Svet
Evropske unije

Bruselj, 6. junij 2025
(OR. en)

9794/25

Medinstitucionalna zadeva:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	6. junij 2025
Prejemnik:	delegacije
Zadeva:	Priporočilo Sveta o načrtu EU za krizno upravljanje kibernetske varnosti – priporočilo Sveta, ki ga je Svet odobril na seji 6. junija 2025

V prilogi vam pošiljamo priporočilo Sveta, ki ga je Svet odobril na seji 6. junija 2025.

PRILOGA

PRIPOROČILO SVETA

o načrtu EU za krizno upravljanje kibernetske varnosti

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti členov 114 in 292 Pogodbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Digitalna tehnologija in globalna povezljivost sta hrbtenica gospodarske rasti, konkurenčnosti in preoblikovanja kritične infrastrukture Unije. Vendar se v medsebojno povezanem in vse bolj digitalnem gospodarstvu povečuje tudi tveganje incidentov na področju kibernetske varnosti in kibernetskih napadov. Poleg tega se zaradi vse večjih geopolitičnih napetosti, konfliktov in strateškega rivalstva povečujejo učinek, obseg in izpopolnjenost zlonamernih kibernetskih dejavnosti. Te dejavnosti so lahko del hibridnih kampanj ali vojaških operacij. Neposredno lahko vplivajo tudi na varnost, gospodarstvo in družbo Unije. Poleg tega imajo lahko učinek prelivanja, predvsem kadar so te dejavnosti usmerjene v mednarodne strateške partnerske države, kot so države kandidatke ali sosednje države.

(2) Velik kibernetski incident lahko povzroči motnjo, ki presega zmožnost države članice za odziv nanj, ali pomembno vpliva na več kot eno državo članico. Tak incident se lahko glede na svoj vzrok in vpliv stopnjuje in sprevrže v popolno krizo, ki vpliva na ustrezno delovanje notranjega trga ali pomeni resno tveganje za javno varnost ter varnost subjektov ali državljanov v več državah članicah ali Uniji kot celoti. Učinkovito krizno upravljanje je bistveno za ohranjanje gospodarske stabilnosti in zaščito evropskih vlad, kritične infrastrukture, podjetij in državljanov ter krepitev mednarodne varnosti in stabilnosti v kibernetskem prostoru. Krizno upravljanje kibernetske varnosti je zato sestavni del krovnega okvira EU za krizno upravljanje.

(3) Glede na medsebojno odvisnost in medsebojno povezanost med okolji IKT subjektov Unije in držav članic lahko incident v subjektu Unije pomeni tveganje za kibernetsko varnost za države članice in obratno. Izmenjava ustreznih informacij in usklajevanje v zvezi z velikimi in večjimi incidenti na področju kibernetske varnosti, kot so opredeljeni v členu 3(8) Uredbe (EU, Euratom) 2023/2841[1], sta ključnega pomena v okviru načrta EU za krizno upravljanje kibernetske varnosti (v nadaljnjem besedilu: kibernetski načrt).

[1] Uredba (EU, Euratom) 2023/2841 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije (UL L, 2023/2841, 18.12.2023, str. 1–27.

(4) V primeru krize, za katero je bila uporabljena enotna ureditev političnega odzivanja EU na krize (IPCR) v skladu z Izvedbenim sklepom Sveta (EU) 2018/1993[2] (v nadaljnjem besedilu: enotna ureditev IPCR), bi moral kibernetski načrt v celoti spoštovati enotno ureditev IPCR za usklajevanje in odzivanje. Politično in strateško usklajevanje bi potekalo v okviru IPCR. Enotna ureditev IPCR je orodje za horizontalno usklajevanje in odzivanje na politični ravni Unije. V skladu z enotno ureditvijo IPCR odločitev o uporabi ali prekinitvi uporabe IPCR sprejme predsedstvo Sveta Evropske unije. Poročila o celostnem zavedanju in analizi razmer (ISAA), ki jih pripravijo službe Komisije in Evropska služba za zunanje delovanje (ESZD), podpirajo delo IPCR tako pri izmenjavi informacij kot pri polni uporabi.

(5) Države članice imajo glavno odgovornost za obvladovanje kibernetskih incidentov in krizno upravljanje kibernetske varnosti. Vendar pa morajo države članice in ustrezni subjekti Unije zaradi morebitne čezmejne in medsektorske narave kibernetskih incidentov sodelovati na tehnični, operativni in politični ravni, da bi zagotovili učinkovito usklajevanje po vsej Uniji. Celotno krizno upravljanje kibernetske varnosti vključuje pripravljenost in skupno situacijsko zavedanje za predvidevanje velikih kibernetskih incidentov, potrebne zmogljivosti za ugotavljanje, katera orodja za odzivanje in obnovo so potrebna, da se ublažijo in omejijo veliki kibernetski incidenti, ter zmogljivosti odzivanja za odvračanje in preprečevanje nadaljnjih incidentov.

[2] Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize (UL L 320, 17.12.2018, str. 28–34).

(6) V Priporočilu Komisije (EU) 2017/1584[3] o usklajenem odzivu na velike kibernetske incidente in krize so določeni cilji in načini sodelovanja med državami članicami in subjekti Unije pri odzivanju na velike kibernetske incidente in krize. Vsebuje opredelitev ustreznih akterjev na tehnični, operativni in politični ravni ter pojasnitev, kako so navedeni akterji vključeni v obstoječe mehanizme kriznega upravljanja Unije, kot je enotna ureditev IPCR. Temeljna načela iz Priporočila (EU) 2017/1584 so še vedno veljavna, in sicer subsidiarnost, dopolnjevanje in zaupnost informacij ter pristop na treh ravneh (tehnični, operativni in politični). To priporočilo temelji na teh temeljnih načelih in je namenjeno nadomestitvi Priporočila (EU) 2017/1584, ki določa nov okvir Unije za krizno upravljanje kibernetske varnosti.

(7) Nekatere opredelitve pojmov, uporabljene v tem priporočilu, temeljijo na opredelitvah pojmov in izrazih, uporabljenih v Direktivi (EU) 2022/2555[4]. Vendar pa se področje uporabe tega priporočila razlikuje od področja uporabe Direktive (EU) 2022/2555. To priporočilo določa okvir Unije za krizno upravljanje kibernetske varnosti v okviru splošne pripravljenosti EU na velike kibernetske incidente in krize, ki izhajajo iz takih incidentov – ne glede na to, kateri sektor ali subjekt je prizadet. Kolikor je to izvedljivo, opredelitve pojmov temeljijo na tistih iz Direktive (EU) 2022/2555.

---

[3] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36–58).

[4] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80–152).

(8) Posodobljen kibernetski načrt je potreben, da se zagotovijo jasne in dostopne smernice, v katerih bo pojasnjeno, kaj je velik kibernetski incident ali kibernetska kriza na ravni Unije, kako se sproži okvir za krizno upravljanje in kakšni so vloge ustreznih omrežij, akterjev in mehanizmov na ravni Unije ter sodelovanje med temi akterji in mehanizmi v celotnem življenjskem ciklu kibernetske krize. Cilj kibernetskega načrta je podpreti širši okvir civilno-vojaških odnosov EU v kontekstu kriznega upravljanja kibernetske varnosti, tudi na podlagi poglabljanja odnosov med EU in Natom, kjer je to mogoče, tudi z vključujočimi, vzajemnimi in nediskriminatornimi izboljšanimi mehanizmi za izmenjavo informacij pri kriznem upravljanju kibernetske varnosti.

(9) Medsektorsko krizno upravljanje na ravni Unije bi bilo treba okrepiti, da bi omogočili celosten odziv na krize, predvsem v primerih, ko veliki kibernetski incidenti in krize povzročajo fizične posledice. To priporočilo dopolnjuje enotno ureditev IPCR in druge mehanizme Unije za krizno upravljanje, vključno s splošnim sistemom Komisije za hitro opozarjanje (ARGUS), mehanizmom Unije na področju civilne zaščite (UCPM), ki ga podpira Center za usklajevanje nujnega odziva (ERCC), ustanovljen v okviru UCPM s Sklepom št. 1313/2013/EU Evropskega parlamenta in Sveta o mehanizmu Unije na področju civilne zaščite[5] („sklep UCPM“), mehanizmom ESZD za odzivanje na krizne razmere (CRM) ter drugimi procesi, kot so tisti, opisani v zbirki orodij EU za kibernetsko diplomacijo[6], naboru orodij EU za odzivanje na hibridne grožnje[7] in v revidiranem protokolu EU za boj proti hibridnim grožnjam[8]. Dopolnjuje tudi Priporočilo Sveta (EU) 2024/4371 o načrtu za usklajeno odzivanje na ravni Unije na motnje na kritični infrastrukturi z velikim čezmejnim pomenom[9] (v nadaljnjem besedilu: načrt EU za kritično infrastrukturo), ki zajema nekibernetsko fizično odpornost in katerega cilj je izboljšati usklajeno odzivanje na ravni Unije na tem področju, in bi moralo biti skladno z navedenim priporočilom.

---

5 Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L 347, 20.12.2013, str. 924–947).

6 Sklepi Sveta o okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti (9916/17)

7 Sklepi Sveta o okviru za usklajen odziv EU na hibridne kampanje (22. junij 2022)

8 Skupni delovni dokument služb Komisije – Protokol EU za preprečevanje hibridnih groženj (SWD(2023) 116 final).

9 UL C, C/2024/4371, 5.7.2024.

(10) Evropska organizacijska mreža za povezovanje v kibernetski krizi (EU-CyCLONe) je mreža za usklajevanje obvladovanja velikih kibernetskih incidentov in kriznega upravljanja na operativni ravni, tudi v primeru medsektorskih velikih kibernetskih incidentov in kibernetskih kriz. Da se obstoječi okviri ne bi dodatno zapletli, se je treba izogibati ustvarjanju sektorskih struktur, ki bi podvajale naloge EU-CyCLONe. EU-CyCLONe bi moral prejemati operativne informacije v zvezi s kibernetsko varnostjo tudi od sektorjev, hkrati pa biti vključen tudi na politični ravni.

(11) Države članice se spodbuja, da izkoristijo vsa finančna sredstva, ki so na voljo za kibernetsko varnost in se zagotavljajo v ustreznih programih Unije. Zagotoviti je treba, da bodo ti programi predstavljali čim manjše upravno breme prosilcem za financiranje in da se sodelovanje držav članic v okviru teh programov olajša z zagotavljanjem ustreznih smernic o izvedljivih možnostih finančne podpore.

(12) To priporočilo prispeva k širšim dejavnostim za pripravljenost, ki jih Unija potrebuje pri soočanju z medsektorskimi krizami, v skladu z načeli, vključenimi v strategijo EU za unijo pripravljenosti, in sicer celostnemu pristopu, ki zajema vse nevarnosti, vključuje celotno vlado in celotno družbo, predvsem glede izboljšanja ozaveščenosti o tveganjih in grožnjah ter medsektorskega odzivanja na krize –

SPREJEL NASLEDNJE PRIPOROČILO:

I: Cilj, področje uporabe in vodilna načela okvira EU za krizno upravljanje kibernetske varnosti

Cilj in področje uporabe

(1) To priporočilo o načrtu EU za krizno upravljanje kibernetske varnosti (v nadaljnjem besedilu: kibernetski načrt) določa okvir Unije za krizno upravljanje kibernetske varnosti v okviru splošne pripravljenosti EU na velike kibernetske incidente in krize. Okvir odraža vloge tako držav članic kot institucij, organov, uradov in agencij Unije („subjekti Unije“) v okviru njihovih pristojnosti, ob vsestranskem spoštovanju nacionalne zakonodaje in notranjih pravil, da se zagotovi celovito in usklajeno ukrepanje na ravni Unije.

(2) Kibernetski načrt bi bilo treba uporabljati v skladu z načrtom EU za kritično infrastrukturo, predvsem v primeru incidentov, ki vplivajo tako na fizično odpornost kot tudi kibernetsko varnost kritične infrastrukture[10].

(3) Kibernetski načrt zagotavlja smernice za odzivanje na velike kibernetske incidente ali kibernetske krize in bi ga bilo treba uporabljati skupaj z vsemi ustreznimi sektorskimi mehanizmi za odzivanje, kot so tisti, navedeni v Prilogi II. Ustrezni deležniki na področju kibernetske varnosti bi morali pomagati pri doseganju ciljev teh sektorskih mehanizmov, tako na nacionalni ravni kot na ravni Unije.

