostavljena je jedinica EU-a za otkrivanje hibridnih prijetnji i sada je u potpunosti operativna, osnovana je radna skupina East Stratcom, a u Finskoj je otvoren Europski centar za suzbijanje hibridnih prijetnji. Velik dio rada usmjeren je na analizu alata i poluga koji se koriste u dezinformiranju ili propagandi, pri čemu je ostvarena uspješna suradnja radne skupine East StratCom, jedinice za otkrivanje hibridnih prijetnji i NATO-a. To je dobra osnova za daljnju izgradnju bolje prihvaćene kulture analize i procjene prijetnji našoj unutarnjoj i vanjskoj sigurnosti s obzirom na hibridne aspekte.

Jedinica za otkrivanje hibridnih prijetnji

2. mjera: osnivanje jedinice EU-a za otkrivanje hibridnih prijetnji (Hybrid Fusion Cell) unutar postojeće strukture Obavještajnog i situacijskog centra EU-a, koja može primati i analizirati povjerljive i javno dostupne informacije o hibridnim prijetnjama. Države članice pozivaju se da uspostave nacionalne kontaktne točke za prijavu hibridnih prijetnji kako bi se osigurala suradnja i sigurna komunikacija s jedinicom EU-a za otkrivanje hibridnih prijetnji.

Jedinica EU-a za otkrivanje hibridnih prijetnji uspostavljena je u okviru Obavještajnog i situacijskog centra EU-a radi primanja i analize povjerljivih i dostupnih informacija o hibridnim prijetnjama dobivenih od različitih dionika. Analize se zatim dijele unutar EU-a i među državama članicama te se na temelju njih donose odluke u EU-u, uključujući procjene prijetnji sigurnosti koje se provode na razini EU-a. Obavještajna uprava vojnog stožera EU-a vojnom analizom pridonosi radu jedinice EU-a za otkrivanje hibridnih prijetnji. Dosad je izrađeno više od 50 procjena i kratkih izvješća o temama hibridnih prijetnji. Jedinica od siječnja 2017. izdaje bilten „Hybrid Bulletin", u kojem analizira trenutačne prijetnje i pitanja u području hibridnih prijetnji te ga izravno dijeli s institucijama i tijelima EU-a i nacionalnim kontaktnim točkama[8]. Pun operativni kapacitet Jedinica je postigla je u svibnju 2017., kako je i planirano. Naposljetku, u tijeku je povezivanje osoblja Jedinice s osobljem NATO-ovog odjela za analizu hibridnih prijetnji (*Hybrid Analysis Branch*), koji se trenutačno uspostavlja, pri čemu se razmjenjuju iskustva stečena u uspostavi jedinice za otkrivanje hibridnih prijetnji i informacije (uz potpuno poštovanje pravila EU-a o razmjeni povjerljivih informacija). Jedinica EU-a za otkrivanje hibridnih prijetnji trenutačno utvrđuje daljnje inicijative za jačanje buduće suradnje i imat će ključnu ulogu u paralelnim vježbama NATO-a planiranima za jesen 2017., tijekom kojih će se ispitivati njezina sposobnost reagiranja, a bit će uključeno i stečeno iskustvo.

[8] Dosad je 21 država članica odredila nacionalne kontaktne točke. To su osobe koje rade u glavnim gradovima država članica i obavljaju zadatke povezane s politikom/otpornošću.

Strateška komunikacija

3. mjera: visoka predstavnica će s državama članicama istražiti načine ažuriranja i koordinacije kapaciteta za proaktivnu stratešku komunikaciju te optimalne upotrebe praćenja medija i angažiranja jezičnih stručnjaka.

Posljednjih je mjeseci među brojnim načinima za potkopavanje protivnika bilo sve više kampanja dezinformiranja i sustavnog širenja lažnih vijesti na društvenim medijima. Kad se društveni mediji koriste kao preferirana platforma, širenjem informacija koje se čine pouzdanima i legitimnima može se promijeniti mišljenje javnosti u korist određenih osoba, organizacija ili vlada. Dalekosežniji je cilj tih hibridnih taktika stvoriti zbrku u našim društvima te diskreditirati demokratske vlade i naše strukture, institucije i izbore. Lažne vijesti često se šire internetskim platformama (vidjeti i 17. mjeru). Komisija i visoka predstavnica pozdravljaju nedavne korake koje su internetske platforme i informativni mediji poduzeli za suzbijanje dezinformacija. Komisija će i dalje poticati takve dobrovoljne mjere.

Visoka predstavnica uspostavila je radnu skupinu East Stratcom, koja predviđa slučajeve i kampanje dezinformiranja te reagira na njih. Tako se znatno poboljšava komunikacija o politikama Unije u istočnom susjedstvu i istovremeno se jača medijsko okruženje u tim zemljama. Radna je skupina u posljednje dvije godine otkrila više od 3 000 pojedinačnih slučajeva dezinformiranja na 18 jezika. Predstojećim pokretanjem novih internetskih stranica „*#EUvsdisinformation*" (*EU protiv dezinformacija*) s internetskim pretraživačem korisnicima će se znatno olakšati pristup. Međutim, istraživanja i analize pokazali su da postoji mnogo veći broj kanala i poruka kojima se svakodnevno šire dezinformacije. U projektu EU-STRAT, koji se financira u okviru programa Obzor 2020., analiziraju se politike i mediji u zemljama istočnog partnerstva.

Visoka predstavnica poziva države članice da podrže rad radnih skupina StratCom kako bi borba protiv sve brojnijih hibridnih prijetnji bila djelotvornija. To će Južnoj radnoj skupini pomoći da poboljša komunikaciju i kontakte s arapskim svijetom, među ostalim i na arapskom jeziku, da razbije mitove i da proširi točne informacije o Europskoj uniji i njezinim politikama. Interakcija s lokalnim novinarima pomoći će da se vijesti prilagode tom kulturnom krugu. Cilj obiju radnih skupina, koje podržava jedinica EU-a za otkrivanje hibridnih prijetnji, jest podržati i nadopuniti rad država članica u tom području. Osim toga, Komisija sufinancira Europsku mrežu za strateško komuniciranje – mrežu za suradnju 26 država članica putem koje one razmjenjuju analize, dobru praksu i ideje o upotrebi strateške komunikacije za borbu protiv nasilnog ekstremizma, uključujući u pogledu dezinformacija.

Centar izvrsnosti za suzbijanje hibridnih prijetnji

4. mjera: države članice pozivaju se da razmotre uspostavu centra izvrsnosti za suzbijanje hibridnih prijetnji.

