



EVROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA ZUNANJE
ZADEVE IN
VARNOSTNO POLITIKO

Bruselj, 19.7.2017
JOIN(2017) 30 final

SKUPNO POROČILO EVROPSKEMU PARLAMENTU IN SVETU

**o izvajanju skupnega okvira o preprečevanju hibridnih groženj -
odziva Evropske unije**

1. UVOD

EU se sooča z enim največjih varnostnih izzivov v svoji zgodovini. Grožnje vse bolj dobivajo nekonvencionalno obliko: nekatere so fizične, kot so nove oblike terorizma, druge izkoriščajo digitalni prostor za kompleksne kibernetične napade. Spet druge, bolj prefinjene, so namenjene nasilnemu izvajanju pritiska vključno z dezinformacijskimi kampanjami in medijsko manipulacijo. Izpodkopati želijo temeljne evropske vrednote, kot so človeško dostojanstvo, svoboda in demokracija. Pri nedavnih usklajenih kibernetičnih napadih po vsem svetu, ki jih je bilo težko pripisati določenemu povzročitelju, so se pokazale šibke točke naših družb in ustanov.

Evropska komisija in visoka predstavnica sta aprila 2016 sprejela skupno sporočilo o preprečevanju hibridnih groženj¹ (v nadaljnjem besedilu: skupni okvir). V tem okviru se priznava čezmejna in kompleksna narava hibridnih groženj, za krepitev splošne odpornosti naših družb pa je predlagan nadresorski pristop. Svet² je pobudo in predlagane ukrepe pozdravil ter pozval Komisijo in visoko predstavnico, da julija 2017 poročata o napredku. EU sicer lahko pomaga državam članicam pri krepitvi odpornosti proti hibridnim grožnjam, vendar so zanje v prvi vrsti odgovorne države članice, saj je preprečevanje hibridnih groženj povezano z nacionalno varnostjo in obrambo.

Skupni okvir za preprečevanje hibridnih groženj je pomemben sestavni del bolj celostnega pristopa EU k varnosti in obrambi. Prispeva k ustvarjanju Evrope, ki ščiti, v skladu s pozivom predsednika Junckerja v govoru o stanju v Uniji septembra 2016. Evropska unija je leta 2016 položila tudi temelje za močnejšo evropsko obrambno politiko, da bi upoštevala pričakovanja državljanov po večji varnosti. V globalni strategiji EU za zunanjo in varnostno politiko³ je bila podrobno predstavljena potreba po celostnem pristopu, ki bi povezal notranjo odpornost z zunanjimi ukrepi EU, ter podan je bil poziv k sinergijam med obrambno politiko in politikami, ki zajemajo notranji trg, industrijo, preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter obveščevalne službe. Komisija je po sprejetju evropskega obrambnega akcijskega načrta novembra 2016 predlagala konkretne pobude, ki bodo prispevale k izboljšanju sposobnosti EU za odziv na hibridne grožnje z odpornejšimi obrambnimi dobavnimi verigami ter močnejšim enotnim trgom za obrambo. Natančneje, 7. junija 2017 je ustanovila evropski obrambni sklad s predlaganim financiranjem v višini 600 milijonov EUR do leta 2020 in 1,5 milijarde EUR v obdobju po letu 2020. V sporočilu o varnostni uniji⁴ je bilo priznано, da je treba preprečevati hibridne grožnje in da je pomembno zagotoviti bolj usklajene notranje in zunanje ukrepe na področju varnosti.

Voditelji EU so v razpravi o prihodnosti Evrope varnosti in obrambi namenili posebno pozornost.⁵ To je bilo priznано v Rimski izjavi z dne 25. marca 2017, v kateri je bila predstavljena vizija varne in zanesljive Unije, zavezane krepitvi svoje skupne varnosti in obrambe. Predsednik Evropskega sveta, predsednik Evropske komisije in generalni sekretar

¹ Skupno sporočilo Evropskemu parlamentu in Svetu z naslovom Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije, JOIN(2016) 18 final.

² Sklepi Sveta o preprečevanju hibridnih groženj, sporočilo za medije 196/16, 19. aprila 2016.

³ Visoka predstavnica jo je Evropskemu svetu predstavila 28. junija 2016.

⁴ COM(2016) 230 final, 20.4.2016.

⁵ Načrt iz Bratislave, ki ga je Evropski svet sprejel 16. septembra 2016, ter Rimski izjava voditeljev 27 držav članic in Evropskega sveta, Evropskega parlamenta in Evropske komisije z dne 25. marca 2017.

Nata so 8. julija 2016 v Varšavi podpisali skupno izjavo, da bi strateškemu partnerstvu med EU in Natom dali nov zagon in novo vsebino. V skupni izjavi je bilo določenih sedem konkretnih področij, na katerih bi bilo treba okrepiti sodelovanje med organizacijama, eno od področij pa je tudi preprečevanje hibridnih groženj. Svet EU in Svet Nata sta nato podprla skupen sklop 42 predlogov za izvedbo, junija 2017 pa je bilo objavljeno prvo poročilo⁶, iz katerega je bil razviden bistven napredek.

V razmisleku Komisije o prihodnosti evropske obrambe⁷, predstavljenem junija 2017, so orisani različni scenariji za reševanje vse večjih varnostnih in obrambnih groženj, s katerimi se srečuje Evropa, in za krepitev lastnih obrambnih sposobnosti Evrope do leta 2025. V vseh treh scenarijih sta varnost in obramba sestavna dela evropskega projekta, da bi lahko zaščitili in zastopali svoje interese doma in na tujem. Evropa mora postati zagotavljalec varnosti in vse bolj zagotavljati svojo lastno varnost. Nobena država članica se s prihodnjimi izzivi, zlasti tistimi v zvezi s preprečevanjem hibridnih groženj, ne more soočiti sama. Sodelovanje na obrambnem in varnostnem področju torej ni le ena izmed možnosti; nujno je zagotoviti Evropo, ki ščiti.

Namen tega poročila je poročati o napredku in nadaljnjih korakih v zvezi z izvajanjem ukrepov na štirih področjih, predlaganih v skupnem okviru; krepitev situacijskega zavedanja, krepitev odpornosti, krepitev sposobnosti držav članic za preprečevanje kriz in odziv nanje ter za usklajeno okrevanje in krepitev sodelovanja z Natom za zagotovitev dopolnjevanja ukrepov. Brati bi ga bilo treba skupaj z mesečnimi poročili o napredku pri vzpostavljanju učinkovite in prave varnostne unije.

2. PREPOZNAVANJE HIBRIDNE NARAVE GROŽNJE

Hibridne dejavnosti postajajo pogosta značilnost evropskega varnostnega okolja. Njihova intenzivnost raste pri čemer povzročajo vse več skrbi vmešavanje v volitve, dezinformacijskih kampanj, zlonamernih kibernetских dejavnosti in storilcev hibridnih dejanj, ki skušajo radikalizirati ranljive člane družbe kot svoje namestniške akterje. Šibke točke za hibridne grožnje niso omejene z nacionalnimi mejami. Usklajen odziv na hibridne grožnje je potreben tudi na ravni EU in Nata. Kot kažejo dogodki od aprila 2016 naprej, se grožnje sicer še vedno ocenjujejo ločeno, vendar se v Uniji vse bolj priznava in razume, da so nekatere dejavnosti hibridne narave in da je potrebno usklajeno ukrepanje. EU si bo še naprej prizadevala izboljšati situacijsko zavedanje in sodelovanje.

Ukrep 1: Države članice, po potrebi ob podpori Komisije in visokega predstavnika, naj začnejo s pripravo raziskave o hibridnih grožnjah za opredelitev ključnih ranljivosti, vključno s posebnimi kazalniki, povezanimi s hibridnimi grožnjami, ki lahko potencialno vplivajo na nacionalne in vseevropske strukture in mreže.