(4) V primeru medsektorske krize s kibernetskimi vidiki na ravni celotne EU, za katero se uporabi IPCR, bi moral Svet usklajevanje odziva na politični ravni Unije izvesti z uporabo enotne ureditve IPCR. Kadar se uporabi IPCR, bi morali ukrepi v okviru kibernetskega načrta podpirati odziv EU na politični ravni in zagotavljati posebno podporo na področju kibernetske varnosti.

[10] Načrt EU za kritično infrastrukturo podrobneje določa usklajevanje v takih primerih v delu I, oddelek 4, Priloge.

Vodilna načela

(5) Za krizno upravljanje kibernetske varnosti na ravni Unije veljajo naslednja vodilna načela:

(a) *Sorazmernost*: večina kibernetskih incidentov, ki prizadenejo države članice, ne dosega ravni, ki bi se lahko štela za velik kibernetski incident ali kibernetsko krizo na nacionalni ravni ali na ravni Unije. V primeru kibernetskih incidentov in groženj države članice prostovoljno in redno sodelujejo in si izmenjujejo informacije v okviru mreže skupin za odzivanje na računalniške varnostne incidente (v nadaljnjem besedilu: mreža CSIRT) in mreže EU-CyCLONe v skladu s standardnimi operativnimi postopki mrež (v nadaljnjem besedilu: SOP).

(b) *Subsidiarnost*: Glavno odgovornost za odzivanje v primeru kibernetskih incidentov, velikih kibernetskih incidentov ali kibernetskih kriz in za njihovo odpravo imajo prizadete države članice. Zaradi morebitnih čezmejnih učinkov bi morali Svet, Komisija, visoki predstavnik, Agencija Evropske unije za kibernetsko varnost (ENISA), Služba za kibernetsko varnost za institucije, organe, urade in agencije Unije (CERT-EU), Europol in vsi drugi ustrezni subjekti Unije sodelovati skozi celoten življenjski cikel krize. Ta vloga izhaja iz prava Unije in odraža, kako veliki kibernetski incidenti in krize prizadenejo enega ali več sektorjev gospodarskih dejavnosti znotraj enotnega trga, vplivajo na varnost in mednarodne odnose Unije, pa tudi same subjekte Unije.

(c) *Dopolnjevanje:* to priporočilo v celoti upošteva obstoječe mehanizme kriznega upravljanja na ravni Unije, ki so navedeni v Prilogi II, še posebej enotno ureditev IPCR, sistem ARGUS in mehanizem ESDZ za krizno odzivanje. To priporočilo upošteva mandate mreže CSIRT in EU-CyCLONe ter Uredbo (EU, Euratom) 2023/2841. Kadar se uporabi IPCR, bi se moralo delo ustreznih mrež, subjektov in uporabljenih sektorskih mehanizmov nadaljevati ter prispevati k političnemu in strateškemu usklajevanju, ki poteka v okviru IPCR, in ga podpirati.

(d) *Zaupnost informacij:* vse izmenjave informacij v okviru tega priporočila bi morale biti v skladu z veljavnimi pravili o varnosti in varstvu osebnih podatkov. Po potrebi bi bilo treba upoštevati neformalne sporazume o zaupnosti, kot je semaforski protokol za označevanje občutljivih informacij. Za izmenjavo tajnih podatkov bi bilo treba ne glede na uporabljeno klasifikacijsko shemo uporabljati obstoječa zavezujoča pravila in sporazume o obdelavi tajnih podatkov skupaj z razpoložljivimi potrjenimi orodji.

(6) V skladu z navedenimi vodilnimi načeli bi morale države članice in subjekti Unije poglobiti sodelovanje na področju kriznega upravljanja kibernetske varnosti, spodbujati medsebojno zaupanje ter graditi na obstoječih omrežjih in mehanizmih. To sodelovanje, v okviru kibernetskega načrta, ima koristi od izvajanja členov 22 in 23 Uredbe (EU, Euratom) 2023/2841. Načrt za obvladovanje kibernetskih kriz, vzpostavljen na podlagi člena 23 Uredbe (EU, Euratom) 2023/2841, med drugim prispeva k redni izmenjavi ustreznih informacij med subjekti Unije in z državami članicami ter opredeljuje ureditve glede usklajevanja in pretoka informacij med subjekti Unije.

II: Opredelitev pojmov

(7) V tem kibernetskem načrtu se uporabljajo naslednje opredelitve pojmov:

(a) „incident“ pomeni dogodek, ki ogroža razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih ti omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni;

(b) „pomemben incident“ pomeni incident, ki:

a. je zadevnemu subjektu povzročil ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube;

b. je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

(c) „velik kibernetski incident“ pomeni incident, ki povzroči motnjo, ki presega zmožnost države članice za odziv nanj, ali incident, ki pomembno vpliva na vsaj dve državi članici;

(d) „kibernetska kriza“ pomeni velik kibernetski incident, ki se je stopnjeval v popolno krizo in ne omogoča ustreznega delovanja notranjega trga ali pomeni resno tveganje za javno varnost ter varnost subjektov ali državljanov v več državah članicah ali Uniji v celoti.

III: Nacionalne strukture in odgovornosti za krizno upravljanje kibernetske varnosti

(8) Glavno odgovornost za odzivanje v primeru velikih kibernetskih incidentov ali kibernetskih kriz imajo prizadete države članice. Vsaka država članica ima v skladu z Direktivo (EU) 2022/2555 enega ali več organov za krizno upravljanje kibernetske varnosti ter eno ali več skupin CSIRT.

(9) S sprejetjem Direktive (EU) 2022/2555 in drugih zakonodajnih in nezakonodajnih instrumentov o kibernetski varnosti so države članice uskladile svoje okvire kibernetske varnosti, tako da so določile minimalna pravila glede delovanja usklajenega regulativnega okvira, uvedle mehanizme za učinkovito sodelovanje med odgovornimi organi v vsaki državi članici ter zagotovile učinkovita pravna sredstva in izvršilne ukrepe, ki so ključni za učinkovito izvrševanje teh obveznosti.

(10) V skladu s členom 9(4) Direktive (EU) 2022/2555 bi morale države članice sprejeti nacionalne načrte za odzivanje na velike kibernetske incidente in krize. Ti načrti med drugim vključujejo nacionalne ukrepe za pripravljenost, postopke za krizno upravljanje kibernetske varnosti ter nacionalne postopke in dogovore med nacionalnimi organi in telesi, da se zagotovi njihovo učinkovito sodelovanje pri usklajenem obvladovanju velikih kibernetskih incidentov in kibernetskih kriz na ravni Unije in podpora temu usklajenemu obvladovanju. Postopki za krizno upravljanje kibernetske zajemajo tudi določbe o njihovi vključitvi v splošni nacionalni okvir za krizno upravljanje in kanale za izmenjavo informacij.

(11) V skladu s členom 9(1) Direktive (EU) 2022/2555 bi morale države članice zagotoviti skladnost z obstoječimi splošnimi nacionalnimi okviri za obvladovanje kriz. V primeru uporabe IPCR bi morali nacionalni organi za krizno upravljanje za namene obveščanja IPCR zbirati prispevke organov za krizno upravljanje kibernetske varnosti in nacionalnih sektorskih kriznih mehanizmov.

(12) V skladu s členom 9(5) Direktive (EU) 2022/2555 bi morala mreža EU-CyCLONe na zahtevo zadevne države članice izmenjati informacije o ustreznih delih nacionalnih načrtov za odzivanje na velike kibernetske incidente in krize, predvsem o določbah za zagotavljanje učinkovitega sodelovanja pri usklajenem obvladovanju velikih kibernetskih incidentov in kibernetskih kriz na ravni Unije in podpore temu usklajenemu obvladovanju, da bi izmenjali najboljše prakse in preučili, ali bi celoten okvir deloval v praksi.

(13) EU-CyCLONe in Medinstitucionalni odbor za kibernetsko varnost (IICB) sta pozvana, da po potrebi izmenjata informacije o skladnosti načrta za krizno upravljanje, ki ga je IICB določil v skladu s členom 23 Uredbe (EU, Euratom) 2023/2841, z nacionalnimi načrti za odzivanje na velike kibernetske incidente in krize.

(14) Mreža EU-CyCLONe bi morala s podporo ENISA kot svojega sekretariata vzdrževati posodobljen seznam nacionalnih organov za krizno upravljanje kibernetske varnosti s kontaktnimi podatki uradnikov in vodstvenih delavcev EU-CyCLONe ter ga dati na voljo članom mreže EU-CyCLONe.

IV: Glavne mreže in akterji v ekosistemu EU za krizno upravljanje kibernetske varnosti

(15) Mreža skupin CSIRT je glavna tehnična mreža za izmenjavo relevantnih informacij o incidentih, zlasti na področju uporabe tega priporočila, v skladu z ustreznimi nalogami, opisanimi v členu 15(3) Direktive (EU) 2022/2555. Prispeva h krepitvi zaupanja ter spodbuja hitro in učinkovito operativno sodelovanje med državami članicami. Njen predsednik lahko sodeluje kot opazovalec v IICB.

(16) CERT-EU je služba za kibernetsko varnost za vse subjekte Unije. Deluje kot vozlišče za izmenjavo informacij o kibernetski varnosti in usklajevanje odzivanja na incidente med subjekti Unije v skladu s členom 13 Uredbe (EU) 2023/2841. Je članica mreže skupin CSIRT in podpira Komisijo v mreži EU-CyCLONe. Deluje na tehnični ravni in je odgovorna za usklajevanje obvladovanja večjih incidentov, ki vplivajo na subjekte Unije.

(17) Mreža EU-CyCLONe deluje kot posrednik med tehnično in politično ravnjo, zlasti med velikimi kibernetskimi incidenti in kibernetskimi krizami. Podpira usklajeno obvladovanje velikih kibernetskih incidentov in kibernetskih kriz na operativni ravni, poleg tega pa zagotavlja redno izmenjavo relevantnih informacij med državami članicami ter institucijami, organi, uradi in agencijami Unije v skladu s členom 16 Direktive (EU) 2022/2555. Njen predsednik lahko sodeluje kot opazovalec v IICB.

(18) ENISA je agencija Unije, ki izvaja naloge, ki so ji dodeljene na podlagi Uredbe (EU) 2019/881[11], z namenom zagotavljanja visoke skupne ravni kibernetske varnosti v Uniji, tudi z dejavnim podpiranjem držav članic ter institucij, organov in agencij Unije. Med drugim sekretariatu za mrežo skupin CSIRT in mreži EU-CyCLONe zagotavlja storitve situacijskega zavedanja, državam članicam pa pomaga z redno organizacijo vaj na področju kibernetske varnosti na ravni Unije. V skladu z Direktivo (EU) 2022/2555 in Uredbo (EU) 2024/2847[12] prejema informacije o pomembnih čezmejnih incidentih in aktivno izrabljenih ranljivostih ter incidentih, ki vplivajo na digitalne proizvode.

(19) Svet Evropske unije (v nadaljnjem besedilu: Svet) je institucija, ki opravlja naloge oblikovanja politike in usklajevanja v skladu s členom 16 Pogodbe o Evropski uniji (PEU), in mu je zaupana IPCR, kar zadeva usklajevanje in odzivanje na politični ravni Unije. Deluje prek svojih sestav, Odbora stalnih predstavnikov in zadevnih pripravljalnih teles, zlasti Horizontalne delovne skupine za kibernetska vprašanja (HWPCI), pa tudi, kadar je to ustrezno, prek enotne ureditve IPCR.

---

[11] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15–69).

[12] Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, str. 1–81).

(20) Komisija je kot institucija, ki je odgovorna za promoviranje splošnega interesa Unije in sprejemanje ustreznih pobud v ta namen ter ki skrbi za uporabo Pogodb in ukrepov, ki jih sprejemajo institucije na podlagi člena 17 PEU, odgovorna za nekatere dejavnosti na ravni Unije na področju splošne pripravljenosti in za nekatere dejavnosti za situacijsko zavedanje, vključno z vodenjem ERCC ter skupnega komunikacijskega in informacijskega sistema za primer nesreč (CECIS), v skladu s sklepom UCPM. Omogoča skladnost in lažje usklajevanje sorodnih ukrepov za odzivanje na krize na ravni Unije na operativni ravni. Druge mreže in akterji se z njo posvetujejo v zvezi z odločitvami o uporabi ali prekinitvi IPCR. Službe Komisije skupaj z ESZD pripravljajo poročila ISAA. V primerih, ko morebiten ali tekoč velik kibernetski incident pomembno vpliva ali bi lahko pomembno vplival na storitve in dejavnosti, ki spadajo na področje uporabe Direktive (EU) 2022/2555, je Komisija članica mreže EU-CyCLONe, v drugih primerih pa je opazovalka. V IICB je kontaktna točka za EU-CyCLONe, v mreži skupin CSIRT pa je opazovalka.