Kao odgovor na poziv za uspostavu centra izvrsnosti Finska je u travnju 2017. uspostavila Europski centar za suzbijanje hibridnih prijetnji. Deset država članica EU-a[9], Norveška i SAD njegovi su članovi, dok su i Europska unija i NATO pozvani da podrže upravni odbor[10]. Misija je Centra poticati strateški dijalog te provoditi istraživanja i analize u suradnji s

[9] Finska, Francuska, Njemačka, Latvija, Litva, Poljska, Švedska, Ujedinjena Kraljevina, Estonija, Španjolska.
[10] Centru se mogu pridružiti i ostale države članice EU-a i saveznici NATO-a.

interesnim zajednicama kako bi se povećala otpornost i sposobnost reagiranja radi suzbijanja hibridnih prijetnji. Očekuje se da će se u Centru ubuduće održavati i vježbe povezane s hibridnim prijetnjama. Centar je već uspostavio bliski kontakt s jedinicom EU-a za otkrivanje hibridnih prijetnji te bi se rad tih dviju organizacija trebao uzajamno nadopunjavati. EU trenutačno procjenjuje načine na koje bi mogao konkretno poduprijeti Centar.

b. JAČANJE OTPORNOSTI

U zajedničkom se okviru otpornost (npr. u području prometa, komunikacija, energetike, financija ili regionalne sigurnosne infrastrukture) smješta u središte djelovanja EU-a radi pružanja otpora propagandnim i informativnim kampanjama, pokušajima ugrožavanja poduzeća, društava i gospodarskih tokova te napadima na infrastrukturu informacijske tehnologije i kibernetičku infrastrukturu. Jačanje otpornosti smatra se preventivnom i odvraćajućom mjerom kojom se stabiliziraju društva i izbjegava eskalacija kriza unutar EU-a i izvan njega. Dodana vrijednost EU-a leži u pružanju pomoći državama članicama i partnerima pri jačanju njihove otpornosti na temelju raznih postojećih instrumenata i programa. Postignut je znatan napredak mjera za jačanje otpornosti u područjima poput kibersigurnosti, ključne infrastrukture, zaštite financijskog sustava od nezakonitog korištenja te suzbijanja nasilnog ekstremizma i radikalizacije.

Zaštita ključne infrastrukture

5. mjera: Komisija će u suradnji s državama članicama i dionicima utvrditi zajedničke alate, uključujući pokazatelje, s ciljem poboljšanja zaštite i otpornosti ključne infrastrukture na hibridne prijetnje u relevantnim sektorima.

Komisija je u kontekstu Europskog programa za zaštitu ključne infrastrukture (EPCIP) poduzela korake za utvrđivanje zajedničkih alata, uključujući pokazatelje slabih točaka, kako bi se povećala otpornost ključne infrastrukture na hibridne prijetnje u relevantnim sektorima. Komisija je u svibnju 2017. organizirala radionicu o hibridnim prijetnjama ključnoj infrastrukturi. Sudjelovale su gotovo sve države članice, operateri ključne infrastrukture, jedinica EU-a za otkrivanje hibridnih prijetnji te NATO kao promatrač. Dogovoreni su zajednički plan i koraci za budući rad na temelju upitnika poslanog nacionalnim tijelima u državama članicama. Komisija će se najesen dodatno savjetovati s dionicima kako bi do kraja 2017. postigli dogovor o pokazateljima.

Europska obrambena agencija radi na utvrđivanju zajedničkih nedostataka u pogledu sposobnosti i istraživanja koji proizlaze iz povezanosti energetskih infrastruktura i obrambenih kapaciteta. Europska će obrambena agencija u jesen 2017. izraditi idejni dokument te osmisliti pilot-mjere za sveobuhvatne metodologije.

Povećanje sigurnosti opskrbe energijom u EU-u

6. mjera: Komisija će u suradnji s državama članicama podupirati nastojanja da se diversificiraju izvori energije te promicati standarde sigurnosti i zaštite kako bi se povećala otpornost nuklearne infrastrukture.

Komisija je u prosincu 2016. dala konkretne prijedloge u paketu za sigurnost opskrbe, a Vijeće i Europski parlament postigli su u travnju 2017. dogovor o novoj uredbi o sigurnosti opskrbe plinom, čiji je cilj sprečavanje kriza u opskrbi plinom. Novim će se pravilima osigurati zajednički pristup mjerama za sigurnost opskrbe među državama članicama

koordiniran na regionalnoj razini. Tako će se EU moći bolje pripremiti na nestašice plina i lakše ih prevladati u slučaju krize ili hibridnog napada. Pritom će se prvi put primijeniti i načelo solidarnosti: države članice moći će u slučaju ozbiljne krize ili napada pomoći susjedima kako europska kućanstva i poduzeća ne bi bila pogođena nestašicama.

EU je postigao napredak i u razvoju ključnih projekata za diversifikaciju ruta i izvora opskrbe energijom u skladu s Okvirnom strategijom za energetsku uniju i Europskom strategijom energetske sigurnosti. Na južnom plinskom koridoru, primjerice, u tijeku su konkretni građevinski radovi na svim glavnim projektima povezanima s plinovodom: proširenje južnokavkaskog plinovoda, transanatolijskog i transjadranskog plinovoda, uzvodnog plinovoda Shah Deniz II te proširenje južnog plinskog koridora prema središnjoj Aziji, posebno Turkmenistanu. Uvoz ukapljenog prirodnog plina (UPP) u Europu u porastu je i dolazi iz novih izvora, primjerice SAD-a. Primjer terminala u Litvi prikazuje kako projekti diversifikacije mogu smanjiti ovisnost o jednom dobavljaču. Sve više takvih nastojanja u području energije i bolje iskorištavanje domaćih izvora energije, pogotovo obnovljivih, također doprinose diversifikaciji ruta i izvora energije.

U području nuklearne sigurnosti Komisija aktivno podržava – posebno putem radionica s nacionalnim tijelima i regulatorima – dosljednu i djelotvornu provedbu dviju direktiva o nuklearnoj sigurnosti i osnovnim sigurnosnim standardima, koje države članice moraju prenijeti u nacionalno zakonodavstvo do kraja 2017., odnosno 2018. Osim toga, program Euratoma za istraživanja i osposobljavanje doprinosi povećanju nuklearne sigurnosti.

Sigurnost prometa i opskrbnog lanca

7. mjera: Komisija će pratiti nove prijetnje u cijelom prometnom sektoru i prema potrebi ažurirati zakonodavstvo. U provedbi Strategije EU-a za sigurnosnu zaštitu u pomorstvu i Strategije EU-a za upravljanje rizicima u carinskim pitanjima te njihovih akcijskih planova, Komisija i visoka predstavnica će (u okviru svojih nadležnosti) u suradnji s državama članicama ispitati kako reagirati u slučaju hibridnih prijetnji, posebno onih koje se odnose na ključnu prometnu infrastrukturu.

U skladu s Komunikacijom o sigurnosnoj uniji Komisija olakšava procjenjivanje prijetnji sigurnosti na razini EU-a s državama članicama, Obavještajnim i situacijskim centrom EU-a i relevantnim agencijama kako bi utvrdila prijetnje sigurnosti prometa i podržala razvoj djelotvornih i proporcionalnih mjera ublažavanja. Rušenje zrakoplova Malaysia Airlinesa na letu MH17 iznad istočne Ukrajine 2014. upozorilo je na rizičnost preleta iznad područja sukoba. U skladu s preporukama Europske radne skupine na visokoj razini za područja sukoba[11], Komisija je uz potporu nacionalnih stručnjaka za sigurnost i zračni promet te ESVD-a razvila metodologiju za „zajedničku procjenu rizika na razini EU-a”, koja omogućuje razmjenu povjerljivih informacija i utvrđivanje zajedničke slike rizika. Europska agencija za sigurnost zračnog prometa (EASA) izdala je u ožujku 2017. prvi informativni bilten o područjima sukoba (*Conflict Zones Information Bulletin*)[12] na temelju rezultata te zajedničke procjene rizika na razini EU-a. Komisija razmatra proširenje aktivnosti procjene rizika koje se provode u području zaštite zračnog prometa na druge vrste prometa (npr. željeznički, pomorski) te će 2018. iznijeti prijedloge za to. Komisija, ESVD i države članice

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

[12] https://ad.easa.europa.eu/czib-docs/page-1

započele su u lipnju 2017. s procjenom rizika u području sigurnosti željeznica kako bi se utvrdili nedostaci i moguće mjere za ublažavanje rizika.