Svet je ustanovil Skupino prijateljev predsedstva, v kateri strokovnjaki iz držav članic skupaj pripravljajo splošno raziskavo, s pomočjo katere bi države članice lažje prepoznale ključne kazalnike hibridnih groženj, jih vključile v mehanizme zgodnjega opozarjanja in obstoječe mehanizme za ocenjevanje tveganja ter jih po potrebi souporabljale. Dosežen je bil dogovor o

⁶<http://www.consilium.europa.eu/sl/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation/>

⁷ Razmislek o prihodnosti evropske obrambe, 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_sl.pdf

pooblastilih in delo že poteka. Splošna raziskava bi morala biti končana do konca leta 2017, potem pa se bodo začele dejanske raziskave. Zaščita pred hibridnimi grožnjami bi se morala vzajemno krečiti. Države članice zato pozivamo, da te raziskave opravijo čim hitreje, saj bodo zagotovile dragocene informacije o obsegu ranljivosti in pripravljenosti po vsej Evropi.

a. KREPITEV OZAVEŠČENOSTI

Izmenjava obveščevalnih analiz in ocenjevalnega dela je orodje, ki je ključnega pomena za ublažitev negotovosti in krepitev situacijskega zavedanja. V zadnjem letu je bil dosežen znaten napredek. Ustanovljeni sta bili hibridna fuzijska celica EU, ki zdaj že v celoti deluje, in projektna skupina EU East StratCom, Finska pa je ustanovila evropski center za preprečevanje hibridnih groženj. Veliko dela je posvečenega analizi orodij in vzvodov na področju dezinformacij in propagande, pri čemer uspešno sodelujejo projektna skupina EU East StratCom EU, hibridna fuzijska celica EU in Nato. To je dobra podlaga za nadaljnjo izgradnjo globlje zasidrane kulture analiziranja in ocenjevanja groženj za našo notranjo in zunanjo varnost s hibridnega vidika.

Hibridna fuzijska celica

Ukrep 2: Oblikovanje hibridne fuzijske celice EU v okviru obstoječe strukture Obveščevalnega in situacijskega centra EU, ki je sposobna prejemati in analizirati tajne podatke in podatke iz odprtih virov o hibridnih grožnjah. Države članice so pozvane, da vzpostavijo nacionalne kontaktne točke za hibridne grožnje, da zagotovijo sodelovanje in varno komuniciranje s hibridno fuzijsko celico EU.

V okviru Obveščevalnega in situacijskega centra EU je bila ustanovljena hibridna fuzijska celica EU, katere naloga je analizirati tajne podatke in podatke iz odprtih virov o hibridnih grožnjah, prejete od različnih zainteresiranih strani. Analiza se nato izmenjuje v EU in med državami članicami ter zagotavlja podatke za postopke strateškega odločanja EU, vključno s podatki za ocene varnostnega tveganja, izvedene na ravni EU. Obveščevalni direktorat Vojaškega štaba EU k delu fuzijske celice prispeva vojaško analizo. Doslej je bilo pripravljenih več kot 50 ocen in poročil o hibridni tematiki. Celica od januarja 2017 izdaja redni Hibridni bilten z analizami trenutnih groženj in hibridnih vprašanj, ki se uporablja neposredno v institucijah in organih EU ter nacionalnih kontaktnih točkah⁸. Celica je postala v celoti operativno sposobna maja 2017, kot je bilo predvideno. Poteka tudi sodelovanje na ravni osebja z nastajajočo celico Nata za hibridno analizo, tako v obliki izmenjave izkušenj, pridobljenih pri vzpostavitvi fuzijske celice, kot v obliki izmenjave informacij (ob upoštevanju pravil EU na področju tajnih podatkov). Hibridna fuzijska celica EU trenutno ugotavlja nadaljnje pobude za krepitev prihodnjega sodelovanja in bo imela ključno vlogo v vzporednih vajah EU in Nata, predvidenih za jesen 2017, na katerih bo potekal preskus odzivnosti hibridne fuzijske celice EU, pridobljena spoznanja pa bodo upoštevana.

Strateško komuniciranje

Ukrep 3: Visoki predstavnik bo skupaj z državami članicami proučil načine za posodobitev in usklajitev zmogljivosti, da se zagotovi proaktivno strateško komuniciranje in optimalna uporaba spremljanja medijev in znanja lingvistov specialistov.

⁸ Do danes je nacionalne kontaktne točke imenovalo 21 držav članic. To so osebe, ki v glavnih mestih držav članic opravljajo naloge v zvezi s politiko/odpornostjo.

V zadnjih mesecih so v širokem naboru ukrepov za spodbujanje nasprotnikov tudi okrepljene dezinformativne kampanje in sistematično širjenje lažnih novic. Kjer imajo med platformami prednost družbeni mediji, lahko informacija, ki je videti zanesljiva in legitimna, spremeni javno mnenje v korist nekaterih posameznikov, organizacij ali vlad. Širši cilj takih hibridnih taktik je ustvarjati zmedo v naših družbah ter diskreditirati demokratične vlade in naše strukture, institucije in volitve. Lažne novice se pogosto širijo prek spletnih platform (glej tudi ukrep 17). Komisija in visoka predstavica pozdravljata nedavne ukrepe spletnih platform in založnikov novinarskih medijev za boj proti dezinformacijam. Komisija bo take prostovoljne ukrepe spodbujala še naprej.

Visoka predstavica je ustanovila projektno skupino EU East StratCom, ki napoveduje primere dezinformacij in dezinformacijske kampanje ter odgovarja nanje. S tem se znatno izboljšuje komunikacija o politikah Unije v vzhodnem sosedstvu, hkrati pa se krepi medijsko okolje v teh državah. Projektna skupina je v preteklih dveh letih odkrila več kot 3 000 posameznih primerov dezinformacij v 18 jezikih. Z novim spletnim mestom *#EUvsdisinformation*, ki bo kmalu začelo delovati in bo omogočalo spletno iskanje, se bo dostop za uporabnike precej izboljšal. Vendar pa je, kot kažejo raziskave in analize, število dezinformacijskih kanalov in sporočil, ki se vsakodnevno širijo, bistveno večje. V projektu EU-STRAT, ki se financira iz programa Obzorje 2020 se analizirajo politike in mediji v državah vzhodnega partnerstva.

Visoka predstavica poziva države članice, da podprejo delo projektnih skupin StratCom, da bi lahko učinkoviteje preprečevali porast hibridnih groženj. To bo projektni skupini Jug (Task Force South) pomagalo pri boljšem komuniciranju in ozaveščanju v arabskem svetu, tudi v arabščini, razbijanju mitov in predstavljanju dejstev o Evropski uniji in njenih politikah. Sodelovanje z lokalnimi novinarji bo prispevalo k temu, da bodo novice ustrezale kulturnemu okolju. Cilj obeh projektnih skupin je podpirati in dopolnjevati prizadevanja v zvezi z državami članicami. Komisija poleg tega sofinancira Evropsko mrežo za strateško komuniciranje, sodelovalno omrežje, v katerem si 26 držav članic izmenjuje analize, dobre prakse in zamisli o uporabi strateškega komuniciranja v boju proti nasilnemu ekstremizmu, tudi o dezinformacijah.

Center odličnosti za „preprečevanje hibridnih groženj“

Ukrep 4: Države članice so pozvane, da preučijo možnost vzpostavitve centra odličnosti za „preprečevanje hibridnih groženj“.

Finska se je na poziv za ustanovitev centra odličnosti odzvala aprila 2017 z ustanovitvijo Evropskega centra za preprečevanje hibridnih groženj. Deset držav članic EU⁹, Norveška in ZDA so članice, Evropska unija in Nato pa sta bila pozvana, da podpreta usmerjevalni odbor¹⁰. Naloga centra je spodbujati strateški dialog, izvajati raziskave in analize v sodelovanju z interesnimi skupnostmi za izboljšanje odpornosti in odzivnosti in s tem pripomoči k preprečevanju hibridnih groženj. Center naj bi bil tudi kraj za prihodnje vaje v zvezi s hibridnimi grožnjami. Center je že navezal tesne stike s hibridno fuzijsko celico EU in organizaciji naj bi se pri delu dopolnjevali. EU trenutno preučuje načine, na katere bi lahko center konkretno podprla.

⁹ Finska, Francija, Nemčija, Latvija, Litva, Poljska, Švedska, Združeno kraljestvo, Estonija, Španija.

¹⁰ V center se lahko včlanijo tudi druge države članice EU in zaveznice Nata.

b. KREPITEV ODPORNOSTI

V skupnem okviru je odpornosti (npr. prometa, komunikacij, energije, financ ali regionalnih varnostnih infrastruktur) namenjeno osrednje mesto v ukrepih EU za odpor proti propagandnim in informacijskim kampanjam, poskusom oviranja poslovnih, družbenih in gospodarskih tokov ter napadom na informacijsko tehnologijo in kibernetsko infrastrukturo. Krepitev odpornosti se v skupnem okviru šteje za preventivni in odvračilni ukrep za utrditev družb in preprečevanje stopnjevanja kriz znotraj in zunaj EU. Dodana vrednost EU je v pomoči državam članicam in partnerjem pri krepitevi odpornosti, za kar so ji na razpolago številni obstoječi instrumenti in programi. Velik napredek je bil dosežen pri ukrepih za krepitev odpornosti na področjih, kot so kibernetska varnost, kritična infrastruktura, zaščita finančnega sistema pred nezakonito uporabo ter prizadevanja za preprečevanje nasilnega ekstremizma in radikalizacije.

