PREPORUKE

PREPORUKA KOMISIJE (EU) 2017/1584

od 13. rujna 2017.

o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 292.,

budući da:

(1) Upotreba informacijskih i komunikacijskih tehnologija i ovisnost o njima postali su ključni elementi u svim sektorima gospodarstva, jer su naša poduzeća i građani međusobno povezani i ovisni jedni o drugima u različitim sektorima i preko granica više nego ikada prije. Kiberincident koji utječe na organizacije u više država članica ili čak u cijeloj Uniji koji bi mogao prouzročiti ozbiljne poremećaje na unutarnjem tržištu i šire u mrežnim i informacijskim sustavima na koja se oslanjaju gospodarstvo, demokracija i društvo Unije mogućnost je za koju države članice i institucije EU-a moraju biti dobro pripremljene.

(2) Kiberincident se može smatrati krizom na razini Unije kada je poremećaj uzrokovan incidentom preopsežan da bi ga dotična država članica mogla riješiti sama ili kada utječe na dvije ili više država članica s tako dalekosežnim tehničkim ili političkim učinkom da je potrebna pravovremena koordinacija i odgovor na političkoj razini Unije.

(3) Kiberincidenti mogu izazvati širu krizu koja utječe na sektore aktivnosti koji nadilaze mrežne i informacijske sustave i komunikacijske mreže; primjeren odgovor mora se temeljiti i na kibernetičkim i na nekibernetičkim mjerama ublažavanja.

(4) Kiberincidente nije moguće predvidjeti, često se pojavljuju i razvijaju unutar vrlo kratkih razdoblja te stoga pogođeni subjekti i oni koji su odgovorni za odgovor na incident i ublažavanje njegovih učinaka moraju brzo uskladiti svoje odgovore. Osim toga, kiberincidenti često nisu ograničeni na određeno zemljopisno područje i mogu se istodobno pojaviti u više zemalja ili brzo proširiti na više njih.

(5) Za učinkovit odgovor na kiberincidente i kiberkrize velikih razmjera na razini EU-a potrebna je brza i učinkovita suradnja među svim relevantnim dionicima koja se temelji na pripravnosti i sposobnosti pojedinih država članica te koordiniranom zajedničkom djelovanju uz potporu kapaciteta Unije. Pravovremen i učinkovit odgovor na incidente stoga se temelji na postojanju prethodno uspostavljenih te, koliko je to moguće, dobro uvježbanih postupaka suradnje i mehanizama, pri čemu su uloge i odgovornosti ključnih aktera na nacionalnoj razini i na razini Unije jasno definirane.

(6) Vijeće je u svojim zaključcima ([1]) o zaštiti kritične informacijske strukture od 27. svibnja 2011. pozvalo države članice EU-a da „pojačaju suradnju među državama članicama te da na temelju iskustava nacionalnog kriznog upravljanja i suradnje s ENISA-om pridonesu razvoju mehanizama suradnje za europske kiberincidente koji će se testirati 2012. u okviru sljedeće vježbe‚Cyber Europe'."

(7) Komunikacija Komisije iz 2016. „Jačanje europskog sustava kibernetičke sigurnosti i poticanje konkurentne i inovativne industrije kibernetičke sigurnosti" ([2]) potaknula je države članice da što više iskoriste mehanizme suradnje iz Direktive NIS ([3]) i pojačaju prekograničnu suradnju povezanu s pripravnošću za kiberincidente većih

([1]) Zaključci Vijeća o zaštiti kritične informacijske strukture „Postignuća i sljedeći koraci: prema globalnoj kibersigurnosti", dokument 10299/11, Bruxelles, 27. svibnja 2011.
([2]) COM(2016) 410 final, 5. srpnja 2016.
([3]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

razmjera. U Komunikaciji se navodi i da bi koordinirani pristup suradnji u slučaju krize u različitim dijelovima kibernetičkih eko-sustava utvrđen „planom" povećao pripravnost i da bi takav plan trebao također osigurati sinergije i usklađenost s postojećim mehanizmima za upravljanje krizama.

(8) U zaključcima Vijeća ([1]) o prethodno spomenutoj komunikaciji države članice pozvale su Komisiju da dostavi takav plan na razmatranje tijelima i ostalim relevantnim dionicima. Međutim, Direktivom NIS nije predviđen okvir suradnje na razini Unije u slučaju kiberincidenata i kiberkriza velikih razmjera.

(9) Komisija se savjetovala s državama članicama na dvije zasebne savjetodavne radionice održane 5. travnja i 4. srpnja 2017. u Bruxellesu, s predstavnicima država članica iz timova za odgovor na računalne sigurnosne incidente (CSIRT), skupinom za suradnju uspostavljenom Direktivom NIS i Horizontalnom radnom skupinom Vijeća za kiberpitanja te predstavnicima Europske službe za vanjsko djelovanje (ESVD), ENISA-e, Europola/EC3 i Glavnog tajništva Vijeća (GTV).

(10) Sadašnji plan za koordinirani odgovor na razini Unije na kiberincidente i kiberkrize velikih razmjera koji je priložen ovoj Preporuci rezultat je prethodno spomenutih savjetovanja i dopunjava Komunikaciju „Jačanje europskog sustava kibernetičke sigurnosti i poticanje konkurentne i inovativne industrije kibernetičke sigurnosti".

(11) U planu se opisuju i utvrđuju ciljevi i načini suradnje između država članica i institucija, tijela, ureda i agencija EU-a (dalje u tekstu „institucije EU-a") pri odgovaranju na kiberincidente i kiberkrize velikih razmjera te kako se postojećim mehanizmima za upravljanje krizama mogu u cijelosti iskoristiti postojeća tijela za kibersigurnost na razini EU-a.

(12) Pri odgovoru na kiberkrizu u smislu uvodne izjave 2. za koordinaciju odgovora na političkoj razini Unije u Vijeću upotrijebit će se aranžmani za integrirani odgovor na političku krizu (IPCR) ([2]); Komisija će upotrijebiti međusektorski postupak koordiniranja krize visokoj razini (ARGUS) ([3]). Ako kriza ima znatan utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku, aktivirat će se mehanizam za odgovor na krize (CRM) Europske službe za vanjsko djelovanje (ESVD) ([3]).

(13) U nekim područjima suradnja u slučaju kiberincidenta ili kiberkrize uređena je sektorskim mehanizmima za upravljanje krizama na razini EU-a. Primjerice, u okviru europskog globalnog navigacijskog satelitskog sustava (GNSS), Odlukom Vijeća 2014/496/ZVSP ([4]) već su definirane uloge Vijeća, Visokog predstavnika, Komisije, Agencije za europski GNSS i država članica u okviru lanca operativnih odgovornosti koji je uspostavljen kako bi se reagiralo na prijetnju Uniji, državama članicama ili GNSS-u, uključujući i u slučaju kibernapada. Stoga se ovom preporukom ne bi trebali dovoditi u pitanje takvi mehanizmi.

(14) Glavnu odgovornost za odgovor u slučaju kiberincidenata ili kiberkriza velikih razmjera koje na njih utječu, imaju države članice. Međutim, važnu ulogu imaju i Komisija, Visoki predstavnik i druge institucije ili službe EU-a, a ta uloga proizlazi iz prava Unije ili iz činjenice da kiberincidenti i kiberkrize mogu utjecati na sva područja gospodarske aktivnosti unutar jedinstvenog tržišta, sigurnost i međunarodne odnose Unije te na same institucije.

(15) Među ključnim akterima na razini Unije uključenima u odgovor na kiberkrize su i nove strukture i mehanizmi uspostavljeni na temelju Direktive NIS, i to mreža timova za odgovor na računalne sigurnosne incidente (CSIRT) te relevantne agencije i tijela kao što su Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA), Europski centar za borbu protiv kiberkriminala pri Europolu (Europol/EC3), Centar EU-a za analizu obavještajnih podataka (INTCEN), Obavještajna uprava vojnog stožera EU-a (EUMS INT) i situacijska soba (SITROOM), koji djeluju zajedno kao Služba za jedinstvenu obavještajnu analizu (SIAC), jedinica EU-a za otkrivanje hibridnih prijetnji (sjedište u INTCEN-u), tim za hitne računalne intervencije institucija EU-a (CERT-EU) i Centar za odgovor na krizne situacije i koordinaciju u Europskoj komisiji.

(16) Suradnja među državama članicama u odgovoru na kiberincidente na tehničkoj razini osigurana je mrežom timova za odgovor na računalne sigurnosne incidente (CSIRT) koja je uspostavljena Direktivom NIS. ENISA osigurava tajništvo za mrežu i aktivno podupire suradnju među CSIRT-ima. Nacionalni CSIRT-i i tim za hitne

([1]) Dokument 14540/16, 15. studenoga 2016.
([2]) Dodatne informacije na raspolaganju su u odjeljku 3.1. Dodatka o upravljanju krizama, mehanizmima suradnje i akterima na razini EU-a
([3]) Ibidem
([4]) Odluka Vijeća 2014/496/ZVSP od 22. srpnja 2014. o aspektima uvođenja, djelovanja i uporabe europskog globalnog navigacijskog satelitskog sustava koji utječu na sigurnost Europske unije i stavljanju izvan snage Zajedničke akcije 2004/552/ZVSP (SL L 219, 25.7.2014., str. 53.).

računalne intervencije institucija EU-a (CERT-EU) surađuju i razmjenjuju informacije na dobrovoljnoj osnovi uključujući, prema potrebi, kao odgovor na kiberincidente koji utječu na jednu državu članicu ili više njih. Na zahtjev predstavnika CSIRT-a države članice, može se razmatrati i, ako je to moguće, odrediti koordinirani odgovor na incident koji je utvrđen u području za koje je nadležna ista ta država članica. Relevantne procedure utvrdit će se u standardnim operativnim postupcima (SOP) mreže CSIRT-a ([1]).

(17) Mreža CSIRT-a zadužena je i za raspravljanje, istraživanje i utvrđivanje daljnjih oblika operativne suradnje, uključujući u vezi s kategorijama rizikâ i incidenata, ranih upozorenja, uzajamne pomoći te načelima i načinima koordinacije kada države članice odgovaraju na prekogranične rizike i incidente.

(18) Skupina za suradnju uspostavljena člankom 11. Direktive NIS zadužena je za strateško usmjeravanje aktivnosti mreže CSIRT-a i raspravljanje o sposobnostima i pripravnosti država članica te, na dobrovoljnoj osnovi, ocjenjivanje nacionalnih strategija za sigurnost mrežnih i informacijskih sustava i učinkovitost CSIRT-a te utvrđivanje najbolje prakse.

(19) Posebna radna skupina unutar skupine za suradnju priprema smjernice za obavješćivanje o incidentima, u skladu s člankom 14. stavkom 7. Direktive NIS, u pogledu okolnosti u kojima su operatori ključnih usluga dužni obavijestiti o incidentima u skladu s člankom 14. stavkom 3. te formatu i postupku za takve obavijesti ([2]).

(20) Svijest i razumijevanje situacije u stvarnom vremenu, izloženost riziku i prijetnje prikupljeni s pomoću izvješćivanja, procjena, istraživanja i analize ključni su za dobro informirano donošenje odluka. Ta „informiranost o stanju" – svih relevantnih dionika – ključna je za učinkovit koordinirani odgovor. Informiranost o stanju uključuje elemente o uzrocima, kao i o učinku i izvoru incidenta. Prepoznato je da to ovisi o razmjeni i dijeljenju informacija među relevantnim strankama u odgovarajućem formatu, upotrebom zajedničke taksonomije za opis incidenta i na primjereno siguran način.

(21) Na kiberincidente se može ogovoriti na različite načine, od utvrđivanja tehničkih mjera, što može uključivati dva ili više tijela koja zajednički istražuju tehničke uzroke incidenta (npr. analiza zlonamjernih programa), ili identificiranja načina na koji organizacije mogu procijeniti jesu li pogođene incidentom (npr. pokazatelji ugroženosti) do operativnih odluka o primjeni takvih mjera i, na političkoj razini, odlukâ o upotrebi drugih instrumenata kao što su okvir za zajednički odgovor na zlonamjerne kiberaktivnosti ([3]) ili operativni protokol EU-a za suzbijanje hibridnih prijetnji ([4]), ovisno o incidentu.