(21) Visoki predstavnik za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) ob pomoči ESZD vodi skupno zunanjo in varnostno politiko Unije (SZVP) ter s svojimi predlogi prispeva k oblikovanju te politike, vključno s skupno varnostno in obrambno politiko (SVOP). Sem spadajo diplomatske, obveščevalne in vojaške strukture ter mehanizmi – zlasti Enotna zmogljivost za analizo obveščevalnih podatkov (SIAC) kot enotna vstopna točka za obveščevalne podatke držav članic, Vojaški štab EU (EUMS) kot vir vojaškega strokovnega znanja, zbirka orodij EU za kibernetsko diplomacijo ter mreža delegacij EU –, ki lahko prispevajo h kriznemu upravljanju z zunanje perspektive. ESZD poleg tega s Komisijo pripravlja poročila ISAA.

(22) V Prilogi II so opisane vloge in pristojnosti ustreznih akterjev na ravni Unije v zvezi s kriznim upravljanjem kibernetske varnosti, vključno z glavnimi mrežami in akterji.

V: Priprava na velike kibernetske incidente in kibernetsko krizo

Krajina groženj

(23) Države članice in ustrezni subjekti Unije bi morali sprejeti potrebne ukrepe za izboljšanje situacijskega zavedanja, saj krajina groženj in z incidenti povezano situacijsko zavedanje zahtevajo različne načine delovanja. Hkrati bi morali sodelovati na podlagi preverjenih in zanesljivih podatkov, vključno s trendi incidentov, taktikami, tehnikami in postopki, ter aktivno izrabljenih ranljivosti.

(24) Države članice bi morale pri izmenjavi informacij na ravni EU v celoti izkoristiti obstoječe platforme za tehnično in operativno sodelovanje, kot so platforme, ki jih uporabljata mreža skupin CSIRT in mreža EU-CyCLONe.

(25) Mreža EU-CyCLONe in mreža skupin CSIRT bi morali – ob podpori agencije ENISA – za izboljšanje situacijskega zavedanja in za lažjo oceno učinka EU uporabljati interno dogovorjen mehanizem poročanja, da bi lahko na podlagi informacij, zbranih na nacionalni ravni, pripravili pregled tehničnih in operativnih dejavnosti EU.

(26) Mreža EU-CyCLONe in mreža skupin CSIRT bi morali:

(a) sodelovati, da bi izboljšali izmenjavo informacij med tehnično in operativno ravnjo ter situacijsko zavedanje kot celoto;

(b) še naprej krepiti zaupanje med njihovimi člani in med mrežama;

(c) ob podpori agencije ENISA v celoti izkoristiti razpoložljiva orodja za izmenjavo informacij, razmisliti o tem, kako ta orodja izboljšati, in zagotoviti interoperabilnost med mrežama.

(27) Mreža EU-CyCLONe, mreža skupin CSIRT in IICB bi morali sodelovati z namenom zagotavljanja učinkovite izmenjave relevantnih informacij.

(28) ENISA ima kot sekretariat za mrežo skupin CSIRT in mrežo EU-CyCLONe osrednjo vlogo pri podpiranju držav članic ter institucij, organov in agencij Unije, da bi dosegli skupno situacijsko zavedanje EU na tehnični in operativni ravni z namenom podpore pri pripravi na velike kibernetske incidente in krize.

(29) Države članice in ustrezni subjekti Unije bi se morali v skladu z Direktivo (EU) 2022/2555 in Uredbo (EU) 2019/881 usklajevati z zasebnim sektorjem, vključno z odprtokodnimi skupnostmi in proizvajalci, da bi izboljšali izmenjavo informacij. Zlasti ENISA bi morala v ta namen uporabljati svoj partnerski program. Poleg tega bi lahko države članice in ustrezni subjekti Unije na temelju obstoječih centrov za izmenjavo in analizo informacij (v nadaljnjem besedilu: centri ISAC) na ravni EU in nacionalni ravni okrepili zmogljivosti na področju kibernetske varnosti in se odzivali na kibernetske incidente, tudi s skupnimi sestanki zasebnega sektorja z mrežo EU-CyCLONe ali mrežo skupin CSIRT.

(30) Mreža EU-CyCLONe bi morala – ob podpori agencije ENISA kot sekretariata ter po posvetovanju z mrežo skupin CSIRT in Skupino za NIS – za izboljšanje izmenjave informacij znotraj mrež in med njimi ter za razjasnitev vzajemnih pričakovanj v zvezi s takšno izmenjavo v 24 mesecih od sprejetja tega priporočila doseči dogovor o skupni usklajeni taksonomiji stopenj resnosti incidentov. Ta taksonomija bi morala omogočiti primerjavo resnosti incidentov po državah članicah z upoštevanjem vpliva na zagotavljanje storitev, števila prizadetih subjektov in pomena vsakega od njih, vpliva na druge storitve in infrastrukturo, pa tudi povzročene denarne in politične škode ter škode za ugled. Temeljiti bi morala na ustreznih obstoječih lestvicah ali taksonomijah, kakršna je referenčna taksonomija za razvrščanje incidentov (ang. *Reference Incident Classification Taxonomy*).

Tehnična raven

(31) Mreža skupin CSIRT je platforma za tehnično sodelovanje in izmenjavo informacij med vsemi državami članicami in prek CERT-EU s subjekti Unije.

(32) V skladu z Direktivo (EU) 2022/2555 ima vsaka skupina CSIRT nalogo spremljanja in analiziranja kibernetskih groženj, ranljivosti in incidentov na nacionalni ravni. Skupine CSIRT bi si morale tako znotraj mreže skupin CSIRT kot dvostransko izmenjevati relevantne informacije o incidentih, skorajšnjih incidentih, kibernetskih grožnjah, tveganjih in ranljivostih ter tako doseči skupno situacijsko zavedanje.

(33) Za okrepitev operativnega sodelovanja na ravni Unije bi morala mreža skupin CSIRT razmisliti o tem, da bi k sodelovanju pri svojem delu povabila organe in agencije Unije, vključene v politiko na področju kibernetske varnosti, kot je Europol.

(34) V skladu z Uredbo (EU) 2023/2841 bi morala CERT-EU zbirati, upravljati in analizirati, hkrati pa z institucijami, organi, uradi in agencijami Unije na netajni infrastrukturi IKT izmenjevati informacije o kibernetskih grožnjah, ranljivostih ter incidentih, po potrebi pa tudi izdati specifične predloge za IICB za smernice in priporočila za institucije, organe, urade in agencije Unije. Morala bi sodelovati in izmenjevati informacije s sorodnimi organi iz držav članic, tudi prek mreže skupin CSIRT.

Operativna raven

(35) V skladu z Direktivo (EU) 2022/2555 bi morala mreža EU-CyCLONe služiti kot platforma za sodelovanje med organi držav članic za obvladovanje kibernetskih kriz in prek Komisije z ustreznimi subjekti Unije, s ciljem zvišanja ravni pripravljenosti za obvladovanje velikih kibernetskih incidentov in kibernetskih kriz ter razvoja skupnega situacijskega zavedanja o velikih kibernetskih incidentih in kibernetskih krizah.

(36) ENISA v skladu z Direktivo (EU) 2022/2555 in Uredbo (EU) 2024/2847 prejema informacije o pomembnih čezmejnih incidentih in aktivno izrabljenih ranljivostih ter incidentih, ki vplivajo na digitalne proizvode. ENISA, ki deluje kot sekretariat, bi morala svetovati mreži skupin CSIRT in mreži EU-CyCLONe s ciljem podpiranja mrež pri ugotavljanju, ali je treba sprejeti dodatne ukrepe, in prispevanja k skupnemu situacijskemu zavedanju.

Politična raven

(37) Države članice in ustrezni subjekti Unije bi morali spremljati mednarodni razvoj dogodkov, ki vplivajo na kibernetsko varnost (tudi kibernetske grožnje, hibridne grožnje ter tuje manipuliranje z informacijami in vmešavanje (FIMI), po potrebi vključno z dezinformacijami). Upoštevati bi morali pobude, kot so skupna poročila o oceni kibernetske varnosti (JCAR), analize, ki jih zagotovi SIAC, in druge ustrezne produkte, ki nudijo specializirane vpoglede.

(38) Visoki predstavnik bi moral države članice še naprej obveščati o diplomatskih prizadevanjih Unije v zvezi s kibernetskimi grožnjami, zlasti tistimi, v katera so vključeni državni akterji, svojem sodelovanju s tretjimi državami in mednarodnimi organizacijami, vključno z Natom, ter izvajanju diplomatskih ukrepov, vključno z omejevalnimi ukrepi, hkrati pa jih vanje vključevati.

(39) Predsedstvo Sveta Evropske unije lahko vzpostavi stran za spremljanje na spletni platformi IPCR, prek katere lahko države članice ter institucije in organi EU izmenjujejo informacije o morebiti razvijajoči se krizi.

Skupne vaje

(40) Komisija bi morala ob usklajevanju z visokim predstavnikom, ob podpori agencije ENISA ter po posvetovanju z mrežo EU-CyCLONe in mrežo skupin CSIRT sestaviti učinkovit letni tekoči program vaj na področju kibernetske varnosti, da bi se pripravili na kibernetske krize in izboljšali organizacijsko učinkovitost. V tekočem programu vaj na področju kibernetske varnosti bi bilo treba upoštevati vaje v okviru UCPM in drugih mehanizmov za odzivanje na krize na ravni Unije, vključno z vajo, predstavljeno v načrtu EU za kritično infrastrukturo. Prvi tekoči program bi moral biti pripravljen v roku 12 mesecev po sprejetju kibernetskega načrta, poznejši programi pa morajo biti dokončani vsako leto do 31. marca. Tekoči program bi bilo treba predložiti v vednost Svetu.

(41) Tekoči program bi moral zajemati tudi vaje, pripravljene z uporabo scenarijev na podlagi usklajenih ocen tveganja na ravni EU. Zajemati bi moral vaje, v katerih sodelujejo vsi ustrezni akterji, zlasti zasebni sektor in NATO.

(42) ENISA bi morala – v vlogi sekretariata mreže skupin CSIRT in mreže EU-CyCLONe – skrbeti za sistematično zbiranje izkušenj, pridobljenih pri vajah, ter opredelitev posledičnih ukrepov in predlaganje načinov za njihovo izvajanje, da bi zagotovila njihovo uspešno izvrševanje in pozitiven učinek na skupno odpornost EU, vključno z zadevnimi SOP.

(43) Vsi akterji in mreže bi morali na podlagi izkušenj, pridobljenih pri vajah, izboljšati usklajevanje v primeru velikega kibernetskega incidenta ali kibernetske krize. Zlasti mreža EU-CyCLONe in mreža skupin CSIRT bi morali v ta namen obravnavati izzive, ugotovljene med vajami, zlasti tiste, ki zadevajo sodelovanje med mrežami, in po potrebi hitro prilagoditi SOP.

(44) Skupina za NIS bi morala mrežo skupin CSIRT, mrežo EU-CyCLONe in agencijo ENISA povabiti, naj predstavijo izkušnje, pridobljene pri vajah, ter opredelijo posledične ukrepe in predlagajo načine za njihovo izvajanje.

(45) Svet lahko povabi predsednike mreže skupin CSIRT, mreže EU-CyCLONe, Skupine za NIS in agencije ENISA, naj predstavijo, kako so se izvajale izkušnje, pridobljene pri vajah.

(46) ENISA je pozvana, naj v sodelovanju s Komisijo in visokim predstavnikom v okviru naslednje vaje CyberEurope organizira vajo za preizkus kibernetskega načrta. V tej vaji bi morali sodelovati vsi ustrezni akterji, vključno s politično ravnjo. ENISA je pozvana, naj s predsedstvom Sveta Evropske unije usklajuje sodelovanje politične ravni. Na vaji lahko sodelujeta tudi zasebni sektor in NATO.

VI: Odkritje incidenta, ki bi se lahko stopnjeval v velik kibernetski incident ali kibernetsko krizo

(47) V skladu s svojimi pooblastili in na podlagi pristopa, ki zajema vse nevarnosti, bi morali vsi akterji ustreznim mrežam prispevati informacije o morebitnem velikem kibernetskem incidentu ali kibernetski krizi.

