EVROPSKA
KOMISIJA

VISOKI PREDSTAVNIK
UNIJE ZA ZUNANJE
ZADEVE IN
VARNOSTNO POLITIKO

Bruselj, 6.4.2016
JOIN(2016) 18 final

SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU IN SVETU

Skupni okvir o preprečevanju hibridnih groženj –

odziv Evropske unije

1. UVOD

V zadnjih letih se je varnostno okolje v Evropski uniji drastično spremenilo. Ključni izzivi za mir in stabilnost v vzhodnem in južnem sosedstvu EU še naprej opozarjajo, da se mora Unija prilagoditi in okrepiti svojo vlogo izvajalca varnostnih storitev, z močnim poudarkom na tesni povezanosti med zunanjo in notranjo varnostjo. Dandanes so mir, varnost in blaginja postavljeni pred preizkušnjo, razlog za to pa so velikokrat nestabilne razmere v neposrednem sosedstvu EU in spreminjajoče se oblike groženj. Predsednik Evropske komisije Jean-Claude Juncker je leta 2014 v svojih političnih usmeritvah poudaril, da „si moramo prizadevati za močnejšo vlogo Evrope v varnostnih in obrambnih zadevah“ ter za združevanje evropskih in nacionalnih instrumentov na bolj učinkovit način kot v preteklosti. Visoki predstavnik se je na podlagi tega in poziva Sveta za zunanje zadeve z dne 18. maja 2015 v tesnem sodelovanju s službami Komisije in Evropsko obrambno agencijo ter ob posvetovanju z državami članicami EU lotil priprave skupnega okvira z izvedljivimi predlogi za pomoč pri preprečevanju hibridnih groženj in izboljšanje odpornosti EU in držav članic ter partnerjev[1]. Evropski svet je junija 2015 opozoril, da je treba za pomoč pri preprečevanju hibridnih groženj uporabiti instrumente EU[2].

Čeprav se opredelitve hibridnih groženj razlikujejo in morajo ostati prilagodljive, da se lahko odzovejo na njihovo spremenljivo naravo, naj bi pojem zajemal kombinacijo prisilnih in subverzivnih dejavnosti, konvencionalnih in nekonvencionalnih metod (npr. diplomatskih, vojaških, gospodarskih, tehnoloških), ki jih državni in nedržavni akterji lahko usklajeno uporabljajo za doseganje posebnih ciljev, pri čemer razmere ne dosežejo praga za uradno razglasitev vojne. Ponavadi je poudarek na izkoriščanju ranljivosti tarče in ustvarjanju dvoumnosti, da se ovirajo procesi odločanja. Obsežne dezinformativne kampanje, uporaba družbenih medijev za nadzor politične pripovedi ali za radikalizacijo, novačenje in usmerjanje proksi akterjev so lahko sredstva za hibridne grožnje.

Kolikor se preprečevanje hibridnih groženj nanaša na nacionalno varnost in obrambo ter vzdrževanje javnega reda in miru, so zanj v prvi vrsti odgovorne države članice, saj je večina nacionalnih ranljivosti omejena na posamezne države. Vendar se številne države članice EU soočajo z enakimi grožnjami, ki so lahko usmerjene tudi v čezmejne mreže ali infrastrukture. Tovrstne grožnje se lahko učinkoviteje obravnava z usklajenim odzivom na ravni EU s politikami in instrumenti EU ter tako gradi na evropski solidarnosti, vzajemni pomoči in polnem potencialu Lizbonske pogodbe. Politike in instrumenti EU lahko in v večji meri tudi že imajo ključno vlogo pri dodatni krepitvi ozaveščenosti. S tem se veča odpornost držav članic pri odzivanju na skupne grožnje. Zunanje delovanje Unije, predlagano s tem okvirom, temelji na načelih, določenih v členu 21 Pogodbe o Evropski uniji (PEU), kot so demokracija, pravna država,

[1] Sklepi Sveta na področju skupne varnostne in obrambne politike (SVOP), maj 2015 [Consilium 8971/15].
[2] Sklepi Evropskega sveta, junij 2015 [EUCO 22/15].

univerzalnost in nedeljivost človekovih pravic ter spoštovanje načel Ustanovne listine Združenih narodov in mednarodnega prava[3].

Cilj tega skupnega sporočila je spodbujati celosten pristop, da bo EU v sodelovanju z državami članicami lahko preprečevala zlasti grožnje hibridne narave z ustvarjanjem sinergij med vsemi ustreznimi instrumenti ter spodbujanjem tesnega sodelovanja med vsemi zadevnimi akterji[4]. Ukrepi nadgrajujejo obstoječe strategije in sektorske politike, ki prispevajo k večji varnosti. Zlasti evropska agenda za varnost[5], prihodnja globalna strategija EU za zunanjo in varnostno politiko ter evropski obrambni akcijski načrt[6], strategija EU za kibernetsko varnost[7], strategija za energetsko zanesljivost[8] in strategija Evropske unije za pomorsko varnost[9] so orodja, ki bi prav tako lahko prispevala k preprečevanju hibridnih groženj.

Ker je tudi Nato dejaven na področju preprečevanja hibridnih groženj, Svet za zunanje zadeve pa je predlagal okrepitev sodelovanja in usklajevanja na tem področju, so nekateri predlogi namenjeni izboljšanju sodelovanja med EU in Natom pri preprečevanju hibridnih groženj.

Predlagani odziv se osredotoča na naslednje elemente: izboljšanje ozaveščenosti, krepitev odpornosti, preprečevanje, odzivanje na krizne razmere in okrevanje.

2. PREPOZNAVANJE HIBRIDNE NARAVE GROŽNJE

Cilj hibridnih groženj je izkoristiti ranljivosti države in pogosto tudi spodkopati temeljne demokratične vrednote in svoboščine. Kot prvi korak bosta visoki predstavnik in Komisija sodelovala z državami članicami, da se s spremljanjem in ocenjevanjem tveganj, ki so lahko usmerjena v ranljivosti EU, okrepi zavedanje o situaciji. Komisija razvija metodologije za oceno varnostnega tveganja, da bi lažje obveščala nosilce odločanja in spodbujala oblikovanje politik na podlagi tveganja na področjih, ki segajo od varnosti v letalstvu do financiranja terorizma in pranja denarja. Poleg tega bi bilo ustrezno, da države članice izvedejo raziskavo, v kateri opredelijo področja, na katerih obstaja nevarnost za hibridne grožnje. Cilj bi bil opredeliti kazalnike hibridnih groženj, jih vključiti v mehanizme zgodnjega opozarjanja in obstoječe mehanizme za ocenjevanje tveganja ter jih po potrebi souporabljati.