(22) Povjerenje europskih građana i poduzeća u digitalne usluge ključno je za procvat jedinstvenog digitalnog tržišta. Stoga komunikacija u kriznim situacijama ima osobito važnu ulogu u ublažavanju negativnih učinaka kiberincidenata i kiberkriza. Komunikacija se može upotrijebiti i u kontekstu okvira za zajednički diplomatski odgovor kao sredstvo za utjecaj na ponašanje (potencijalnih) napadača koji djeluju iz trećih zemalja. Usklađivanje informiranja javnosti kako bi se ublažili negativni učinci kiberincidenata i kiberkriza te informiranja javnosti u cilju utjecaja na napadača ključni su za učinkovit politički odgovor.

(23) Učinkovita mjera za ublažavanje kiberincidenata ili kiberkriza velikih razmjera moglo bi biti i informiranje javnosti o tome kako mogu ublažiti učinke incidenta na razini korisnika i organizacije (npr. popravcima sustava ili poduzimanjem dodatnih mjera za izbjegavanje prijetnje itd.).

(24) Komisija u okviru programa „Kibersigurnost infrastrukture za digitalne usluge" Instrumenta za povezivanje Europe (CEF) razvija mehanizam za suradnju između nacionalnih timova za računalne sigurnosne incidente (CSIRT) sudjelujućih država članica za platformu osnovnih usluga pod nazivom MeliCERTes, u cilju poboljšanja njihove razine pripravnosti, suradnje i odgovora na nove kiberprijetnje i kiberincidente. Komisija konkurentnim pozivima na podnošenje prijedloga za dodjelu bespovratnih sredstava u okviru CEF-a sufinancira CSIRT-e u državama članicama u cilju poboljšanja njihovih operativnih kapaciteta na nacionalnoj razini.

([1]) U pripremi; očekuje se da će se donijeti krajem 2017.
([2]) Smjernice bi trebale biti završene do kraja 2017.
([3]) Zaključci Vijeća o okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („Alati za kiberdiplomaciju"), dokument 9916/17.
([4]) Zajednički radni dokument službi Komisije, Operativni protokol EU-a za suzbijanje hibridnih prijetnji, „EU Playbook", SWD(2016) 227 final, 5. srpnja 2016.

(25) Vježbe na području kibersigurnosti na razini EU-a ključne su za poticanje i poboljšanje suradnje među državama članicama i u privatnom sektoru. U tu svrhu ENISA od 2010. organizira redovite sveeuropske vježbe za kiberincidente („Cyber Europe").

(26) Vijeće u svojim Zaključcima ([1]) o provedbi Zajedničke izjave predsjednika Europskog vijeća, predsjednika Europske komisije i glavnog tajnika Organizacije sjevernoatlantskog ugovora poziva na jačanje suradnje u kibervježbama putem uzajamnog sudjelovanja osoblja u vježbama, osobito u vježbama „Cyber Coalition" i „Cyber Europe".

(27) Sve veće nove prijetnje i nedavni kiberincidenti znak su da se Unija suočava sa sve većim rizikom, stoga bi države članice trebale bez odlaganja djelovati u skladu s ovom preporukom, a u svakom slučaju do kraja 2018.,

DONIJELA JE OVU PREPORUKU:

(1) Države članice i institucije EU-a trebale bi uspostaviti okvir EU-a za odgovor na kiberkrize koji uključuje ciljeve i načine suradnje predstavljene u planu uz poštovanje osnovnih načela opisanih u tom dokumentu.

(2) Okvirom EU-a za odgovor na kiberkrize trebalo bi posebno odrediti relevantne aktere, institucije EU-a i tijela država članica na svim potrebnim razinama – tehničkoj, operativnoj, strateškoj/političkoj – te po potrebi razviti standardne operativne postupke kojima bi se utvrdio način suradnje među tim akterima u kontekstu mehanizama EU-a za upravljanje krizama. Naglasak bi trebalo staviti na omogućivanje razmjene informacija bez nepotrebnog odlaganja i koordiniranje odgovora tijekom kiberincidenata i kiberkriza velikih razmjera.

(3) U tu svrhu nadležna tijela država članica trebala bi surađivati kako bi dodatno utvrdila protokole za dijeljenje informacija i suradnju. Skupina za suradnju trebala bi razmjenjivati iskustva u tim pitanjima s relevantnim institucijama EU-a.

(4) Države članice trebale bi osigurati da njihovi nacionalni mehanizmi za upravljanje krizama budu odgovarajući odgovor na kiberincidente te utvrditi potrebne postupke za suradnju na razini EU-a u kontekstu okvira EU-a.

(5) U pogledu postojećih mehanizama EU-a za upravljanje krizama, u skladu s planom države članice trebale bi zajedno sa službama Komisije i ESVD-om utvrditi praktične smjernice za provedbu u pogledu integracije nacionalnih tijela i postupaka za upravljanje krizama i kibersigurnost u postojeće mehanizme EU-a za upravljanje krizama, odnosno u integrirani politički odgovor na krize (IPCR) i mehanizam za odgovor na krize (CRM) ESVD-a. Države članice trebale bi posebno osigurati da su uspostavljene primjerene strukture koje omogućuju učinkovit protok informacija među njihovim nacionalnim tijelima za upravljanje krizama i njihovim predstavnicima na razini EU-a u kontekstu kriznih mehanizama EU-a.

(6) Države članice trebale bi u potpunosti iskoristiti mogućnosti koje im se nude programom „Kibersigurnost: infrastrukture za digitalne usluge" Instrumenta za povezivanje Europe (CEF) i surađivati s Komisijom kako bi se osiguralo da mehanizam za suradnju u okviru platforme osnovnih usluga, koji je trenutačno u pripremi, pruži potrebne funkcionalnosti i ispuni njihove zahtjeve za suradnju i za vrijeme kiberkriza.

(7) Države članice trebale bi uz pomoć ENISA-e i na temelju prethodnog djelovanja u ovom području surađivati na razvoju i donošenju zajedničke taksonomije i obrasca za situacijska izvješća u kojima će se opisati tehnički uzroci i učinci kiberincidenata kako bi dodatno pojačale svoju tehničku i operativnu suradnju za vrijeme kriza. U tom pogledu države članice trebale bi uzeti u obzir tekući rad unutar skupine za suradnju na smjernicama za obavješćivanje o incidentima, posebno aspekte povezane s formatom nacionalnih obavijesti.

(8) Postupke utvrđene u tom okviru trebalo bi testirati i po potrebi revidirati nakon iskustava stečenih sudjelovanjem država članica u kibervježbama na nacionalnoj i regionalnoj razini te na razini Unije, kao i kiberdiplomaciji i kibervježbama NATO-a. Posebno bi ih trebalo testirati u kontekstu vježbi „Cyber Europe" u organizaciji ENISA-e. Vježba „Cyber Europe 2018." prva je prilika za to.

([1]) ST 15283/16, 6. prosinca 2016.

(9) Države članice i institucije EU-a trebale bi redovito vježbati svoj odgovor na kiberincidente i kiberkrize velikih razmjera na nacionalnoj i europskoj razini, uključujući, ako je neophodno, svoj politički odgovor te, prema potrebi, uz uključivanje subjekata iz privatnog sektora.

Sastavljeno u Bruxellesu 13. rujna 2017.

Za Komisiju

Mariya GABRIEL

Članica Komisije

PRILOG

Plan za koordinirani odgovor na prekogranične kiberincidente i kiberkrize velikih razmjera

UVOD

Plan se primjenjuje na kiberincidente koji uzrokuju poremećaje prevelike da bi ih određena država članica mogla sama riješiti te poremećaje koji utječu na dvije države članice ili institucije EU-a ili više njih, a imaju toliko širok i znatan utjecaj tehničkog ili političkog značaja da je potrebna pravodobna koordinacija politika te odgovor na političkoj razini Unije.

Takvi se kiberincidenti velikih razmjera smatraju „kiberkrizama".

U slučaju kiberkrize u EU-u, Vijeće s pomoću integriranih aranžmana EU-a za politički odgovor na krize (IPCR) provodi koordinaciju na političkoj razini Unije.

Koordinacija unutar Komisije održat će se u skladu sa sustavom za brzo uzbunjivanje ARGUS.

Ako kriza ima znatan utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku (ZSOP), aktivira se ESVD-ov mehanizam za odgovor na krize.

U Planu se opisuje kako bi se za te učinkovite mehanizme upravljanja krizama trebalo u potpunosti koristiti postojećim subjektima za kibersigurnost na razini EU-a te mehanizama suradnje između država članica.

U tu se svrhu u Planu uzima u obzir niz vodećih načela (proporcionalnost, supsidijarnost, komplementarnost i povjerljivost informacija), predstavljaju temeljni ciljevi suradnje (djelotvoran odgovor, kolektivna informiranost o stanju, informiranje javnosti) na tri razine (strateška/politička, operativna i tehnička), mehanizmi i akteri te aktivnosti u cilju postizanja temeljnih ciljeva.

Plan se ne odnosi na cijeli ciklus upravljanja kriznim situacijama (sprečavanje/ublažavanje, pripravnost, odgovor i oporavak), nego je usmjeren na odgovor. No, usmjeren je i na određene aktivnosti, posebno one povezane s postizanjem kolektivne informiranosti o stanju.

Važno je napomenuti i da kiberincidenti mogu biti uzrok ili dio šire krize koja utječe na druge sektore. S obzirom na to da se očekuje da će većina kiberkriza imati učinak na fizički svijet, svaki se prikladan odgovor mora oslanjati i na aktivnosti ublažavanja u području kibersigurnosti i na aktivnosti iz drugih područja. Aktivnosti za odgovor na kiberkrize trebalo bi koordinirati s drugim mehanizmima upravljanja krizama na razini EU-a te na nacionalnoj ili sektorskoj razini.

Naposljetku, Planom se ne zamjenjuju i ne bi se trebali dovoditi u pitanje postojeći sektorski ili politički mehanizmi, aranžmani ili instrumenti, primjerice program za europski globalni navigacijski satelitski sustav (GNSS) ([1]).

Vodeća načela

U radu na postizanju ciljeva, u utvrđivanju potrebnih aktivnosti i raspodjeli zadaća i odgovornosti odgovarajućih aktera ili mehanizama primjenjivala su se sljedeća vodeća načela, a treba ih poštovati i tijekom pripreme budućih provedbenih smjernica.

Proporcionalnost: Velika većina kiberincidenata koja pogađa države članice ne može se smatrati ni nacionalnim „krizama", a pogotovo ne europskima. Temelj suradnje među državama članicama za odgovor na takve incidente jest mreža timova za odgovor na računalne sigurnosne incidente (CSIRT-i) uspostavljena Direktivom NIS ([2]). Nacionalni timovi za odgovor na računalne sigurnosne incidente dobrovoljno i svakodnevno surađuju i razmjenjuju informacije, među ostalim, kada je to potrebno, kao odgovor na kiberincidente koji pogađaju jednu državu članicu ili više njih, u skladu sa standardnim operativnim postupcima (SOP) mreže timova za odgovor na računalne sigurnosne incidente. U Planu bi se stoga u potpunosti trebali iskoristiti ti standardni operativni postupci te bi se u njemu trebale odražavati sve dodatne zadaće u pogledu kiberkriza.

([1]) Odluka 2014/496/ZVSP.
([2]) Direktiva (EU) 2016/1148.

Supsidijarnost: Ključno načelo jest načelo supsidijarnosti. Države članice imaju primarnu odgovornost za odgovor u slučaju kiberincidenata ili kiberkriza velikih razmjera koje na njih utječu. No, Komisija, Europska služba za vanjsko djelovanje i druge institucije, uredi, agencije i tijela EU-a također imaju važnu ulogu. Ta je uloga jasno utvrđena u aranžmanima za IPCR, ali proizlazi i iz prava Unije ili iz činjenice da kiberincidenti i kiberkrize mogu imati učinak na sve dijelove gospodarske aktivnosti unutar jedinstvenog tržišta, sigurnosne i međunarodne veze Unije kao i na same institucije.