(48) V skladu z Uredbo (EU) 2025/38[13] bi morala čezmejna kibernetska vozlišča, kadar pridobijo informacije v zvezi z morebitnim ali tekočim velikim kibernetskim incidentom, za namene skupnega situacijskega zavedanja zagotoviti, da se organom držav članic in Komisiji prek mreže EU-CyCLONe in mreže skupin CSIRT brez nepotrebnega odlašanja zagotovijo relevantne informacije.

[13] Uredba (EU) 2025/38 Evropskega parlamenta in Sveta z dne 19. decembra 2024 o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskih groženj in incidentov ter pripravo in odzivanje nanje ter spremembi Uredbe (EU) 2021/694 (Akt o kibernetski solidarnosti) (UL L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

(49) Ko je opažen pomemben incident, zlasti takšen, ki povzroči takojšen učinek, se lahko o njem uradno obvesti skupina CSIRT ali pa ga slednja odkrije, odkrijejo pa ga lahko tudi organi držav članic za obvladovanje kibernetskih kriz ali drugi sektorski organi držav članic. Države članice naj izmenjujejo informacije, povezane s takšnim incidentom, v okviru mrež, ki bi morale razmisliti o sprejetju ustreznih ukrepov. Mreža skupin CSIRT in mreža EU-CyCLONe se lahko uporabita neodvisno druga od druge, odvisno od narave incidenta in zahtevanega odziva. Obe mreži pa naj še naprej sodelujeta druga z drugo na podlagi dogovorjenih postopkovnih ureditev. Za odločitev o uporabi je odgovorna izključno in samostojno vsaka posamezna mreža.

(50) Mreža skupin CSIRT bi morala mreži EU-CyCLONe svetovati, ali se opaženi kibernetski incident lahko šteje za morebiten ali tekoč velik kibernetski incident.

(51) Kot je navedeno v Direktivi (EU) 2022/2555, bi se morali mreža skupin CSIRT in mreža EU-CyCLONe brez odlašanja dogovoriti o postopkovnih ureditvah v primeru morebitnega ali tekočega velikega kibernetskega incidenta, da bi zagotovili tehnično-operativno usklajevanje ter pravočasne in relevantne informacije politični ravni.

VII: Odzivanje na velik kibernetski incident ali kibernetsko krizo na ravni Unije

Odziv na velik kibernetski incident ali kibernetsko krizo, za katero IPCR ni polno uporabljena

(52) Učinkovitost odziva na velike kibernetske incidente ali kibernetske krize na ravni EU je odvisna od učinkovitosti tehničnega, operativnega in političnega sodelovanja v vsevladnem pristopu, po možnosti tudi z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

(53) Sodelujoči akterji bi morali na vsaki posamezni ravni opravljati specifične dejavnosti za dosego skupnega situacijskega zavedanja in usklajenega odziva. S takšnimi ukrepi se zagotovi urejeno in učinkovito razširjanje informacij.

(54) Odziv bi moral biti ustrezen učinku velikega kibernetskega incidenta ali kibernetske krize. V skladu z Direktivo (EU) 2022/2555 bi morali organi držav članic za obvladovanje kibernetskih kriz na nacionalni ravni zagotoviti skladnost in usklajevanje med sektorskimi odzivi na kibernetsko krizo.

(55) V primeru velikega kibernetskega incidenta ali kibernetske krize bi se morali vsi akterji in mreže pri odzivu tesno usklajevati, in sicer na naslednji način:

(a) na tehnični ravni:

i. prizadete države članice in njihove skupine CSIRT bi se morale v sodelovanju s prizadetimi subjekti odzivati na incidente in po potrebi zagotoviti pomoč;

ii. skupine CSIRT bi morale v medsebojnem sodelovanju prek mreže skupin CSIRT izmenjati relevantne tehnične informacije o incidentu; skupine CSIRT sodelujejo v svojih prizadevanjih za analizo razpoložljivih tehničnih artefaktov in drugih tehničnih informacij, povezanih z incidentom, da bi ugotovili vzrok in določili morebitne tehnične blažilne ukrepe;

iii. kadar se skupina CSIRT ali organ države članice za obvladovanje kibernetskih kriz seznani s pomembnim incidentom, naj to informacijo deli znotraj mreže skupin CSIRT ali mreže EU-CyCLONe;

iv. mreža skupin CSIRT bi morala ob podpori agencije ENISA zbrati nacionalna poročila, ki so jih posredovale skupine CSIRT in ki bi jih bilo treba predložiti mreži EU-CyCLONe;

v. kadar bi se kibernetski incident lahko stopnjeval v velik kibernetski incident ali kibernetsko krizo, bi morala mreža skupin CSIRT izmenjati ustrezne informacije z mrežo EU-CyCLONe, ta pa bi morala s temi informacijami seznaniti Svet;

vi. mreža skupin CSIRT bi morala z vzdrževanjem tesnih stikov z Europolom zagotavljati izmenjavo relevantnih tehničnih informacij; mreža skupin CSIRT in Europol bi morala vzpostaviti kontaktne točke in tako izboljšati izmenjavo informacij, kadar je to relevantno, v primeru velikega kibernetskega incidenta;

(b) na operativni ravni:

i. države članice bi morale z ustreznimi ukrepi ublažiti učinek incidenta na nacionalni ravni;

ii. mreža skupin CSIRT bi morala mreži EU-CyCLONe zagotoviti tehnične ocene tekočih incidentov, ki jih ta lahko uporabi;

iii. mreža EU-CyCLONe bi morala oceniti posledice in učinek zadevnih velikih kibernetskih incidentov in kibernetskih kriz ter predlagati morebitne blažilne ukrepe, hkrati pa podpirati usklajeno obvladovanje velikih kibernetskih incidentov in kibernetskih kriz ter odločanje na politični ravni;

iv. če bi bilo treba zaradi velikega kibernetskega incidenta z medsektorskim učinkom uporabiti ukrepe za odzivanje na ravni Unije, zlasti ustrezne horizontalne in sektorske mehanizme kriznega upravljanja na ravni Unije iz Priloge II,

(a) lahko ustrezni akterji – odvisno od vrste sektorskih mehanizmov kriznega upravljanja na ravni Unije – zahtevajo uporabo navedenega mehanizma;

(b) zadevni subjekti v primeru uporabe takšnega sektorskega mehanizma podpirajo sektorske subjekte pri blaženju učinka incidenta;

(c) bi morala Komisija olajšati pretok potrebnih informacij med kontaktnimi točkami za ustrezne horizontalne in sektorske krizne mehanizme na ravni Unije iz Priloge II ter mrežo EU-CyCLONe, hkrati pa si prizadevati za celovito medsektorsko analizo in predlagati možnosti za ustrezen celovit načrt odzivanja;

(d) bi morala Komisija prek mreže EU-CyCLONe, po potrebi v sodelovanju z visokim predstavnikom, zagotoviti skladnost in usklajevanje operativnih ukrepov na ravni EU na kibernetskem področju s povezanimi ukrepi za odzivanje na ravni Unije, zlasti v zvezi z zahtevki za pomoč v okviru UCPM;

(e) bi bilo treba – če je bila vzpostavljena stran za spremljanje na spletni platformi IPCR – med državami članicami in subjekti Unije prek navedene spletne platforme izmenjati tudi informacije o incidentu, njegovih učinkih in sprejetih ukrepih;

v. države članice lahko zahtevajo storitve iz EU rezerve za kibernetsko varnost v skladu s členom 15 Uredbe (EU) 2025/38. Storitve EU rezerve za kibernetsko varnost bi bilo treba brez poseganja v morebitne prihodnje izvedbene akte na podlagi navedene uredbe uporabiti v 24 urah od zahteve.

(c) na politični ravni:

i. Svet lahko od ključnih deležnikov, zlasti Komisije, visokega predstavnika in mreže EU-CyCLONe, zahteva, da se ustrezno politično in strateško odzovejo;

ii. Svet bi lahko ob podpori Komisije in visokega predstavnika odločil o ustreznih ukrepih v odziv na velik kibernetski incident, tudi z morebitnim diplomatskim odzivom v skladu s poglavjem IX;

iii. države članice lahko glede na naravo in učinek incidenta uporabijo dodatne mehanizme ali instrumente za obvladovanje kibernetskih kriz;

iv. kadar se IPCR uporablja v načinu izmenjave informacij, se sproži podporna zmogljivost ISAA, s čimer se okrepijo izmenjave informacij prek spletne platforme IPCR ter zagotavlja skupen pregled nad razmerami. Situacijska poročila mreže EU-CyCLONe in mreže skupin CSIRT bi morala biti še naprej glavni instrument za predstavitev skupnega situacijskega zavedanja na operativni oziroma tehnični ravni. Na ta poročila se lahko oprejo poročila ISAA;

v. V primeru incidenta, zaradi katerega je treba uporabiti ukrepe za odzivanje na krize na ravni Unije, zlasti ustrezne horizontalne in sektorske mehanizme za obvladovanje kriz na ravni Unije iz Priloge II, bi moral Svet v sodelovanju s Komisijo in visokim predstavnikom zagotoviti skladnost in usklajevanje med odzivi na kibernetsko krizo in povezanimi ukrepi za odzivanje na ravni Unije;

vi. kadar se zahtevajo ustrezni mehanizmi, zlasti storitve rezerve za kibernetsko varnost, bi se morale službe Komisije in po potrebi ESZD ter ustrezna telesa Sveta, zlasti HWPCI in Horizontalna delovna skupina za krepitev odpornosti in preprečevanje hibridnih groženj (HWP-ERCHT), če je to primerno, usklajevati glede oblikovanja in izvajanja ukrepov ter ustreznega postopka odločanja z dodatnimi ukrepi v skladu z naborom orodij za odzivanje na hibridne grožnje[14] v primeru zlonamernih kibernetskih dejavnosti, ki so del širše hibridne kampanje.

Odziv na velik kibernetski incident ali kibernetsko krizo, pri katerem se IPCR uporablja v načinu polne uporabe

(56) Izvesti bi bilo treba korake, navedene v zgornjem oddelku „Odziv na velik kibernetski incident ali kibernetsko krizo, pri katerem se IPCR ne uporablja v načinu polne uporabe“.

(57) Pri polni uporabi IPCR se poročila ISAA uporabljajo za zagotavljanje skupnega situacijskega zavedanja na politični ravni. Situacijska poročila mreže EU-CyCLONe in mreže skupin CSIRT bi morala bit še naprej glavni instrument za predstavitev skupnega situacijskega zavedanja na operativni oziroma tehnični ravni. Na ta poročila se lahko oprejo poročila ISAA.

(58) V primeru velikega kibernetskega incidenta ali kibernetske krize, ki privede do polne uporabe IPCR, bi se morali vsi akterji odzvati tesno usklajeno v skladu z vsevladnim pristopom, kot sledi:

(a) usklajevanje odzivanja Unije na politični ravni izvaja Svet z uporabo ureditev IPCR;

[14] Nabor orodij za odzivanje na hibridne grožnje je okvir za usklajen odziv na hibridne kampanje, ki vplivajo na EU in njene države članice, zajema pa na primer ukrepe za preprečevanje, sodelovanje, stabilizacijo, omejevanje in obnovo ter podpira solidarnost in medsebojno pomoč.

(b) mreža EU-CyCLONe bi morala v sodelovanju z mrežo skupin CSIRT politični ravni zagotoviti jasne informacije o učinku, možnih posledicah ter ukrepih za odzivanje na incident in njegovo odpravo, tudi s prispevanjem k poročilom ISAA;

(c) predsedstvo Sveta Evropske unije bi poleg zmogljivosti ISAA sklicalo okrogle mize IPCR, da bi se omogočilo politično in strateško usklajevanje odzivanja EU z ukrepi v okviru kibernetskega načrta in delom ustreznih sektorskih mehanizmov, ki prispevajo k delu IPCR. Na okroglih mizah se lahko poleg tega ugotovijo specifične vrzeli v odzivanju, posamezni akterji EU pa pozovejo, naj jih obravnavajo in o njih poročajo na prihodnjih okroglih mizah, da bi podprli politično in strateško usklajevanje v okviru IPCR;

(d) predsedstvo Sveta Evropske unije bi moralo razmisliti o povabilu mreži EU-CyCLONe na ustrezna srečanja, med drugim na okrogle mize v okviru ureditve IPCR in druge ustrezne seje Sveta;

(e) organi držav članic za krizno upravljanje bi morali zagotoviti skladnost in usklajevanje med sektorskimi odzivi na kibernetsko krizo, ki jih podpirajo organi za obvladovanje kibernetskih kriz;

(f) morebitne diplomatske odzive bi bilo treba preučiti in izvesti v skladu s poglavjem IX.