Znatni pomaci u području zaštite zračnog prometa i upravljanja zračnim prometom ostvareni su i u 7. okvirnom programu te u istraživačkim projektima u području sigurnosti u okviru programa Obzor 2020. U području civilnog zrakoplovstva Komisija s Europskom agencijom za sigurnost zračnog prometa i dionicima razvija dvije nove inicijative za jačanje kibersigurnosti, pri čemu rješava i pitanje hibridnih prijetnji: osnivanje Tima za hitne računalne intervencije u zračnom prometu te uspostava radne skupine za kibersigurnost u Zajedničkom poduzeću za istraživanje o upravljanju zračnim prometom jedinstvenog europskog neba (SESAR), nadležne za upravljanje zračnim prometom jedinstvenog europskog neba. Europska obrambena agencija Zajedničkom poduzeću SESAR i Europskoj agenciji za sigurnost zračnog prometa pruža vojne informacije o kibersigurnosti u zračnom prometu putem „Europske platforme za stratešku koordinaciju u području kibersigurnosti", koja će na zahtjev država članica i industrije pružati pomoć u koordinaciji na razini EU-a za sve aktivnosti u zračnom prometu. U skladu s Planom o kibernetičkoj sigurnosti u zračnom prometu, Europska agencija za sigurnost zračnog prometa analizirala je 2016. nedostatke u postojećim pravilima, a posebno u pogledu definicije i uspostave Europskog centra za kibernetičku sigurnost u zrakoplovstvu. Taj je centar sada operativan i surađuje s Timom za hitne računalne intervencije EU-a (CERT-EU) (Memorandum o razumijevanju potpisan je u veljači 2017.) radi izrade analiza prijetnji u zračnom prometu te s agencijom Eurocontrol (donesen je plan suradnje), a razvijene su i internetske stranice za distribuciju javno dostupnih analiza. Do jeseni 2017. uspostavit će se program standardizacije i sigurna razmjena informacija.

<u>Upravljanje rizicima u carinskim pitanjima</u>

U području carina Komisija prije svega nastoji znatno poboljšati sustav analize ranih informacija o teretu i carinski sustav za upravljanje rizikom. To obuhvaća cijeli raspon rizika u području carina, uključujući prijetnje sigurnosti i cjelovitosti međunarodnih opskrbnih lanaca te relevantnim ključnim infrastrukturama (npr. izravne prijetnje lučkim objektima, zračnim lukama ili kopnenim granicama koje predstavlja uvoz). Unapređenjem sustava nastoji se osigurati da carinske službe u EU-u od trgovaca dobiju sve potrebne informacije o kretanju robe, da budu u mogućnosti učinkovitije razmjenjivati te informacije među državama članicama, da primjenjuju zajednička pravila i pravila pojedinačnih država članica u pogledu rizika te da budu sposobni učinkovitije prepoznati rizične pošiljke na temelju intenzivnije suradnje s drugim tijelima, a posebno drugim agencijama za izvršavanje zakonodavstva i sigurnosnim agencijama. Informatički razvoj potreban da bi Komisija mogla unaprijediti te sustave trenutačno je u početnoj fazi te će relevantna ulaganja na središnjoj razini biti izvršena u narednim mjesecima.

<u>Svemir</u>

<u>8. mjera</u>: u kontekstu svemirske strategije i europskog akcijskog plana obrane Komisija će predložiti povećanje otpornosti svemirske infrastrukture na hibridne prijetnje, konkretno kroz mogućnost proširivanja nadzora i praćenja u svemiru kako bi se obuhvatile hibridne prijetnje, pripreme za sljedeću generaciju GovSatCom-a na europskoj razini te uvođenje programa Galileo u područje ključnih infrastruktura koje su ovisne o sinkronizaciji vremena.

Komisija će tijekom pripreme regulatornog okvira za vladine satelitske komunikacije (GovSatCom) te za nadzor i praćenje u svemiru 2018. u svoje procjene uključiti aspekte

otpornosti na hibridne prijetnje. U skladu sa svemirskom strategijom Komisija će tijekom pripreme razvoja programa Galileo i Copernicus procijeniti koliko bi te usluge mogle pomoći u smanjivanju osjetljivosti ključnih infrastruktura. Evaluacijsko izvješće trebalo bi biti spremno u jesen 2017., a prijedlog o novoj generaciji programa Copernicus i Galileo 2018. Europska obrambena agencija radi na projektima zajedničkog razvoja sposobnosti u području svemirskih komunikacija, vojnog pozicioniranja, navigacije, određivanja vremena i promatranja Zemlje. Svi će projekti biti usmjereni na zahtjeve u pogledu otpornosti s obzirom na postojeće i nove hibridne prijetnje.

Obrambene sposobnosti

9. mjera: visoka predstavnica, koju prema potrebi podupiru države članice, u suradnji s Komisijom predložit će projekte za prilagođavanje obrambenih sposobnosti i razvoj važan za EU, posebno kako bi se suzbile hibridne prijetnje jednoj državi članici ili više njih.

Europska obrambena agencija u suradnji s Komisijom, ESVD-om i stručnjacima iz država članica provela je 2016. i 2017. tri simulacijske vježbe sa scenarijima hibridnih prijetnji. Njihovi zaključci bit će uključeni u preispitivanje Plana za razvoj sposobnosti te će posljedični razvoj ključnih sposobnosti potreban za suzbijanje hibridnih prijetnji biti uključen u nove prioritete EU-a u pogledu razvoja sposobnosti. Tijekom rada na preispitivanju kataloga zahtjeva iz 2005. uzet će se u obzir dimenzija hibridnih prijetnji. Europska obrambena agencija završila je u travnju 2017. izvješće o analizi vojnih implikacija koje proizlaze iz hibridnih napada usmjerenih na ključnu lučku infrastrukturu, o čemu će biti riječi na radionici s pomorskim stručnjacima u listopadu 2017. Još jedna posebna analiza uloge vojske u kontekstu borbe protiv malih bespilotnih letjelica održat će se 2018. Nadalje, prioriteti u pogledu sposobnosti za povećanje otpornosti na hibridne prijetnje koje utvrde države članice mogli bi od 2019. ispunjavati uvjete i za dodjelu potpore iz Europskog fonda za obranu. Komisija poziva države članice da dostave prijedloge projekata u području sposobnosti za jačanje otpornosti EU-a na hibridne prijetnje, a suzakonodavce da osiguraju brzo donošenje.

10. mjera: Komisija će u suradnji s državama članicama podići svijest i povećati otpornost na hibridne prijetnje unutar postojećih mehanizama pripravnosti i koordinacije, posebno Odbora za zdravstvenu sigurnost.