Komplementarnost: U Planu se u potpunosti uzimaju u obzir postojeći mehanizmi upravljanja krizama na razini EU-a, odnosno integrirani aranžmani EU-a za politički odgovor na krize (IPCR), ARGUS, ESVD-ov mehanizam za odgovor na krize, uključuje strukture i mehanizme iz nove Direktive NIS, odnosno mrežu timova za odgovor na računalne sigurnosne incidente, kao i relevantne agencije i tijela, i to Agenciju Europske unije za mrežnu i informacijsku sigurnost (ENISA), Europski centar za kiberkriminal pri Europolu (Europol/EC3), Centar EU-a za analizu obavještajnih podataka (INTCEN), Obavještajnu upravu vojnog stožera EU-a (EUMS INT) i situacijsku sobu (SITROOM) u INTCEN-u, koji djeluju zajedno kao Služba za jedinstvenu obavještajnu analizu (SIAC); jedinicu EU-a za otkrivanje hibridnih prijetnji (INTCEN); i tim za hitne računalne intervencije za institucije, tijela i agencije EU-a (CERT-EU). Pritom bi se Planom trebala osigurati što je moguće veća komplementarnost interakcija i suradnje te da ima što manje preklapanja.

Povjerljivost informacija: Sve razmjene informacija u okviru Plana moraju biti u skladu s primjenjivim pravilima o sigurnosti ([1]), o zaštiti osobnih podataka i Protokolom o semaforu ([2]). Za razmjenu klasificiranih podataka, bez obzira na to koji se program klasifikacije primjenjuje, upotrebljavaju se dostupni akreditirani alati ([3]). Kad je riječ o obradi osobnih podataka, poštuju se primjenjiva pravila EU-a, posebno Opća uredba o zaštiti podataka ([4]), Direktiva o e-privatnosti ([5]) i Uredba ([6])„o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka".

Temeljni ciljevi

Suradnja u okviru Plana slijedi pristup u tri prethodno navedene razine: politička, operativna i tehnička. Suradnja na svakoj razini može uključivati razmjenu informacija i zajedničke mjere te nastoji ostvariti sljedeće temeljne ciljeve.

— Omogućiti učinkovit odgovor: Odgovoriti se može na različite načine, od identificiranja tehničkih mjera koje mogu uključivati dva ili više tijela koji zajednički istražuju tehničke uzroke incidenta (npr. analiza zlonamjernih programa) ili identificiranja načina na koji organizacije mogu procijeniti je li incident na njih utjecao (npr. pokazatelji ugroženosti) do operativnih odluka o primjeni takvih mjera, i na političkoj razini, ovisno o incidentu, odluke o pokretanju drugih instrumenata, primjerice diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („alati za kiberdiplomaciju") ili operativnog protokola EU-a za suzbijanje hibridnih prijetnji, ovisno o incidentu.

— Informirati o stanju: za koordinirani odgovor ključno je dovoljno dobro poznavanje tekućih događaja od strane svih relevantnih dionika na svim trima razinama (tehnička, operativna, politička). Informiranost o stanju može uključivati tehničke elemente o uzrocima te o učinku i izvoru incidenta. S obzirom na to da kiberincidenti mogu utjecati na širok raspon sektora (financije, energetika, promet, zdravstvo itd.), ključno je da odgovarajuće informacije, u odgovarajućem formatu, u zadanom roku dopru do svih bitnih dionika.

([1]) Odluka Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji (SL L 72, 17.3.2015., str. 41.) i Odluka Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 72, 17.3.2015., str. 53.); Odluka Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku od 19. travnja 2013. o sigurnosnim pravilima Europske službe za vanjsko djelovanje (SL C 190, 29.6.2013., str. 1.); Odluka Vijeća 2013/488/EU od 23. rujna 2013. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 274, 15.10.2013., str. 1.).

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

([3]) Ti su kanali za prijenos u lipnju 2016. uključivali CIMS (Sustav za upravljanje klasificiranim podacima), ACID (algoritam za dešifriranje), RUE (sigurnosni sustav za stvaranje, razmjenu i pohranu dokumenata RESTREINT UE/EU RESTRICTED) i SOLAN. Drugi načini, npr. prijenos klasificiranih podataka uključuju PGP ili S/MIME.

([4]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

([5]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

([6]) Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12.1.2001., str. 1.) – u postupku revizije.

— Usuglasiti se oko ključnih poruka tijekom informiranja javnosti ([1]): Komunikacija o krizama važna je za ublažavanje negativnih učinaka kiberincidenata i kiberkriza, a mogu se upotrijebiti i kao sredstvo za utjecanje na ponašanje (potencijalnih) počinitelja incidenata. Odgovarajuća poruka može služiti i kao jasan pokazatelj vjerojatnih posljedica diplomatske reakcije u cilju utjecanja na ponašanje počinitelja incidenta. Kako bi politički odgovor bio učinkovit, bitno je uskladiti informiranje javnosti u cilju ublažavanja negativnih učinaka kiberincidenata i kiberkriza s informiranjem javnosti u cilju utjecanja na počinitelje incidenata. U području kibersigurnosti iznimno je važno širenje točne konkretne informacije o tome kako se mogu ublažiti posljedice incidenta (npr. popravak sustava ili poduzimanje dodatnih mjera za izbjegavanje prijetnje itd.).

SURADNJA MEĐU DRŽAVAMA ČLANICAMA TE IZMEĐU DRŽAVA ČLANICA I AKTERA EU-A NA TEHNIČKOJ, OPERATIVNOJ I STRATEŠKOJ/POLITIČKOJ RAZINI

Učinkovit odgovor na kiberincidente ili kiberkrize velikih razmjera na razini EU-a ovisi o djelotvornoj tehničkoj, operativnoj i strateškoj/političkoj suradnji.

Na svakoj razini uključeni akteri moraju provesti posebne aktivnosti za postizanje tri temeljna cilja:

— koordinirani odgovor,

— kolektivna informiranost o stanju,

— informiranje javnosti.

Tijekom incidenta ili krize, niže razine suradnje upozorit će, informirati i poduprijeti više razine, a one će za niže razine osigurati smjernice ([2]) i donijeti odluke, prema potrebi.

Suradnja na tehničkoj razini

Opseg djelatnosti:

— rješavanje incidenta ([3]) tijekom kiberkrize,

— praćenje i nadzor incidenta, uključujući sustavne analize prijetnji i rizika.

Potencijalni akteri:

Središnji mehanizam za suradnju na tehničkoj razini u Planu jest mreža timova za odgovor na računalne sigurnosne incidente, kojom predsjeda predsjedništvo i tajništvo koje osigurava ENISA.

— Države članice:

  — nadležna tijela i jedinstvene kontaktne točke uspostavljene Direktivom NIS,

  — timovi za odgovor na računalne sigurnosne incidente (CSIRT-i),

— Tijela/uredi/agencije EU-a:

  — ENISA,

  — Europol/EC3,

  — CERT-EU,

([1]) Ovdje je važno napomenuti da se informiranje javnosti može odnositi na informiranje šire javnosti o incidentu te na priopćavanje tehničkih ili operativnih informacija ključnim i/ili pogođenim sektorima. To može zahtijevati upotrebu povjerljivih distribucijskih kanala i upotrebu posebnih tehničkih alata/platformi. U svakom slučaju, komunikacija s operaterima i širom javnosti u svim državama članicama isključivo je pravo i odgovornost svake države članice. Stoga, u skladu s prethodno navedenim načelom supsidijarnosti, države članice i nacionalni timovi za odgovor na računalne sigurnosne incidente imaju krajnju odgovornost za informacije koje se distribuiraju na njihovu državnom području, odnosno svojim partnerima.

([2]) „dopuštenja za djelovanje” – u kontekstu kiberkrize, za utvrđivanje odgovarajućih mjera za ublažavanje posljedica ključna je brza reakcija. Kako bi se omogućila brza reakcija, jedna država članica može drugoj izdati dobrovoljna „dopuštenja za djelovanje”, bez savjetovanja s višim razinama ili institucijama EU-a i ne nužno putem svih uobičajenih službenih kanala ako to nije potrebno u određenom incidentu (npr. tim za odgovor na računalne sigurnosne incidente ne bi se trebao savjetovati s višim razinama kako bi proslijedio vrijedne informacije timu za odgovor na računalne sigurnosne incidente u drugoj državi članici).

([3]) „rješavanje incidenta” znači svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega;

— Europska komisija:

  — ERCC (operativna služba koja radi 24 sata na dan, sve dane u tjednu, a nalazi se u GU-u ECHO) i imenovana vodeća služba (koja će se izabrati između GU-ova CNECT i HOME, ovisno o vrsti incidenta), Glavno tajništvo (tajništvo za ARGUS), GU za ljudske resurse (Uprava za sigurnost), GU za informatiku (Operacije sigurnosti informacijske tehnologije),

  — za druge agencije EU-a ([1]) odgovarajuća matična glavna uprava Komisije ili ESVD-a (prva kontaktna točka),

— Europska služba za vanjsko djelovanje (ESVD):

  — SIAC (Služba za jedinstvenu obavještajnu analizu: EU INTCEN i EUMS INT),

  — Situacijska soba EU-a i imenovana zemljopisna ili tematska služba,

  — Jedinica EU-a za otkrivanje hibridnih prijetnji (dio EU INTCEN-a, kibersigurnost u kontekstu hibridnih prijetnji).

Kolektivna informiranost o stanju:

— Kao dio redovne suradnje na tehničkoj razini u cilju podupiranja informiranosti o stanju Unije, ENISA bi trebala redovito pripremati Tehničko izvješće o kibersigurnosnoj situaciji u EU-u o incidentima i prijetnjama, na temelju javno dostupnih informacija, vlastitih analiza i izvješća koja s njom (na dobrovoljnoj bazi) dijele timovi država članica za odgovor na računalne sigurnosne incidente (CSIRT-i), ili jedinstvene kontaktne točke utvrđene Direktivom NIS, Europski centar za kiberkriminal pri Europolu (EC3), Tim za hitne računalne intervencije (CERT-EU) te Centar EU-a za analizu obavještajnih podataka (INTCEN) pri Europskoj službi za vanjsko djelovanje (ESVD). Izvješće bi trebalo stavljati na raspolaganje relevantnim instancama pri Vijeću, Komisiji, visokoj predstavnici/potpredsjednici i mreži timova za odgovor na računalne sigurnosne incidente.

— U slučaju većih incidenata, predsjednik mreže timova za odgovor na računalne sigurnosne incidente (CSIRT-i) uz pomoć agencije ENISA priprema izvješće o stanju nakon kiberincidenta ([2]), koje se podnosi predsjedništvu Vijeća, Komisiji i visokoj predstavnici/potpredsjednici preko tima za odgovor na računalne sigurnosne incidente (CSIRT-i) rotirajućeg predsjedništva.

— *Sve ostale agencije EU-a* podnose izvješće svojim matičnim GU-ima, koji zatim izvješćuju glavnu službu Komisije.

— *CERT-EU* podnosi tehnička izvješća mreži timova za odgovor na računalne sigurnosne incidente, institucijama i agencijama EU-a (prema potrebi) i ARGUS-u (ako je aktiviran).

— *Europol/EC3* ([3]) *i CERT-EU* mreži timova za odgovor na računalne sigurnosne incidente osiguravaju stručne forenzičke analize tehničkih predmeta i drugih tehničkih informacija.

— ESVD SIAC: U ime INTCEN-a, jedinica EU-a za otkrivanje hibridnih prijetnji podnosi izvješće relevantnim odjelima ESVD-a.

Odgovor:

— *Mreža timova za odgovor na računalne sigurnosne incidente* razmjenjuje tehničke podatke i analize o incidentu, primjerice IP adrese, pokazatelje ugroženosti ([4]) itd. Takve informacije trebalo bi dostaviti ENISA-i bez nepotrebnog odlaganja, najkasnije u roku od 24 sata od trenutka kada je incident utvrđen.

— U skladu sa standardnim operativnim postupcima mreže timova za odgovor na računalne sigurnosne incidente, njezini članovi zajedno analiziraju dostupne tehničke predmete i druge tehničke informacije koji se odnose na incident, s ciljem utvrđivanja uzroka i mogućih tehničkih mjera za ublažavanje.