VIII: Komuniciranje z javnostjo

(59) Čeprav je komuniciranje s prebivalstvom posamezne države članice o tekočem velikem kibernetskem incidentu ali kibernetski krizi, tudi v okviru ozaveščanja, v nacionalni pristojnosti, bi si morale države članice, Komisija in visoki predstavnik prizadevati za čim bolj usklajeno komuniciranje z javnostjo. Po potrebi se lahko vključi neformalna mreža kriznih posrednikov IPCR.

(60) Za namene priprave na velike kibernetske incidente in kibernetske krize so države članice ter po potrebi Komisija in CERT-EU pozvane k izmenjavi informacij o svojem komuniciranju v okviru mreže EU-CyCLONe in mreže skupin CSIRT, vključno z najboljšimi praksami, kot so obvestila ali kampanje ozaveščanja. Agencija ENISA bi morala zagotoviti orodja, ki bi podpirala takšno izmenjavo in zagotavljala enostaven dostop.

(61) Države članice so pozvane, naj v primeru velikega kibernetskega incidenta ali kibernetske krize v okviru mreže EU-CyCLONe izmenjujejo informacije o svojem komuniciranju z javnostjo, da bi krepile skupno ozaveščenost in uskladile zadevne ukrepe. Mreža EU-CyCLONe lahko na lastno pobudo ali na zahtevo Sveta temu posreduje pregled takšnih pristopov.

IX: Diplomatski odziv in sodelovanje s strateškimi partnerji

(62) Visoki predstavnik bi moral v tesnem sodelovanju s Komisijo in drugimi ustreznimi subjekti Unije:

(a) podpirati odločanje v Svetu, tudi z analizami, poročili in predlogi, o uporabi morebitnih ukrepov v okviru zbirke orodij EU za kibernetsko diplomacijo. To bo omogočilo uporabo celotnega nabora orodij Unije, ki so na voljo za preprečevanje zlonamernih kibernetskih dejavnosti, odvračanje od njih in odzivanje nanje, okrepilo njen položaj kibernetske varnosti ter spodbujalo mednarodni mir, varnost in stabilnost v kibernetskem prostoru;

(b) olajšati pretok potrebnih informacij s strateškimi partnerji, po potrebi tudi z Natom, kadar se ugotovi relevanten incident;

(c) okrepiti usklajevanje s strateškimi partnerji, po potrebi tudi z Natom, o odzivanju na zlonamerne kibernetske dejavnosti stalnih akterjev groženj, zlasti pri uporabi zbirke orodij EU za kibernetsko diplomacijo, v skladu z izvedbenimi smernicami.

(63) Države članice, visoki predstavnik, Komisija in drugi ustrezni subjekti Unije bi morali sodelovati s strateškimi partnerji in mednarodnimi organizacijami, da bi spodbujali dobre prakse in odgovorno ravnanje držav v kibernetskem prostoru ter zagotovili hiter in usklajen odziv v primeru morebitnih ali velikih kibernetskih incidentov.

(64) Sodelovanje med Evropsko unijo in Natom bi moralo potekati v skladu z dogovorjenimi vodilnimi načeli vključenosti, vzajemnosti in preglednosti ter ob doslednem spoštovanju avtonomnega odločanja Unije.

(65) Komisija in visoki predstavnik bi morala ob upoštevanju obstoječih sporazumov, kot je tehnični sporazum CERT-EU/NATO iz leta 2016, vzpostaviti kontaktne točke za usklajevanje z Natom v primeru kibernetske krize za izmenjavo potrebnih informacij o razmerah in uporabi mehanizmov za odzivanje na krize, da bi se povečala sodelovanje pri odzivanju in njegova učinkovitost. V ta namen bi morala Unija preučiti možnosti za izboljšanje izmenjave informacij z Natom na vključujoč, vzajemen in nediskriminatoren način, zlasti z zagotavljanjem orodij za varno komunikacijo ob upoštevanju standardov za izmenjavo informacij različnih držav članic.

(66) Službe Komisije in ESZD bi morale v okviru tekočega programa Unije za kibernetske vaje iz poglavja V razmisliti o organizaciji vaje za osebje z Natom, da bi preizkusili sodelovanje med civilnimi in vojaškimi subjekti v primeru velikega kibernetskega incidenta ali kibernetske krize, kadar se države članice ali zaveznice Nata poskušajo odzvati na kibernetski napad, ki vpliva na njihovo varnost. Vaja bi morala potekati na vključujoč in nediskriminatoren način ter ob doslednem spoštovanju dogovorjenih načel parametrov sodelovanja med EU in Natom. Treba bi jo bilo izvesti v okviru integrirane vaje kriznega upravljanja EU Integrated Resolve (vzporedna in usklajena vaja, PACE). Sprejeti bi bilo treba vse potrebne ukrepe za zagotovitev sodelovanja vseh akterjev iz kibernetskega načrta.

(67) V posvetovanju s Svetom, Komisijo in visokim predstavnikom bi bilo treba razmisliti tudi o skupnih vajah na področju kibernetske varnosti na ravni Unije z državami Zahodnega Balkana, Republiko Moldavijo, Ukrajino ter drugimi strateškimi partnerji in podobno mislečimi tretjimi državami.

X: Usklajevanje obvladovanja kibernetskih kriz z vojaškimi akterji na ravni EU

(68) Države članice bi morale še naprej krepiti sodelovanje med civilnimi in vojaškimi kibernetskimi akterji na nacionalni ravni.

(69) Mreža EU-CyCLONe in mreža skupin CSIRT bi morala opredeliti možne načine in postopke za sodelovanje z ustreznimi vojaškimi akterji EU, kot sta konferenca kibernetskih poveljnikov EU in operativna mreža vojaških skupin za odzivanje na izredne računalniške razmere (MICNET), da bi se izkoristil skupni vojaško-civilni vidik, zlasti prek skupnih srečanj. Mreža EU-CyCLONe in mreža CSIRT bi morala Svet obveščati o napredku v zvezi s takšnim sodelovanjem.

(70) Prizadeta država članica je pozvana, naj obvesti mrežo EU-CyCLONe in ESZD, če se v okviru velikega kibernetskega incidenta ali kibernetske krize uporabijo ustrezne nacionalne ali večnacionalne zmogljivosti za vojaško odzivanje, o zagotavljanju teh informacij pa se medsebojno dogovorita uporabnik in ponudnik take zmogljivosti za odzivanje.

(71) Komisija in visoki predstavnik bi morala v okviru tekočega programa Unije za kibernetske vaje iz poglavja V razmisliti o organizaciji skupne vaje, da bi preizkusili sodelovanje med civilnimi in vojaškimi kibernetskimi akterji v primeru velikega kibernetskega incidenta, ki vpliva na države članice.

XI: Obnova in izkušnje, pridobljene med kibernetsko krizo

(72) Države članice, ustrezni subjekti in mreže Unije bi morali sodelovati v fazi obnove po kibernetski krizi, da bi zagotovili hitro ponovno vzpostavitev osnovnih funkcij. V takšno sodelovanje bi morale biti po potrebi vključene tudi skupnosti organov odkrivanja in pregona. V tej fazi je sodelovanje z zasebnim sektorjem ključnega pomena, zlasti za lažje reševanje podatkov in ponovno vzpostavitev sistemov. Prednost pri učinkovitem usklajevanju med deležniki bi morala imeti zmanjšanje motenj in zagotavljanje neprekinjenega poslovanja.

(73) Države članice, ustrezni subjekti in mreže Unije bi morali v fazi obnove sodelovati na podlagi izkušenj, pridobljenih med kibernetskimi krizami ali obvladovanjem kibernetskih incidentov v preteklosti, pa tudi na podlagi poročil o incidentih, zlasti v okviru evropskega mehanizma za pregledovanje kibernetskih incidentov, vzpostavljenega z Uredbo (EU) 2025/38.

(74) Mreža EU-CyCLONe bi morala mreži skupin CSIRT, Skupini za NIS in Svetu zagotoviti celovit seznam izkušenj, pridobljenih med kibernetskimi krizami ali obvladovanjem kibernetskih incidentov v preteklosti, in najboljših praks. Agencija ENISA bi morala zagotoviti, da se te pridobljene izkušnje ustrezno upoštevajo v prihodnjih dejavnostih na področju pripravljenosti in pri načrtovanju prihodnjih vaj.

XII: Varna komunikacija

(75) Komisija bi morala na podlagi pregleda obstoječih orodij za varno komunikacijo[15] do konca leta 2026 predlagati interoperabilen sklop varnih komunikacijskih rešitev. Svet, Komisija, visoki predstavnik, mreža EU-CyCLONe in mreža skupin CSIRT bi se morali o tem sklopu dogovoriti do konca leta 2027. Te rešitve bi se morale opirati na ukrepe na področju varne komunikacije, ki bi jih institucije EU lahko sprejele na podlagi strategije EU za unijo pripravljenosti, in zajemati celoten nabor potrebnih komunikacijskih načinov (govor, podatki, videokonference, sporočanje, sodelovanje ter izmenjava dokumentov in posvetovanje). Rešitve bi morale izpolnjevati skupno opredeljene zahteve za varstvo občutljivih netajnih podatkov. Uporabiti bi bilo treba rešitve, ki temeljijo na odprtem protokolu z odprtokodnimi izvedbami, primernimi za komuniciranje v realnem času, ki jih upravlja subjekt s sedežem v EU.

(76) Mreža EU-CyCLONe in mreža skupin CSIRT bi morala imeti možnost, da za izmenjavo tajnih podatkov stopnje RESTREINT UE/EU RESTRICTED po potrebi uporabita varne komunikacijske kanale, ki so institucijam, organom in agencijam EU na voljo za izmenjavo tajnih podatkov med seboj in z državami članicami.

---

15 WK 862/2023.

(77) Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetsko varnost (ECCC), ustanovljen z Uredbo (EU) 2021/887[16], bi moral brez poseganja v prihodnji večletni finančni okvir razmisliti o financiranju iz programa Digitalna Evropa za pomoč državam članicam pri uvajanju orodij za varno komunikacijo. Izogibati se je treba vsakršnemu podvajanju naložb v interoperabilne varne sisteme.

(78) Subjekti EU in države članice bi morali zlasti oblikovati rezervne načrte, v katerih so običajni komunikacijski kanali, ki temeljijo na internetu ali telekomunikacijskih omrežjih, moteni ali niso na voljo.

(79) Za učinkovito odzivanje na kibernetske krize bi bilo treba vzpostaviti mehanizme za komunikacijo in izmenjavo informacij med mrežami organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter mrežami za kibernetsko varnost, zlasti na tehnični ravni. Ti mehanizmi bi morali spoštovati vlogo vsake strani in se izogibati vmešavanju v tekoče operacije ter zagotavljati redundantnost komunikacij. Kritični komunikacijski sistem EU (EUCCS), ki se razvija, lahko koristi skupnemu odzivu z ustreznimi kibernetskimi skupnostmi.

XIII: Končne določbe

(80) Mreža EU-CyCLONe bi morala v sodelovanju z mrežo CSIRT in drugimi glavnimi akterji v ekosistemu EU za obvladovanje kibernetskih kriz ter ob podpori agencije ENISA v enem letu po objavi priporočila pripraviti podrobne diagrame poteka postopka, v katerih bi bili opisani pretok informacij med zadevnimi akterji, postopki odločanja in poročila, pripravljeni med obvladovanjem velikih kibernetskih incidentov ali kibernetskih kriz, kot je opisano v tem priporočilu. Diagrami poteka bi morali zajemati različne načine in ravni sodelovanja. Po potrebi bi jih bilo treba posodobiti.

---

[16] Uredba (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov (UL L 202, 8.6.2021, str. 1–31).

(81) Svet lahko v podporo učinkoviti uporabi revidiranega kibernetskega načrta in na podlagi izkušenj, pridobljenih med skupnimi kibernetskimi vajami, ki se izvajajo na podlagi tega načrta, po potrebi pripravi sklop izvedbenih smernic. Te smernice bi lahko obravnavale praktične izzive, ki se ugotovijo med vajami, ter odpravile ugotovljene vrzeli in manjkajoče povezave pri usklajevanju, komuniciranju in operativni interakciji.