<u>Ukrep 1</u>: Države članice, po potrebi ob podpori Komisije in visokega predstavnika, naj začnejo s pripravo raziskave o hibridnih grožnjah za opredelitev ključnih ranljivosti,

[3] Listina Evropske unije o temeljnih pravicah je za institucije EU in države članice pri izvajanju prava Unije zavezujoča.
[4] Za morebitne zakonodajne predloge bodo veljale zahteve Komisije glede boljšega pravnega urejanja v skladu s smernicami Komisije za boljše pravno urejanje (SWD(2015) 111).
[5] COM(2015) 185 final.
[6] Načrtovana za leto 2016.
[7] Okvir politike EU za kibernetsko obrambo [Consilium 15585/14] in skupno sporočilo „Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor“, februar 2013 [JOIN(2013) 1].
[8] Skupno sporočilo o evropski strategiji za energetsko varnost, maj 2014 [SWD(2014) 330].
[9] Skupno sporočilo „Za odprto in varno svetovno področje pomorstva: elementi strategije Evropske unije za pomorsko varnost“, 6.3.2014, (JOIN(2014) 9 final).

vključno s posebnimi kazalniki, povezanimi s hibridnimi grožnjami, ki lahko potencialno vplivajo na nacionalne in vseevropske strukture in mreže.

3. ORGANIZACIJA ODZIVA EU: KREPITEV OZAVEŠČENOSTI

3.1. Hibridna fuzijska celica EU

Pomembno je, da ima EU v sodelovanju s svojimi državami članicami zadostno raven zavedanja o situaciji, zato da lahko prepozna vse spremembe varnostnega okolja, povezane s hibridnimi dejavnostmi državnih in/ali nedržavnih akterjev. Za učinkovito preprečevanje hibridnih groženj je treba izboljšati izmenjavo informacij in spodbujati ustrezno souporabo obveščevalnih podatkov med sektorji ter med Evropsko unijo, njenimi državami članicami in partnerji.

Hibridna fuzijska celica EU bo zagotavljala enotno točko za analizo hibridnih groženj, vzpostavljena pa bo v okviru Obveščevalnega in situacijskega centra EU (EU INTCEN) Evropske službe za zunanje delovanje (ESZD). Ta fuzijska celica bi zbirala, analizirala in dajala v souporabo tajne podatke in podatke iz odprtih virov, ki se nanašajo posebej na kazalnike in opozorila, povezane s hibridnimi grožnjami, različnih deležnikov v okviru Evropske službe za zunanje delovanje (vključno z delegacijami EU), Komisije (z agencijami EU[10]) in držav članic. V povezavi z obstoječimi podobnimi organi na ravni EU[11] in na nacionalni ravni bi fuzijska celica analizirala zunanje vidike hibridnih groženj, ki zadevajo EU in njeno sosedstvo, da bi tako hitro preučila pomembne incidente in zagotavljala podatke za postopke strateškega odločanja EU, vključno z zagotavljanjem podatkov za oceno varnostnega tveganja, izvedeno na ravni EU. Za obdelavo analitičnih rezultatov fuzijske celice in ravnanje z njimi bi veljala pravila Evropske unije o varstvu tajnih informacij in podatkov[12]. Celica se bi morala povezati z obstoječimi organi na ravni EU in nacionalni ravni. Države članice bi morale vzpostaviti nacionalne kontaktne točke, povezane s hibridno fuzijsko celico EU. Zaposlene znotraj in zunaj EU (vključno s tistimi, ki so napoteni v delegacije, operacije in misije EU) in na ravni držav članic je treba prav tako usposobiti, da prepoznajo prve znake hibridnih groženj.

<u>Ukrep 2</u>: Oblikovanje hibridne fuzijske celice EU v okviru obstoječe strukture Obveščevalnega in situacijskega centra EU (EU INTCEN), 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.

3.2. Strateško komuniciranje

Povzročitelji hibridnih groženj lahko sistematično širijo dezinformacije, vključno s ciljno usmerjenimi kampanjami v družbenih medijih, ter si tako prizadevajo za radikalizacijo

[10] V skladu z njihovimi pristojnostmi.
[11] Na primer Europolov Evropski center za boj proti kibernetski kriminaliteti in za boj proti terorizmu, Frontex, skupina EU za odzivanje na računalniške grožnje (CERT-EU).
[12] Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995.

posameznikov, destabilizacijo družbe ter nadzor nad politično pripovedjo. Sposobnost odzivanja na hibridne grožnje z odločno strategijo **strateškega komuniciranja** je bistvenega pomena. Zagotavljanje hitrega odzivanja z dejstvi in ozaveščanje javnosti o hibridnih grožnjah sta pomembna dejavnika za krepitev odpornosti družbe.

Strateško komuniciranje bi moralo v celoti izkoristiti orodja družbenih medijev ter tradicionalnih vizualnih, zvočnih in spletnih medijev. Evropska služba za zunanje delovanje, ki nadgrajuje dejavnosti projektne skupine za strateško komuniciranje v vzhodnih in arabskih državah, bi morala čim bolje izkoristiti znanje jezikoslovcev, ki obvladajo relevantne jezike, ki niso jeziki EU, in strokovnjakov za družbene medije, ki lahko spremljajo informacije zunaj EU in zagotavljajo ciljno usmerjeno komuniciranje kot odziv na dezinformacije. Države članice bi morale poleg tega oblikovati usklajene mehanizme strateškega komuniciranja v podporo pripisovanju in boju proti dezinformacijam, da se razkrijejo hibridne grožnje.

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

3.3. Center odličnosti za „preprečevanje hibridnih groženj“

Na podlagi izkušenj nekaterih držav članic in partnerskih organizacij[13] bi lahko en mednarodni inštitut ali mreža inštitutov delovala kot center odličnosti za obravnavanje hibridnih groženj. Tak center bi lahko preučeval, kako se hibridne strategije uporabljajo, in podpiral razvoj novih konceptov in tehnologih znotraj zasebnega sektorja in industrije, s katerimi se bi državam članicam pomagalo krepiti odpornost. Raziskave bi lahko prispevale k uskladitvi evropskih in nacionalnih politik, doktrin in konceptov ter zagotavljanju, da se pri sprejemanju odločitev lahko upoštevajo zapletenosti in dvoumnosti, povezane s hibridnimi grožnjami. Tovrsten center bi moral oblikovati programe za pospeševanje raziskav in dejavnosti za iskanje praktičnih rešitev za obstoječe izzive, ki jih prinašajo hibridne grožnje. Prednosti tovrstnega centra bi temeljile na strokovnem znanju, ki bi ga razvili sodelujoči iz različnih držav in sektorjev, in sicer civilnega, vojaškega, zasebnega in akademskega.

Tak center bi lahko tesno sodeloval z obstoječimi centri odličnosti EU[14] in Nata[15] ter tako dobil vpogled v izkušnje o hibridnih grožnjah, pridobljene s področja kibernetske obrambe, strateškega komuniciranja, civilno-vojaškega sodelovanja ter odzivanja na energijske izzive in krize.