— ENISA pomaže timovima za odgovor na računalne sigurnosne incidente u njihovim tehničkim aktivnostima, oslanjajući se na svoje stručno znanje te u skladu sa svojim mandatom ([5]).

([1]) Ovisno o vrsti incidenta i njegovu učinku na različite sektore (financije, promet, energetika, zdravstvo itd.), bit će uključene i relevantne agencije ili tijela EU-a.

([2]) U Izvješću o stanju nakon kiberincidenta na razini EU-a sabrana su nacionalna izvješća koja podnose nacionalni timovi za odgovor na računalne sigurnosne incidente (CSIRT-i). Format izvješća trebao bi biti opisan u standardnim operativnim postupcima mreže timova za odgovor na računalne sigurnosne incidente.

([3]) U skladu s pravnim okvirom za EC3 i prema uvjetima i postupcima utvrđenima tim pravnim okvirom.

([4]) Pokazatelj ugroženosti (IOC) u računalnoj forenzici jest predmet koji se promatra na mreži ili u operativnom sustavu i koji uz visok stupanj pouzdanosti pokazuje prodor u računalo. Tipični su pokazatelji ugroženosti virusni potpisi i IP adrese, MD5 *hashtagovi* zlonamjernih datoteka ili URL-a te nazivi domena poslužitelja za upravljanje i kontrolu *botnet*.

([5]) Prijedlog Uredbe o ENISA-i, europskoj agenciji za kibernetičku sigurnost i stavljanju izvan snage Uredbe (EU) br. 526/2013 i o certifikaciji u području kibersigurnosti za informacijsku i komunikacijsku tehnologiju („Akt o kibersigurnosti”), 13. rujna 2017.

— Timovi za odgovor na računalne sigurnosne incidente država članica koordiniraju svoje tehničke aktivnosti uz pomoć ENISA-e i Komisije.

— ESVD SIAC: U ime INTCEN-a, jedinica EU-a za otkrivanje hibridnih prijetnji određuje početni postupak prikupljanja dokaza u pokretu.

Informiranje javnosti:

— Timovi za odgovor na računalne sigurnosne incidente izrađuju tehničke preporuke ([1]) i upozorenja o opasnosti ([2]) te ih, nakon postupaka odobrenja koji se primjenjuju u svakom pojedinačnom slučaju, šire u svojim zajednicama i javnosti.

— ENISA olakšava stvaranje i distribuciju informacija zajedničke mreže timova za odgovor na računalne sigurnosne incidente.

— ENISA koordinira svoje aktivnosti informiranja javnosti s mrežom timova za odgovor na računalne sigurnosne incidente i službom glasnogovornika Komisije.

— ENISA i EC3 koordiniraju svoje aktivnosti informiranja javnosti na temelju kolektivne informiranosti o stanju dogovorene među državama članicama. Koordiniraju svoje aktivnosti informiranja javnosti sa službom glasnogovornika Komisije.

— Ako kriza ima znatan utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku (ZSOP), informiranje javnosti trebalo bi se koordinirati s Europskom službom za vanjsko djelovanje i službom glasnogovornika visoke predstavnice/potpredsjednice.

Suradnja na operativnoj razini

Opseg mjera:

— priprema donošenja odluka na političkoj razini,

— koordinacija upravljanja kiberkrizom (prema potrebi),

— procjena posljedica i učinka na razini EU-a i prijedlog mogućih mjera za njihovo ublažavanje.

Potencijalni akteri:

— Države članice:

  — nadležna tijela i jedinstvene kontaktne točke uspostavljene Direktivom NIS,

  — timovi za odgovor na računalne sigurnosne incidente (CSIRT), agencije za kibersigurnost,

  — druga nacionalna sektorska tijela (u slučaju da je incidentom ili krizom pogođeno više sektora),

— Tijela/uredi/agencije EU-a:

  — ENISA,

  — Europol/EC3,

  — CERT-EU,

— Europska komisija:

  — glavni tajnik (odnosno njegov zamjenik) Glavno tajništvo (postupak ARGUS),

  — GU CNECT/GU HOME,

  — sigurnosno tijelo Komisije,

  — druge glavne uprave (u slučaju da je incidentom ili krizom pogođeno više sektora),

([1]) Savjeti tehničke prirode povezani s uzrocima incidenta i moguće mjere ublažavanja
([2]) Informacije o tehničkoj ugroženosti koja se iskorištava kako bi se naštetilo informacijskim sustavima

— Europska služba za vanjsko djelovanje (ESVD):

  — glavni tajnik za odgovor na krize (odnosno njegov zamjenik) i Služba za jedinstvenu obavještajnu analizu (SIAC) (Centar EU-a za analizu obavještajnih podataka (EU INTCEN) i Obavještajna uprava vojnog stožera EU-a (EUMS INT)),

  — Jedinica EU-a za otkrivanje hibridnih prijetnji,

— Vijeće:

  — predsjedništvo (horizontalna radna skupina predsjedništva za kiberpitanja ili Coreper ([1])) uz potporu glavnog tajništva Vijeća (GTV) ili Političkog i sigurnosnog odbora (PSO) ([2]) te, u slučaju aktivacije, uz potporu aranžmanâ za integrirani politički odgovor na krize (IPCR).

Informiranost o stanju:

— potpora izradi političko-strateških izvješća o stanju (npr. izvješća o integriranom osvješćivanju situacije i analizi (ISAA) u slučaju aktivacije aranžmanâ za integrirani politički odgovor na krize (IPCR)),

— *Horizontalna radna skupina Vijeća za kiberpitanja* priprema sastanak Coreper-a ili PSO-a, prema potrebi,

— U slučaju aktivacije IPCR-a:

  — predsjedništvo može organizirati okrugle stolove kao potporu pripremi za Coreper ili Politički i sigurnosni odbor (PSO), u kojem sudjeluju relevantni dionici iz država članica, institucije, agencije i treće strane kao što su zemlje izvan EU-a i međunarodne organizacije. To su krizni sastanci u cilju utvrđivanja uskih grla i izrade prijedloga za djelovanje u pogledu pitanja koja zadiru u više područja.

  — *nadležna služba Komisije ili Europska služba za vanjsko djelovanje (ESVD)* kao vodstvo za integrirano osvješćivanje situacije i analizu (ISAA) priprema izvješće o ISAA-u uz doprinose Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), mreže timova za odgovor na računalne sigurnosne incidente (CSIRT), Europskog centra za kibernetički kriminal (EC3) pri Europolu, Obavještajne uprave vojnog stožera EU-a (EUMS INT), Centra za analizu obavještajnih podataka (INTCEN) i svih drugih relevantnih aktera. Izvješće o integriranom osvješćivanju situacije i analizi (izvješće o ISAA-u) jest procjena na razini EU-a na temelju korelacije tehničkih incidenata i procjene krize (analiza prijetnje, procjena rizika, netehničke posljedice i učinci, aspekti incidenta ili krize koje nisu kibernetičke prirode itd.) prilagođeno potrebama na operativnoj i političkoj razini,

— U slučaju aktivacije ARGUS-a:

  — Tim za hitne računalne intervencije (CERT-EU) i Europski centar za kibernetički kriminal (EC3) ([3]) izravno pridonose razmjeni informacija unutar Komisije,

— U slučaju aktivacije mehanizma za odgovor na krizne situacije ESVD-a:

  — Služba za jedinstvenu obavještajnu analizu (SIAC) intenzivirat će prikupljanje informacija i objediniti informacije iz svih izvora te pripremiti analizu i procjenu incidenta.

Odgovor (na zahtjev s političke razine):

— prekogranična suradnja s jedinstvenom kontaktnom točkom i nacionalnim nadležnim tijelima (Direktiva o MIS-u) radi ublažavanja posljedica i učinaka,

— aktivacija svih tehničkih mjera za ublažavanje i koordinacija tehničkih kapaciteta potrebnih za zaustavljanje ili smanjenje učinka napadâ na ciljane informacijske sustave,

— suradnja i, ako se tako odluči, koordinacija tehničkih kapaciteta u cilju zajedničkog ili kolaborativnog odgovora u skladu sa ***standardnim operativnim postupcima mreže timova za odgovor na računalne sigurnosne incidente***,

— procjena potrebe za suradnjom s relevantnim trećim stranama,

— (u slučaju aktivacije) donošenje odluka unutar međusektorskog postupka koordiniranja krize na visokoj razini (ARGUS),

— (u slučaju aktivacije) priprema odlukâ i koordinacija u skladu s aranžmanima za integrirani politički odgovor na krize (IPCR),

— (u slučaju aktivacije) potpora donošenju odluka u Europskoj službi za vanjsko djelovanje putem mehanizma za odgovor na krizne situacije ESVD-a, uključujući u pogledu kontakata s trećim zemljama i međunarodnim organizacijama te u pogledu svih mjera u cilju zaštite misija u okviru zajedničke sigurnosne i obrambene politike te operacija i delegacija EU-a.

([1]) Odbor stalnih predstavnika Vijeća ili Coreper (članak 240. Ugovora o funkcioniranju Europske unije – UFEU) odgovoran je za pripremu rada Vijeća Europske unije.

([2]) Politički i sigurnosni odbor jest odbor Vijeća Europske unije koji se bavi zajedničkom vanjskom i sigurnosnom politikom (ZVSP) iz članka 38. Ugovora o Europskoj uniji.

([3]) U skladu s pravnim okvirom za EC3 i prema uvjetima i postupcima utvrđenima tim pravnim okvirom.

Informiranje javnosti:

— dogovor o porukama za javnost o incidentu,

— Ako kriza ima znatan utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku (ZSOP), informiranje javnosti trebalo bi se koordinirati s Europskom službom za vanjsko djelovanje i službom glasnogovornika visoke predstavnice/potpredsjednice.

Suradnja na strateškoj/političkoj razini

Potencijalni akteri:

— za države članice, ministri nadležni za kibersigurnost,

— za Europsko vijeće, njegov predsjednik,

— za Vijeće, rotirajuće predsjedništvo,

— kada mjere u okviru „Alata za kiberdiplomaciju”, Politički i sigurnosni odbor (PSO) i Horizontalna radna skupina,

— za Europsku komisiju, predsjednik ili delegirani potpredsjednik/povjerenik,

— visoka predstavnica Unije za vanjske poslove i sigurnosnu politiku/potpredsjednica Europske komisije.

Opseg djelatnosti: strateško i političko upravljanje kibernetičkim i nekibernetičkim aspektima krize, uključujući mjere u skladu s okvirom za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti.

Kolektivna informiranost o stanju:

— utvrditi učinke poremećaja izazvanih krizom na funkcioniranje Unije.

Odgovor:

— aktiviranje dodatnih mehanizama upravljanja krizom odnosno instrumenata, ovisno o prirodi i učinku incidenta. To može uključivati npr. Mehanizam za civilnu zaštitu,

— poduzimanje mjera unutar okvira za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti,

— pogođenim državama članicama staviti na raspolaganje hitnu potporu, primjerice aktivacijom Fonda za hitne kibersigurnosne intervencije ([1]) kad bude primjenjiv,

— suradnja i koordinacija s međunarodnim organizacijama, prema potrebi, kao što su Ujedinjeni narodi (UN), Organizacija za europsku sigurnost i suradnju (OESS) i osobito NATO,

— procjena implikacija za nacionalnu sigurnost i obranu.

Informiranje javnosti:

odluka o zajedničkoj strategiji za komunikaciju s javnošću;

ODGOVOR KOORDINIRAN S DRŽAVAMA ČLANICAMA NA RAZINI EU-A U OKVIRU ARANŽMANÂ ZA INTEGRIRANI POLITIČKI ODGOVOR NA KRIZE (IPCR).