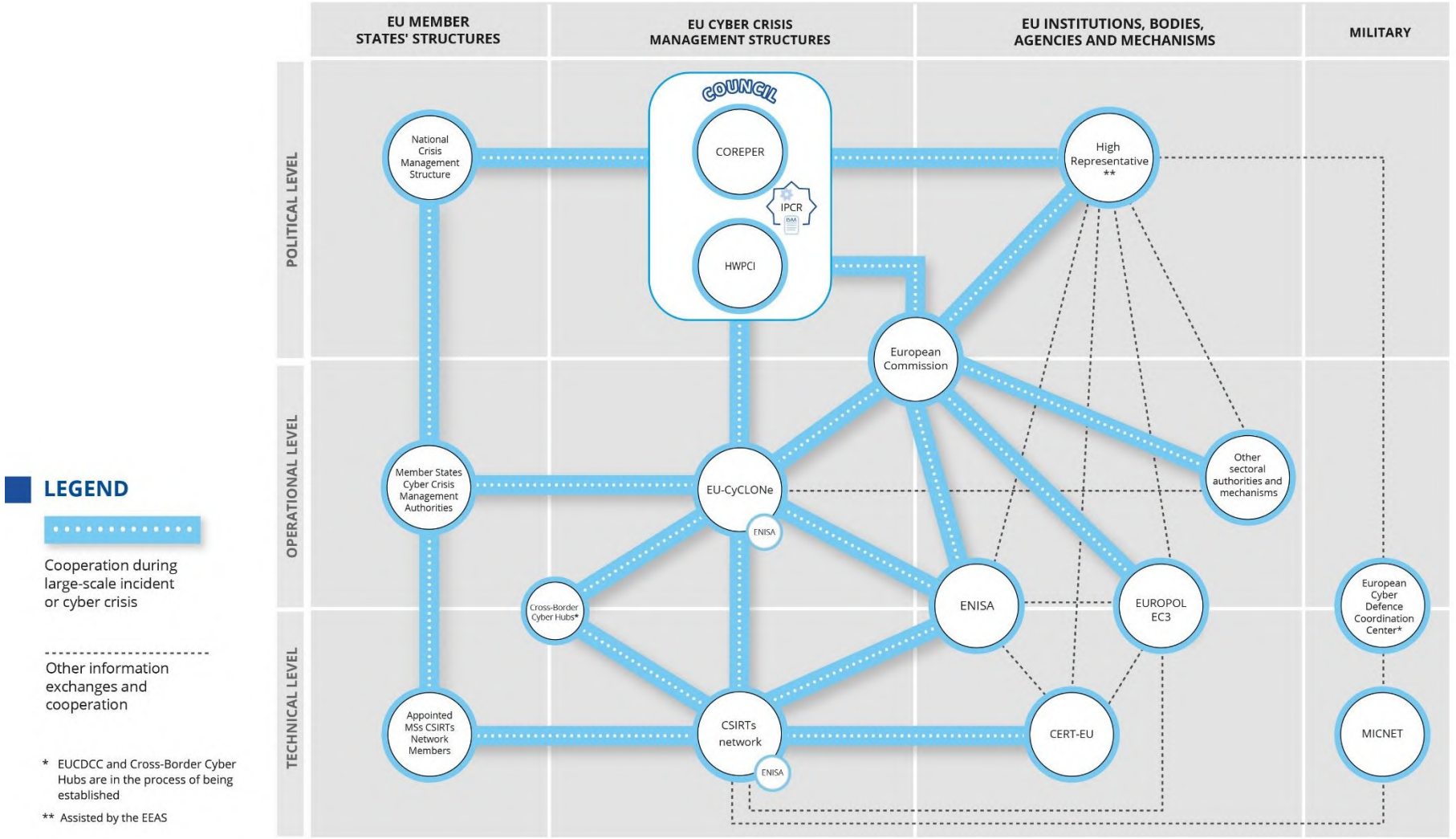
(82) Komisija bi morala to priporočilo v sodelovanju z državami članicami pregledati vsaj vsaka štiri leta po njegovi objavi. Po vsakem pregledu bi morala objaviti poročilo in ga predložiti Svetu. Komisija in države članice bi morale upoštevati zlasti vpliv spreminjajočega se okolja groženj, rezultate skupnih vaj in zakonodajne spremembe, zlasti vse morebitne spremembe, ki izhajajo iz revizije Uredbe (EU) 2019/881.

V Bruslju,

Za Svet

predsednik/predsednica

PRILOGA I – Načrt Unije za odzivanje na kibernetsko krizo



PRILOGA II – USTREZNI AKTERJI NA RAVNI UNIJE (SUBJEKTI IN MREŽE) IN MEHANIZMI ZA OBVLADOVANJE KRIZ

(1) Sodelovanje glavnih akterjev v življenjskem ciklu obvladovanja kibernetskih kriz (veliki kibernetski incidenti in kibernetske krize)

	Pripravljenost	Odkrivanje	Odzivanje na velike kibernetske incidente ali kibernetsko krizo			Komuniciranje z javnostjo	Obnova in pridobljene izkušnje
			na tehnični ravni	na operativni ravni	na politični ravni		
Države članice	X	X	X	X	X	X	X
Komisija	X			X	X	X	
Visoki predstavnik s pomočjo ESZD	X			X	X	X	
Svet	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
Mreža skupin CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Vloge in pristojnosti ustreznih akterjev in mehanizmov na ravni Unije (po abecednem vrstnem redu) v zvezi z obvladovanjem kibernetskih kriz

Akter	Stopnja	Vloga in pristojnost	Referenca
CERT-EU	Tehnična / operativna	Usklajuje odzivanje na krize na tehnični ravni in obvladovanje večjih incidentov, ki vplivajo na subjekte Unije. Vzdržuje zbirko razpoložljivega tehničnega strokovnega znanja, ki bi bilo potrebno za odzivanje v primeru večjih incidentov, in pomaga IICB pri usklajevanju načrtov subjektov Unije za obvladovanje kibernetskih kriz v primeru večjih incidentov. Članica mreže skupin CSIRT. Podpira Komisijo v mreži EU-CyCLONe, namenjeni usklajenemu obvladovanju velikih kibernetskih incidentov in kriz. Deluje kot vozlišče za izmenjavo informacij o kibernetski varnosti in usklajevanje odzivanja na incidente ter olajšuje izmenjavo informacij o incidentih, kibernetskih grožnjah, ranljivostih	Uredba (EU, Euratom) 2023/2841 Uredba (EU) 2025/38

Akter	Stopnja	Vloga in pristojnost	Referenca
		in skorajšnjih incidentih med subjekti in partnerji Unije. Zahteva vzpostavitev EU rezerve za kibernetsko varnost v imenu subjektov Unije. Sodeluje z Natovim centrom za kibernetsko varnost na podlagi tehničnega sporazuma.	
Svet Evropske unije	Politična	Naloge oblikovanja politike in usklajevanja. Odgovoren je za IPCR, ki zadeva usklajevanje in odzivanje na politični ravni Unije.	Člen 16 Pogodbe o Evropski uniji
Predsedstvo Sveta Evropske unije	Politična	V posvetovanju s Komisijo in visokim predstavnikom ter po potrebi s prizadetimi državami članicami odloča (razen ob uveljavljanju solidarnostne klavzule na podlagi člena 222 Pogodbe o delovanju Evropske unije) o uporabi IPCR.	Člen 16 Pogodbe o Evropski uniji Izvedbeni sklep Sveta (EU) 2018/1993
Čezmejna kibernetska vozlišča	Tehnična	„čezmejno kibernetsko vozlišče“ je večdržavna platforma, vzpostavljena s pisno konzorcijsko pogodbo, ki v usklajeni mrežni strukturi	Uredba (EU) 2025/38

Akter	Stopnja	Vloga in pristojnost	Referenca
		združuje nacionalna kibernetska vozlišča iz vsaj treh držav članic in je namenjena izboljšanju spremljanja, odkrivanja in analiziranja kibernetskih groženj za preprečevanje incidentov ter podpiranju priprave analitike kibernetskih groženj, zlasti z izmenjavanjem ustreznih, po potrebi anonimiziranih, podatkov in informacij, pa tudi z izmenjavanjem najsodobnejših orodij in skupnim razvijanjem zmogljivosti za kibernetsko odkrivanje, analizo ter preprečevanje in zaščito v zaupanja vrednem okolju; Tesno sodelujejo z mrežo skupin CSIRT za izmenjavo informacij. Zagotavljajo informacije v zvezi z morebitnim ali potekajočim velikim kibernetskim incidentom organom držav članic in Komisiji prek mreže EU-CyCLONe in mreže skupin CSIRT.	
Mreža skupin CSIRT	Tehnična	Prispeva h krepitvi zaupanja in spodbuja hitro operativno	Direktiva (EU) 2022/2555

Akter	Stopnja	Vloga in pristojnost	Referenca
		sodelovanje med državami članicami. Je glavna mreža za izmenjavo ustreznih informacij o incidentih, skorajšnjih incidentih, kibernetskih grožnjah, tveganjih in ranljivostih. Na prošnjo člana, ki bi ga incident lahko prizadel, mreža izmenjuje in obravnava informacije v zvezi s tem incidentom in z njim povezanimi kibernetskimi grožnjami. Mreža lahko tudi olajša usklajen odziv na incident, ki je bil ugotovljen v pristojnosti člana prosilca. Pomaga državam članicam pri obvladovanju čezmejnih incidentov in preučuje nadaljnje oblike sodelovanja, tudi medsebojno pomoč. Prejema informacije od držav članic glede njihovih zahtev za EU rezervo za kibernetsko varnost.	Uredba (EU) 2025/38

Akter	Stopnja	Vloga in pristojnost	Referenca
Konferenca kibernetskih poveljnikov		Forum za kibernetske poveljnike na nacionalni ravni v državah članicah, v okviru katerega sodelujejo in izmenjujejo ključne informacije v zvezi s potekajočimi operacijami v kibernetskem prostoru in strategijami za blaženje velikih kibernetskih incidentov. Organizira ga šestmesečno predsedstvo Sveta Evropske unije ob podpori Evropske obrambne agencije (EDA) in Evropske službe za zunanje delovanje (ESZD), tudi Vojaškega štaba Evropske unije (VŠEU).	Skupno sporočilo o politiki EU za kibernetsko obrambo (2022)
Komisija	Operativna/ politična	Izvršilni organ Evropske unije. Zagotavlja nemoteno delovanje notranjega trga. Omogoča skladnost in lažje usklajevanje sorodnih ukrepov na ravni Unije za odzivanje na krize. Nekatere dejavnosti na ravni Unije na področju splošne pripravljenosti na podlagi sklepa UCPM, vključno z vodenjem Centra za usklajevanje nujnega	Člen 17 Pogodbe o Evropski uniji Izvedbeni sklep (EU) 2018/1993 Sklep št. 1313/2013/EU Direktiva (EU) 2022/2555 Uredba (EU) 2025/38

Akter	Stopnja	Vloga in pristojnost	Referenca
		odziva in skupnega komunikacijskega in informacijskega sistema za primer nesreč. Opazovalka v mreži EU-CyCLONe in članica v primeru morebitnega ali potekajočega velikega incidenta, ki pomembno vpliva ali bi lahko pomembno vplival na storitve in dejavnosti, ki spadajo na področje uporabe Direktive (EU) 2022/2555. Opazovalka v mreži skupin CSIRT. Splošna odgovornost za izvajanje EU rezerve za kibernetsko varnost. Kontaktna točka v Medinstitucionalnem odboru za kibernetsko varnost za izmenjavo ustreznih informacij v zvezi z večjimi incidenti z mrežo EU-CyCLONe. Svetuje predsedstvu Sveta v zvezi z odločitvami za uporabo ali prekinitev uporabe IPCR (razen	Uredba (EU, Euratom) 2023/2841

Akter	Stopnja	Vloga in pristojnost	Referenca
		ob uveljavljanju solidarnostne klavzule na podlagi člena 222 PDEU). Službe Komisije skupaj z ESZD pripravljajo poročila ISAA.	
Agencija Evropske unije za kibernetsko varnost (ENISA)	Tehnična/ operativna	Izvaja naloge za doseganje visoke ravni kibernetske varnosti v Uniji, tudi z dejavnim podpiranjem držav članic in institucij Unije. Zagotavlja sekretariat za mrežo skupin CSIRT in mrežo EU-CyCLONe. Pripravlja redno poglobljeno tehnično poročilo o stanju na področju kibernetske varnosti v EU glede incidentov in kibernetskih groženj (skupaj z EC3 in CERT-EU ter v tesnem sodelovanju z državami članicami). Sodeluje pri razvoju skupnega odziva na velike čezmejne incidente ali krize, tako da zlasti: - združuje in analizira poročila iz nacionalnih virov;	Direktiva (EU) 2022/2555 Uredba (EU) 2019/881 Uredba (EU) 2025/38 Uredba (EU) 2024/2847