Zaščita kritične infrastrukture

Ukrep 5: Komisija bo v sodelovanju z državami članicami in zainteresiranimi stranmi opredelila skupna orodja, vključno s kazalniki, z namenom izboljšanja zaščite in odpornosti kritične infrastrukture proti hibridnim grožnjam v relevantnih sektorjih.

Komisija je v zvezi z evropskim programom za zaščito kritične infrastrukture (EPCIP) nadaljevala delo na področju odkrivanja skupnih orodij, vključno s kazalniki ranljivosti, da bi okrepila odpornost kritične infrastrukture proti hibridnim grožnjam v ustreznih sektorjih. Komisija je maja 2017 organizirala delavnico o hibridnih grožnjah za kritično infrastrukturo, v kateri so sodelovale skoraj vse države članice, upravljavci kritične infrastrukture, hibridna fuzijska celica EU in Nato kot opazovalec. Na podlagi vprašalnika, ki je bil poslan nacionalnim organom držav članic, je bil dosežen dogovor o skupnem časovnem načrtu in korakih za prihodnje delo. Komisija se bo nadalje jeseni posvetovala z zainteresiranimi stranmi, da bi do konca leta 2017 dosegli soglasje o kazalnikih.

Evropska obrambna agencija se ukvarja z ugotavljanjem skupnih pomanjkljivosti pri zmogljivostih in raziskavah, ki izvirajo iz prepleta energetske infrastrukture in obrambnih zmogljivosti. Jeseni 2017 bo pripravila konceptualni dokument ter pilotne ukrepe za celostne metodologije.

Zanesljivejša oskrba z energijo

Ukrep 6: Komisija bo v sodelovanju z državami članicami podprla prizadevanja za diverzifikacijo virov energije ter spodbujala standarde varnosti in varovanja za povečanje odpornosti jedrskih infrastruktur.

Komisija je decembra 2016 v svežnju o zanesljivi oskrbi z energijo podala konkretne predloge, aprila 2017 pa sta Svet in Evropski parlament dosegla dogovor o novi uredbi o zanesljivosti oskrbe s plinom, katere namen je preprečiti krize v oskrbi s plinom. Nova pravila bodo zagotovila regionalno usklajen in skupen pristop k ukrepom za zanesljivo oskrbo z energijo med državami članicami. Tako se bo EU lažje pripravila na motnje v oskrbi s plinom v primeru krize ali hibridnega napada in jih lažje obvladovala. Prvič bo uporabljeno načelo solidarnosti: države članice bodo v primeru hude krize ali napada lahko pomagale sosedam, tako da evropskih gospodinjstev in podjetij ne bodo doleteli izpadi.

EU je dosegla napredek tudi pri razvoju ključnih projektov pri diverzifikaciji poti in virov dobave energije v skladu z okvirno strategijo za energetske unijo in evropsko strategijo za energetske varnost. Na primer v južnem plinskem koridorju potekajo konkretna gradbena dela na vseh večjih projektih plinovodov: razširitev plinovoda v Zakavkazju, transanatolski in transjadranski plinovod, pridobivalni plinovod Šah Deniz II ter razširitev južnega plinskega koridorja v Srednjo Azijo, predvsem Turkmenistan. Uvoz utekočinjenega zemeljskega plina (UZP) v Evropo narašča in prihaja iz novih virov, kot so ZDA. Primer terminala v Litvi kaže, kako je mogoče s projekti diverzifikacije zmanjšati odvisnost od enega samega dobavitelja. K diverzifikaciji energetskih poti in virov prispevajo tudi okrepljena prizadevanja na področju energije in boljše izkoriščanje domačih, zlasti obnovljivih virov energije.

Na področju jedrske varnosti Komisija dejavno, zlasti prek delavnic z nacionalnimi in regulativnimi organi, podpira dosledno in učinkovito izvajanje direktive o jedrski varnosti in direktive o temeljnih varnostnih standardih, ki ju morajo države članice prenesti do leta 2017 oziroma 2018. Poleg tega program za raziskave in usposabljanje Evropske skupnosti za atomsko energijo prispeva k večji jedrski varnosti.

Varnost prometa in oskrbovalne verige

Ukrep 7: Komisija bo spremljala nastajajoče grožnje v prometnem sektorju in bo po potrebi posodobila zadevno zakonodajo. Pri izvajanju strategije EU za pomorsko varnost ter strategije in akcijskega načrta EU za obvladovanje tveganja na carinskem področju bosta Komisija in visoki predstavnik (v okviru svojih pristojnosti) v sodelovanju z državami članicami preučila, kako se odzvati na hibridne grožnje, zlasti tiste, povezane s kritično prometno infrastrukturo.

Komisija v skladu s sporočilom o varnostni uniji omogoča lažje ocene varnostnih tveganj na ravni EU z državami članicami, Obveščevalnim in situacijskim centrom EU in ustreznimi agencijami za ugotavljanje groženj za varnost prometa ter podporo oblikovanju učinkovitih in sorazmernih ukrepov za zmanjšanje tveganja. Pri sestrelitvi letala družbe Malaysia Airlines na letu MH17 leta 2014 nad vzhodno Ukrajino se je pokazalo, kako veliko je tveganje pri preletu konfliktnih območij. V skladu s priporočili projektne skupine na visoki ravni o konfliktnih območjih¹¹ je Komisija ob podpori nacionalnih strokovnjakov za letalstvo in varnost ter Evropske službe za zunanje delovanje (ESZD) oblikovala metodologijo „skupne ocene tveganja EU“, ki omogoča izmenjavo tajnih podatkov in opredelitev skupne slike tveganja. Na podlagi rezultatov skupne ocene tveganja EU je Evropska agencija za varnost v letalstvu (EASA) marca 2017 izdala prvi informacijski bilten o konfliktnih območjih¹². Komisija preučuje možnost, da bi dejavnosti ocene tveganja, opravljene na področju varovanja v letalstvu, razširili na druge vrste prometa (npr. železniški in pomorski promet), predlogi pa bodo podani leta 2018. Komisija, ESZD in države članice so junija 2017 začele izvajati oceno tveganja na področju varnosti na železnicah, da bi ugotovile vrzeli in možne ukrepe za zmanjšanje tveganj.

V zvezi z varovanjem v letalstvu in upravljanjem zračnega prometa je bilo precej narejenega tudi v projektih varnostnih raziskav v sedmem okvirnem programu in programu Obzorje 2020. Na področju civilnega letalstva Komisija skupaj z Evropsko agencijo za varnost v letalstvu in zainteresiranimi stranmi pripravlja dve novi pobudi za okrepitev kibernetike

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>

varnosti, ki bi pripomogli tudi k obvladovanju hibridnih groženj: vzpostavitev skupine za odzivanje na računalniške grožnje v letalstvu in ustanovitev projektne skupine za kibernetisko varnost v skupnem podjetju SESAR, odgovornem za upravljanje zračnega prometa na enotnem evropskem nebu. Evropska obrambna agencija zagotavlja vojaške podatke glede kibernetiske varnosti v letalstvu skupnemu podjetju SESAR, pa tudi Evropski agenciji za varnost v letalstvu prek evropske platforme za strateško koordinacijo na področju kibernetiske varnosti, ki bo na zahtevo držav članic in industrije pomagala pri usklajevanju vseh dejavnosti v letalstvu na ravni EU. Evropska agencija za varnost v letalstvu je leta 2016 v skladu z načrtom za kibernetisko varnost v letalstvu analizirala vrzeli v obstoječih pravilih, zlasti v opredelitvi in ustanovitvi evropskega centra za kibernetisko varnost v letalstvu; ta center zdaj že deluje in sodeluje s Skupino za odzivanje na računalniške grožnje-EU (CERT-EU) (memorandum o soglasju je bil podpisan februarja 2017), ki pripravlja analize groženj v letalstvu, ter z Eurocontrolom (sprejet je bil časovni načrt za sodelovanje), vzpostavljena pa je bila tudi spletna stran za razširjanje analiz iz odprtih virov. Do jeseni 2017 bosta sprejeta program standardizacije in zaščiteni izmenjavi podatkov.