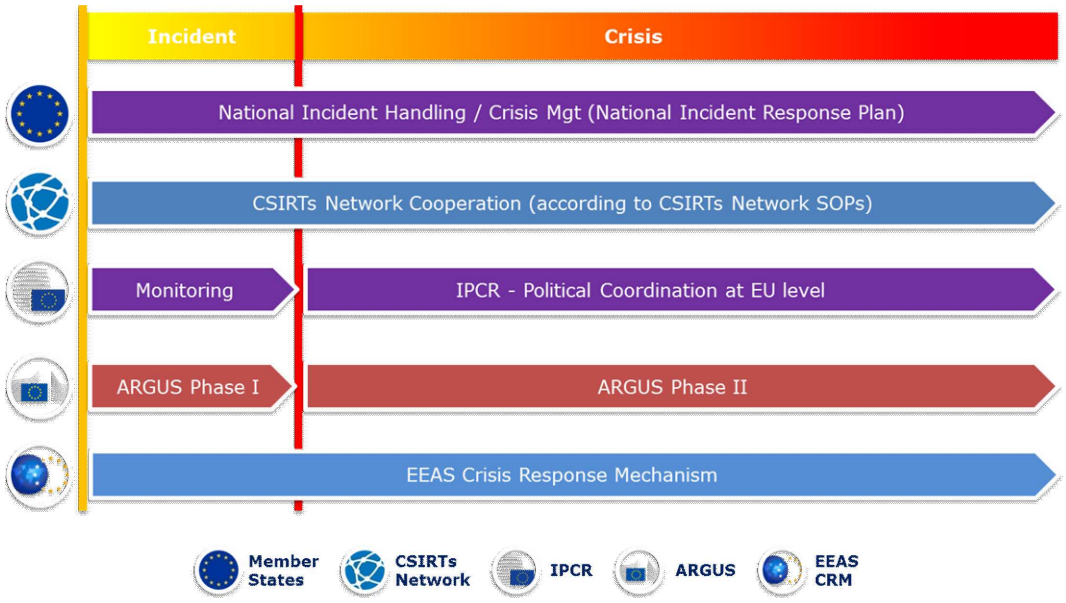
U skladu s načelom komplementarnosti na razini EU-a u ovom odjeljku uvodi se glavni cilj i odgovornosti i aktivnosti tijelâ država članica, mreže timova za odgovor na računalne sigurnosne incidente (CSIRT), Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), Tima za hitne računalne intervencije (CERT-EU), Europskog centra za kibernetički kriminal (EC3) pri Europolu, Centra za analizu obavještajnih podataka (INTCEN), Jedinice EU-a za otkrivanje hibridnih prijetnji te Horizontalne radne skupine Vijeća za kiberpitanja unutar procesa integriranog političkog odgovora na krize (IPCR). Pretpostavlja se da će akteri djelovati u skladu s utvrđenim postupcima na razini EU-a ili nacionalnoj razini.

Bitno je napomenuti da se, kako je prikazano na slici 1., aktivnosti na nacionalnoj razini te suradnja unutar mreže timova za odgovor na računalne sigurnosne incidente (CSIRT) (ako je neophodna) odvijaju tijekom cijelog trajanja incidenta/krize u skladu s načelima supsidijarnosti i proporcionalnosti, bez obzira na aktivaciju mehanizama EU-a za upravljanje krizom.

([1]) Fond za hitne kibersigurnosne intervencije jest mjera predložena u zajedničkoj komunikaciji „Otpornost, odvraćanje i obrana: izgradnja snažne kibersigurnosti za EU”, JOIN(2017) 450/1.

Slika 1.

Odgovor na kiberincident/kiberkrizu na razini EU-a



Sve aktivnosti opisane u nastavku teksta moraju se provoditi u skladu sa standardnim operativnim postupcima/pravilima uključenih mehanizama suradnje te u skladu s utvrđenim mandatima i nadležnostima pojedinačnih aktera i institucija. Mogu biti potrebne neke nadopune ili modifikacije tih postupaka/pravilâ kako bi se postigla najbolja moguća suradnja i učinkovit odgovor na kiberincidente i kiberkrize velikih razmjera.

Nisu svi akteri navedeni u nastavku teksta dužni djelovati tijekom svakog incidenta. Bez obzira na to, Planom i relevantnim standardnim operativnim postupcima mehanizama suradnje trebalo bi predvidjeti njihovo potencijalno uključivanje.

S obzirom na to da stupnjevi utjecaja kiberincidenta ili kiberkrize na društvo mogu biti različiti, primjeren odgovor i visok stupanj fleksibilnosti u pogledu uključenosti sektorskih aktera na svim razinama oslanjat će se na kibernetičke i nekibernetičke mjere ublažavanja.

Upravljanje kibersigurnosnim krizama – Integriranje kibersigurnosti u proces integriranog političkog odgovora na krize (IPCR)

Aranžmani za integrirani politički odgovor na krize (IPCR), opisani u standardnim operativnim postupcima za IPCR ([1]), slijede korake opisane u nastavku teksta (upotreba nekih od tih koraka ovisit će o situaciji).

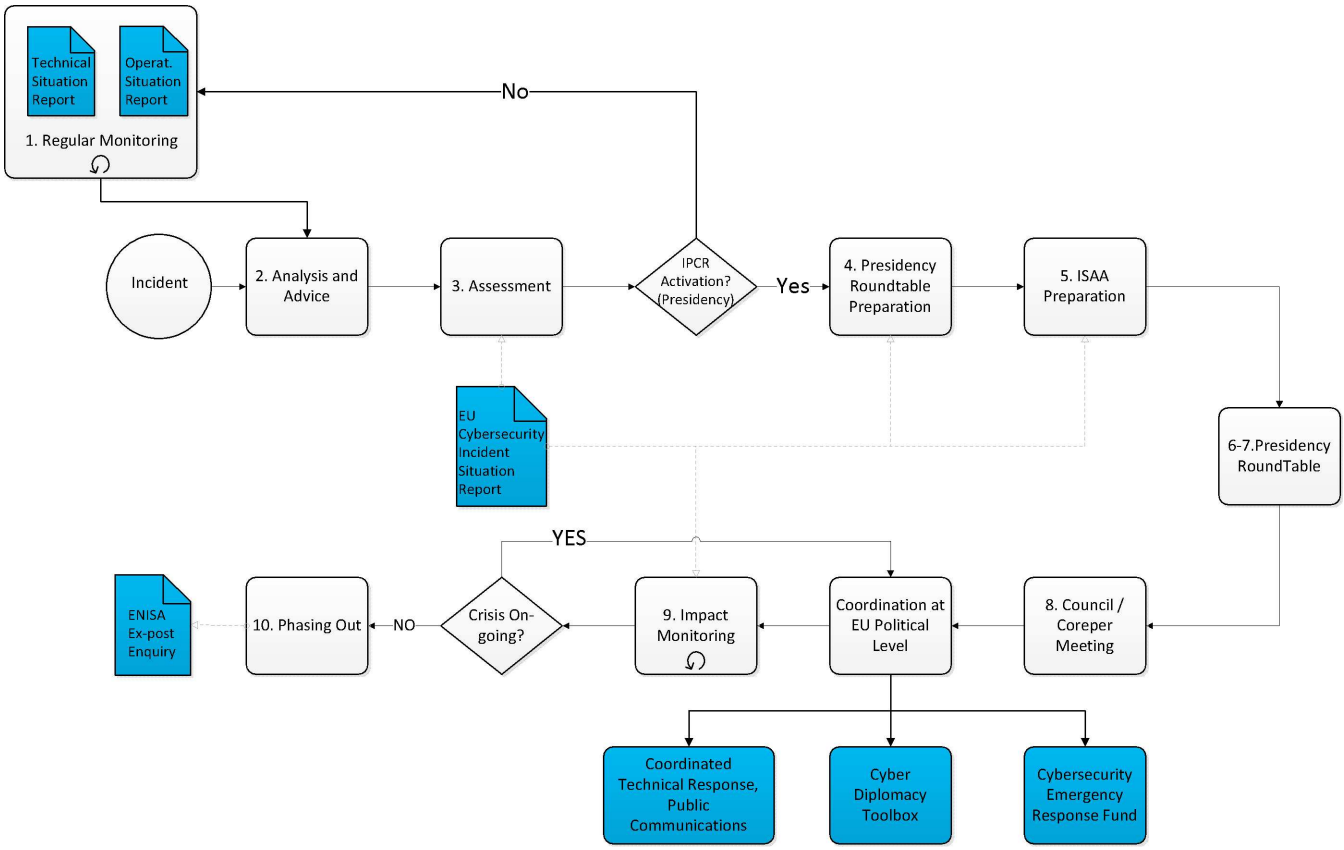
Uz svaki korak navedeni su aktivnosti i akteri specifični za područje kibersigurnosti. Kako bi se olakšalo čitanje, uz svaki korak naveden je citat iz standardnih operativnih postupaka za IPCR, a nakon toga aktivnosti iz Plana. Taj pristup „korak po korak” također omogućuje utvrđivanje postojećih **nedostataka** u potrebnim sposobnostima i postupcima koji priječe učinkovit odgovor na kiberkrize.

Slika 2. (u nastavku ([2])) grafički je prikaz procesa IPCR-a u kojem su novi elementi koji se uvode naglašeni u plavoj boji.

([1]) Iz dokumenta 12607/15 „Standardni operativni postupci za IPCR”, koji je donijela Skupina prijatelja predsjedništva i primio na znanje Coreper u listopadu 2015.
([2]) Veća verzija te slike nalazi se u dodatku.

Slika 2.

Kibersigurnosni elementi IPCR-a



Napomena: S obzirom na prirodu hibridnih prijetnji u kibernetičkom području, koje su dizajnirane tako da ostanu ispod praga prepoznatljive krize, EU mora poduzeti preventivne mjere i mjere pripravnosti. Jedinica EU-a za otkrivanje hibridnih prijetnji ima zadaću brzo analizirati relevantne incidente i informirati odgovarajuće koordinacijske strukture. Jedinica za otkrivanje hibridnih prijetnji redovito podnosi izvješća koja mogu pridonijeti informiranom stvaranju sektorskih politika kako bi se pojačala pripravnost.

— **Korak 1. – Redovito sektorsko praćenje i upozoravanje**: postojeća redovita sektorska izvješća o stanju i upozorenja pružaju predsjedništvu Vijeća indikacije o krizi u nastajanju i njezinu mogućem razvoju.

— **Utvrđeni nedostatak**: Zasad nema redovitih i koordiniranih izvješća o kibersigurnosnoj situaciji ni upozorenja u pogledu kibersigurnosnih incidenata (i prijetnji) na razini EU-a.

— **Plan: Praćenje kibersigurnosne situacije u EU-u i izvještavanje o njoj**

— Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA) izrađuje **Redovito tehničko izvješće o kibersigurnosnoj situaciji u EU-u**, o kibersigurnosnim incidentima i prijetnjama, na temelju javno dostupnih informacija, vlastitih analiza i izvješća koja s njom (na dobrovoljnoj bazi) dijele timovi država članica za odgovor na računalne sigurnosne incidente (CSIRT), ili jedinstvene kontaktne točke utvrđene Direktivom o MIS-u, Europski centar za kiberkriminal pri Europolu (EC3), Tim za hitne računalne intervencije (CERT-EU) te Centar EU-a za analizu obavještajnih podataka (INTCEN) pri Europskoj službi za vanjsko djelovanje (ESVD). Izvješće bi trebalo stavljati na raspolaganje relevantnim instancama pri Vijeću, Komisiji i mreži timove za odgovor na računalne sigurnosne incidente (CSIRT).

— U ime Službe za jedinstvenu obavještajnu analizu (SIAC), Jedinica EU-a za otkrivanje hibridnih prijetnji trebala bi sastaviti **operativno situacijsko izvješće o kibersigurnosti u EU-u**. Izvješće je također potpora okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti.

— Oba izvješća dostavljaju se dionicima na razini EU-a i na nacionalnoj razini kako bi se pridonijelo njihovoj informiranosti o stanju i informiranom donošenju odluka te olakšalo prekograničnu regionalnu suradnju.

Nakon otkrivanja incidenta

— **Korak 2. – Analiza i savjeti**: na temelju raspoloživog praćenja i upozoravanja službe Komisije, ESVD i GTV međusobno se informiraju o mogućim razvojima situacije, kako bi mogli savjetovati predsjedništvo Vijeća o mogućoj aktivaciji mehanizma integriranog političkog odgovora na krize (IPCR), u potpunosti ili u obliku razmjene informacija.