Akter	Stopnja	Vloga in pristojnost	Referenca
		- zagotavlja pretok informacij med tehnično, operativno in politično ravnijo; - na zahtevo olajšuje obvladovanje incidentov; - podpira subjekte Unije pri komuniciranju z javnostjo; - na zahtevo podpira države članice pri komuniciranju z javnostjo; - preizkuša zmogljivosti odzivanja na incidente in redno organizira vaje na področju kibernetske varnosti. Deluje kot javni naročnik, kadar ji je bilo delno ali v celoti zaupano delovanje in upravljanje EU rezerve za kibernetsko varnost. Vsaki dve leti organizira obsežno vsestransko vajo na področju kibernetske varnosti na ravni Unije, ki vključujejo tehnične, operativne ali strateške elemente. V sodelovanju z zadevno državo članico in drugimi ustreznimi deležniki pripravi poročilo o pregledu incidenta, da oceni vzroke, posledice in možnosti za ublažitev incidenta (na zahtevo Komisije ali mreže EU-CyCLONe	

Akter	Stopnja	Vloga in pristojnost	Referenca
		in z odobritvijo zadevne države članice). Obvešča EU-CyCLONe, kadar so informacije, sporočene v okviru obveznosti poročanja Akta o kibernetski odpornosti pomembne za usklajeno obvladovanje velikih kibernetskih incidentov in kriz na operativni ravni.	
Evropska organizacijska mreža za povezovanje v kibernetski krizi (mreža EU-CyCLONe)	Operativna	Podpira usklajeno obvladovanje velikih kibernetskih incidentov in kriz na operativni ravni. Zagotavlja redno izmenjavo ustreznih informacij med državami članicami ter institucijami, organi, uradi in agencijami Unije. Usklajuje obvladovanje velikih kibernetskih incidentov in kriz ter podpira odločanje na politični ravni v zvezi s takimi incidenti in krizami. Ocenjuje posledice in vpliv relevantnih velikih kibernetskih	Direktiva (EU) 2022/2555 Uredba (EU) 2025/38

Akter	Stopnja	Vloga in pristojnost	Referenca
		incidentov in kriz ter predlaga morebitne blažilne ukrepe. Na zahtevo zadevne države članice obravnava nacionalne načrte za odzivanje na velike kibernetske incidente in krize. Skupaj z agencijo ENISA in Komisijo pripravi predlogo za lažjo predložitev zahtevkov za podporo iz EU rezerve za kibernetsko varnost. Prejema informacije od držav članic glede njihovih zahtev za EU rezervo za kibernetsko varnost. Prejema informacije v zvezi z morebitnim ali potekajočim velikim kibernetskim incidentom od čezmejnih kibernetskih vozlišč ali mreže skupin CSIRT.	
Visoki predstavnik Unije za zunanje zadeve in varnostno politiko ob podpori Evropske	Politična	Vodi in usklajuje prizadevanja Unije za obravnavanje zunanjih varnostnih groženj na področju hibridnih in kibernetskih groženj. Odgovoren je za kibernetsko diplomacijo Unije in instrumente	Sklep Sveta 2010/427/EU

Akter	Stopnja	Vloga in pristojnost	Referenca
službe za zunanje delovanje		kibernetske obrambe za odvračanje od zunanjih groženj in odzivanje nanje, pri čemer med drugim uporablja nabor orodij Unije za odzivanje na hibridne grožnje in zbirko orodij Unije za kibernetsko diplomacijo. Sodeluje z zunanjimi partnerji, tudi v okviru SVOP. Skrbi za pripravljenost Unije in situacijsko zavedanje držav članic o hibridnih in kibernetskih grožnjah ter njihovo zmogljivost za odzivanje nanje, na primer s praktičnimi vajami, usposabljanjem in mrežami. Obravnava varnostne in obrambne vidike vesoljskih sredstev Unije, zlasti v okviru skupne varnostne in obrambne politike (SVOP) Unije. Podpira konferenco kibernetskih poveljnikov EU. Podpira operativno mrežo vojaških skupin EU za odzivanje	

Akter	Stopnja	Vloga in pristojnost	Referenca
		na izredne računalniške razmere (MICNET). Svetuje predsedstvu Sveta v zvezi z odločitvami za uporabo ali prekinitev uporabe IPCR (razen ob uveljavljanju solidarnostne klavzule na podlagi člena 222 PDEU). ESZD skupaj s službami Komisije pripravlja poročila ISAA.	
Center EU za koordinacijo kibernetske obrambe	Horizontalni	Njegov prvotni cilj je predvsem okrepiti skupno situacijsko zavedanje Unije in njenih držav članic o zlonamernih dejavnostih v kibernetskem prostoru, zlasti v zvezi z vojaškimi misijami in operacijami v okviru SVOP.	Skupno sporočilo o politiki EU za kibernetsko obrambo (2022)
Europol	Operativna	Zagotavlja operativno in tehnično podporo pristojnim organom držav članic za preprečevanje kibernetske kriminalitete in odvračanje od nje. Pomaga pristojnim organom držav članic na njihovo zahtevo pri odzivanju na kibernetske napade domnevno kaznivega izvora.	Uredba (EU) 2016/794, vključno z vsemi spremembami

Akter	Stopnja	Vloga in pristojnost	Referenca
Medinstitucionalni odbor za kibernetsko varnost		Pripravi načrt za obvladovanje kibernetskih kriz, da se na operativni ravni podpre usklajeno obvladovanje večjih incidentov, ki vplivajo na subjekte Unije, in prispeva k redni izmenjavi ustreznih informacij. Usklajuje sprejemanje načrtov za obvladovanje kibernetskih kriz za posamezne subjekte Unije. Na podlagi predloga CERT-EU sprejme smernice ali priporočila o sodelovanju pri odzivanju na pomembne incidente, ki zadevajo subjekte Unije.	Uredba (EU, Euratom) 2023/2841
Operativna mreža vojaških skupin za odzivanje na izredne računalniške razmere (MICNET)	Tehnična	Spodbuja odločnejši in bolj usklajen odziv na kibernetske grožnje, ki vplivajo na obrambne sisteme v Uniji, vključno s tistimi, ki se uporabljajo v vojaških misijah in operacijah v okviru SVOP. Podpira jo Evropska obrambna agencija.	Skupno sporočilo o kibernetski obrambi iz leta 2022
Enotna zmogljivost za analizo		Sestavljata jo (1) Obveščevalni in situacijski center EU (EU INTCEN) ter (2) Obveščevalni	Členi 38 in 42 do 46 Pogodbe o Evropski uniji

Akter	Stopnja	Vloga in pristojnost	Referenca
obveščevalnih podatkov (SIAC)		direktorat Vojaškega štaba EU (EUMS INT) SIAC. Zagotavlja strateške obveščevalne podatke o zunanji politiki, terorizmu ter kibernetskih in hibridnih grožnjah ter obdeluje vojaške obveščevalne podatke za misije SVOP ter podpira operacije Unije na področju obrambe in kriznega upravljanja. Pod vodstvom visokega predstavnika.	

(3) Ustrezni mehanizmi in platforme na ravni Unije za obvladovanje kriz

Mehanizem	Horizontalni / sektorski / kibernetski	Opis	Referenca
ARGUS	Horizontalni	Postopek Komisije za usklajevanje in splošni sistem Komisije za opozarjanje, ki omogoča skladno odzivanje v primeru večje čezmejne krize, ko je potrebno ukrepanje na ravni EU. Povezuje vse ustrezne službe in kabinete, ki odločajo o ukrepih in jih usklajujejo. Komisiji omogoča izmenjavo ustreznih informacij o nastajajočih večsektorskih krizah ali predvidljivih ali neposrednih grožnjah, ki zahtevajo ukrepanje na ravni Unije.	Sporočilo Komisije C(2005) 662
Center ESZD za krizno odzivanje	Horizontalni	Enotna vstopna točka za vsa vprašanja, povezana s krizo, v ESZD in stalna zmogljivost za odzivanje na krize, ki deluje 24 ur na dan vse dni v tednu, za izredne razmere, ki ogrožajo varnost osebja v delegacijah EU, in/ali za odzivanje na krize, ki vplivajo na državljane Unije v tujini. Združuje strokovnjake za varnost, konzularne strokovnjake in	Strateški kompas za varnost in obrambo – Za Evropsko unijo, ki varuje svoje državljane in državljanke, vrednote in interese ter prispeva k mednarodnemu miru

Mehanizem	Horizontalni / sektorski / kibernetski	Opis	Referenca
		strokovnjake za situacijsko zavedanje, hkrati pa se opira na predane strokovnjake na terenu v delegacijah Unije.	in varnosti (21. marec 2022)
Načrt za kritično infrastrukturo	Horizontalni	Usklajuje odziv na ravni Unije na motnje na kritični infrastrukturi z velikim čezmejnim pomenom.	Priporočilo Sveta C/2024/4371
Sistem opozarjanja glede kibernetske varnosti	Kibernetski	Zagotavlja napredne zmogljivosti Unije za izboljšanje zmogljivosti odkrivanja, analize in obdelave podatkov v zvezi s kibernetskimi grožnjami in preprečevanjem incidentov v Uniji.	Uredba (EU) 2025/38
Zbirka orodij za kibernetsko diplomacijo (okvir za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti)	Kibernetski	Omogoča skupni diplomatski odziv Unije na zlonamerne kibernetske dejavnosti, kar prispeva k preprečevanju konfliktov, odpravljanju kibernetskih groženj in večji stabilnosti v mednarodnih odnosih.	Sklepi Sveta z dne 19. junija 2017 Revidirane izvedbene smernice 10289/23, 8. junij 2023
EU rezerva za kibernetsko varnost	Kibernetski	Mobilizira strokovnjake in vire za kibernetsko varnost med krizami, da se podprejo prizadevanja za	Uredba (EU) 2025/38

Mehanizem	Horizontalni / sektorski / kibernetski	Opis	Referenca
		odzivanje v državah članicah, institucijah, organih ali agencijah Unije.	
Omrežni kodeks sektorskih pravil za vidike kibernetske varnosti čezmejnih pretokov električne energije	Sektorski	Določa redno pripravo ocene tveganja za kibernetsko varnost v sektorju električne energije na ravni Unije in držav članic, regionalni ravni ter ravni subjektov. Vsebuje posebne določbe o obvladovanju kriz ter sodelovanju z mrežo skupin CSIRT in mrežo EU-CyCLONe v primerih, ko velik kibernetski incident vpliva na druge sektorje, ki so odvisni od zanesljivosti oskrbe z električno energijo.	Delegirana uredba Komisije (EU) 2024/1366
Nabor orodij za odzivanje na hibridne grožnje	Horizontalni	Vključuje sklop določb, ki zagotavljajo pregled nad tem, katera orodja so na ravni EU na voljo za odzivanje na vse vrste hibridnih groženj, njihovo usklajeno uporabo in usklajenost naših ukrepov na vseh področjih. Nabor orodij za odzivanje na hibridne grožnje pomaga zagotoviti, da odločanje temelji na	Sklepi Sveta o okviru za usklajen odziv EU na hibridne kampanje, 22. junij 2022 Izvedbene smernice za okvir za usklajen odziv EU na hibridne

Mehanizem	Horizontalni / sektorski / kibernetski	Opis	Referenca
		celovitem situacijskem zavedanju in pridobljenih izkušnjah.	kampanje, 14. december 2022
Skupine za hitro odzivanje na hibridne grožnje	Horizontalni	Skupine EU za hitro odzivanje na hibridne grožnje so del nabora orodij EU za odzivanje na hibridne grožnje in se opirajo na ustrezno sektorsko civilno in vojaško strokovno znanje na nacionalni ravni in ravni EU, da bi državam članicam, misijam in operacijam skupne varnostne in obrambne politike ter partnerskim državam zagotovile prilagojeno in ciljno usmerjeno kratkoročno pomoč v boju proti hibridnim grožnjam in kampanjam.	Usmerjevalni okvir za vzpostavitev skupin EU za hitro odzivanje na hibridne grožnje v praksi (21. maj 2024) Operativne smernice za napotitev skupin za hitro odzivanje na hibridne grožnje, Coreper odobril 4. decembra 2024
IPCR	Horizontalni	Podpira hitro in usklajeno odločanje na politični ravni Unije v primeru večjih in kompleksnih kriz. Odločitev o uporabi in prekinitvi uporabe sprejme predsedstvo Sveta, ki se posvetuje (razen kadar se uveljavlja solidarnostna klavzula) s prizadetimi državami članicami, Komisijo in visokim predstavnikom.	Izvedbeni sklep Sveta (EU) 2018/1993