S ciljem jačanja pripravnosti i otpornosti na hibridne prijetnje, uključujući izgradnju kapaciteta unutar zdravstvenih i prehrambenih sustava, Komisija podupire države članice osposobljavanjem, simulacijskim vježbama, olakšavanjem razmjene iskustava i smjernica te financiranjem zajedničkih mjera. To se odvija posebice kao dio okvira EU-a za zdravstvenu sigurnost u području ozbiljnih prekograničnih prijetnji zdravlju te u okviru programa javnog zdravlja za provedbu međunarodnih zdravstvenih propisa, koji je zakonodavna osnova koja obvezuje 196 zemalja, uključujući države članice, i cilj mu je spriječiti akutne i prekogranične opasnosti za javno zdravlje u cijelom svijetu i reagirati na njih. Kako bi ispitale međusektorsku pripravnost i sposobnost reagiranja u zdravstvenom sektoru, službe Komisije provest će u jesen 2017. vježbu o složenim i višedimenzionalnim hibridnim prijetnjama. Komisija i države članice pripremaju zajedničku akciju u području cijepljenja, uključujući predviđanje ponude i potražnje za cjepivima te istraživanja o inovativnim postupcima proizvodnje cjepiva radi jačanja opskrbe cjepivima i poboljšanja zdravstvene sigurnosti na razini EU-a (2018.–2020.). Komisija surađuje i s Europskom agencijom za sigurnost hrane i Europskim centrom za sprečavanje i kontrolu bolesti kako bi se prilagodili naprednim znanstvenim tehnikama istraživanja radi preciznijeg prepoznavanja i utvrđivanja izvora prijetnji zdravlju te, na temelju toga, brzog svladavanja incidenata koji ugrožavaju sigurnost

hrane. Komisija je uspostavila mrežu ulagača u istraživanje – Globalnu istraživačku suradnju za pripravnost na zarazne bolesti – kako bi se osigurao usklađen istraživački odgovor u roku od 48 sati od svakog izbijanja značajnije bolesti.

<u>11. mjera</u>: Komisija prije svega potiče države članice da uspostave i u potpunosti iskoriste mrežu 28 CSIRT-ova i CERT-EU (tim za hitne računalne intervencije u EU-u) te okvir za stratešku suradnju. Komisija bi u suradnji s državama članicama trebala osigurati da sektorske inicijative koje su usmjerene na kiberprijetnje (npr. u području zračnog prometa, energetike, pomorstva) budu u skladu s međusektorskim sposobnostima obuhvaćenima Direktivom o sigurnosti mrežnih i informacijskih sustava radi prikupljanja podataka, stručnog znanja i brzih odgovora.

Nakon nedavnih globalnih kibernapada uz upotrebu ucjenjivačkog (*ransomware*) i zlonamjernog (*malware*) softvera s ciljem onesposobljavanja tisuća računalnih sustava ponovno se u prvom planu našla hitna potreba za povećanjem kiberotpornosti i sigurnosnih mjera u EU-u. Kao što je najavljeno u preispitivanju na sredini provedbenog razdoblja jedinstvenog digitalnog tržišta, Komisija i visoka predstavnica sada preispituju strategiju za kibersigurnost EU-a iz 2013., posebno donošenjem paketa predviđenog za rujan 2017. Cilj će biti djelotvorniji međusektorski odgovor na te prijetnje, čime će se povećati povjerenje u digitalno društvo i gospodarstvo. Preispitat će se i mandat agencije EU-a za mrežnu i informacijsku sigurnost (ENISA) kako bi se definirala njezina uloga u promijenjenom ekosustavu kibersigurnosti. Europsko vijeće[13] pozdravilo je namjeru Komisije da preispita strategiju za kibersigurnost.

Donošenje Direktive o sigurnosti mrežnih i informacijskih sustava[14] u srpnju 2016. bilo je važan korak prema jačanju otpornosti u području kibersigurnosti na europskoj razini. Tom su Direktivom utvrđena prva pravila na razini EU-a o kibersigurnosti, poboljšane su sposobnosti u području kibersigurnosti te je ojačana suradnja među državama članicama. Njome se također od poduzeća u ključnim sektorima zahtijeva da poduzmu odgovarajuće sigurnosne mjere te da relevantno nacionalno tijelo obavijeste o svim ozbiljnim kiberincidentima. Ti sektori uključuju energetiku, promet, opskrbu vodom, zdravstvo, bankarstvo i infrastrukturu financijskog tržišta. Internetska tržišta, usluge računalstva u oblaku i pretraživači morat će poduzimati slične mjere. Dosljednu provedbu u različitim sektorima, kao i preko granica, osigurat će Skupina za suradnju u području usluga mrežnih informacija, koju je uspostavila Komisija 2016. i koja ima zadatak izbjegavanja fragmentacije tržišta. U tom se kontekstu Direktiva o sigurnosti mrežnih i informacijskih sustava smatra referentnim okvirom za sve sektorske inicijative u području kibersigurnosti. Nadalje, tom se Direktivom stvara mreža timova za odgovor na računalne sigurnosne incidente (CSIRT), u kojoj su okupljeni svi relevantni dionici. Komisija i CERT-EU usporedno s tim aktivno prate kiberprijetnje i s nacionalnim tijelima razmjenjuju informacije kako bi se osiguralo da informatički sustavi institucija EU-a budu sigurni i otporni na kibernapade. Incident s ucjenjivačkim softverom *WannaCry* iz svibnja 2017. bio je prva prilika za operativnu suradnju i razmjenu informacija u Mreži putem širenja savjeta. Kako bi se ublažila prijetnja i pomoglo žrtvama, tim za hitne računalne intervencije EU-a održavao je bliske kontakte s Europskim centrom za kiberkriminalitet (EC3) pri Europolu, timovima za odgovor na računalne sigurnosne incidente (CSIRT) zahvaćenih zemalja, jedinicama za kiberkriminalitet i ključnim industrijskim partnerima. Razmjenom nacionalnih izvješća o stanju uspostavljen je zajednički uvid u stanje

[13] Zaključci Europskog vijeća od 22. i 23. lipnja 2017.
[14] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

u cijelom EU-u. To je iskustvo omogućilo bolju pripremljenost Mreže na buduće incidente (npr. *NonPetya*), a utvrđeno je i nekoliko nedostataka, koje se nastoji ukloniti.

12. mjera: Komisija će, zajedno s državama članicama, surađivati s industrijom u kontekstu ugovornog javno-privatnog partnerstva za kibersigurnost kako bi se razvile i ispitale tehnologije za bolju zaštitu korisnika i infrastruktura od kibernetičkih aspekata hibridnih prijetnji.

Komisija je u srpnju 2016., u suradnji s državama članicama, s industrijom potpisala ugovorno javno-privatno partnerstvo za kibersigurnost, na temelju čega će se u okviru Programa EU-a za istraživanja i inovacije Obzor 2020. uložiti 450 milijuna EUR u razvoj i ispitivanje tehnologija za bolju zaštitu korisnika i infrastruktura od kiberprijetnji i hibridnih prijetnji. U okviru Partnerstva izrađen je prvi paneuropski strateški program istraživanja, koji je bio usmjeren na povećavanje otpornosti ključne infrastrukture i građana na kibernapade. Poboljšana je i koordinacija među dionicima, što je dovelo do povećanja učinkovitosti i djelotvornosti financiranja za kibersigurnost u okviru programa Obzor 2020. Partnerstvo paralelno radi i na pitanjima certifikacije u području kibersigurnosti za informacijsku i komunikacijsku tehnologiju te nastoji riješiti problem ozbiljnog nedostatka stručnjaka za kibersigurnost na tržištu. S obzirom na znatne potrebe u pogledu civilnih istraživanja i visoke razine otpornosti u obrani, Skupina za istraživanja i tehnologiju u području kibernetike Europske obrambene agencije pridonosi područjima istraživanja koja je utvrdila Europska organizacija za kibernetičku sigurnost u svojem strateškom programu za istraživanja i inovacije.