  — **Plan:**

    — Za Komisiju, GU CNECT, GU HOME, GU HR.DS i GU DIGIT, uz podršku Agencije Europske unije za mrežnu i informacijsku sigurnost (ENISA), EC3 i CERT-EU.

    — Europska služba za vanjsko djelovanje (ESVD). Oslanjajući se na rad situacijske sobe (SITROOM) i obavještajnih izvora, Jedinica EU-a za otkrivanje hibridnih prijetnji pruža uvid u stanje o stvarnim i potencijalnim hibridnim prijetnjama za EU i njegove partnere, uključujući i kiberprijetnje. Zato, kad analiza i procjena Jedinice EU-a za otkrivanje hibridnih prijetnji upućuju na postojanje mogućih prijetnji protiv države članice, partnerske zemlje ili organizacije, Centar EU-a za analizu obavještajnih podataka (INTCEN) informirat će (najprije) na operativnoj razini u skladu s utvrđenim postupcima. Operativna razina potom će pripremiti preporuke za političku stratešku razinu, uključujući moguću aktivaciju aranžmanâ za upravljanje krizom u obliku praćenja (npr. ESVD-ov mehanizam za odgovor na krize ili stranica za praćenje u okviru IPCR-a).

    — Predsjednik mreže timova za odgovor na računalne sigurnosne incidente (CSIRT) uz pomoć agencije ENISA priprema izvješće o stanju nakon kiberincidenta ([1]) koje se podnosi predsjedništvu Vijeća, Komisiji i visokoj predstavnici/potpredsjednici preko tima za odgovor na računalne sigurnosne incidente (CSIRT) rotirajućeg predsjedništva.

— **Korak 3. – Procjena/odluka o aktivaciji aranžmanâ za integrirani politički odgovor na krize (IPCR)**: predsjedništvo Vijeća procjenjuje potrebu za političkom koordinacijom, razmjenom informacija ili donošenjem odluka na razini EU-a. U tu svrhu, predsjedništvo Vijeća može sazvati neformalni okrugli stol. Predsjedništvo inicijalno utvrđuje područja koja zahtijevaju uključivanje Coreper-a ili Vijeća. To će biti temelj za smjernice za izradu izvješćâ o integriranom osvješćivanju situacije i analizi (izvješća o ISAA-u). S obzirom na svojstva krize, njezine moguće posljedice i s tim povezane političke potrebe, predsjedništvo će odlučiti o primjerenosti sazivanja sastanaka relevantnih radnih skupina Vijeća i/ili Coreper-a i/ili Političkog i sigurnosnog odbora (PSO).

  — **Plan:**

    — Sudionici okruglog stola:

      — Službe Komisije i ESVD savjetovat će predsjedništvo u skladu sa svojim područjima nadležnosti.

      — Predstavnici država članica u Horizontalnoj radnoj skupini za kiberpitanja uz podršku stručnjaka iz glavnih gradova (CSIRT-ovi, tijela nadležna za kibersigurnost i drugi).

      — Političke/strateške smjernice za izvješća o integriranom osvješćivanju situacije i analizi (izvješća o ISAA-u) na temelju najnovijeg izvješća o stanju nakon kiberincidenta na razini EU-a i dodatnih informacija dobivenih od sudionika okruglog stola.

      — Relevantne radne skupine i odbori:

        — Horizontalna radna skupina za kiberpitanja.

  Komisija, ESVD i Glavno tajništvo Vijeća (GTV) uz potpuni pristanak i pridruživanje predsjedništva, mogu donijeti odluku o aktivaciji IPCR-a u obliku razmjene informacija uspostavom stranice posvećene krizi, kako bi se pripremio teren za moguću punu aktivaciju.

— **Korak 4. – Aktivacija IPCR-a/prikupljanje i razmjena informacija**: nakon aktivacije (bilo potpune, bilo u obliku razmjene informacija), osniva se stranica posvećena krizi na *web*-platformi za IPCR koja omogućuje određenu razmjenu informacija usredotočenu na aspekte koji će pridonijeti izvješćima o integriranom osvješćivanju situacije i analizi (o ISAA-u) i pripremi rasprave na političkoj razini. Koja će služba voditi izradu izvješća o ISAA-u (jedna od službi Komisije ili ESVD) ovisit će o okolnostima konkretnog slučaja.

— **Korak 5. – izrada izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u)**: pokrenut će se izrada izvješća o ISAA-u. Komisija/ESVD podnosi izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u) kako je navedeno u standardnim operativnim postupcima za ISAA i može dodatno poticati razmjenu informacija na *web*-platformi za IPCR ili upućivati konkretne zahtjeve za pružanje informacija. Izvješća o integriranom osvješćivanju

([1]) U Izvješću o stanju nakon kiberincidenta na razini EU-a sabrana su nacionalna izvješća koja podnose nacionalni timovi za odgovor na računalne sigurnosne incidente (CSIRT-i). Format izvješća trebao bi biti opisan u standardnim operativnim postupcima mreže timova za odgovor na računalne sigurnosne incidente.

situacije i analizi (o ISAA-u) bit će prilagođena potrebama političke razine (npr. Coreper ili Vijeće) koju određuje predsjedništvo Vijeća i navodi u svojim smjernicama, omogućavajući strateški pregled situacije i informiranu raspravu o točkama dnevnog reda koje je utvrdilo predsjedništvo Vijeća. U skladu sa standardnim operativnim postupcima za izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u), na temelju prirode kiberkrize određuje se hoće li izvješće izraditi jedna od službi Komisije (GU CNECT, GU HOME) ili ESVD.

Nakon aktivacije integriranog političkog odgovora na krize (IPCR) predsjedništvo Vijeća izložit će posebna područja na koja se treba usredotočiti u izvješću o integriranom osvješćivanju situacije i analizi (o ISAA-u) kako bi se njime poduprla politička koordinacija i/ili proces donošenja odluka u Vijeću. Predsjedništvo Vijeća također će, nakon savjetovanja sa službama Komisije/ESVD-om, odrediti vrijeme za izradu izvješća;

— **Plan:**

— Izvješće o integriranom osvješćivanju situacije i analizi (o ISAA-u) uključuje doprinose relevantnih službi i to:

— mreže timova za odgovor na računalne sigurnosne incidente u obliku izvješća na razini EU-a o stanju nakon kiberincidenta;

— Europskog centra za kiberkriminal pri Europolu (EC3), situacijske sobe (SITROOM), Jedinice EU-a za otkrivanje hibridnih prijetnji, Tima za hitne računalne intervencije (CERT-EU). Jedinica EU-a za otkrivanje hibridnih prijetnji dat će doprinose i potporu službi koja vodi izradu izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u) te okruglom stolu integriranog političkog odgovora na krize, prema potrebi.

— Sektorske agencije i tijela EU-a ovisno o tome koji su sektori pogođeni.

— Tijela država članica (osim timova za odgovor na računalne sigurnosne incidente).

— Prikupljanje povratnih informacija za izvješće o integriranom osvješćivanju situacije i analizi (o ISAA-u) ([1]):

— Komisija i agencije EU-a: IT sustav međusektorskog postupka koordiniranja krize na visokoj razini (ARGUS) bit će okosnica za integrirano osvješćivanje situacije i analizu (ISAA). Svaka agencija EU-a svoje će doprinose dostaviti svojoj odgovornoj glavnoj upravi, koja će potom relevantne informacije proslijediti u ARGUS. Službe Komisije i agencije EU-a prikupljat će informacije od postojećih sektorskih mreža u državama članicama te od međunarodnih organizacija i drugih relevantnih izvora.

— Za ESVD: EU-ova situacijska soba, uz podršku drugih relevantnih odjela ESVD-a, bit će okosnica i jedinstvena kontaktna točka za integrirano osvješćivanje situacije i analizu (ISAA). ESVD prikupljat će informacije od trećih zemalja i relevantnih međunarodnih organizacija.

— **Korak 6. – Priprema za neformalni okrugli stol predsjedništva Vijeća**: predsjedništvo Vijeća, uz pomoć Glavnog tajništva Vijeća (GTV), određuje vrijeme održavanja, dnevni red, sudionike i očekivani ishod (moguće rezultate) neformalnog okruglog stola predsjedništva. GTV u ime predsjedništva Vijeća prosljeđuje relevantne informacije na *web*-platformu za IPCR i izdaje obavijest o sastanku.

— **Korak 7. – Okrugli stol predsjedništva Vijeća/pripremne mjere za političku koordinaciju na razini EU-a/donošenje odluka**: predsjedništvo Vijeća saziva neformalni okrugli stol radi pregleda situacije te pripreme i pregleda elemenata na koje treba upozoriti Coreper ili Vijeće. Neformalni okrugli stol predsjedništva bit će i forum za razvoj i preispitivanje svih prijedloga za djelovanje, koji se podnose Coreper-u/Vijeću, te za raspravu o njima.

— **Plan:**

— Horizontalna radna skupina Vijeća za kiberpitanja priprema sastanke Coreper-a ili Političkog i sigurnosnog odbora (PSO).

— **Korak 8. – Politička koordinacija i donošenje odluka na sastanku Coreper-a/Vijeća**: rezultati sastanaka Coreper-a/Vijeća tiču se koordinacije odgovora na svim razinama, odluka o izvanrednim mjerama, političkim izjavama itd. Te odluke ujedno čine ažurirane političke/strateške smjernice za daljnju izradu izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u).

— **Plan:**

— Politička odluka o koordinaciji odgovora na kiberkrizu provodi se kroz aktivnosti (odgovarajućih aktera) prethodno opisane u odjeljku 1. „Suradnja na strateškoj/političkoj, operativnoj i tehničkoj razini" u pogledu **odgovora** i **komunikacije s javnošću**.

— Izrada izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u) nastavlja se na temelju suradnje na tehničkoj, operativnoj i političkoj/strateškoj razini u pogledu **informiranosti o stanju**, što je također prethodno opisano u odjeljku 1.

([1]) Standardni operativni postupci za integrirano osvješćivanje situacije i analizu (ISAA).

— **Korak 9. – Praćenje učinka**: služba koja vodi izradu izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u) daje (uz potporu svih koji doprinose ISAA-u) informacije o razvoju krize i o učinku donesenih političkih odluka. Ta povratna veza bit će potpora procesu koji se razvija i odluci predsjedništva Vijeća u nastavljanju uključenosti EU-ove političke razine ili u postupnom okončanju integriranog političkog odgovora na krize (IPCR);

— **Korak 10. – Postupno okončanje**: nakon istog postupka kao pri aktivaciji, predsjedništvo Vijeća može sazvati neformalni okrugli stol radi procjene je li potrebno nastaviti s aktivnostima u okviru integriranog političkog odgovora na krize (IPCR). Predsjedništvo Vijeća može odlučiti hoće li sniziti stupanj aktivacije ili je okončati.

— **Plan:**

— ENISA može biti pozvana da, u skladu sa svojim mandatom, provede *ex-post* tehničku istragu incidenta ili joj doprinese.

DODATAK

1. UPRAVLJANJE KRIZAMA, MEHANIZMI SURADNJE I AKTERI NA RAZINI EU-A

Mehanizmi za upravljanje krizama

Aranžmani za integrirani odgovor na političke krize (IPCR): aranžmani za integrirani odgovor na političke krize (IPCR), koje je Vijeće odobrilo 25. lipnja 2013. ([1]), osmišljeni su da olakšaju pravodobnu koordinaciju i odgovor na političkoj razini EU-a u slučaju velikih kriza. IPCR je i potpora koordinaciji, na političkoj razini, odgovora na pozivanje na klauzulu solidarnosti (članak 222. UFEU-a), kako je definirano u Odluci Vijeća 2014/415/EU o aranžmanima Unije za provedbu klauzule solidarnosti od 24. lipnja 2014. Standardnim operativnim postupcima (SOP) za IPCR ([2]) utvrđuju se aktivacijski postupak i daljnja djelovanja.