Obvladovanje tveganja na carinskem področju

S carinskega vidika se Komisija osredotoča na znatno nadgradnjo predhodnih informacij o tovoru in sistema za obvladovanje tveganja na carinskem področju. To zajema carinska tveganja v celotnem obsegu, tudi glede groženj za varnost in celovitost mednarodnih dobavnih verig ter za ustrezne kritične infrastrukture (npr. neposredne grožnje za objekte v morskih pristaniščih, na letališčih ali kopenskih mejah, ki jih povzroča uvoz). Cilj nadgradnje je, da bi carinski organi EU dobivali od trgovcev vse potrebne informacije o pretoku blaga; da bi si te informacije lahko učinkoviteje izmenjevali med državami članicami; da bi uporabljali skupna pravila o tveganju ter posebna pravila držav članic o tveganju; da bi se lahko ob okrepljenem sodelovanju z drugimi organi, zlasti agencijami za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter varnostnimi agencijami, učinkoviteje usmerili v tvegane pošiljke. Razvoj IT, potreben za izvedbo te nadgradnje s strani Komisije, je trenutno v začetni fazi, ustrezne naložbe na osrednji ravni pa bodo izvedene v prihodnjih mesecih.

Vesolje

Ukrep 8: Komisija bo v okviru prihodnje vesoljske strategije in evropskega obrambnega akcijskega načrta predlagala povečanje odpornosti vesoljske infrastrukture proti hibridnim grožnjam, zlasti z morebitno razširitvijo obsega nadzora in spremljanja v vesolju, da bi ta zajel tudi hibridne grožnje, pripravami za naslednjo generacijo vladnih satelitskih komunikacij (GovSatCom) na evropski ravni in uvedbo sistema Galileo za kritične infrastrukture, ki so odvisne od časovne sinhronizacije.

Komisija bo pri pripravi naslednjega regulativnega okvira o vladnih satelitskih komunikacijah (GovSatCom) ter nadzoru in spremljanju v vesolju leta 2018 v svojo oceno vključila vidike odpornosti proti hibridnim grožnjam. V skladu z vesoljsko strategijo bo pri pripravi razvoja sistemov Galileo in Copernicus ocenila, kakšne so možnosti, da bi ti storitvi pomagali zmanjšati ranljivost kritičnih infrastruktur. Ocenjevalno poročilo bi moralo biti pripravljeno jeseni 2017, predlog za naslednjo generacijo sistemov Copernicus in Galileo pa 2018. Evropska obrambna agencija se ukvarja s skupnimi projekti za razvoj zmogljivosti na področju vesoljskih komunikacij, določanja položaja v vojaške namene, navigacije in določanja časa ter opazovanja Zemlje. V ospredju vseh projektov bodo zahteve za odpornost glede na sedanje in nastajajoče hibridne grožnje.

Obrambne zmogljivosti

Ukrep 9: *Visoki predstavnik bo, po potrebi ob podpori držav članic, skupaj s Komisijo predlagal projekte za možne načine prilagoditve obrambnih zmogljivosti in njihovega razvoja s pomenom za EU, zlasti za preprečevanje hibridnih groženj proti državi članici ali več državam članicam.*

Evropska obrambna agencija je v letih 2016 in 2017 skupaj s strokovnjaki iz Komisije, ESZD in držav članic izvedla tri simulacijske vaje s scenariji hibridnih groženj. Njihove ugotovitve bodo uporabljene pri pregledu načrta za razvoj zmogljivosti, tako da bo razvoj potrebnih ključnih zmogljivosti za preprečevanje hibridnih groženj, ki bo sledil, vključen v nove prednostne naloge razvoja zmogljivosti EU. Pri pregledu kataloga zahtev iz leta 2005 bo upoštevana razsežnost hibridnih groženj. Evropska obrambna agencija je aprila 2017 dokončala poročilo o analizi vojaških posledic hibridnih groženj za kritično pristaniško infrastrukturo, o katerem bo potekala razprava na delavnici s strokovnjaki za pomorstvo oktobra 2017. Druga posebna analiza vojaške vloge v zvezi z obrambo pred malimi droni je predvidena za leto 2018. Poleg tega bi bile z letom 2019 prednostne naloge na področju zmogljivosti za krepitev odpornosti pred hibridnimi grožnjami, ki so jih ugotovile države članice, lahko upravičene do podpore v okviru Evropskega obrambnega sklada. Komisija poziva zakonodajalca, da zagotovi hitro sprejetje, države članice pa, da podajo predloge za projekte zmogljivosti za krepitev odpornosti EU pred hibridnimi grožnjami.

Ukrep 10: *Komisija bo v sodelovanju z državami članicami izboljšala ozaveščenost o hibridnih grožnjah in odpornost proti njim v okviru obstoječih mehanizmov pripravljenosti in usklajevanja, zlasti Odbora za zdravstveno varnost.*

Da bi izboljšali pripravljenost in odpornost proti hibridnim grožnjam, tudi z gradnjo zmogljivosti znotraj zdravstvenih in prehranskih sistemov, Komisija podpira države članice z usposabljanjem, simulacijskimi vajami, omogočanjem lažje izmenjave smernic z izkušnjami in financiranjem skupnih ukrepov. Te dejavnosti omogočata zlasti okvir EU za zdravstveno varnost o resnih čezmejnih nevarnostih za zdravje in program javnega zdravja za izvajanje Mednarodnega zdravstvenega pravilnika, zakonodajnega stebrja, ki je zavezujoč za 196 držav vključno z državami članicami in katerega cilj je preprečevanje resnih čezmejnih nevarnosti za zdravje ter odziv nanje po vsem svetu. Komisija bo medsektorsko pripravljenost in odziv v zdravstvenem sektorju preskusila jeseni 2017 z izvedbo vaje o kompleksnih, večrazsežnostnih hibridnih grožnjah. Komisija in države članice pripravljajo skupni ukrep o cepljenju, vključno z napovedjo ponudbe cepiva in povpraševanja po njem ter raziskavami inovativnih postopkov za proizvodnjo cepiva, da bi zagotovila zanesljivejšo oskrbo s cepivom in izboljšala zdravstveno varnost na ravni EU (2018–2020). Komisija poleg tega sodeluje z Evropsko agencijo za varnost hrane in Evropskim centrom za preprečevanje in obvladovanje bolezni, da bi se prilagodila naprednim tehnikam znanstvenega raziskovanja, s katerimi bi lahko natančneje odkrivala nevarnosti za zdravje in ugotavljala njihov izvor ter tako lažje obvladovala izbruhe v zvezi z varnostjo hrane. Ustanovila je omrežje financiranih raziskav – globalno raziskovalno sodelovanje za pripravljenost na nalezljive bolezni – za usklajen raziskovalni odziv v 48 urah od vsakega hujšega izbruha.

Ukrep 11: *Komisija poziva države članice, naj kot prednostno nalogo vzpostavijo in v celoti izkoristijo mrežo med 28 nacionalnimi skupinami za odzivanje na računalniško varnostjo povezane incidente (CSIRT) in skupino za odzivanje na računalniške grožnje (CERT-EU) ter tudi okvir za strateško sodelovanje. Komisija mora skupaj z državami članicami zagotoviti, da so sektorske pobude glede kibernetičnih groženj (npr. letalstvo, energija, pomorstvo) skladne s medsektorskimi zmogljivostmi iz direktive o varnosti omrežij in informacij za združevanje informacij, strokovnega znanja in hitro odzivanje.*

Ob nedavnih kibernetičkih napadih z uporabo izsiljevalskega programja in zlonamerne programske opreme, ki so onespobili na tisoče računalniških sistemov po vsem svetu, se je znova pokazalo, kako nujno je okrepiti kibernetičsko odpornost in varnostne ukrepe v EU. Kot je bilo napovedano v vmesnem pregledu enotnega digitalnega trga, Komisija in visoka predstavnica zdaj pregledujeta strategijo Evropske unije za kibernetičsko varnost iz leta 2013, zlasti s sprejetjem svežnja, predvidenega za september 2017. Njegov cilj bo učinkovitejši medsektorski odziv na te grožnje, ki bi okrepil zaupanje v digitalno družbo in gospodarstvo. Pregledan bo tudi mandat Agencije Evropske unije za varnost omrežij in informacij (ENISA), da bi opredelili njeno vlogo v spremenjenem okolju kibernetičske varnosti. Evropski svet¹³ je pozdravil namero Komisije, da pregleda strategijo za kibernetičsko varnost.