13. mjera: Komisija će objaviti smjernice za vlasnike pametnih mreža kako bi ojačali kibersigurnost svojih instalacija. U kontekstu inicijative za oblikovanje tržišta električne energije Komisija će razmotriti predlaganje planova za pripravnost na rizik i postupovnih pravila za razmjenu informacija i osiguravanje solidarnosti među državama članicama u vrijeme krize, uključujući pravila o prevenciji i ublažavanju kibernapada.

U energetskom sektoru Komisija priprema sektorsku strategiju za kibersigurnost, koja obuhvaća uspostavu Platforme stručnjaka za energetiku u području kibersigurnosti kako bi se ojačala provedba Direktive o sigurnosti mrežnih i informacijskih sustava. Studijom iz veljače 2017. utvrđene su najbolje raspoložive tehnike za povećanje razine kibersigurnosti pametnih mjernih sustava, kao potpora toj platformi. Komisija je pokrenula i mrežnu platformu Centar EU-a za razmjenu informacija o incidentima i prijetnjama (*Incident and Threat Information Sharing EU Centre*, ITIS-EUC), na kojoj se analiziraju i razmjenjuju informacije o kiberprijetnjama i incidentima u energetskom sektoru.

Jačanje otpornosti financijskog sektora na hibridne prijetnje

14. mjera: Komisija će u suradnji s ENISA-om[15], državama članicama te relevantnim međunarodnim, europskim i nacionalnim tijelima i financijskim institucijama promicati i olakšavati razvoj platformi i mreža za razmjenu informacija o prijetnjama te uklanjati čimbenike koji ometaju razmjenu takvih informacija.

Prepoznajući da su kiberprijetnje među glavnim rizicima za financijsku stabilnost, Komisija je preispitala regulatorni okvir za platne usluge u Europskoj uniji, koji se sada provodi.

[15] Agencija Europske unije za mrežnu i informacijsku sigurnost.

Preispitanom Direktivom o platnim uslugama[16] uvedene su nove odredbe za povećanje sigurnosti platnih instrumenata i pouzdaniju autentifikaciju klijenta s ciljem smanjivanja broja prijevara, posebno u plaćanjima na internetu. Novi zakonodavni okvir primjenjivat će se od siječnja 2018. Komisija trenutačno uz pomoć Europskog nadzornog tijela za bankarstvo i uz savjetovanje s dionicima razvija regulatorne tehničke standarde, čija se objava očekuje do kraja 2017., za pouzdanu autentifikaciju klijenata te zajedničku i sigurnu komunikaciju kako bi se postigla sigurnost platnih transakcija. Nadalje, Komisija je na međunarodnoj razini blisko surađivala s odgovarajućim partnerima iz skupine G7 na „temeljnim načelima skupine G7 za kibersigurnost u financijskom sektoru", koja su u listopadu 2016. podržali ministri financija i guverneri središnjih banaka skupine G7. Ta su načela osmišljena za subjekte iz financijskog sektora (privatne i javne) te pridonose usklađenom pristupu kibersigurnosti unutar financijskog sektora kako bi se zajednički uklanjale kiberprijetnje, uključujući povećane i sofisticiranije kiberprijetnje.

Promet

15. mjera: Komisija i visoka predstavnica (u okviru svojih područja nadležnosti) u suradnji s državama članicama ispitat će načine postupanja u slučaju hibridnih prijetnji, posebno onih koje se odnose na kibernapade u prometnom sektoru.

Provedba akcijskog plana Strategije europske unije za sigurnosnu zaštitu u pomorstvu[17] pridonijet će smanjivanju suzdržanosti u razmjeni informacija te zajedničkom korištenju sredstava civilnih i vojnih tijela. Zahvaljujući pristupu na svim razinama uprave povećana je suradnja među raznim subjektima. Zajednički civilno-vojni strateški program istraživanja Komisije i ESVD-a trebao bi biti dovršen do kraja 2017., sa završnom radionicom o zaštiti ključne pomorske infrastrukture. Taj bi se rad ubuduće mogao proširiti i obuhvatiti nove prijetnje koje ugrožavaju podvodne cjevovode, prijenos energije i komunikacijske kablove, uključujući one s optičkim vlaknima, a dolaze izvan nacionalnih voda.

U nedavno provedenoj studiji[18] ocijenjen je kapacitet za procjenu rizika nacionalnih tijela koja obavljaju funkcije obalne straže. Utvrđene su najveće prepreke suradnji i predloženi su praktični načini da se poboljša suradnja pomorskih tijela na razini EU-a i nacionalnoj razini u tom konkretnom području. Procjena rizika nužna je za suzbijanje pomorskih prijetnji, a još je važnija u evaluaciji i sprečavanju hibridnih prijetnji jer su za njih potrebna dodatna i složenija razmatranja. Rezultati te studije bit će predstavljeni na različitim forumima povezanima s obalnom stražom kako bi se predložene preporuke mogle procijeniti i provesti radi povećanja suradnje u tom području, pri čemu su glavni ciljevi pripravnost i odgovor na hibridne prijetnje.

Borba protiv financiranja terorizma

16. mjera: Komisija će se koristiti provedbom akcijskog plana za suzbijanje financiranja terorizma kako bi i na taj način doprinijela suzbijanju hibridnih prijetnji.

---

[16] Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu (SL L 337, 23.12.2015., str. 35.).

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf i 2. izvješće o provedbi akcijskog plana Strategije Europske unije za sigurnosnu zaštitu u pomorstvu, predstavljeno državama članicama 21. lipnja 2017.

[18] Studija „Evaluacija kapaciteta za procjenu rizika na razini tijela država članica koja obavljaju funkcije obalne straže", 2017., https://ec.europa.eu/maritimeaffairs/documentation/studies

Prouzročiteljima hibridnih prijetnji i njihovim pristašama potrebna su financijska sredstva da bi proveli svoje planove. Nastojanja EU-a u borbi protiv financiranja kaznenih djela i terorizma u okviru Europskog programa sigurnosti i akcijskog plana za suzbijanje financiranja terorizma također mogu doprinijeti suzbijanju hibridnih prijetnji. Komisija je u prosincu 2016. predstavila tri zakonodavna prijedloga o kaznenim sankcijama za pranje novca i nezakonita gotovinska plaćanja te o zamrzavanju i oduzimanju imovine[19].
Sve su države članice morale do 26. lipnja 2017. u nacionalno zakonodavstvo prenijeti 4. Direktivu o sprečavanju pranja novca[20], a Komisija je u srpnju 2016. podnijela ciljani zakonodavni prijedlog za nadopunu i jačanje te direktive dodatnim mjerama[21].

Komisija je 26. lipnja 2017. izdala nadnacionalne procjene rizika koje su predviđene 4. Direktivom o sprečavanju pranja novca. Iznijela je i prijedlog uredbe za sprečavanje uvoza i skladištenja kulturnih dobara nezakonito uvezenih iz trećih zemalja u EU[22]. Kasnije ove godine izvijestit će o tekućoj procjeni potrebe za mogućim dodatnim mjerama za praćenje financiranja terorizma u EU-u, a preispituje i zakonodavstvo o suzbijanju prijevara i krivotvorenja u području bezgotovinskih sredstava plaćanja[23].

U Osmom izvješću o napretku prema uspostavi učinkovite i istinske sigurnosne unije dostupno je više pojedinosti o stanju provedbe akcijskog plana za suzbijanje financiranja terorizma.