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

[13] Centri odličnosti Nata.
[14] Npr. Inštitut EU za varnostne študije, centri odličnosti EU za preprečevanje kemičnih, bioloških, radioloških in jedrskih nevarnosti.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

4. ORGANIZACIJA ODZIVA EU: KREPITEV ODPORNOSTI

Odpornost pomeni zmožnost prenesti obremenitve ter se opomoči in biti okrepljen zaradi izzivov. Za učinkovito preprečevanje hibridnih groženj je treba obravnavati morebitne ranljivosti ključnih infrastruktur, oskrbovalnih verig in družbe. Z uporabo instrumentov in politik EU lahko infrastruktura na ravni EU postane odpornejša.

4.1. Zaščita kritične infrastrukture

Pomembno je zaščititi kritične infrastrukture (npr. verige preskrbe z energijo, promet), saj bi nekonvencionalen napad povzročiteljev hibridne grožnje na katero koli „mehko tarčo“ lahko povzročil resne gospodarske ali družbene pretrese. Zaščito kritične infrastrukture zagotavlja evropski program za zaščito kritične infrastrukture[16] s pristopom medsektorskih sistemov ob upoštevanju vseh nevarnosti in soodvisnosti, ki temelji na izvajanju dejavnosti v okviru delovnih postopkov preprečevanja, pripravljenosti in odzivanja. Direktiva o evropskih kritičnih infrastrukturah[17] določa postopek za ugotavljanje in določanje evropskih ključnih infrastruktur ter skupni pristop za oceno potrebe po izboljšanju njihove zaščite. Zlasti je treba ponovno začeti izvajati dejavnosti iz Direktive za okrepitev odpornosti kritičnih infrastruktur, povezanih s prometom (npr. glavnih letališč in trgovskih pristanišč EU). Komisija bo ocenila, ali je treba razviti skupna orodja, vključno s kazalniki, za izboljšanje odpornosti kritične infrastrukture proti hibridnim grožnjam v vseh relevantnih sektorjih.

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

4.1.1. Energijska omrežja

Nemotena proizvodnja in distribucija energije je bistvenega pomena za EU, večji izpadi energije pa bi lahko bili škodljivi. Bistveni element pri preprečevanju hibridnih groženj je nadaljnja diverzifikacija evropskih virov energije, njenih dobaviteljev in poti, da se zagotovi bolj zanesljiva in odporna oskrba z energijo. Komisija prav tako izvaja ocene tveganja in varnosti („stresne teste“) jedrskih elektrarn v EU. Za zagotovitev diverzifikacije energetskih virov so se okrepila prizadevanja v okviru strategije za energetsko unijo: po zaslugi južnega plinskega koridorja je na primer mogoče, da plin iz kaspijske regije doseže Evropo in da se v severni Evropi vzpostavijo vozlišča za utekočinjeni plin z več dobavitelji. Temu primeru bi morali slediti tudi v osrednji in vzhodni Evropi ter na območju Sredozemlja, kjer je vzpostavitev plinskega vozlišča v

[16] Sporočilo Komisije o Evropskem programu za varovanje ključne infrastrukture, 12.12.2006, COM(2006) 786 final.

[17] Direktiva Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite, UL L 345, 23.12.2008.

fazi razvoja[18]. K temu cilju bo prav tako pozitivno prispeval razvoj trga za utekočinjeni zemeljski plin.

Glede jedrskega materiala in jedrskih objektov Komisija podpira razvoj in sprejem najvišjih varnostnih standardov, s čimer bi se krepila odpornost. Komisija spodbuja dosleden prenos in izvajanje direktive o jedrski varnosti[19], ki določa jasna pravila o preprečevanju nesreč in blažitvi njihovih posledic, ter določb direktive o temeljnih varnostnih standardih[20] o mednarodnem sodelovanju pri pripravljenosti in odzivanju na izredne dogodke, zlasti med sosednjimi državami članicami ter s sosednjimi državami.

***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.**

4.1.2 Varnost prometa in oskrbovalne verige

Promet je bistvenega pomena za delovanje Unije. Hibridni napadi na prometno infrastrukturo (kot so letališča, cestne infrastrukture, pristanišča in železnice) imajo lahko resne posledice, ki vodijo do motenj v prometnih in oskrbovalnih verigah. Komisija pri izvajanju zakonodaje o varnosti v letalstvu in pomorski varnosti[21] opravlja redne preglede[22] in si z dejavnostmi na področju varnosti v kopenskem prometu prizadeva za rešitev vprašanja novih hibridnih groženj. V tem kontekstu se okvir EU obravnava z revidirano uredbo o varnosti v letalstvu[23], ki je del Letalske strategije za Evropo[24]. Poleg tega so grožnje pomorski varnosti obravnavane v strategiji Evropske unije za pomorsko varnost in njenem akcijskem načrtu[25]. Slednji EU in njenim državam članicam omogoča, da se celostno spoprimejo z izzivi pomorske varnosti, vključno s preprečevanjem hibridnih groženj, z medsektorskim sodelovanjem med civilnimi in vojaškimi akterji, da

[18] Za o doslej doseženem napredku glej sporočilo Stanje energetske unije 2015 (COM(2015) 572 final).
[19] Direktiva Sveta 2009/71/Euratom z dne 25. junija 2009 o vzpostavitvi okvira Skupnosti za jedrsko varnost jedrskih objektov, kakor je bila spremenjena z Direktivo Sveta 2014/87/Euratom z dne 8. julija 2014.
[20] Direktiva Sveta 2013/59/Euratom z dne 5. decembra 2013 o določitvi temeljnih varnostnih standardov za varstvo pred nevarnostmi zaradi ionizirajočega sevanja in o razveljavitvi direktiv 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom in 2003/122/Euratom.
[21] Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002; Commission Implementing Regulation (EU) No 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security; Direktiva Evropskega parlamenta in Sveta 2005/65/ES z dne 26. oktobra 2005 o krepitvi varnosti v pristaniščih; Uredba (ES) št. 725/2004 Evropskega parlamenta in Sveta z dne 31. marca 2004 o povečanju zaščite na ladjah in v pristaniščih.
[22] V skladu z zakonodajo EU mora Komisija opravljati preglede za zagotovitev, da države članice pravilno izvajajo zahteve glede varnosti v letalstvu in pomorske varnosti. To vključuje preglede ustreznega organa v državi članici ter tudi preglede na letališčih in pristaniščih, letalskih prevoznikov, ladij in subjektov, ki izvajajo varnostne ukrepe. Cilj pregledov Komisije je zagotoviti, da države članice v celoti izvajajo standarde EU.
[23] Uredba Komisije (EU) 2016/4 z dne 5. januarja 2016 o spremembi Uredbe (ES) št. 216/2008 Evropskega parlamenta in Sveta glede bistvenih okoljevarstvenih zahtev; Uredba (ES) št. 216/2008 Evropskega parlamenta in Sveta z dne 20. februarja 2008 o skupnih predpisih na področju civilnega letalstva in ustanovitvi Evropske agencije za varnost v letalstvu.
[24] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij: Letalska strategija za Evropo, COM/2015/0598 final, 7.12.2015.
[25] Svet je decembra 2014 sprejel akcijski načrt za izvajanje strategije Evropske unije za pomorsko varnost; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf.

se zaščiti kritična pomorska infrastruktura, svetovna oskrbovalna veriga, pomorska trgovina ter morski naravni in energetski viri. Zanesljivost mednarodne oskrbovalne verige je obravnavana tudi v strategiji in akcijskem načrtu Evropske unije za obvladovanje tveganja na carinskem področju[26].