Sprejetje direktive o omrežjih in informacijskih sistemih (NIS)¹⁴ julija 2016 je bilo pomemben korak v smeri zagotavljanja odpornosti na področju kibernetičske varnosti na evropski ravni. Direktiva določa prva pravila kibernetičske varnosti, ki veljajo za vso Evropo, izboljšuje zmogljivosti kibernetičske varnosti in krepi sodelovanje med državami članicami. Določa tudi, da morajo podjetja v kritičnih sektorjih sprejeti primerne varnostne ukrepe in resne kibernetičske incidente prijaviti ustreznemu nacionalnemu organu. Med temi sektorji so infrastruktura za energijo, promet, oskrba z vodo, zdravstvo, bančništvo in finančni trg. Podobne ukrepe bodo morale sprejeti tudi spletne tržnice, storitve računalništva v oblaku in spletni iskalniki. Dosledno izvajanje v različnih sektorjih in čezmejno izvedbo bo zagotovila skupina za sodelovanje na področju omrežnih informacijskih storitev, ki jo je Komisija ustanovila leta 2016 in katere naloga je preprečevati drobljenje trga. V zvezi s tem se direktiva o omrežnih in informacijskih sistemih šteje za referenčni okvir za sektorske pobude na področju kibernetičske varnosti. Poleg tega se z Direktivo vzpostavlja mreža skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT), v kateri so zbrane vse ustrezne zainteresirane strani. Vzporedno s tem Komisija in CERT-EU dejavno spremljata razmere na področju kibernetičkih groženj in izmenjujeta informacije z nacionalnimi organi, da bi zagotovila, da bodo sistemi informacijske tehnologije institucij EU varni in odporni proti kibernetičskemu napadu. Prvo priložnost za operativno izmenjavo informacij in sodelovanje v smislu posredovanja nasvetov je mreža dobila maja 2017 ob incidentu z izsiljevalskim programjem WannaCry. Skupina EU za odzivanje na računalniške grožnje je bila prav tako v tesnem stiku z Evropskim centrom za boj proti kibernetičski kriminaliteti (EC3) pri Europolu, skupinami za odzivanje na incidente na področju računalniške varnosti (CSIRT) v prizadetih državah, enotami za kibernetičsko kriminaliteto in ključnimi partnerji iz industrije, da bi ublažila grožnjo in pomagala žrtvam. Izmenjava nacionalnih poročil o stanju je omogočila situacijsko zavedanje po vsej EU. S temi izkušnjami je bila mreža bolje pripravljena na naslednje incidente (npr. „NonPetya“). Ugotovljenih je bilo tudi več izzivov, ki se sedaj rešujejo.

Ukrep 12: Komisija bo skupaj z državami članicami v okviru pogodbenega javno-zasebnega partnerstva za kibernetičsko varnost sodelovala z industrijo, da se razvijejo in preskusijo tehnologije za boljšo zaščito uporabnikov in infrastruktur pred kibernetičskimi vidiki hibridnih groženj.

Ob usklajevanju z državami članicami je Komisija julija 2016 z industrijo podpisala pogodbeno javno-zasebno partnerstvo (cPPP) za kibernetičsko varnost, s katerim vlaga do 450

¹³ Sklepi Evropskega sveta z dne 22–23. junija 2017.

¹⁴ Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, UL L 194, 19.7.2016, str. 1.

milijonov EUR iz programa EU za raziskave in inovacije Obzorje 2020 za razvoj in preskušanje tehnologij za boljšo zaščito uporabnikov in infrastruktur pred kibernetскими in hibridnimi grožnjami. Rezultat partnerstva je prvi vseevropski strateški raziskovalni program, v ospredju katerega je krepitev odpornosti kritične infrastrukture ter državljanov pred kibernetскими napadi. Partnerstvo je okrepilo sodelovanje med zainteresiranimi stranmi in s tem omogočilo učinkovitejše in uspešnejše financiranje kibernetiske varnosti v okviru programa Obzorje 2020. V partnerstvu poteka vzporedno delo v zvezi s certificiranjem informacijske in komunikacijske tehnologije z vidika kibernetiske varnosti ter reševanjem hudega pomanjkanja strokovnjakov, usposobljenih za kibernetisko varnost, na trgu. Zaradi velikih potreb po civilnih raziskavah in visoki stopnji odpornosti, ki je potrebna v obrambi, skupina za kibernetiske raziskave in tehnologijo pri Evropski obrambni agenciji prispeva k področjem raziskav, ki jih je ugotovila Evropska organizacija za kibernetisko varnost v svojem strateškem programu za raziskave in inovacije.

Ukrep 13: Komisija bo izdala smernice za lastnike pametnih omrežij za izboljšanje kibernetiske varnosti njihove infrastrukture. V okviru pobude za zasnovo trga električne energije bo Komisija proučila možnost, da bi predlagala „načrte pripravljenosti na tveganja“ ter postopkovna pravila za souporabo informacij in zagotavljanje solidarnosti med državami članicami v času krize, vključno s pravili o tem, kako preprečiti kibernetiske napade in ublažiti njihove posledice.

Komisija v energetske sektorju z vzpostavitvijo platforme za kibernetisko varnost na področju energetike pripravlja sektorsko strategijo kibernetiske varnosti, da bi izboljšala izvajanje direktive o varnosti omrežij in informacij. V študiji, izvedeni februarja 2017, so bile ugotovljene najboljše razpoložljive tehnike za okrepitev kibernetiske varnosti pametnih merilnih sistemov, ki podpirajo to platformo. Komisija je vzpostavila tudi spletno platformo „Center EU za souporabo informacij o incidentih in grožnjah“, na kateri se analizirajo in izmenjujejo informacije o kibernetiskih grožnjah in incidentih v energetske sektorju.

Povečanje odpornosti finančnega sektorja na hibridne grožnje

Ukrep 14: Komisija bo v sodelovanju z agencijo ENISA¹⁵, državami članicami, zadevnimi mednarodnimi, evropskimi in nacionalnimi organi ter finančnimi institucijami spodbujala in olajšala vzpostavitev platform in mrež za souporabo informacij o grožnjah ter obravnavala dejavnike, ki ovirajo izmenjavo takšnih informacij.

Komisija se zaveda, da so kibernetiske grožnje med glavnimi tveganji za finančno stabilnost, zato je pregledala regulativni okvir o plačilnih storitvah v Evropski uniji, ki ga je zdaj treba izvesti. Z revidirano direktivo o plačilnih storitvah¹⁶ so bile uvedene nove določbe za povečanje varnosti plačilnih instrumentov in močno avtentikacijo strank, da se zmanjšajo goljufije, zlasti pri spletnih plačilih. Novi zakonodajni okvir se bo začel uporabljati januarja 2018. Komisija zdaj s pomočjo Evropskega bančnega organa in v posvetovanju z zainteresiranimi stranmi pripravlja regulativne tehnične standarde, ki naj bi bili objavljeni do konca leta 2017, o močni avtentikaciji strank ter o skupni in varni komunikaciji za operativno zagotavljanje varnih plačilnih transakcij. Poleg tega je Komisija na mednarodni ravni tesno sodelovala s partnerji iz skupine G7 pri pripravi „Temeljnih načel skupine G7 o kibernetiski varnosti v finančnem sektorju“, ki so jih finančni ministri in guvernerji centralnih bank iz držav skupine G7 potrdili

¹⁵ Agencija Evropske unije za varnost omrežij in informacij.

¹⁶ Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu (UL L 337, 23.12.2015, str. 35).

oktobra 2016. Načela so namenjena subjektom finančnega sektorja (zasebnim in javnim) ter prispevajo k usklajenemu pristopu kibernetске varnosti znotraj finančnega sektorja, da bi skupaj reševali kibernetске grožnje, vključno z večjimi in bolj izpopolnjenimi kibernetскими grožnjami.

Promet

Ukrep 15: Komisija in visoki predstavnik bosta (v okviru svojih pristojnosti) v sodelovanju z državami članicami preučila, kako se odzvati na hibridne grožnje, zlasti tiste v zvezi s kibernetскими napadi v prometnem sektorju.