<u>Promicanje zajedničkih vrijednosti EU-a te uključivih, otvorenih i otpornih društava</u>

Jačanje otpornosti na radikalizaciju i nasilni ekstremizam

Vjersku i ideološku radikalizaciju te etničke i manjinske sukobe mogu pokrenuti vanjski subjekti potporom određenim skupinama ili nastojanjima da izazovu sukobe među skupinama. Pojavili su se i novi izazovi, poput prijetnji pojedinaca, novih putova radikalizacije, potencijalno i u kontekstu migracijske krize, te porasta desničarskog ekstremizma (uključujući nasilje protiv migranata) i rizika od polarizacije. Iako se u kontekstu sigurnosne unije mnogo radi na problematici radikalizacije, taj bi rad posredno mogao biti važan i iz perspektive hibridnih prijetnji utoliko što prouzročitelji hibridnih prijetnji mogu manipulirati osobama podložnima radikalizaciji.

<u>17. mjera:</u> Komisija provodi mjere protiv radikalizacije koje su utvrđene u Europskom programu sigurnosti i analizira potrebu za jačanjem postupaka uklanjanja nezakonitog sadržaja, pozivajući posrednike da provedu dubinsku analizu u upravljanju mrežama i sustavima.

Sprečavanje radikalizacije

[19] Treće izvješće o napretku prema uspostavi učinkovite i istinske sigurnosne unije, COM(2016) 831 final.
[20] Direktiva (EU) 2015/849 Europskog parlamenta i Vijeća od 20. svibnja 2015. o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, o izmjeni Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2005/60/EZ Europskog parlamenta i Vijeća i Direktive Komisije 2006/70/EZ (Tekst značajan za EGP), SL L 141, 5.6.2015., str. 73.–117.
[21] Za dodatne pojedinosti vidjeti Treće izvješće o napretku prema uspostavi učinkovite i istinske sigurnosne unije (COM(2016) 831 final) te Osmo izvješće o napretku prema uspostavi učinkovite i istinske sigurnosne unije (COM(2017) 354 final).
[22] COM(2017) 26.6.2017., COM(2017) 340 final, SWD(2017) 275 final 0.
[23] Osmo izvješće o napretku prema uspostavi učinkovite i istinske sigurnosne unije, COM(2017) 354 final.

Komisija i dalje provodi svoje višedimenzionalne mjere kao odgovor na radikalizaciju, kako je utvrđeno u lipnju 2016. u Komunikaciji o podupiranju sprečavanja radikalizacije koja vodi k nasilnom ekstremizmu[24], u kojoj su utvrđene ključne mjere poput promicanja uključivog obrazovanja i zajedničkih vrijednosti, rješavanja problema ekstremističke propagande na internetu i radikalizacije u zatvorima, jačanja suradnje s trećim zemljama te poboljšanja istraživanja radi boljeg razumijevanja promjenjive prirode radikalizacije i stjecanja bolje osnove za političke odgovore. Mreža za osvješćivanje o radikalizaciji (RAN) radi s lokalnim subjektima na razini zajednica te tako obavlja glavni dio rada Komisije na podršci državama članicama u tom području. Dodatne pojedinosti dostupne su u Osmom izvješću o napretku prema uspostavi učinkovite i istinske sigurnosne unije[25].

Radikalizacija na internetu i govor mržnje

Komisija se u skladu s Europskim programom sigurnosti[26] zalaže za smanjenje dostupnosti nezakonitog sadržaja na internetu, posebno u suradnji s jedinicom EU-a za rad u vezi s prijavljenim internetskim sadržajima pri Europolu i internetskim forumom EU-a[27]. Znatan napredak postignut je i na temelju Kodeksa ponašanja za borbu protiv nezakonitog govora mržnje na internetu[28]. Dodatne pojedinosti dostupne su u Osmom izvješću o napretku prema uspostavi učinkovite i istinske sigurnosne unije[29]. Te će se mjere pojačati i s obzirom na zaključke Europskog vijeća[30], sastanak na vrhu skupine G7[31] te sastanak na vrhu skupine G20 u Hamburgu[32].

Internetske platforme imaju ključnu ulogu u borbi protiv nezakonitog ili potencijalno štetnog sadržaja. Kako je utvrđeno u preispitivanju na sredini provedbenog razdoblja strategije jedinstvenog digitalnog tržišta[33], Komisija će osigurati bolju koordinaciju dijaloga na platformama usmjerenih na mehanizme i tehnička rješenja za uklanjanje nezakonitog sadržaja. Prema potrebi te bi mehanizme trebalo potkrijepiti smjernicama o aspektima kao što su prijavljivanje i uklanjanje nezakonitog sadržaja. Komisija će dati smjernice i o pravilima o odgovornosti.

Jačanje suradnje s trećim zemljama

18. mjera: ***visoka predstavnica će u suradnji s Komisijom pokrenuti istraživanje rizika hibridnih prijetnji u susjednim regijama. Visoka predstavnica, Komisija i države članice koristit će se***

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf
[25] COM(2017) 354 final
[26] Dodatne pojedinosti dostupne su u Osmom izvješću o napretku prema uspostavi učinkovite i istinske sigurnosne unije, COM(2017) 354 final.
[27] Dodatne pojedinosti dostupne su u Osmom izvješću o napretku prema uspostavi učinkovite i istinske sigurnosne unije, COM(2017) 354 final.
[28] Kodeks ponašanja u pogledu nezakonitog govora mržnje na internetu, 31. svibnja 2016., http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] Dodatne pojedinosti dostupne su u Osmom izvješću o napretku prema uspostavi učinkovite i istinske sigurnosne unije, COM(2017) 354 final.
[30] Zaključci Vijeća od 22. i 23. lipnja 2017.
[31] Sastanak na vrhu skupine G7 u Taormini, Italija, 26. i 27. svibnja 2017.
[32] Sastanak na vrhu skupine G20 u Hamburgu, Njemačka, 7. i 8. srpnja 2017.
[33] Usporediti Komunikaciju Komisije COM(2017) 228 final.

instrumentima koji su im na raspolaganju kako bi izgradili kapacitete partnera i ojačali njihovu otpornost na hibridne prijetnje. Misije ZSOP-a mogle bi se koristiti za pomoć partnerima u jačanju njihovih kapaciteta, neovisno o instrumentima EU-a ili kao njihova dopuna.

Europska unija više je usmjerena na izgradnju kapaciteta i povećanje otpornosti partnerskih zemalja u sigurnosnom sektoru, među ostalim jačanjem poveznica između sigurnosti i razvoja, razvojem sigurnosne dimenzije revidirane Europske politike susjedstva te pokretanjem dijaloga o sigurnosti i borbi protiv terorizma sa zemljama Sredozemlja. U tom je cilju pokrenut pilot-projekt istraživanja rizika u suradnji s Republikom Moldovom. Svrha mu je pomoći u utvrđivanju ključnih slabosti zemlje i osigurati da pomoć EU-a bude usmjerena upravo na ta područja. Rezultati pilot-projekta pokazali su da se samo istraživanje smatralo korisnim. Na temelju stečenog iskustva Komisija i ESVD dat će preporuke za određivanje prioritetnih mjera u pogledu povećanja djelotvornosti, strateške komunikacije, zaštite ključne infrastrukture i kibersigurnosti.