<u>Ukrep 7</u>: 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.

4.1.3 Vesolje

Hibridne grožnje bi lahko bile usmerjene v vesoljske infrastrukture, zaradi česar bi posledice trpelo več sektorjev. EU je oblikovala okvir za podporo nadzoru in spremljanju v vesolju[27], da se vzpostavi mreža tovrstnih sredstev, ki so v lasti držav članic, in tako omogoči izvajanje storitev nadzora in spremljanja v vesolju[28] za opredeljene uporabnike (države članice, institucije EU, lastnike in upravljavce vesoljskih plovil ter organe civilne zaščite). Komisija bo v okviru prihodnje vesoljske strategije za Evropo preučila nadaljnji razvoj na tem področju, da bo lahko spremljala hibridne groženje, usmerjene proti vesoljskim infrastrukturam.

Satelitske komunikacije (SatComs) so ključni elementi za krizno upravljanje, odzivanje na nesreče, policijski nadzor ter varovanje meje in obale. So glavni steber obsežnih infrastruktur, kot so prometni in vesoljski sistemi ali sistemi daljinsko pilotiranih zrakoplovov. Komisija v skladu s pozivom Evropskega sveta za pripravo naslednje generacije vladnih satelitskih komunikacij (GovSatCom) v sodelovanju z Evropsko obrambno agencijo proučuje načine za združitev povpraševanja v okviru prihodnje vesoljske strategije in evropskega obrambnega akcijskega načrta.

Veliko kritičnih infrastruktur temelji na natančnih časovnih informacijah za uskladitev svojih omrežij (npr. na področju energije in telekomunikacij) ali opremljanje transakcij s časovnim žigom (npr. finančni trgi). Odvisnost od signala časovne sinhronizacije enotnega globalnega navigacijskega satelitskega sistema ne zagotavlja odpornosti, potrebne za preprečevanje hibridnih groženj. Evropski globalni navigacijski satelitski sistem Galileo bi zagotovil drug zanesljiv časovni vir.

<u>Ukrep 8</u>: Komisija bo v okviru prihodnje vesoljske strategije in evropskega obrambnega akcijskega načrta predlagala povečanje odpornosti vesoljske

[26] Sporočilo Komisije Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru o strategiji in akcijskem načrtu EU za obvladovanje tveganja na carinskem področju: obvladovanje tveganj, krepitev varnosti dobavne verige in olajševanje trgovine, COM(2014) 527 final.
[27] Glej Sklep št. 541/2014/EU Evropskega parlamenta in Sveta.
[28] Kot so opozorila za izogibanje trčenjem v orbiti, opozorila glede razbitja ali trčenja in tveganih ponovnih vstopov vesoljskih objektov v zemeljsko atmosfero.

infrastrukture proti hibridnim grožnjam, zlasti z morebitno razširitvijo obsega nadzora in spremljanja v vesolju, da bi ta zajel tudi hibridne groženje, pripravami za naslednjo generacijo vladnih satelitskih komunikacij (GovSatCom) na evropski ravni in uvedbo sistema Galileo za kritične infrastrukture, ki so odvisne od časovne sinhronizacije.

4.2. Obrambne zmogljivosti

Obrambne zmogljivosti je treba okrepiti, da se poveča odpornost EU proti hibridnim grožnjam. Pomembno je opredeliti relevantna ključna področja zmogljivosti, na primer nadzorne in izvidniške zmogljivosti. Evropska obrambna agencija je lahko katalizator za razvoj vojaških zmogljivosti (na primer s skrajšanjem ciklov razvoja obrambnih zmogljivosti, naložbami v tehnologijo, sisteme in prototipe, odprtjem obrambnega sektorja za inovativne komercialne tehnologije), povezanih s hibridnimi grožnjami. Morebitni ukrepi se bi lahko preučili v okviru prihodnjega evropskega obrambnega akcijskega načrta.

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.

4.3. Varovanje javnega zdravja in prehranska varnost

Zdravje prebivalstva lahko ogrozi manipulacija prenosljivih bolezni ali kontaminacija hrane, tal, zraka in pitne vode s kemičnimi, biološkimi, radiološkimi in jedrskimi (KBRJ) agensi. Poleg tega lahko namerno širjenje bolezni živali ali rastlin resno vpliva na prehransko varnost Unije ter ima velik gospodarski in družbeni učinek na ključna področja prehranske verige EU. Obstoječe strukture EU za zdravstveno varnost, varstvo okolja in varnost hrane se lahko uporabijo za odzivanje na hibridne grožnje, ki uporabljajo te metode.

V skladu z zakonodajo EU o čezmejnih nevarnostih za zdravje[29] obstoječi mehanizmi zagotavljajo usklajevanje pripravljenosti na resne čezmejne nevarnosti za zdravje, tako da prek sistema zgodnjega opozarjanja in odzivanja povezujejo države članice, agencije in znanstvene odbore EU[30]. Odbor za zdravstveno varnost, ki usklajuje odzivanje držav članic na grožnje, lahko deluje kot informacijska točka o ranljivostih v javnem zdravju[31], da bi zagotovil vključitev hibridnih groženj (zlasti biološkega terorizma) v smernice o kriznem komuniciranju (simulacija kriznih razmer) in v dejavnosti krepitve zmogljivosti z državami članicami. Na področju varnosti hrane pristojni organi prek sistema hitrega obveščanja za živila in krmo (RASFF) in sistema za skupno obvladovanje tveganja na carinskem področju (CRMS) izmenjujejo podatke o analizi tveganja, da bi spremljali

[29] Sklep št. 1082/2013/EU Evropskega parlamenta in Sveta z dne 22. oktobra 2013 o resnih čezmejnih nevarnostih za zdravje in o razveljavitvi Odločbe št. 2119/98/ES (UL L 293/1, 5.11.2013).
[30] Commission Decision C(2015) 5383 of 7.8.2015 on establishment of Scientific Committees in the field of public health, consumer safety and the environment.
[31] V skladu s Sklepom št. 1082/2013/EU Evropskega parlamenta in Sveta z dne 22. oktobra 2013 o resnih čezmejnih nevarnostih za zdravje in o razveljavitvi Odločbe št. 2119/98/ES, UL L 293/1.

tveganja za zdravje, ki jih povzroča kontaminirana hrana. Za zdravje živali in rastlin bodo s pregledom pravnega okvira EU[32] obstoječi „zbirki orodij“[33] dodani novi elementi, ki bodo zagotovili boljšo pripravljenost na hibridne grožnje.