ARGUS: Sustav za koordinaciju odgovora na krize koji je Europska komisija uspostavila 2005. kao specifični postupak koordinacije za slučaj veće krizne situacije koja zahvaća više sektora. Temelji se na općem sustavu za brzo uzbunjivanje (informatičkom alatu) istog naziva. Sustavom ARGUS predviđene su dvije faze, pri čemu se u fazi II. (u slučaju veće krizne situacije koja zahvaća više sektora) sazivaju sastanci Odbora za koordinaciju kriznih situacija (CCC) pod nadležnošću predsjednika Komisije ili povjerenika kojem je ta odgovornost dodijeljena. U Odboru za koordinaciju kriznih situacija sudjeluju predstavnici relevantnih Glavnih uprava Komisije, kabineta i drugih službi EU-a u cilju vođenja i koordinacije Komisijina odgovora na krizne situacije. Odbor za koordinaciju kriznih situacija, kojim predsjeda zamjenik glavnog tajnika, procjenjuje situaciju, razmatra opcije i poduzima provedive odluke u vezi s alatima i instrumentima EU-a u nadležnosti Komisije te osigurava provedbu tih odluka ([3]) ([4]).

Mehanizam za odgovor na krize (CRM) Europske službe za vanjsko djelovanje: Mehanizam za odgovor na krize (CRM) ESVD-a strukturirani je sustav kojim ESVD odgovara na vanjske krize i krizne situacije ili one s bitnom vanjskom dimenzijom, uključujući i hibridne prijetnje, koje mogu utjecati ili stvarno utječu na interese EU-a ili njezinih država članica. Na sastancima mehanizma za odgovor na krize (CRM) osigurano je sudjelovanje odgovarajućih dužnosnika Komisije i Glavnog tajništva Vijeća, što potiče sinergiju diplomatskih, sigurnosnih i obrambenih djelovanja s financijskim i trgovinskim instrumentima te instrumentima za suradnju kojima upravlja Komisija. Tijekom trajanja krize može se aktivirati krizna ćelija.

Mehanizmi suradnje

Mreža timova za odgovor na računalne sigurnosne incidente (CSIRT): Mreža timova za odgovor na računalne sigurnosne incidente objedinjuje sve nacionalne i vladine timove za odgovor na računalne sigurnosne incidente i Tim za hitne računalne intervencije (CERT-EU). Svrha je mreže omogućiti i poboljšati razmjenu informacija među timovima za odgovor na računalne sigurnosne incidente (CSIRT) o prijetnjama i kiberincidentima i njihovu suradnju pri odgovoru na kiberincidente i kiberkrize.

Horizontalna radna skupina Vijeća za kiberpitanja: radna skupina osnovana je kako bi se osigurala strateška i horizontalna koordinacija područja kiberpolitike u Vijeću, a može sudjelovati u zakonodavnim i nezakonodavnim aktivnostima.

Akteri

Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA): Agencija Europske unije za mrežnu i informacijsku sigurnost osnovana je 2004. Agencija blisko surađuje s državama članicama i privatnim sektorom pružanjem savjeta i rješenja u područjima kao što su sveeuropske vježbe u vezi s kiberincidentima, razvoj nacionalnih strategija za kibersigurnost, suradnja timova za odgovor na računalne sigurnosne incidente (CSIRT) i izgradnja kapaciteta. ENISA izravno surađuje s timovima za odgovor na računalne sigurnosne incidente (CSIRT) u cijelom EU-u i obavlja funkciju tajništva mreže CSIRT-ova.

ERCC: Centar za koordinaciju odgovora na krizne situacije u Europskoj komisiji (u okviru Glavne uprave za europsku civilnu zaštitu i europske operacije humanitarne pomoći (ECHO)) podržava i koordinira široki raspon aktivnosti prevencije, pripravnosti i odgovorâ 24 sata na dan, 7 dana u tjednu. Centar je započeo s radom 2013. i ima ulogu čvorišta u sustavu Komisijina odgovora na krizne situacije (povezan je s ostalim kriznim stožerima EU-a), među ostalim i kao središnja kontaktna točka integriranog političkog odgovora na krize (IPCR) 24 sata na dan, 7 dana u tjednu.

([1]) 10708/13 „Dovršetak postupka preispitivanja aranžmana za koordinaciju odgovora na hitne i krizne situacije: aranžmani EU-a za integrirani odgovor na političku krizu”, koji je Vijeće odobrilo 24. lipnja 2013.
([2]) 12607/15 „Standardni operativni postupci za IPCR”, koji je donijela Skupina prijatelja predsjedništva i primio na znanje Coreper u listopadu 2015.
([3]) Odredbe Komisije o općem sustavu za brzo uzbunjivanje „ARGUS”, COM(2005) 662 final, 23. prosinca 2005.
([4]) Odluka Komisije 2006/25/EZ, Euratom od 23. prosinca 2005. o izmjeni njezinog Poslovnika (SL L 19, 24.1.2006., str. 20.) o uspostavi sustava za brzo uzbunjivanje „ARGUS”.

Europol/EC3: Europski centar za kiberkriminal (EC3) osnovan je 2013. pri Europolu i potpora je odgovoru tijelâ za izvršavanje zakonodavstva na kiberkriminal u EU. EC3 pruža operativnu i analitičku potporu istragama koje provode države članice, središnje je čvorište za razmjenu informacija i obavještajnih podataka o kaznenim djelima i podržava operacije i istrage koje provode države članice operativnim analizama, koordinacijom i stručnim znanjem te visoko specijaliziranom tehničkom i digitalnom forenzičkom potporom.

CERT-EU: Tim za hitne računalne intervencije (CERT-EU) institucija, tijela i agencija EU-a ima mandat poboljšati zaštitu institucija, tijela i agencija EU-a protiv kiberprijetnji. Član je mreže timova za odgovor na računalne sigurnosne incidente (CSIRT). CERT-EU ima tehničke sporazume o razmjeni informacija o kiberprijetnjama sa službom NATO CIRC, određenim trećim zemljama i glavnim komercijalnim akterima u području kibersigurnosti.

Obavještajna zajednica EU-a obuhvaća Centar EU-a za analizu obavještajnih podataka (**INTCEN**) i Obavještajnu upravu vojnog stožera EU-a (EUMS INT) u skladu s aranžmanom SIAC **Službe za jedinstvenu obavještajnu analizu** (SIAC). Misija je Službe za jedinstvenu obavještajnu analizu izrada obavještajnih analiza, rano upozoravanje i pružanje uvida u stanje visokoj predstavnici Unije za vanjske poslove i sigurnosnu politiku i Europskoj službi za vanjsko djelovanje (ESVD). SIAC svoje usluge u području zajedničke vanjske i sigurnosne politike (ZVSP), zajedničke sigurnosne i obrambene politike (ZSOP) i borbe protiv terorizma pruža raznim tijelima EU-a koja donose odluke kao i državama članicama. EU INTCEN i EUMS INT nisu operativne agencije i nemaju mogućnost prikupljanja podataka. Operativna obavještajna razina u nadležnosti je država članica. SIAC se bavi jedino strateškim analizama.

Jedinica EU-a za otkrivanje hibridnih prijetnji: U Zajedničkoj komunikaciji o suzbijanju hibridnih prijetnji iz travnja 2016. utvrđuje se da je jedinica EU-a za otkrivanje hibridnih prijetnji (EU HFC) središnja točka za sve analize izvora o hibridnim prijetnjama u EU-u: njezin je mandat u prosincu 2016. odobrila Komisija na temelju savjetovanja među službama. Jedinica EU-a za otkrivanje hibridnih prijetnji smještena je u Centru EU-a za analizu obavještajnih podataka (INTCEN) i dio je Službe za jedinstvenu obavještajnu analizu (SIAC), stoga surađuje s Obavještajnom upravom vojnog stožera EU-a (EUMS INT) i dodijeljen joj je stalni pripadnik vojnih snaga. Pojam „hibridni" odnosi se na namjerno djelovanje državnog ili nedržavnog subjekta koje obuhvaća kombinaciju višestrukih tajnih/javnih, vojnih/civilnih instrumenata i sredstava pritiska, kao što su kibernapadi, kampanje dezinformiranja, špijunaža, gospodarski pritisak, upotreba zamjenskih vojnih snaga („rat preko posrednika") ili druge subverzivne aktivnosti. EU HFC surađuje s razgranatom mrežom kontaktnih točaka, i unutar Komisije i u državama članicama, radi pružanja integriranog odgovora/pristupa cjelovitog upravljanja koji su potrebni radi suočavanja s različitim izazovima.

Situacijska soba EU-a: Situacijska soba EU-a dio je Obavještajnog i situacijskog centra EU-a (EU INTCEN), koji Europskoj službi za vanjsko djelovanje osigurava operativne kapacitete u cilju trenutačnog i učinkovitog odgovora na krizna stanja. Riječ je o stalnom civilno-vojnom tijelu u stalnoj pripravnosti koje provodi globalno praćenje i osigurava uvid u stanje s kapacitetom 24 sata na dan, 7 dana u tjednu.

Relevantni instrumenti

Okvir za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti: Okvir je dogovoren u lipnju 2017. i dio je pristupa EU-a kiberdiplomaciji, kojim se pridonosi sprečavanju sukoba, ublažavaju kiberprijetnji i većoj stabilnosti u međunarodnim odnosima. Okvir u cijelosti iskorištava mjere u području zajedničke vanjske i sigurnosne politike, a prema potrebi i primjenu restriktivnih mjera. Upotreba mjera unutar Okvira trebala bi poticati suradnju, olakšati ublažavanje trenutačnih i dugoročnih prijetnji i dugoročno utjecati na postupanje odgovornog počinitelja i potencijalnih agresora.

2. KOORDINACIJA KIBERKRIZA U ARANŽMANIMA ZA INTEGRIRANI ODGOVOR NA POLITIČKU KRIZU (IPCR) – HORIZONTALNI ELEMENT KOORDINACIJE I POLITIČKA ESKALACIJA

Aranžmani za integrirani odgovor na političku krizu mogu se upotrijebiti (i upotrebljavani su) za rješavanje tehničkih i operativnih pitanja, ali uvijek iz političke/strateške perspektive.

U smislu eskalacije integrirani odgovor na političku krizu (IPCR) može se upotrijebiti, ovisno o razini krize, prelaskom s načina rada „praćenje" na način rada „razmjena informacija", što je prva razina aktivacije IPCR-a, te „punu aktivaciju".

O punoj aktivaciji odlučuje rotirajuće predsjedništvo Vijeća EU-a. Način rada „razmjena informacija" mogu aktivirati Komisija, ESVD i Glavno tajništvo Vijeća. Načini rada „praćenje" i „razmjena informacija" pokreću različite razine razmjene informacija, pri čemu „razmjena informacija" aktivira zahtjev za izradu izvješća o integriranom osvješćivanju

situacije i analizi (izvješće o ISAA-u). U slučaju pune aktivacije organiziraju se sastanci okruglog stola IPCR-a, a sastancima se pridružuje predsjedništvo (obično predsjednik Coreper-a II ili stručnjak u tom području na razini savjetnika stalnog predstavništva, a iznimno su se okrugli stolovi održavali na ministarskoj razini).

Akteri:

Rotirajuće predsjedništvo (obično predsjednik Coreper-a) u rukovodećoj ulozi

Za Europsko vijeće, ured predsjednika

Za Europsku komisiju, razina zamjenika glavnog tajnika/glavne uprave i/ili stručnjaci u tom području

Za ESVD, razina zamjenika glavnog tajnika/glavnog direktora i/ili stručnjaci u tom području

Za Glavno tajništvo Vijeća, ured glavnog tajnika, tim za integrirani politički odgovor na krize i odgovorne glavne uprave

Opseg djelatnosti: Stvaranje zajedničke integrirane slike situacije i jačanje svijesti o uskim grlima ili nedostacima na svakoj od tri razine radi njihova rješavanja na političkoj razini, donošenje odluka za stolom ako su unutar ovlasti sudionika ili izrada prijedloga djelovanja koji se upućuju Coreper-u II i sve do Vijeća.