Ubuduće bi i druge susjedne zemlje mogle imati koristi od tog istraživanja i iskoristiti ta prva iskustva, ali uz određene prilagodbe kako bi se u obzir uzele različite nacionalne situacije na lokalnoj razini i posebne prijetnje te kako bi se izbjeglo udvostručavanje u odnosu na tekuće dijaloge o sigurnosti i borbi protiv terorizma. Komisija i visoka predstavnica donijele su 7. lipnja 2017. opću Zajedničku komunikaciju o strateškom pristupu otpornosti u vanjskom djelovanju EU-a[34]. Cilj je podržati partnerske zemlje kako bi postale otpornije na današnje globalne izazove. U Komunikaciji se potvrđuje potreba za prelaskom s pristupa koji se temelji na suzbijanju krize na strukturiraniji, dugoročni pristup ranjivostima, s naglaskom na predviđanju, sprečavanju i pripravnosti.

<u>Kiberotpornost kao temelj razvoja</u>

EU podupire zemlje izvan Europe u povećanju otpornosti njihovih informacijskih mreža. Sve veća digitalizacija ima intrinsičnu sigurnosnu dimenziju zbog koje postoje posebni izazovi s obzirom na otpornost sustava informacijskih mreža na svjetskoj razini jer kibernapadi ne poznaju granice. EU podupire treće zemlje u jačanju njihovih sposobnosti da na odgovarajući način spriječe slučajne kvarove i kibernapade te reagiraju na njih. Nakon pilot-projekta u području kibersigurnosti u bivšoj jugoslavenskoj Republici Makedoniji, Kosovu[35] i Moldovi, završenog 2016., Komisija će pokrenuti novi program za povećanje kiberotpornosti trećih zemalja u razdoblju 2017.–2020., uglavnom u Africi i Aziji, ali i u Ukrajini. Cilj je tog projekta povećati sigurnost i pripravnost ključnih informacijskih mreža i infrastrukture u trećim zemljama na temelju pristupa na svim razinama uprave, uz istovremeno osiguravanje poštovanja ljudskih prava i vladavine prava.

<u>Zaštita zračnog prometa</u>

Civilno zrakoplovstvo i dalje je velik i simboličan cilj terorista, ali može biti i dio hibridne kampanje. Iako je EU razvio čvrst okvir za zaštitu zračnog prometa, letovi iz trećih zemalja mogli bi biti podložniji takvim prijetnjama. U skladu s Rezolucijom Vijeća sigurnosti UN-a 2309 (2016) Komisija pojačava napore za izgradnju kapaciteta u trećim zemljama. U siječnju

[34]Zajednička komunikacija Europskom parlamentu i Vijeću: Strateški pristup otpornosti u vanjskom djelovanju EU-a, JOIN(2017) 21 final.

[35] Ovim se nazivom ne dovode u pitanje stajališta o statusu te je on u skladu s RVSUN-om 1244 (1999) i mišljenjem Međunarodnog suda o proglašenju neovisnosti Kosova.

2017. započela je s novom integriranom procjenom rizika kako bi se osiguralo utvrđivanje prioriteta i koordinacija rada na izgradnji kapaciteta na razini EU-a i država članica te s međunarodnim partnerima. Komisija je 2016. pokrenula četverogodišnji projekt za zaštitu civilnog zrakoplovstva u Africi i na Arapskom poluotoku kako bi se suzbila prijetnja terorizma usmjerenog na civilno zrakoplovstvo. Projekt je usmjeren na razmjenu stručnog znanja među državama partnerima i stručnjacima iz država članica Europske konferencije civilnog zrakoplovstva te na aktivnosti mentorstva, izobrazbe i obuke. Te će se aktivnosti intenzivirati tijekom 2017.

c. SPREČAVANJE KRIZE, ODGOVOR NA KRIZU I OPORAVAK

Iako se dugoročnim politikama na nacionalnoj razini i razini EU-a mogu ublažiti posljedice, kratkoročno je neophodno povećati sposobnost država članica i Unije da spriječe hibridne prijetnje, odgovore na njih i oporave se od njih na brz i usklađen način. Ključan je brz odgovor na događaje koje su uzrokovale hibridne prijetnje. Protekle je godine ostvaren znatan napredak u tom području te je sada u EU-u uspostavljen operativni protokol kojim je utvrđen postupak upravljanja krizom u slučaju hibridnog napada. Ubuduće će se provoditi redovito praćenje i vježbe.

19. mjera: ***visoka predsjednica i Komisija uspostavit će u suradnji s državama članicama zajednički operativni protokol i provoditi redovite vježbe kako bi se poboljšala sposobnost donošenja strateških odluka kao odgovor na složene hibridne prijetnje na temelju postupaka za upravljanje krizom i integrirani politički odgovor na krize.***

U zajedničkom okviru preporučeno je uspostavljanje mehanizama za brzi odgovor na događaje koje su uzrokovale hibridne prijetnje kako bi se koordinirali mehanizmi za odgovor EU-a[36] i sustavi za rano upozoravanje. Da bi se to postiglo, službe Komisije i ESVD objavili su operativni protokol EU-a za suzbijanje hibridnih prijetnji (*EU Playbook*)[37], u kojem se opisuju načini na koje u slučaju hibridne prijetnje treba koordinirati, povezivati i analizirati obavještajne informacije, prikupljati informacije za postupke donošenja politika, organizirati vježbe i izobrazbu te surađivati s partnerskim organizacijama, posebno NATO-om. Slično tome, NATO je izradio priručnik za povećanu interakciju NATO-a i EU-a za sprečavanje i suzbijanje hibridnih prijetnji u području kiberobrane, strateške komunikacije, uvida u stanje i upravljanja krizom. *EU Playbook* ispitat će se u jesen 2017. u okviru Paralelne i usklađene vježbe Europske unije, koja uključuje interakciju s NATO-om.

20. mjera*: Komisija i visoka predstavnica će u okviru svojih područja nadležnosti ispitati primjenjivost i praktične posljedice primjene članka 222. UFEU-a i članka 42. stavka 7. UEU-a u slučaju dalekosežnog i ozbiljnog hibridnog napada.*

U članku 42. stavku 7. UEU-a riječ je o oružanoj agresiji na državnom području države članice, dok je u članku 222. UFEU-a (klauzula solidarnosti) riječ o terorističkom napadu ili prirodnoj nepogodi ili nesreći izazvanoj ljudskim djelovanjem na državnom području države članice. U slučaju hibridnih napada, koji su kombinacija kaznenih i subverzivnih radnji, vjerojatnije je da će se primijeniti potonji članak. Pozivanjem na klauzulu solidarnosti aktivira

[36] Aranžmani za EU-ov integrirani politički odgovor na krize (IPCR), koje je aktiviralo Vijeće, Komisijin sustav ARGUS i CRM ESVD-a.
[37] Radni dokument službi Komisije (2016) 227 donesen 7. srpnja 2016.

se koordinacija na razini Vijeća (aranžmani za integrirani politički odgovor na krize – IPCR) te se uključuju relevantne institucije, agencije i tijela EU-a, kao i programi i mehanizmi EU-a za pomoć. U Odluci Vijeća od 2014/415/EU utvrđuju se aranžmani Unije za provedbu klauzule solidarnosti. Ti načini primjene i dalje su valjani te nema potrebe za preispitivanjem Odluke Vijeća. Ako hibridni napad uključuje oružanu agresiju, može se aktivirati i članak 42. stavak 7. U tom slučaju pomoć i potporu pružaju i države članice i EU. Komisija i visoka predstavnica i dalje će procjenjivati najdjelotvornije načine suočavanja s takvim napadima.