Izvajanje akcijskega načrta za evropsko strategijo pomorske varnosti¹⁷ bo pripomoglo k odpravi vrtilčkarstva pri izmenjavi informacij in souporabi sredstev med civilnimi in vojaškimi organi. Nadresorski pristop je privedel do tesnejšega sodelovanja med različnimi akterji. Skupni civilno-vojaški strateški raziskovalni program Komisije in ESZD naj bi bil zaključen do konca leta 2017 z delavnico o varovanju kritične pomorske infrastrukture. To delo bi lahko v prihodnosti razširili na nastajajoče grožnje, usmerjene v podvodne cevovode, prenos energije ter optična vlakna in tradicionalna komunikacijska kabelska omrežja, ki prihajajo zunaj nacionalnih teritorialnih voda.

V nedavni študiji¹⁸ so bile ocenjene zmogljivosti nacionalnih organov za izvedbo ocene tveganja, ki opravljajo naloge obalne straže. Ugotovljene so bile največje ovire za sodelovanje in podana praktična priporočila za okrepitev sodelovanja med pomorskimi organi na ravni EU in nacionalni ravni na tem posebnem področju. Ocena tveganja je bistvenega pomena pri preprečevanju pomorskih groženj ter ima še bolj pomembno vlogo pri ocenjevanju in preprečevanju hibridnih groženj, saj je pri njih treba upoštevati še dodatne in bolj zapletene vidike. Rezultati te študije bodo predstavljeni na različnih forumih, povezanih z obalno stražo, tako da se bodo predlagana priporočila lahko ocenila in izvedla, s čimer se bo okrepilo sodelovanje na tem področju s pripravljenostjo in odzivom na hibridne grožnje kot glavnima ciljema.

Boj proti financiranju terorizma

Ukrep 16: Komisija bo zagotovila, da bo izvajanje akcijskega načrta o financiranju terorizma prav tako prispevalo k preprečevanju hibridnih groženj.

Povzročitelji hibridnih groženj in njihovi podporniki za uresničitev svojih načrtov potrebujejo sredstva. Prizadevanja EU za boj proti financiranju kriminala in terorizma v okviru evropske agende za varnost in akcijskega načrta o financiranju terorizma lahko prav tako prispevajo k preprečevanju hibridnih groženj. Komisija je decembra 2016 predložila tri zakonodajne predloge, vključno s kazenskimi sankcijami za pranje denarja in nedovoljena gotovinska plačila ter tudi o zamrznitvi in zaplembi premoženja¹⁹.

¹⁷ https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf in drugo poročilo o izvajanju akcijskega načrta iz strategije EU za pomorsko varnost, ki je bil državam članicam predstavljen 21. junija 2017.

¹⁸ Študija o „Ocena zmogljivosti ocenjevanja tveganja na ravni organov držav članic, ki opravljajo naloge obalne straže“ (Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions), 2017, <https://ec.europa.eu/maritimeaffairs/documentation/studies>.

¹⁹ Tretje poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2016) 831 final).

Vse države članice so morale do 26. junija 2017 prenesti četrto direktivo o preprečevanju pranja denarja²⁰, julija 2016 pa je Komisija predložila ciljno usmerjen zakonodajni predlog za dopolnitev in okrepitev direktive z dodatnimi ukrepi²¹.

Komisija je 26. junija 2017 izdala oceno tveganja na nadnacionalni ravni, predvideno s četrto direktivo o preprečevanju pranja denarja. Prav tako je predložila predlog uredbe za preprečitev uvoza in skladiščenja kulturnih dobrin, ki so brez dovoljenja izvožene iz tretjih držav, v EU²². Pozneje letos bo Komisija poročala o rednem ocenjevanju potrebe po morebitnih dodatnih ukrepih za sledenje financiranju terorizma v EU. Komisija prav tako pregleduje zakonodajo o boju proti goljufijam in ponarejanju v zvezi z negotovinskimi plačilnimi sredstvi²³.

Osmo poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije vsebuje več podrobnosti o stanju izvajanja akcijskega načrta proti financiranju terorizma.

Spodbujanje skupnih vrednot EU ter vključujočih, odprtih in odpornih družb

Krepitev odpornosti proti radikalizaciji in nasilnemu ekstremizmu

Versko in ideološko radikalizacijo ter etnične in manjšinske konflikte lahko sprožijo zunanji akterji s podpiranjem določenih skupin ali s spodbujanjem konfliktov med skupinami. Pojavili so se dodatni izzivi, kot so volkovi samotarji, novi načini radikalizacije, morebiti tudi v okviru migrantske krize, ter tudi porast desničarskega ekstremizma (vključno z nasiljem proti migrantom) in nevarnost polarizacije. Čeprav se vprašanja glede radikalizacije nadalje rešujejo v okviru varnostne unije, pa so ta lahko posredno pomembna z vidika hibridnih groženj, v kolikor lahko povzročitelji hibridnih groženj manipulirajo s posamezniki, dovzetnimi za radikalizacijo.

Ukrep 17: Komisija izvaja ukrepe proti radikalizaciji, opredeljene v evropski agendi za varnost, in analizira potrebo po okrepitvi postopkov za odstranitev nezakonitih vsebin, pri čemer poziva k skrbnosti posrednikov pri upravljanju omrežij in sistemov.

Preprečevanje radikalizacije

Komisija še naprej izvaja večstranski odziv na radikalizacijo, določen v sporočilu iz junija 2016 o spodbujanju preprečevanja radikalizacije, ki vodi v nasilni ekstremizem²⁴, s ključnimi ukrepi, kot so spodbujanje vključujočega izobraževanja in skupnih vrednot, boj proti ekstremistični propagandi na spletu in radikalizaciji v zaporih, okrepitev sodelovanja s tretjimi državami in raziskav za boljše razumevanje spreminjajoče se narave radikalizacije in boljše odzive politik. Mreža za ozaveščanje o radikalizaciji je bila v ospredju prizadevanj

²⁰Direktiva (EU) 2015/849 Evropskega parlamenta in Sveta z dne 20. maja 2015 o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranje terorizma, spremembi Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta ter razveljavitvi Direktive 2005/60/ES Evropskega parlamenta in Sveta in Direktive Komisije 2006/70/ES (Besedilo velja za EGP) (UL L 141, 5.6.2015, str. 73–117).

²¹ Za več podrobnosti glej Tretje poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2016) 831 final) in Osmo poročilo o napredku v smeri učinkovite in prave Unije (COM(2017) 354 final).

²² COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.

²³ Osmo poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2017) 354 final).

²⁴ http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

Komisije za podporo državam članicam na tem področju, pri čemer je sodelovala z lokalnimi izvajalci na ravni skupnosti. Več podrobnosti je na voljo v Osmem poročilu o napredku v smeri učinkovite in prave Unije²⁵.

Radikalizacija in sovražni govor na spletu

Komisija je v skladu z evropsko agendo za varnost²⁶ sprejela ukrepe za zmanjševanje dostopnosti nezakonitih vsebin na spletu, zlasti z Europolovo enoto EU za prijavljanje internetnih vsebin in forumom EU o internetu²⁷. Pomemben napredek je bil dosežen tudi s kodeksom ravnanja za boj proti nezakonitemu sovražnemu govoru na spletu²⁸. Več podrobnosti je na voljo v Osmem poročilu o napredku v smeri učinkovite in prave Unije²⁹. Ti ukrepi bodo okrepljeni, tudi ob upoštevanju sklepov Evropskega sveta³⁰, vrha skupine G7³¹ in vrha skupine G20 v Hamburgu³².

Spletne platforme imajo ključno vlogo pri preprečevanju nezakonitih ali morebitno škodljivih vsebin. Komisija bo v okviru strategije za enotni digitalni trg, kot je določeno v vmesnem pregledu³³, zagotovila boljše usklajevanje dialogov s platformami s poudarkom na mehanizmi in tehničnih rešitvah za odstranjevanje nezakonitih vsebin. Po potrebi bi moral biti cilj okrepiti te mehanizme s smernicami o vidikih, kot sta prijava in odstranjevanje nezakonitih vsebin. Komisija bo pripravila tudi smernice o pravilih glede odgovornosti.

Krepitev sodelovanja s tretjimi državami

***Ukrep 18:* Visoki predstavnik bo v sodelovanju s Komisijo začel s pripravo raziskave o hibridnih grožnjah v sosednjih regijah. Visoki predstavnik, Komisija in države članice bodo uporabili instrumente, ki so jim na voljo, za krepitev zmogljivosti partnerjev in njihove odpornosti proti hibridnim grožnjam. Misije skupne varnostne in obrambne politike se lahko uporabijo samostojno ali kot dopolnitev instrumentov EU, da bi partnerjem pomagale pri krepitvi njihovih zmogljivosti.**

Evropska unija je namenila večjo pozornost krepitvi zmogljivosti in odpornosti na področju varnostnega sektorja v partnerskih državah, med drugim z vzpostavljanjem povezav med varnostjo in razvojem ter razvojem varnostne razsežnosti prenovljene evropske sosedске politike ter vzpostavitev dialogov o protiterorizmu in varnosti z državami na območju Sredozemlja. V zvezi s tem se je v sodelovanju z Republiko Moldavijo začel izvajati pilotni projekt raziskave o tveganjih. Njegov namen je pomagati ugotoviti ključne šibke točke v državi in zagotoviti, da je pomoč EU usmerjena zlasti na ta področja. Rezultati pilotnega

²⁵ COM(2017) 354 final.