Kolektivna informiranost o stanju:

(bez aktivacije): Mogu se generirati stranice za praćenje u okviru integriranog odgovora na političku krizu (IPCR) radi praćenja razvoja situacija koje mogu eskalirati u krizu s posljedicama za EU

(način rada „razmjena informacija" u okviru integriranog odgovora na političku krizu): Služba koja vodi izradu izvješća o integriranom osvješćivanju situacije i analizi (o ISAA-u) sastavit će izvješće na temelju informacija koje su dostavile službe Komisije, ESVD i države članice (putem upitnika IPCR-a),

(puna aktivacija integriranog odgovora na političku krizu): uz izvješća o integriranom osvješćivanju situacije i analizi, na neformalnim okruglim stolovima integriranog odgovora na političku krizu okupljaju se razni zainteresirani akteri iz država članica, Komisije, ESVD-a, relevantnih agencija itd. radi raspravljanja o uskim grlima ili nedostacima

Suradnja i odgovor:

Aktiviranje/sinkroniziranje dodatnih mehanizama za upravljanje krizom odnosno instrumenata, ovisno o prirodi i učinku incidenta. Primjerice, mogu uključivati Mehanizam za civilnu zaštitu, Okvir za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti ili „Zajednički okvir za suzbijanje hibridnih prijetnji".

Komunikacija u kriznim situacijama:

Predsjedništvo nakon savjetovanja s relevantnim službama Komisije, Glavnim tajništvom Vijeća i ESVD-om može aktivirati kriznu komunikacijsku mrežu integriranog odgovora na političku krizu radi potpore izradi zajedničkih poruka ili razrade najučinkovitijih komunikacijskih alata.

3. UPRAVLJANJE KIBERSIGURNOSNIM KRIZAMA U ARGUS-U – RAZMJENA INFORMACIJA UNUTAR EUROPSKE KOMISIJE

Suočena s neočekivanim krizama koje su zahtijevale djelovanje na europskoj razini, primjerice terorističkim napadima u Madridu u ožujku 2004., tsunamijem u jugoistočnoj Aziji u prosincu 2004. i terorističkim napadima u Londonu u srpnju 2005., Komisija je 2005. osnovala sustav za koordinaciju odgovora pod nazivom ARGUS, koji se temelji na istoimenom općem sustavu za brzo uzbunjivanje ([1]) ([2]). Svrha mu je omogućiti specifični **postupak koordinacije krize** u slučaju veće krizne situacije koja zahvaća više sektora radi razmjene informacija o krizi u stvarnom vremenu te osigurati brzo donošenje odluka.

U sustavu ARGUS utvrđene su dvije faze s obzirom na ozbiljnost događaja:

Faza I.: primjenjuje se za „razmjenu informacija" o krizi ograničena dosega

([1]) Komisija Europskih zajednica, 23. prosinca 2005., Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Odredbe Komisije o općem sustavu za brzo uzbunjivanje „ARGUS", COM(2005) 662 final.

([2]) Odluka 2006/25/EZ, Euratom.

Primjeri nedavnih zabilježenih događaja koji pripadaju u fazu I. šumski su požari u Portugalu i Izraelu, napad u Berlinu 2016., poplave u Albaniji, uragan Matthew na Haitiju i suša u Boliviji. Bilo koja glavna uprava može pokrenuti postupak za događaj iz faze I. ako smatra da je situacija u području njezine nadležnosti dovoljno ozbiljna da nalaže razmjenu informacija ili da ona može biti korisna. Primjerice, GU CNECT ili GU HOME mogu pokrenuti postupak za događaj iz faze I. ako smatraju da je kibersituacija u području njihove nadležnosti dovoljno ozbiljna da nalaže razmjenu informacija ili da ona može biti korisna.

Faza II.: pokreće se u slučaju veće krizne situacije koja zahvaća više sektora ili predvidive odnosno neposredne prijetnje Uniji.

U fazi II. pokreće se specifični postupak koordinacije koji Komisiji omogućuje donošenje odluka i upravljanje brzim, koordiniranim i dosljednim odgovorom na najvišoj razini u području njezine nadležnosti i u suradnji s drugim institucijama. Faza II. primjenjuje se u slučaju veće krizne situacije koja zahvaća više sektora ili u slučaju predvidive odnosno neposredne prijetnje da će doći do te krizne situacije. Primjeri stvarnih događaja koji pripadaju u fazu II. jesu migracijska/izbjeglička kriza (od 2015. do danas), trostruka katastrofa u Fukushimi (2011.) i erupcija vulkana *Eyjafjallajökull* na Islandu (2010.).

Fazu II. aktivira Predsjednik na vlastitu inicijativu ili na zahtjev člana Komisije. Predsjednik može dodijeliti političku odgovornost za odgovor Komisije povjereniku zaduženom za službu na koju se predmetna kriza najviše odnosi ili tu odgovornost može preuzeti na sebe.

U fazi II. predviđeni su hitni sastanci Odbora za koordinaciju kriznih situacija (CCC). Sastanci se sazivaju pod nadležnošću predsjednika Komisije ili povjerenika kojem je ta odgovornost dodijeljena. Sastanke organizira glavni tajnik putem informatičkog instrumenta ARGUS. Odbor za koordinaciju kriznih situacija (CCC) specifična je operativna struktura za upravljanje krizom koja je uspostavljena u cilju vođenja i koordinacije Komisijina odgovora na krizne situacije, a okuplja predstavnike relevantnih Glavnih uprava Komisije, kabineta i drugih službi EU-a. **Odbor za koordinaciju kriznih situacija**, kojim predsjeda zamjenik glavnog tajnika, **procjenjuje situaciju, razmatra opcije i osigurava provedbu odluka i djelovanja** i istodobno osigurava usklađenost i dosljednost odgovora. Potporu Odboru za koordinaciju kriznih situacija pruža Glavno tajništvo.

4. MEHANIZAM ZA ODGOVOR NA KRIZU (CRM) EUROPSKE SLUŽBE ZA VANJSKO DJELOVANJE

Mehanizam Europske službe za vanjsko djelovanje za odgovor na krizu (CRM) aktivira se nakon nastanka određene ozbiljne situacije ili krizne situacije koja se odnosi na vanjsku dimenziju EU-a ili je na bilo koji način uključuje. Mehanizam za odgovor na krizu (CRM) aktivira zamjenik glavnog tajnika za odgovor na krize, nakon savjetovanja s visokim predstavnikom/potpredsjednikom ili glavnim tajnikom. Visoki predstavnik/potpredsjednik, glavni tajnik, Glavno tajništvo, drugi zamjenik glavnog tajnika ili država članica mogu zatražiti od zamjenika glavnog tajnika za odgovor na krize da pokrene mehanizam za odgovor na krizu.

Mehanizam za odgovor na krizu (CRM) pridonosi usklađenosti EU-a pri odgovoru na krize u okviru sigurnosne strategije. Konkretno, CRM potiče sinergiju diplomatskih, sigurnosnih i obrambenih djelovanja s financijskim i trgovinskim instrumentima te instrumentima za suradnju kojima upravlja Komisija.

Mehanizam za odgovor na krizu povezan je s Komisijinim općim sustavom za brzo uzbunjivanje (ARGUS) i aranžmanima EU-a za integrirani odgovor na političku krizu (IPCR) radi iskorištavanja sinergija u slučaju istodobne aktivacije. Situacijska soba u Europskoj službi za vanjsko djelovanje komunikacijsko je čvorište između ESVD-a i sustavâ za brzo uzbunjivanje u Vijeću i Komisiji.

Obično je prvi korak povezan s provedbom mehanizma za odgovor na krizu sazivanje **kriznog sastanka** među višim rukovodstvom ESVD-a, Komisije i Vijeća na koje se predmetna kriza izravno odnosi. Na kriznom sastanku procjenjuju se kratkoročni učinci krize i može se dogovoriti poduzimanje hitnih mjera, aktiviranje krizne ćelije ili krizne platforme. Ta se djelovanja mogu poduzeti bilo kojim redoslijedom.

Krizna ćelija operativna je soba manjih razmjera u kojoj se okupljaju predstavnici ESVD-a, Komisije i Vijeća koji sudjeluju u odgovoru na kriznu situaciju radi stalnog praćenja krizne situacije i pružanja potpore donositeljima odluka u sjedištu ESVD-a. Nakon aktivacije krizna ćelija djeluje 24 sata na dan, sedam dana u tjednu.

U okviru **krizne platforme** okupljaju se relevantne službe ESVD-a, Komisije i Vijeća radi procjene srednjoročnih i dugoročnih učinaka kriza i dogovora o daljnjem djelovanju. Njome predsjeda visoki predstavnik/potpredsjednik, glavni tajnik ili zamjenik glavnog tajnika za odgovor na krize. Kriznom platformom procjenjuje se učinkovitost djelovanja EU-a u zemlji ili regiji pogođenima krizom, odlučuje o izmjenama dodatnih mjera i razmatraju prijedlozi za djelovanje Vijeća. Krizna je platforma *ad hoc* sastanak, stoga nije stalno aktivna.

Radnu skupinu čine predstavnici službi uključenih u odgovor i može se aktivirati radi praćenja i olakšavanja provedbe odgovora EU-a. Ona evaluira učinak djelovanja EU-a, izrađuje dokumente i opcije politika, surađuje pri izradi političkog okvira za pristup krizama (PFCA), surađuje pri izradi komunikacijske strategije i utvrđuje sve druge aranžmane kojima se može olakšati provedba odgovora EU-a.

5. REFERENTNI DOKUMENTI

U nastavku se nalazi popis referentnih dokumenata koji su uzeti u obzir pri izradi plana:

— Europski okvir suradnje u slučaju kiberkriza, verzija 1., 17. listopada 2012.

— Izvješće o suradnji u slučaju kiberkriza i upravljanju njima, ENISA, 2014.

— Konkretne informacije za odgovor na sigurnosne incidente, ENISA, 2014.

— Uobičajeni postupci za upravljanje krizama na razini EU-a i njihova primjenjivost na kiberkrize, ENISA, 2015.

— Strategije odgovora na incidente i suradnje u slučaju kiberkrize, ENISA, 2016.

— Standardni operativni kiberpostupci EU-a, ENISA, 2016.

— Vodič dobre prakse za upotrebu taksonomija pri sprječavanju i otkrivanju incidenata, ENISA, 2017.

— Komunikacija o jačanju europskog sustava kibernetičke sigurnosti i poticanju konkurentne i inovativne industrije kibernetičke sigurnosti, COM(2016) 410 final, 5. srpnja 2016.

— Zaključci Vijeća o jačanju europskog sustava kiberotpornosti i poticanju konkurentne i inovativne industrije kibersigurnosti – zaključci Vijeća (15. studenoga 2016.), 14540/16

— Odluka Vijeća 2014/415/EU od 24. lipnja 2014. o aranžmanima Unije za provedbu klauzule solidarnosti (SL L 192, 1.7.2014., str. 53.)

— Dovršetak postupka preispitivanja aranžmana za koordinaciju odgovora na hitne i krizne situacije: aranžmani EU-a za integrirani odgovor na političku krizu (IPCR), 10708/13, 7. lipnja 2013.

— Integrirano osvješćivanje situacije i analiza (ISAA) – Standardni operativni postupci, DS 1570/15, 22. listopada 2015.

— Odredbe Komisije o općem sustavu za brzo uzbunjivanja „ARGUS”, COM(2005) 662 final, 23. prosinca 2005.

— Odluka Komisije 2006/25/EZ, Euratom od 23. prosinca 2005. o izmjeni njezinog Poslovnika (SL L 19, 24.1.2006., str. 20.).

— Način rada ARGUS-a, Europska komisija, 23. listopada 2013.

— Zaključci Vijeća o okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („Alati za kiberdiplomaciju”), dokument 9916/17.

— Operativni protokol EU-a za suzbijanje hibridnih prijetnji, „EU Playbook”, SWD(2016) 227

— Mehanizam Europske službe za vanjsko djelovanje za odgovor na krizu, 8. studenoga 2016. (Ares(2017)880661). Zajednički radni dokument službi Komisije, Operativni protokol EU-a za suzbijanje hibridnih prijetnji, „EU Playbook”, SWD(2016) 227 final, 5. srpnja 2016.

— Zajednička komunikacija Europskom parlamentu i Vijeću: Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije, JOIN/2016/018 final, 6. travnja 2016.

— EEAS(2016) 1674 – Radni dokument Europske službe za vanjsko djelovanje – Jedinica EU-a za otkrivanje hibridnih prijetnji – Pravilnik

6. KIBERSIGURNOSNI ELEMENTI U POSTUPKU IPCR-A