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.

4.4. Kibernetska varnost

EU ima velike koristi od medsebojno povezane in digitalne evropske družbe. Kibernetski napadi lahko ovirajo digitalne storitve po vsej EU in takšne napade bi lahko izkoristili povzročitelji hibridnih groženj. Izboljšanje odpornosti komunikacijskih in informacijskih sistemov v Evropi je pomembna podpora digitalnemu enotnemu trgu. Strategija EU za kibernetsko varnost in evropska agenda za varnost zagotavljata splošen strateški okvir za pobude EU o kibernetski varnosti in kibernetski kriminaliteti. EU je bila dejavna pri razvoju ozaveščenosti, mehanizmov sodelovanja in odzivanja v okviru rezultatov strategije za kibernetsko varnost. Natančneje, predlagana direktiva o varnosti omrežij in informacij[34] obravnava tveganja za kibernetsko varnost, ki vplivajo na širok spekter ponudnikov ključnih storitev na področju energije, prometa, financ in zdravstva. Ti ponudniki in tudi ponudniki ključnih digitalnih storitev (npr. računalništva v oblaku) bi morali sprejeti ustrezne varnostne ukrepe in o resnih incidentih poročati nacionalnim organom, pri čemer bi morali opozoriti na vsakršno značilnost hibridnih groženj. Ko bosta Direktivo sprejela sozakonodajalca, bosta njen učinkovit prenos v nacionalno zakonodajo in izvajanje spodbudila zmogljivosti kibernetske varnosti med državami članicami, s čimer se bo prek izmenjave informacij in dobrih praks o preprečevanju hibridnih groženj okrepilo njihovo sodelovanje na področju kibernetske varnosti. Direktiva namreč določa vzpostavitev mreže 28 nacionalnih skupin za odzivanje na z računalniško varnostjo povezane incidente (CSIRT – Computer Security Incidents Response Teams) in skupine za odzivanje na računalniške grožnje (CERT-EU – Computer Emergency Response Team)[35] za operativno sodelovanje na prostovoljni osnovi.

Komisija je za spodbuditev sodelovanja med javnim in zasebnim sektorjem ter evropskih pristopov h kibernetski varnosti vzpostavila platformo za varnost omrežij in informacij, ki je odgovorna za izdajo smernic o dobrih praksah glede obvladovanja tveganj. Čeprav so države članice tiste, ki določijo varnostne zahteve in podrobnosti o obveščanju o

[32] Uredba (EU) 2016/429 Evropskega parlamenta in Sveta o prenosljivih boleznih živali in o spremembi ter razveljavitvi določenih aktov na področju zdravja živali („Pravila o zdravju živali“), UL L 84, 31.3.2016. O predlogu uredbe Evropskega parlamenta in Sveta o zaščitnih ukrepih proti škodljivim organizmom („zakonodaja o zdravju rastlin“) sta Evropski parlament in Svet 16. decembra 2015 dosegla politični dogovor.

[33] Npr. banke cepiv EU, izpopolnjeni elektronski informacijski sistem o živalskih boleznih, večje obveznosti za ukrepe laboratorijev in drugih subjektov, ki se ukvarjajo s patogeni.

[34] Predlog Komisije za Direktivo Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji, COM(2013) 48 final, 7.2.2013. Svet EU in Evropski parlament sta dosegla politični dogovor o predlagani direktivi, ki bi morala biti kmalu uradno sprejeta.

[35] Skupina za odzivanje na računalniške grožnje (CERT-EU) za institucije EU.

nacionalnih incidentih, Komisija spodbuja visoko stopnjo konvergence pri pristopih k obvladovanju tveganj, zlasti s pomočjo Agencije Evropske unije za varnost omrežij in informacij (ENISA).

<u>Ukrep 11</u>: Komisija poziva države članice, naj kot prednostno nalogo vzpostavijo in v celoti izkoristijo mrežo med 28 nacionalnimi skupinami za odzivanje na z 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 kibernetskih groženj (npr. letalstvo, energija, pomorstvo) skladne s medsektorskimi zmogljivostmi iz direktive o varnosti omrežij in informacij za združevanje informacij, strokovnega znanja in hitro odzivanje.

4.4.1. Industrija

Večje zanašanje na računalništvo v oblaku in obsežni podatki pomenijo večjo ranljivost za hibridne grožnje. Strategija za digitalni enotni trg vzpostavlja pogodbeno javno-zasebno partnerstvo za kibernetsko varnost[36], ki bo osredotočeno na raziskave in inovacije ter bo Uniji pomagalo ohraniti visoko stopnjo tehnološke zmogljivosti na tem področju. S pogodbenimi javno-zasebnimi partnerstvi se bo vzpostavilo zaupanje med različnimi udeleženci na trgu ter razvile sinergije med povpraševanjem in ponudbo. Čeprav bodo pogodbeno javno-zasebno partnerstvo in spremljevalni ukrepi osredotočeni na izdelke in storitve za zagotavljanje civilne kibernetske varnosti, bi morali rezultati teh pobud omogočiti boljšo zaščito uporabnikov tehnologije pred hibridnimi grožnjami.

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

4.4.2. Energija

Oblikovanje pametnih domov in naprav, razvoj pametnega omrežja ter naraščajoča digitalizacija energijskega sistema prinašajo tudi večjo ranljivost za kibernetske napade. Evropska strategija za energetsko zanesljivost[37] in strategija za energetsko unijo[38] podpirata pristop, ki upošteva vse nevarnosti in v katerega je vključena odpornost proti hibridnim grožnjam. Tematska mreža za zaščito kritične energetske infrastrukture spodbuja sodelovanje med izvajalci v energetskem sektorju (nafta, plin, elektrika). Komisija je vzpostavila spletno platformo za analizo in souporabo informacij o grožnjah in incidentih[39]. Skupaj z deležniki[40] prav tako pripravlja celovito strategijo energetskega

[36] Naj bi se začelo izvajati sredi leta 2016.
[37] Sporočilo Komisije Evropskemu parlamentu in Svetu: Evropska strategija za energetsko varnost, COM/2014/0330 final.
[38] Sporočilo „Okvirna strategija za trdno energetsko unijo s podnebno politiko, usmerjeno v prihodnost“, COM/2015/080 final.
[39] Center EU za souporabo informacij o incidentih in grožnjah (ITIS – Incident and Threat Information Sharing).

sektorja za kibernetsko varnost pri dejavnostih pametnega omrežja, da se zmanjšajo ranljivosti. Čeprav so trgi električne energije vse bolj povezani, pa so pravila in postopki za ravnanje v kriznih razmerah še vedno nacionalni. Zagotoviti moramo, da vlade sodelujejo pri pripravah na tveganja ter njihovem preprečevanju in zmanjševanju ter da vsi zadevni akterji ravnajo na podlagi skupnih pravil.