²⁶ Za več podrobnosti glej Osmo poročilo o napredku v smeri učinkovite in prave varnostne Unije, COM(2017) 354 final.

²⁷ Za več podrobnosti glej Osmo poročilo o napredku v smeri učinkovite in prave varnostne Unije, COM(2017) 354 final.

²⁸ Kodeks ravnanja za boj proti nezakonitemu sovražnemu govoru na spletu, 31. maj 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

²⁹ Za več podrobnosti glej Osmo poročilo o napredku v smeri učinkovite in prave varnostne Unije, COM(2017) 354 final.

³⁰ Sklepi Sveta z dne 22. in 23. junija 2017.

³¹ Vrh skupine G7 v Taormini v Italiji, 26–27.5.2017.

³² Vrh skupine G20 v Hamburgu v Nemčiji, 7–8.7.2017.

³³ Glej zgornje Sporočilo Komisije COM(2017) 228 final.

projekta so pokazali, da se je sama raziskava izkazala za koristno. Na podlagi pridobljenih izkušenj bosta Komisija in ESZD pripravili priporočila, naj se kot prednostni opredelijo ukrepi v okviru krepitve učinkovitosti, strateških komunikacij, varovanja kritične infrastrukture in kibernetike varnosti.

V prihodnosti bi rezultati te prve raziskave lahko koristili še drugim sosednjim državam, čeprav s posebnimi prilagoditvami, ki bi upoštevale različne nacionalne in lokalne razmere in posebne grožnje ter brez podvajanja z dialogi o protiterorizmu in varnosti, ki že potekajo. Poleg tega sta Komisija in visoka predstavnica 7. junija 2017 sprejeli skupno sporočilo z naslovom *Strateški pristop k odpornosti pri zunanjem delovanju EU*³⁴. Cilj je podpreti partnerske države, da postanejo odpornejše na današnje globalne izzive. Priznava se, da je treba z omejevanja krize preiti na bolj strukturiran in dolgoročnejši pristop k šibkim točkam, pri čemer je poudarek na predvidevanju, preprečevanju in pripravljenosti.

Kibernetika odpornost za razvoj

EU podpira države zunaj Evrope, da bi okrepile odpornost svojih informacijskih mrež. Vedno večja digitalizacija je neločljivo povezana z varnostjo, kar prinaša posebne izzive za odpornost sistemov informacijskih mrež na svetovni ravni, saj kibernetični napadi ne poznajo meja. EU podpira tretje države, da okrepijo svoje zmožnosti za ustrezno preprečevanje nepredvidenih napak in kibernetičnih napadov ter odzivanje nanje. Komisija bo po pilotnem projektu za kibernetično varnost v nekdanji jugoslovanski republiki Makedoniji, na Kosovu³⁵ in Moldaviji, ki je bil izveden leta 2016, vzpostavila nov program za okrepitev kibernetike odpornosti v tretjih državah, zlasti v Afriki in Aziji v obdobju 2017–2020 ter tudi v Ukrajini. Njegov cilj je povečati varnost in pripravljenost kritične informacijske infrastrukture in mrež v tretjih državah na podlagi naresorskega pristopa, pri čemer se zagotavlja spoštovanje človekovih pravic in pravne države.

Varovanje v letalstvu

Civilno letalstvo je za teroriste še vedno pomemben in simbolični cilj, vendar je lahko tarča tudi v okviru hibridne kampanje. EU je sicer oblikovala zanesljiv okvir varovanja v letalstvu, vendar so leti iz tretjih držav lahko bolj ogroženi. Komisija v skladu z resolucijo Varnostnega sveta OZN 2309 (2016) povečuje svoja prizadevanja za krepitev zmogljivosti v tretjih državah. Januarja 2017 je objavila novo celostno oceno tveganja, da se zagotovi prednostno razvrščanje in usklajevanje prizadevanj za krepitev zmogljivosti, ki se izvajajo na ravni EU in držav članic ter tudi z mednarodnimi partnerji. Leta 2016 je začela izvajati štiriletni projekt za varnost civilnega letalstva v Afriki in na Arabskem polotoku za boj proti grožnji terorizma v civilnem letalstvu. Projekt se osredotoča na izmenjavo strokovnega znanja med partnerskimi državami in strokovnjaki iz držav članic Evropske konference civilnega letalstva ter dejavnosti mentorstva, usposabljanja in svetovanja. Dejavnosti bodo dodatno okrepljene v letu 2017.

³⁴Skupno sporočilo Evropskemu parlamentu in Svetu: *Strateški pristop k odpornosti pri zunanjem delovanju EU*, JOIN(2017) 21 final.

³⁵ To poimenovanje ne posega v stališča glede statusa ter je v skladu z RVSN 1244 in mnenjem Meddržavnega sodišča o razglasitvi neodvisnosti Kosova.

c. PREPREČEVANJE KRIZ, ODZIVANJE NANJE IN OKREVANJE

Čeprav je posledice mogoče zmanjšati z dolgoročnimi politikami na nacionalni ravni in ravni EU, pa je kratkoročno bistvenega pomena, da se okrepijo sposobnosti držav članic in Unije za preprečevanje hibridnih groženj, odzivanje nanje in okrevanje na hiter in usklajen način. Hiter odziv na dogodke, ki so posledica hibridnih groženj, je ključnega pomena. V zadnjem letu je bil na tem področju dosežen velik napredek in tako je v EU zdaj vzpostavljen operativni protokol, ki določa postopek za krizno upravljanje v primeru hibridnega napada. V prihodnosti se bo izvajalo redno spremljanje in izvajanje.

Ukrep 19: Visoki predstavnik in Komisija bosta v sodelovanju z državami članicami vzpostavila skupni operativni protokol in izvajala redne dejavnosti za izboljšanje sposobnosti strateškega odločanja v odziv na zapletene hibridne grožnje na podlagi kriznega upravljanja in postopkov enotnega političnega odzivanja na krize.

V skupnem okviru je bila priporočena vzpostavitev mehanizmov za hitro odzivanje na dogodke, ki so posledica hibridnih groženj, da se uskladijo mehanizmi EU za odzivanje³⁶ in sistemi zgodnjega opozarjanja. V ta namen so službe Komisije in ESZD izdali operativni protokol EU za preprečevanje hibridnih groženj (EU Playbook)³⁷, ki opredeljuje načine za usklajevanje, združevanje in analizo obveščevalnih podatkov, vzpostavitev postopkov oblikovanja politik, vaje in usposabljanja ter sodelovanje s partnerskimi organizacijami, zlasti Natom, v primeru hibridnih groženj. Podobno je Nato razvil operativni protokol za okrepljeno sodelovanje med EU in Natom pri preprečevanju in boju proti hibridnim grožnjam na področjih kibernetске obrambe, strateškega komuniciranja, situacijskega zavedanja in kriznega upravljanja. Operativni protokol EU za preprečevanje hibridnih groženj bo preizkušen jeseni 2017 v okviru vzporednih in usklajenih vaj Evropske unije, ki vključuje sodelovanje z Natom.

Ukrep 20: Komisija in visoki predstavnik bosta v okviru svojih pristojnosti proučila uporabnost in praktične posledice člena 222 PDEU in člena 42(7) PEU v primeru obsežnega in resnega hibridnega napada.

V členu 42(7) PEU je omenjen oboroženi napad na ozemlje države članice, medtem ko se člen 222 PDEU (solidarnostna klavzula) sklicuje na teroristični napad, naravno nesrečo in nesrečo, ki jo je povzročil človek, na ozemlju države članice. Uporaba slednjega je bolj verjetna v primeru hibridnih napadov, ki so kombinacija kaznivih/subverzivnih dejanj. Z uveljavitvijo solidarnostne klavzule se začne postopek usklajevanja na ravni Sveta (enotno politično odzivanje na krize, IPCR) in sodelovanje z ustreznimi institucijami, agencijami in organi EU ter izvajanje programov in mehanizmov pomoči EU. Sklep Sveta 2014/415/EU določa načine izvajanja solidarnostne klavzule s strani Unije. Ti načini uporabe ostajajo v veljavi in ni potrebe po reviziji Sklepa Sveta. Če hibridni napad vključuje oboroženi napad, je mogoče tudi sklicevanje na člen 42(7). V takem primeru pomoč in podporo zagotovijo države članice in tudi EU. Komisija in visoka predstavnica bosta še naprej ocenjevala najučinkovitejše načine za obravnavanje takih napadov.