Mehanizem	Horizontalni / sektorski / kibernetski	Opis	Referenca
		GSS, službe Komisije in ESZD se lahko v posvetovanju s predsedstvom dogovorijo tudi o uporabi IPCR v načinu izmenjave informacij. Podlaga za delo IPCR so poročila ISAA, ki jih pripravljajo službe Komisije in ESZD. Taka poročila temeljijo na ustreznih informacijah in analizah, ki jih zagotavljajo države članice (npr. iz ustreznih nacionalnih kriznih centrov) ter ustrezni organi in agencije Unije.	
Protokol EU za odzivanje organov kazenskega pregona na izredne razmere	Horizontalni	Orodje za podporo organom Unije za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj pri takojšnjem odzivanju na večje čezmejne kibernetske napade s hitro oceno, varno in pravočasno izmenjavo kritičnih informacij ter učinkovitim usklajevanjem mednarodnih vidikov njihovih preiskav.	Sklepi Sveta (26. junij 2018) o usklajenem odzivu EU na velike kibernetske incidente in krize.
Enote za hitro odzivanje na	Kibernetski	Enote za hitro odzivanje na kibernetske grožnje v okviru PESCO	Člen 42(6) in člen 46 Pogodbe o Evropski

Mehanizem	Horizontalni / sektorski / kibernetski	Opis	Referenca
kibernetske grožnje v okviru PESCO		so civilno-vojaška zmogljivost kibernetske obrambe, ki so jo skupaj razvile države članice EU, namenjene pa so hitremu odzivanju na kibernetske incidente in kibernetske krize ter izvajanju preventivnih ukrepov, kot so ocene ranljivosti in spremljanje volitev. Enote za hitro odzivanje na kibernetske grožnje v okviru PESCO imajo nalogo, da na zahtevo zagotavljajo kibernetsko podporo državam članicam EU, institucijam, organom, uradom in agencijam EU, vojaškim misijam in operacijam EU v okviru SVOP ter partnerskim državam.	uniji in Protokol št. 10 k Pogodbi o Evropski uniji.

Struktura za odzivanje na vesoljske grožnje	Sektorski (vesoljske grožnje, vključno s kibernetskimi)	Struktura za odzivanje na vesoljske grožnje glede odgovornosti, ki jih izvajata Svet in visoki predstavnik za preprečevanje grožnje varnosti zaradi namestitve, delovanja ali uporabe vzpostavljenih sistemov in storitev, ki se zagotavljajo v okviru Vesoljskega programa Unije.	Sklep Sveta (SZVP) 2021/698
Okvir za usklajevanje v primeru sistemskih kibernetskih incidentov (EU-SCICF)	Sektorski	Okvir za komunikacijo in usklajevanje, ki se še razvija in ki bo obravnaval in upravljal morebitne sistemske kibernetske dogodke v finančnem sektorju. Temeljil bo na eni od predvidenih vlog evropskih nadzornih organov v skladu z Uredbo (EU) 2022/2554, in sicer postopnem omogočanju učinkovitega usklajenega odziva na ravni Unije v primeru večjega čezmejnega incidenta, povezanega z informacijsko in komunikacijsko tehnologijo (IKT), ali s tem povezane grožnje, ki bi imela sistemski učinek na celotni finančni sektor Unije.	Priporočilo Evropskega odbora za sistemska tveganja z dne 2. decembra 2021 o vseevropskem okviru za sistemsko usklajevanje kibernetskih incidentov za ustrezne organe (ESRB/2021/17)
Mehanizem Unije na področju civilne zaščite	Horizontalni	Zagotavlja sodelovanje na področju civilne zaščite, da bi se izboljšali	Sklep št. 1313/2013/EU

		preprečevanje nesreč ter pripravljenost in odzivanje nanje.	
CISE – skupno okolje za izmenjavo informacij	Specifično za pomorstvo, zajema sedem sektorjev.	CISE je omrežje, ki povezuje sisteme organov EU/EGP, pristojnih za pomorski nadzor. CISE omogoča nemoteno in avtomatizirano izmenjavo ustreznih informacij prek meja in med različnimi sektorji.	Strateški kompas za varnost in obrambo – Za Evropsko unijo, ki varuje svoje državljane in državljanke, vrednote in interese ter prispeva k mednarodnemu miru in varnosti (21. marec 2022)

(4) Visoko kritični sektorji in drugi kritični sektorji v skladu z Direktivo (EU) 2022/2555 ter sektorski krizni mehanizmi na ravni Unije (če je ustrezno)		
Sektorji	**Podsektor**	**Sektorski krizni mehanizmi, ki se uporabljajo**
Energija	Električna energija	Koordinacijska skupina za električno energijo
	Daljinsko ogrevanje in hlajenje	ni relevantno
	Nafta	Koordinacijska skupina za nafto Skupina organov Evropske unije, pristojnih za dejavnosti na morju (EUOAG)
	Plin	Koordinacijska skupina za plin
	Vodik	ni relevantno
Promet	Zračni prevoz	Evropska koordinacijska celica za krizne razmere v letalstvu (EACCC)
	Železniški prevoz	ni relevantno

	Voda	Evropska agencija za nadzor ribištva (EFCA) SafeSeaNet (SSN) Integrirane pomorske storitve Podatkovno središče za prepoznavanje in sledenje ladjam na velike razdalje (LRIT) Službe EMSA za pomoč na morju
	Cestni prevoz	ni relevantno
	Horizontalni	Mreža kontaktnih točk za prevoz, vzpostavljena s kriznim načrtom za promet (COM(2022) 211 final)
Bančne storitve		EU-SCICF
Infrastruktura finančnega trga		EU-SCICF Evropski mehanizem za finančno stabilizacijo

Zdravje		Sistem zgodnjega obveščanja in odzivanja Ustanova za operacije v nujnih zdravstvenih primerih (Health Emergency Operations Facility – HEOF) Sistem hitrega obveščanja o komponentah tkiv in celic ter krvi (Rapid alert system for tissue and cell and blood Components – RATC/RAB) Okvir za izredne razmere v javnem zdravju Sistem hitrega obveščanja o kemičnih incidentih (RASCHEM) Evropski portal za spremljanje nalezljivih bolezni Organ za pripravljenost in odzivanje na izredne zdravstvene razmere (HERA) Obveščevalni sistem na področju zdravja (MediSys) Izvršna usmerjevalna skupina za pomanjkanje medicinskih pripomočkov Sistem hitrega obveščanja na področju farmakovigilance

		Zdravstvena projektna skupina EU Odbor za zdravstveno varnost
Pitna voda		ni relevantno
Odpadna voda		ni relevantno
Digitalna infrastruktura		ni relevantno
Upravljanje storitev IKT		ni relevantno
Javna uprava		ni relevantno
Vesolje		Struktura za odzivanje na vesoljske grožnje
Poštne in kurirske storitve		ni relevantno
Ravnanje z odpadki		ni relevantno
Izdelava, proizvodnja in distribucija kemikalij		Sistem hitrega obveščanja o kemičnih incidentih (RASCHEM)

Pridelava, predelava in distribucija živil		Evropski sistem spremljanja pridelkov Globalno odkrivanje anomalij v kmetijski proizvodnji (ASAP) Evropska mreža informacijskih sistemov za zdravje rastlin (EUROPHYT) Veterinarska skupina EU za izredne dogodke (EUVET) Sistem hitrega obveščanja za živila in krmo (RASFF) Evropski mehanizem za pripravljenost in odzivanje na krize na področju prehranske varnosti (EFSCM) Akt o izrednih razmerah na notranjem trgu in njegovi odpornosti (IMERA)
Predelovalne dejavnosti	Medicinski pripomočki	ni relevantno
	Računalniki, elektronski in optični izdelki	ni relevantno
	Stroji in oprema	ni relevantno
	Proizvodnja motornih vozil, prikolic in polprikolic	ni relevantno
	Proizvodnja drugih vozil in plovil	ni relevantno

Digitalni ponudniki		ni relevantno
Raziskave		ni relevantno

Priloga III – Okvir EU za krizno upravljanje na področju kibernetske varnosti in povezani instrumenti

Unija je od leta 2017 oblikovala svoj okvir za kibernetsko varnost z več instrumenti, ki vsebujejo določbe, pomembne za obvladovanje kibernetskih kriz:

- Uredba (EU) 2019/881 Evropskega parlamenta in Sveta[1],
- Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta[2],
- Izvedbena uredba Komisije (EU) 2024/2690[3], Uredba (EU, Euratom) 2023/2841 Evropskega parlamenta in Sveta[4],
- Uredba (EU) 2021/887 Evropskega parlamenta in Sveta[5],
- Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta[6] in
- Uredba (EU) 2025/38 Evropskega parlamenta in Sveta (Akt o kibernetski solidarnosti)[7].

Posebni sektorski krizni ukrepi na področju kibernetske varnosti vključujejo Delegirano uredbo Komisije (EU) 2024/1366[8] ter prihodnji okvir za usklajevanje v primeru sistemskih kibernetskih incidentov (EU-SCICF) v okviru Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta[9].

Direktiva 2013/40[10] določa podlago za opredelitev kaznivih dejanj, povezanih s kibernetskimi napadi, pravila Unije o čezmejnem dostopu do elektronskih dokazov, zlasti Uredba (EU) 2023/1543 Evropskega parlamenta in Sveta[11], ko se bo začela izvajati, pa bo znatno olajšala ukrepe preprečevanja, odkrivanja in preiskovanja kaznivih dejanj na tem področju.

Politika EU za kibernetsko obrambo[12] določa vlogo operativne mreže vojaških skupin za odzivanje na izredne računalniške razmere EU (MICNET) in konference kibernetskih poveljnikov EU ter predvideva ustanovitev centra EU za koordinacijo kibernetske obrambe.

V nekaterih kritičnih sektorjih iz prilog I in II k Direktivi (EU) 2022/2555 obstajajo drugi mehanizmi za situacijsko zavedanje in odzivanje na krize, ki niso povezani s kibernetsko varnostjo.

V priporočilu Sveta o načrtu za usklajeno odzivanje na ravni Unije na motnje na kritični infrastrukturi z velikim čezmejnim pomenom[13] je določeno sodelovanje med ustreznimi akterji, kadar incident prizadene tako fizične vidike kot kibernetsko varnost kritične infrastrukture.

[1] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Izvedbena uredba Komisije (EU) 2024/2690 z dne 17. oktobra 2024 o določitvi pravil za uporabo Direktive (EU) 2022/2555 v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov, v katerih se incident šteje za pomembnega, kar zadeva ponudnike storitev DNS, registre TLD imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnega centra, ponudnike omrežij za dostavo vsebin, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev, ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (UL L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Uredba (EU, Euratom) 2023/2841 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije (UL L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Uredba (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov (UL L 202, 8.6.2021, str. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Uredba (EU) 2025/38 Evropskega parlamenta in Sveta z dne 19. decembra 2024 o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskih groženj in incidentov ter pripravo in

odzivanje nanje ter spremembi Uredbe (EU) 2021/694 (Akt o kibernetski solidarnosti) (UL L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Delegirana uredba Komisije (EU) 2024/1366 z dne 11. marca 2024 o dopolnitvi Uredbe (EU) 2019/943 Evropskega parlamenta in Sveta z oblikovanjem omrežnega kodeksa s sektorskimi pravili za vidike kibernetske varnosti čezmejnih pretokov električne energije (UL L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Uredba (EU) 2023/1543 Evropskega parlamenta in Sveta z dne 12. julija 2023 o evropskem nalogu za posredovanje in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih postopkih ter za izvrševanje zapornih kazni po kazenskem postopku in Direktiva (EU) 2023/1544 Evropskega parlamenta in Sveta z dne 12. julija 2023 o določitvi harmoniziranih pravil o imenovanju imenovanih poslovnih enot in pravnih zastopnikov za namen zbiranja elektronskih dokazov v kazenskih postopkih (UL L 191, 28.7.2023, str. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52022JC0049

[13] *UL C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=OJ:C_202404371