Ukrep 13: Komisija bo izdala smernice za lastnike pametnih omrežij za izboljšanje kibernetske 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 kibernetske napade in ublažiti njihove posledice.

4.4.3. Zagotavljanje zanesljivih finančnih sistemov

Za delovanje gospodarstva EU sta potrebna zanesljiv finančni in plačilni sistem. Bistveno je, da se finančni sistem in njegova infrastruktura zaščitita pred kibernetskimi napadi ne glede na motiv ali naravo napadalca. Za obravnavanje hibridnih groženj proti finančnim storitvam EU mora industrija grožnjo razumeti, preskusiti svojo obrambo in imeti potrebno tehnologijo, da industrijo zaščiti pred napadom. Zato je souporaba informacij o grožnjah med udeleženci na finančnem trgu ter z ustreznimi organi in ključnimi ponudniki storitev ali strankami bistvenega pomena, vendar mora izpolnjevati zahteve glede varnosti in varstva podatkov. Komisija si bo v skladu z delom na mednarodnih forumih, vključno z delom skupine G7 v tem sektorju, prizadevala opredeliti dejavnike, ki ovirajo ustrezno souporabo informacij o grožnjah, in predlagati rešitve. Pomembno je zagotoviti redno preskušanje in izboljševanje protokolov za zaščito podjetij in relevantnih infrastruktur, vključno s stalnim nadgrajevanjem tehnologij, ki povečujejo varnost.

Ukrep 14: Komisija bo v sodelovanju z agencijo ENISA[41], 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.

4.4.4. Promet

Sodobni prometni sistemi (železniški, cestni, zračni, pomorski) so odvisni od informacijskih sistemov, ki bi lahko bili tarča kibernetskih napadov. Zaradi njihove čezmejne razsežnosti ima EU na tem področju posebno vlogo. Komisija bo v sodelovanju z državami članicami še naprej preučevala kibernetske grožnje in tveganja, povezana z nezakonitimi vmešavanji v prometne sisteme. Komisija v sodelovanju z Evropsko

[40] V okviru platforme strokovnjakov za energijo na področju kibernetske varnosti (EECSP – Energy Expert CyberSecurity Platform).
[41] Agencija Evropske unije za varnost omrežij in informacij.

agencijo za varnost v letalstvu pripravlja načrt za kibernetsko varnost v letalstvu[42]. Grožnje pomorski varnosti so prav tako obravnavane v strategiji Evropske unije za pomorsko varnost in njenem akcijskem načrtu.

<u>Ukrep 15</u>: 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 kibernetskimi napadi v prometnem sektorju.

4.5. Usmerjenost v financiranje hibridnih groženj

Povzročitelji hibridnih groženj za izvajanje svojih dejavnosti potrebujejo finančna sredstva. Finančna sredstva se lahko porabijo za podpiranje terorističnih skupin ali bolj prefinjene načine destabilizacije, kot je podpiranje skupin pritiska in obrobnih političnih strank. EU je okrepila prizadevanja za boj proti financiranju kriminala in terorizma, kot je določeno v evropski agendi za varnost, zlasti v okviru akcijskega načrta[43]. Z revidiranim evropskim okvirom za preprečevanje pranja denarja je tako okrepljen boj proti financiranju terorizma in pranju denarja ter olajšano delo nacionalnih finančnoobveščevalnih enot pri prepoznavanju in spremljanju sumljivih denarnih nakazil in izmenjavi informacij, obenem pa se zagotavlja sledljivost prenosa sredstev v Evropski uniji. Zato bi lahko prispeval tudi k preprečevanju hibridnih groženj. V okviru instrumentov skupne zunanje in varnostne politike se bi lahko preučili prilagojeni in učinkoviti omejevalni ukrepi za preprečevanje hibridnih groženj.

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

4.6. Krepitev odpornosti proti radikalizaciji in nasilnemu ekstremizmu

Čeprav teroristična dejanja in nasilni ekstremizem sama po sebi nista hibridne narave, si lahko povzročitelji hibridnih groženj za tarčo izberejo ranljive člane družbe, med njimi novačijo ter jih radikalizirajo prek sodobnih komunikacijskih kanalov (vključno s spletnimi družbenimi mediji in proksi skupinami) in propagande.

Da bi Komisija rešila vprašanje ekstremističnih spletnih vsebin, v okviru strategije za digitalni enotni trg preučuje potrebo po morebitnih novih ukrepih, ob ustreznem upoštevanju njihovega učinka na temeljne pravice do svobode izražanja in obveščanja. To bi lahko vključevalo stroge postopke za odstranjevanje nezakonitih vsebin, ne da bi se pri tem odstranile zakonite vsebine („mehanizem prijavljanja in ukrepanja“), ter večjo odgovornost in skrbnost posrednikov pri upravljanju njihovih omrežij in sistemov. S tem

[42] Evropski parlament in Svet trenutno razpravljata o predlogu nove uredbe o Evropski agenciji za varnost v letalstvu, ki ga je Komisija predložila decembra 2015. Predlog uredbe Evropskega parlamenta in Sveta o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter razveljavitvi Uredbe (ES) št. 216/2008 Evropskega parlamenta in Sveta (COM/2015/0613 final – 2015/0277 (COD)).

[43] Sporočilo Komisije Evropskemu parlamentu in Svetu o akcijskem načrtu za okrepitev boja proti financiranju terorizma (COM(2016) 50 final).

bi bil dopolnjen obstoječi prostovoljni pristop, v okviru katerega spletna podjetja in družbeni mediji (zlasti pod okriljem foruma EU o internetu) v sodelovanju z Europolovo enoto EU za prijavljanje internetnih vsebin hitro odstranjujejo teroristično propagando.

V okviru evropske agende za varnost se radikalizacija preprečuje z izmenjavo izkušenj in razvojem dobrih praks, vključno s sodelovanjem s tretjimi državami. Cilj svetovalne skupine za strateško obveščanje v zvezi s Sirijo je okrepiti razvoj in razširjanje alternativnih sporočil za preprečevanje teroristične propagande. Mreža za ozaveščanje o radikalizaciji nudi podporo državam članicam in izvajalcem, ki imajo opravka z radikaliziranimi posamezniki (vključno s tujimi terorističnimi bojevniki) ali tistimi, ki se zdijo dovzetni za radikalizacijo. Mreža za ozaveščanje o radikalizaciji zagotavlja usposabljanja in svetovanje ter bo nudila podporo prednostnim tretjim državam, v katerih obstaja pripravljenost za sodelovanje. Komisija poleg tega spodbuja pravosodno sodelovanje med akterji kazenskega pravosodja, vključno z Eurojustom, pri preprečevanju terorizma in radikalizacije v vseh državah članicah, vključno z reševanjem vprašanja tujih terorističnih bojevnikov in povratnikov.