Sprejetje navedenega operativnega protokola EU neposredno podpira to oceno, ki se bo izvajala v okviru vzporednih in usklajenih vaj EU (PACE – Parallel and Coordinated

³⁶ Ureditve EU enotnega političnega odzivanja na krize (IPCR – Integrated Political Crisis Response) Sveta, sistem Komisije ARGUS ter krizno upravljanje in odzivanje ESZD.

³⁷ Delovni dokument služb Komisije (2016) 227, sprejet 7. julija 2016.

Exercise) oktobra 2017. S to vajo bodo preizkušeni različni mehanizmi EU in sposobnost medsebojnega sodelovanja, da se pospeši sprejemanje odločitev, kadar dvoumnost, ki je posledica hibridnih groženj, zmanjšuje jasnost.

Ukrep 21: Visoki predstavnik bo v sodelovanju z državami članicami vključil, izkoristil in uskladi zmogljivosti vojaškega ukrepanja pri preprečevanju hibridnih groženj v okviru skupne varnostne in obrambne politike.

Kot odziv na pooblastitev za vključevanje vojaških zmogljivosti v podporo skupne zunanje in varnostne politike ter skupne varnostne in obrambne politike ter po seminarju z vojaškimi strokovnjaki decembra 2016 in smernicah Delovne skupine Vojaškega odbora iz maja 2017 je bilo julija dokončano vojaško svetovanje o „vojaškem prispevku EU k preprečevanju hibridnih groženj v okviru skupne varnostne in obrambne politike“, ki se bo nadaljevalo v okviru izvedbenega načrta razvoja konceptov.

d. SODELOVANJE MED EU IN NATOM

Ukrep 22: Visoki predstavnik bo v sodelovanju s Komisijo nadaljeval z neuradnim dialogom ter okrepil sodelovanje in usklajevanje z Natom v zvezi s situacijskim zavedanjem, strateškimi komunikacijami, kibernetko varnostjo ter preprečevanjem kriz in odzivanjem nanje, da se preprečijo hibridne grožnje, pri čemer je treba upoštevati načeli vključenosti in avtonomnosti obeh organizacij pri sprejemanju odločitev.

Na podlagi skupne izjave, ki sta jo podpisala predsednika Evropskega sveta in Evropske komisije skupaj z generalnim sekretarjem zveze Nato v Varšavi 8. julija 2016 sta EU in Nato razvila skupen sklop 42 predlogov za izvajanje, ki sta jih Svet EU in Svet Nata pozneje potrdila v ločenih, vendar vzporednih postopkih 6. decembra 2016³⁸. Junija 2017 sta visoka predstavnica/podpredsednik in generalni sekretar Nata objavila poročilo o splošnem napredku pri 42 ukrepih iz skupne izjave. Preprečevanje hibridnih groženj je eno od sedmih področij sodelovanja, navedenih v skupni izjavi, in predstavlja deset od 42 ukrepov. Poročilo kaže, da so skupna prizadevanja v zadnjem letu prinesla vidne rezultate. Navedeni so bili že številni posebni ukrepi, namenjeni preprečevanju hibridnih groženj, vključno z Evropskim centrom odličnosti za preprečevanje hibridnih groženj, boljšim situacijskim zavedanjem, vzpostavitev hibridne fuzijske celice EU in njenega sodelovanja z novo ustanovljeno celico Nata za hibridno analizo ter sodelovanjem med skupinami za strateško komuniciranje. Osebe Nata in EU bo prvič sodelovalo pri izvajanju svojega odziva na hibridni scenarij. S to vajo naj bi preverili izvajanje več kot tretjine skupnih predlogov. EU bo letos izvedla svojo vzporedno in usklajeno vajo ter se pripravlja, da bo leta 2018 prevzela vodilno vlogo.

Glede odpornosti je osebje EU in Nata vključeno v vzajemno poročanje, med drugim o mehanizmu EU za enotno politično odzivanje na krize. Redni stiki med osebjem Nata in EU, vključno s sodelovanjem v delavnicah in v Natu ali v usmerjevalnem odboru Evropske obrambne agencije, so omogočili izmenjavo informacij o osnovnih zahtevah Nata za nacionalno odpornost. Nadaljnje sodelovanje med Komisijo in Natom za krepitev odpornosti je načrtovano za jesen. V naslednjem poročilu o napredku pri sodelovanju med EU in Natom bodo podane možnosti za razširitev sodelovanja med organizacijama.

³⁸ <http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/>

3. ZAKLJUČEK

V skupnem okviru so opisani ukrepi za pomoč pri preprečevanju hibridnih groženj ter izboljšanje odpornosti na ravni EU in na nacionalni ravni ter izboljšanje odpornosti za partnerje. Čeprav Komisija in visoka predstavnica uspešno ukrepata na vseh področjih v tesnem sodelovanju z državami članicami in partnerji, je bistvenega pomena, da se ta zagon ohrani in prilagodi novim in neprestano spreminjajočim se hibridnim grožnjam. Države članice so v prve v vrsti, ki so odgovorne za prepričevanje hibridnih groženj, povezanih z nacionalno varnostjo ter vzdrževanjem javnega reda in miru. Nacionalno odpornost in skupna prizadevanja za zaščito pred hibridnimi grožnjami je treba razumeti kot elemente, ki se medsebojno krepijo in so del istega skupnega prizadevanja. Države članice zato spodbujamo, naj čim prej izvedejo raziskave o hibridnih grožnjah, saj bodo te zagotovile dragocene informacije o obsegu ranljivosti in pripravljenosti v Evropi. Možnosti hibridne fuzijske celice EU bi bilo treba kar najbolj izkoristiti ter pri tem graditi na pomembnem napredku pri ozaveščanju. Visoka predstavnica poziva države članice, naj podprejo dejavnosti projektne skupine za strateško komuniciranje, da bodo učinkovitejše pri preprečevanju porasta hibridnih groženj. EU bo v celoti podpirala Evropski center za preprečevanje hibridnih groženj, ki ga vodi Finska.

Edinstvena prednost EU je v pomoči državam članicam in partnerjem pri krepitvi odpornosti, za kar so ji na razpolago številni obstoječi instrumenti in programi. Velik napredek je bil dosežen pri ukrepih za krepitev odpornosti na področjih, kot so promet, energija, kibernetska varnost, kritična infrastruktura, zaščita finančnega sistema pred nezakonito uporabo ter prizadevanja za preprečevanje nasilnega ekstremizma in radikalizacije. Ukrepi EU za krepitev odpornosti se bodo še naprej izvajali, saj se narava hibridnih groženj spreminja. Zlasti bo EU razvila kazalnike za izboljšanje zaščite in odpornosti kritične infrastrukture pred hibridnimi grožnjami v relevantnih sektorjih.

Iz evropskega obrambnega sklada in s pomočjo držav članic so lahko sofinancirane prednostne naloge na področju zmogljivosti za krepitev odpornosti pred hibridnimi grožnjami. S prihodnjim svežnjem o kibernetski varnosti in tudi medsektorskimi ukrepi, katerih cilj je izvajanje direktive o varnosti omrežij in informacij, bodo zagotovljene nove platforme za preprečevanje hibridnih groženj po vsej EU.

Komisija in visoka predstavnica pozivata države članice in zainteresirane strani, naj na področjih, na katerih je potrebno, dosežejo hiter dogovor ter zagotovijo hitro in učinkovito izvajanje številnih ukrepov, predstavljenih v tem sporočilu, katerih cilj je krepitev odpornosti. EU bo nadaljevala in poglobila že zdaj plodno sodelovanje z Natom.

Unija se še naprej zavezuje, da bo uporabila vse ustrezne instrumente EU za reševanje vprašanja zapletenih hibridnih groženj. Podpora prizadevanjem držav članic ostaja prednostna naloga Unije, ki skupaj s svojimi ključnimi partnerji deluje kot močnejši in odzivnejši zagotavljelec varnosti.