Donošenjem prethodno spomenutog operativnog protokola EU-a izravno se podržava ta procjena te će se provoditi kao dio Paralelne i usklađene vježbe EU-a (PACE – *Parallel and Coordinated Exercise*) u listopadu 2017. Tom vježbom ispitat će se razni mehanizmi i sposobnost EU-a za interakciju s ciljem brzog donošenja odluke u nejasnim situacijama koje su nastale zbog hibridne prijetnje.

21. mjera: ***visoka predstavnica u suradnji s državama članicama uključit će, iskoristiti i koordinirati sposobnosti vojnog djelovanja u suzbijanju hibridnih prijetnji u okviru zajedničke sigurnosne i obrambene politike.***

Kao odgovor na zadaću integracije vojnih sposobnosti za potporu ZVSP-u/ZSOP-u te na temelju seminara s vojnim stručnjacima u prosincu 2016. i smjernica radne skupine Vojnog odbora Europske unije iz svibnja 2017., u srpnju 2017. finalizirani su vojni savjeti o „vojnom doprinosu EU-a za suzbijanje hibridnih prijetnji u okviru ZSOP-a" te će se provoditi na temelju provedbenog plana konceptualnog razvoja.

d. SURADNJA EU-A I NATO-A

22. mjera*: visoka predstavnica u suradnji s Komisijom nastavit će neformalni dijalog te pojačavati koordinaciju i suradnju s NATO-om u pogledu uvida u stanje, strateške komunikacije, kibersigurnosti te „prevencije krize i odgovora na nju" radi suzbijanja hibridnih prijetnji, uz poštovanje načela uključivosti i autonomije postupaka donošenja odluka svake organizacije.*

Na temelju zajedničke izjave koju su potpisali predsjednici Europskog vijeća i Europske komisije te glavni tajnik NATO-a u Varšavi 8. srpnja 2016., EU i NATO razvili su zajednički skup 42 prijedloga za provedbu, koje su potom u zasebnim, usporednim postupcima 6. prosinca 2016. i potvrdila vijeća EU-a i NATO-a[38]. Visoka predstavnica/potpredsjednica i glavni tajnik NATO-a objavili su u lipnju 2017. izvješće o ukupnom napretku postignutom u 42 mjere iz zajedničke izjave. Suzbijanje hibridnih prijetnji jedno je od sedam područja suradnje utvrđenih u zajedničkoj izjavi i obuhvaća 10 od 42 djelovanja. U izvješću je vidljivo da su na temelju zajedničkog djelovanja posljednjih godina ostvareni bitni rezultati. Mnoge posebne mjere usmjerene na suzbijanje hibridnih prijetnji već su spomenute, uključujući Europski centar izvrsnosti za suzbijanje hibridnih prijetnji, bolji uvid u stanje, uspostavljanje jedinice EU-a za otkrivanje hibridnih prijetnji i njezinu interakciju s nedavno uspostavljenim NATO-ovim odjelom za analizu hibridnih prijetnji te suradnju timova za stratešku komunikaciju. Osoblje NATO-a i EU-a prvi će put zajedno uvježbavati svoj odgovor na scenarij pojave hibridne prijetnje. Očekuje se da će se tako ispitati provedba više od trećine zajedničkih prijedloga. EU će ove godine provesti svoju paralelnu i usklađenu vježbu te se priprema za preuzimanje vodeće uloge 2018.

[38] http://www.consilium.europa.eu/hr/press/press-releases/2016/12/06-eu-nato-joint-declaration/

U području otpornosti osoblje EU-a i NATO-a sudjelovalo je u uzajamnom obavješćivanju, među ostalim o mehanizmu EU-a za integriran politički odgovor na krize. Redovni kontakti osoblja NATO-a i EU-a, među ostalim na radionicama ili sudjelovanjem u upravnom odboru Europske obrambene agencije, omogućili su razmjenu informacija o osnovnim zahtjevima NATO-a za nacionalnu otpornost. Za jesen se planiraju daljnji kontakti Komisije i NATO-a u pogledu povećanja otpornosti. U sljedećem izvješću o napretku suradnje EU-a i NATO-a predložit će se mogućnosti za proširenje suradnje tih dviju organizacija.

3. ZAKLJUČAK

U zajedničkom okviru navode se mjere osmišljene za pomoć u suzbijanju hibridnih prijetnji i povećanje otpornosti na razini EU-a i na nacionalnoj razini te za partnere. Iako Komisija i visoka predstavnica u bliskoj suradnji s državama članicama i partnerima postižu postavljene ciljeve u svim područjima, nužno je da se taj zamah zadrži kako bi se lakše suočili s trenutačnim i novim hibridnim prijetnjama. Države članice imaju glavnu odgovornost za suzbijanje hibridnih prijetnji povezanih s nacionalnom sigurnošću te održavanjem zakona i reda. Nacionalna otpornost i zajednički rad na zaštiti od hibridnih prijetnji moraju se smatrati komplementarnim elementima istih općih nastojanja. Stoga se države članice potiče da što prije provedu istraživanja o hibridnim rizicima jer će ona poslužiti kao izvor vrijednih informacija o razini osjetljivosti i pripravnosti u cijeloj Europi. Na temelju znatnog napretka u podizanju svijesti trebalo bi što bolje iskoristiti potencijal jedinice EU-a za otkrivanje hibridnih prijetnji. Visoka predstavnica poziva države članice da podrže rad radnih skupina StratCom kako bi borba protiv sve brojnijih hibridnih prijetnji bila djelotvornija. EU će u potpunosti podržati Europski centar za suzbijanje hibridnih prijetnji, kojim upravlja Finska.

Jedinstvena snaga EU-a leži u pružanju pomoći državama članicama pri jačanju njihove otpornosti na temelju raznih postojećih instrumenata i programa. Postignut je znatan napredak mjera za jačanje otpornosti u područjima poput prometa, energetike, kibersigurnosti, ključne infrastrukture, zaštite financijskog sustava od nezakonite upotrebe te nastojanja da se suzbiju nasilni ekstremizam i radikalizacija. Kako se hibridne prijetnje budu razvijale, tako će se nastaviti i rad EU-a na jačanju otpornosti. EU će, konkretno, razviti pokazatelje za poboljšanje zaštite i otpornosti ključne infrastrukture na hibridne prijetnje u relevantnim sektorima.

Prioriteti u pogledu sposobnosti za povećanje otpornosti na hibridne prijetnje mogu se sufinancirati iz Europskog fonda za obranu i država članica. Predstojeći paket za kibersigurnost te međusektorske mjere usmjerene na provedbu Direktive o mrežnoj i informacijskoj sigurnosti pružit će nove platforme za suzbijanje hibridnih prijetnji u cijelom EU-u.

Komisija i visoka predstavnica pozivaju države članice i dionike, prema potrebi, da brzo postignu dogovor te osiguraju brzu i djelotvornu provedbu brojnih mjera usmjerenih na povećanje otpornosti i opisanih u ovoj Komunikaciji. EU će poboljšavati i produbljivati svoju već plodnu suradnju s NATO-om.

Unija se i dalje zalaže za mobilizaciju svih relevantnih instrumenata EU-a radi suzbijanja složenih hibridnih prijetnji. Potpora radu država članica i dalje je prioritet Unije, koja sa svojim partnerima djeluje kao jači i djelotvorniji pružatelj sigurnosti.