EU pri svojem **zunanjem delovanju** poleg zgoraj navedenih pristopov prav tako izvaja ukrepe za preprečevanje nasilnega ekstremizma, vključno z zunanjim udejstvovanjem in ozaveščanjem ter preprečevanjem (boj proti financiranju radikalizacije in terorizma), kakor tudi z ukrepi za obravnavanje temeljnih gospodarskih, političnih in družbenih dejavnikov, ki terorističnim skupinam omogočajo priložnosti za razcvet.

<u>Ukrep 17:</u> 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.

4.7. Krepitev sodelovanja s tretjimi državami

Kot je poudarjeno v evropski agendi za varnost, je EU namenila večjo pozornost krepitvi zmogljivosti na področju varnostnega sektorja v ***partnerskih državah***, med drugim z vzpostavljanjem povezav med varnostjo in razvojem ter razvojem varnostne razsežnosti prenovljene evropske sosedske politike[44]. S temi ukrepi se lahko prav tako spodbuja odpornost partnerjev proti hibridnim dejavnostim.

Komisija namerava dodatno okrepiti izmenjavo operativnih in strateških informacij z državami, ki se pripravljajo na pristop, ter se v okviru vzhodnega partnerstva in južnega sosedstva, kakor je primerno, prizadevati za boj proti organiziranemu kriminalu, terorizmu, neregularnim migracijam in trgovanju z lahkim orožjem. Na področju boja proti terorizmu je EU okrepila sodelovanje s tretjimi državami z vzpostavitvijo posodobljenih varnostnih dialogov in akcijskih načrtov.

[44] Skupno sporočilo Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Pregled evropske sosedske politike, JOIN(2015) 50 final, 18.11.2015.

Cilj zunanjih finančnih instrumentov EU je vzpostavitev delujočih in odgovornih institucij v tretjih državah[45], ki so predpogoj za učinkovito odzivanje na varnostne grožnje in za krepitev odpornosti. V tem okviru so ključna orodja reforma varnostnega sektorja in krepitev zmogljivosti v podporo varnosti in razvoju[46]. V okviru instrumenta za prispevanje k stabilnosti in miru[47] je Komisija razvila ukrepe za krepitev kibernetske odpornosti in sposobnosti partnerjev za odkrivanje in odzivanje na kibernetske napade in kibernetsko kriminaliteto, s katerimi se lahko preprečujejo hibridne grožnje v tretjih državah. EU financira dejavnosti krepitve zmogljivosti v partnerskih državah za zmanjšanje varnostnih tveganj, povezanih s kemičnimi, biološkimi, radiološkimi in jedrskimi nevarnostmi[48].

Države članice bi lahko nazadnje v duhu celostnega pristopa h kriznemu upravljanju uporabile orodja in misije skupne varnostne in obrambne politike, in sicer samostojno ali kot dopolnilo instrumentom EU v uporabi, da bi partnerjem pomagale pri krepitvi njihovih zmogljivosti. Možni so naslednji ukrepi: (i) podpora strateškemu komuniciranju, (ii) svetovanje za ključna ministrstva, ki so izpostavljena hibridnim grožnjam; (iii) dodatna podpora za upravljanje meja v izrednih razmerah. Lahko bi se preučile nadaljnje sinergije med instrumenti skupne varnostne in obrambne politike ter akterji na področju varnosti, carine in pravosodja, vključno z ustreznimi agencijami EU[49], Interpolom in evropskimi žandarskimi silami, v skladu z njihovimi pristojnostmi.

<u>Ukrep 18</u>: 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.

5. PREPREČEVANJE KRIZ, ODZIVANJE NANJE IN OKREVANJE

Kot je opisano v oddelku 3.1, je cilj predlagane hibridne fuzijske celice EU analizirati ustrezne kazalnike za preprečevanje hibridnih groženj in odzivanje nanje ter informiranje

[45] Glej prejšnjo opombo; Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o strategiji širitve EU (*EU Enlargement Strategy*), 10.11.2015, COM(2015) 611 final; Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Povečanje učinka razvojne politike EU: agenda za spremembe, 13.10.2011, COM(2011) 637 final.

[46] Skupno sporočilo „Krepitev zmogljivosti v podporo varnosti in razvoju – usposabljanje partnerjev za preprečevanje in obvladovanje kriz“ (JOIN(2015) 17 final).

[47] Uredba (EU) št. 230/2014 Evropskega parlamenta in Sveta z dne 11. marca 2014 o vzpostavitvi instrumenta za prispevanje k stabilnosti in miru (UL L 77/1, 15.3.2014).

[48] Med drugim so bila zajeta naslednja področja: nadzor meja, krizno upravljanje, prvi odziv, nedovoljena trgovina, nadzor izvoza blaga z dvojno rabo, nadzor in kontrola nad boleznimi, jedrska forenzika, okrevanje po incidentu in zaščita objektov z visokim tveganjem. S tretjimi državami se lahko delijo primeri dobrih praks, pridobljenih z orodji, razvitimi v okviru akcijskega načrta EU na področju kemičnih, bioloških, radioloških in jedrskih nevarnosti, kot sta evropski center za usposabljanje na področju jedrske varnosti in sodelovanje EU v mednarodni delovni skupini za nadzorovanje meje.

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST.

nosilcev odločanja v EU. Čeprav je bremena 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 zvezi s tem bi lahko bil učinkovit mehanizem odzivanja za vidike hibridnih groženj, ki zahtevajo odziv civilne zaščite, spodbujanje nacionalnih ukrepov civilne zaščite in zmogljivosti evropskega centra za usklajevanje nujnega odziva[50]. To se lahko doseže z usklajevanjem z drugimi mehanizmi EU za odzivanje in sistemi zgodnjega opozarjanja, zlasti s situacijsko sobo ESZD za zunanjo varnost in s centrom za strateško analizo in odzivanje za notranjo varnost.

Solidarnostna klavzula (člen 222 PDEU) omogoča ukrepanje Unije in tudi ukrepanje med državami članicami, če je država članica žrtev terorističnega napada, naravne nesreče ali nesreče, ki jo je povzročil človek. Ukrepanje Unije, da bi pomagala državi članici, se izvaja z uporabo Sklepa Sveta 2014/415/EU[51]. Ureditve usklajevanja v Svetu bi morale temeljiti na enotnem političnem odzivanju EU na krize[52]. V skladu s temi ureditvami Komisija in visoki predstavnik (v okviru svojih pristojnosti) opredelita ustrezne instrumente Unije, Svetu pa predložita predloge za sklepe o izrednih ukrepih.

Člen 222 PDEU prav tako obravnava razmere, ki vključujejo neposredno pomoč ene ali več držav članic državi članici, ki je žrtev terorističnega napada ali nesreče. V zvezi s tem se Sklep Sveta 2014/415/EU ne uporablja. Če je država članica EU izpostavljena znatnim hibridnim grožnjam, morata glede na dvoumnosti, povezane s hibridnimi dejavnosti, Komisija in visoki predstavnik (v okviru svojih pristojnosti) kot skrajno možno rešitev oceniti, ali je primerno uporabiti solidarnostno klavzulo.

V primerjavi s členom 222 PDEU pa je v primeru večkratnih resnih hibridnih groženj, ki vključujejo oborožen napad na državo članico EU, za zagotovitev primernega in pravočasnega odziva možno sklicevanje na člen 42(7) PEU. Obsežne in skrajne hibridne grožnje lahko prav tako zahtevajo okrepljeno sodelovanje in usklajevanje z Natom.

Države članice se spodbuja, da pri pripravi svojih sil upoštevajo morebitne hibridne grožnje. Za hitro in učinkovito sprejemanje odločitev v primeru hibridnega napada morajo države članice izvajati redne dejavnosti na operativni in politični ravni za preskušanje nacionalnih in večnacionalnih zmožnosti odločanja. Cilj bi bil vzpostavitev skupnega operativnega protokola med državami članicami, Komisijo in visokim predstavnikom, v katerem so začrtani učinkoviti postopki, ki jih je treba upoštevati v primeru hibridnih groženj, od začetne faze prepoznavanja do končne faze napada, ter opredeljena vloga vseh institucij Unije in akterjev v tem procesu.

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] Sklep Sveta 2014/415/EU o načinu izvajanja solidarnostne klavzule s strani Unije (UL L 192, 1.7.2014, str. 53).
[52] http://www.consilium.europa.eu/sl/documents-publications/publications/2014/eu-ipcr/.

Kot pomemben sestavni del skupne varnostne in obrambne politike bi udejstvovanje lahko zagotavljalo (a) civilno in vojaško usposabljanje, (b) misije mentorstva in svetovanja za izboljšanje varnostnih in obrambnih zmogljivosti ogrožene državne, (c) načrtovanje ravnanja v nepredvidljivih razmerah za prepoznavanje znakov hibridnih groženj in krepitev zmogljivosti zgodnjega opozarjanja, (d) podporo upravljanju nadzora meje v izrednih razmerah, (e) podporo na specializiranih področjih, kot so zmanjševanje tveganja na področju kemičnih, bioloških, radioloških in jedrskih nevarnosti in evakuacija brez bojevanja.

***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.*

***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.*

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

6. KREPITEV SODELOVANJA Z NATOM

Hibridne grožnje ne pomenijo izziva le za EU, ampak tudi za druge pomembne partnerske organizacije, kot so Združeni narodi (ZN), Organizacija za varnost in sodelovanje v Evropi (OVSE) in zlasti Nato. Za učinkovit odziv je potreben dialog ter usklajevanje med organizacijami na politični in operativni ravni. Tesnejše sodelovanje med EU in Natom bi obema organizacijama omogočilo, da se bolje pripravita in učinkovito odzivata na hibridne grožnje, in sicer z medsebojnim dopolnjevanjem na podlagi načela vključenosti, ob hkratnem spoštovanju avtonomije odločanja obeh organizacij in pravil o varstvu podatkov.

Organizaciji imata skupne vrednote in se spopadata s podobnimi izzivi. Tako države članice EU kot tudi zaveznice Nata pričakujejo, da jih zadevni organizaciji podpirata s hitrim, odločnim in usklajenim ukrepanjem v primeru krize oziroma da po možnosti preprečita nastanek krize. Opredeljena je bila vrsta področij za tesnejše sodelovanje in usklajevanje med EU in Natom, vključno z zavedanjem o situaciji, strateškim komuniciranjem, kibernetsko varnostjo ter preprečevanjem kriz in odzivanjem nanje. Stalen neuradni dialog med EU in Natom o hibridnih grožnjah bi bilo treba okrepiti za uskladitev dejavnosti teh dveh organizacij na tem področju.

Za razvoj komplementarnosti odzivov EU/Nato je pomembno, da imata obe organizaciji enako predstavo o zavedanju o situaciji pred in med krizo. To bi lahko dosegli ne le z redno souporabo analiz in pridobljenih izkušenj, temveč tudi z neposrednim sodelovanjem med hibridno fuzijsko celico EU in hibridno celico Nata. Za zagotovitev hitrega in učinkovitega odzivanja pa je prav tako pomembno, da se okrepi vzajemna

ozaveščenost obeh organizacij o zadevnih postopkih kriznega upravljanja. Odpornost je mogoče okrepiti z zagotavljanjem dopolnjevanja pri določanju primerjalnih meril za kritične dele njihovih infrastruktur ter tudi tesnega sodelovanja pri strateškem komuniciranju in kibernetski obrambi. V celoti vključujoče skupne dejavnosti na politični in tudi strokovni ravni bi prispevale k večji učinkovitosti sposobnosti odločanja obeh organizacij. Proučevanje nadaljnjih možnosti za dejavnosti usposabljanja bi pomagalo razviti primerljivo raven strokovnega znanja na ključnih področjih.

<u>Ukrep 22</u>: Visoki predstavnik bo v sodelovanju s Komisijo nadaljeval z neuradnim dialogom ter okrepil sodelovanje in usklajevanje z Natom v zvezi z zavedanjem o situaciji, strateškimi komunikacijami, kibernetsko 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.

7. ZAKLJUČKI

V tem skupnem sporočilu so opisani ukrepi za pomoč pri preprečevanju hibridnih groženj ter izboljšanje odpornosti na ravni EU in na nacionalni ravni ter izboljšanje odpornosti partnerjev. Ker je poudarek na **izboljšanju ozaveščenosti**, sta predlagana vzpostavitev namenskih mehanizmov za izmenjavo informacij z državami članicami in usklajevanje zmogljivosti EU za pripravo strateških komunikacij. Predstavljeni so ukrepi 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. Na vsakem od teh področij bosta ključen prvi korak izvajanje dogovorjenih strategij s strani EU in držav članic ter polno izvajanje obstoječe zakonodaje s strani držav članic, hkrati pa so za okrepitev teh prizadevanj predstavljeni bolj konkretni ukrepi.

Glede **preprečevanja hibridnih groženj, odzivanja nanje in okrevanja** je bil podan predlog, da se preuči izvedljivost uporabe solidarnostne klavzule iz člena 222 PDEU (kot je opredeljena v zadevnem sklepu) in člena 42(7) PEU v primeru obsežnega in resnega hibridnega napada. Sposobnost strateškega odločanja se bi lahko okrepila z vzpostavitvijo skupnega operativnega protokola.

Nazadnje se predlaga, da se **okrepita sodelovanje** in **usklajevanje med EU in Natom** pri skupnih prizadevanjih za preprečevanje hibridnih groženj.

Pri izvajanju tega skupnega okvira se visoki predstavnik in Komisija zavezujeta, da bosta uporabila ustrezne instrumente EU, ki so jima na voljo. Za EU je pomembno, da si skupaj z državami članicami prizadeva za zmanjšanje tveganj, povezanih z izpostavljenostjo morebitnim hibridnim grožnjam državnih in nedržavnih akterjev.