EVROPSKO RAČUNSKO SODIŠČE

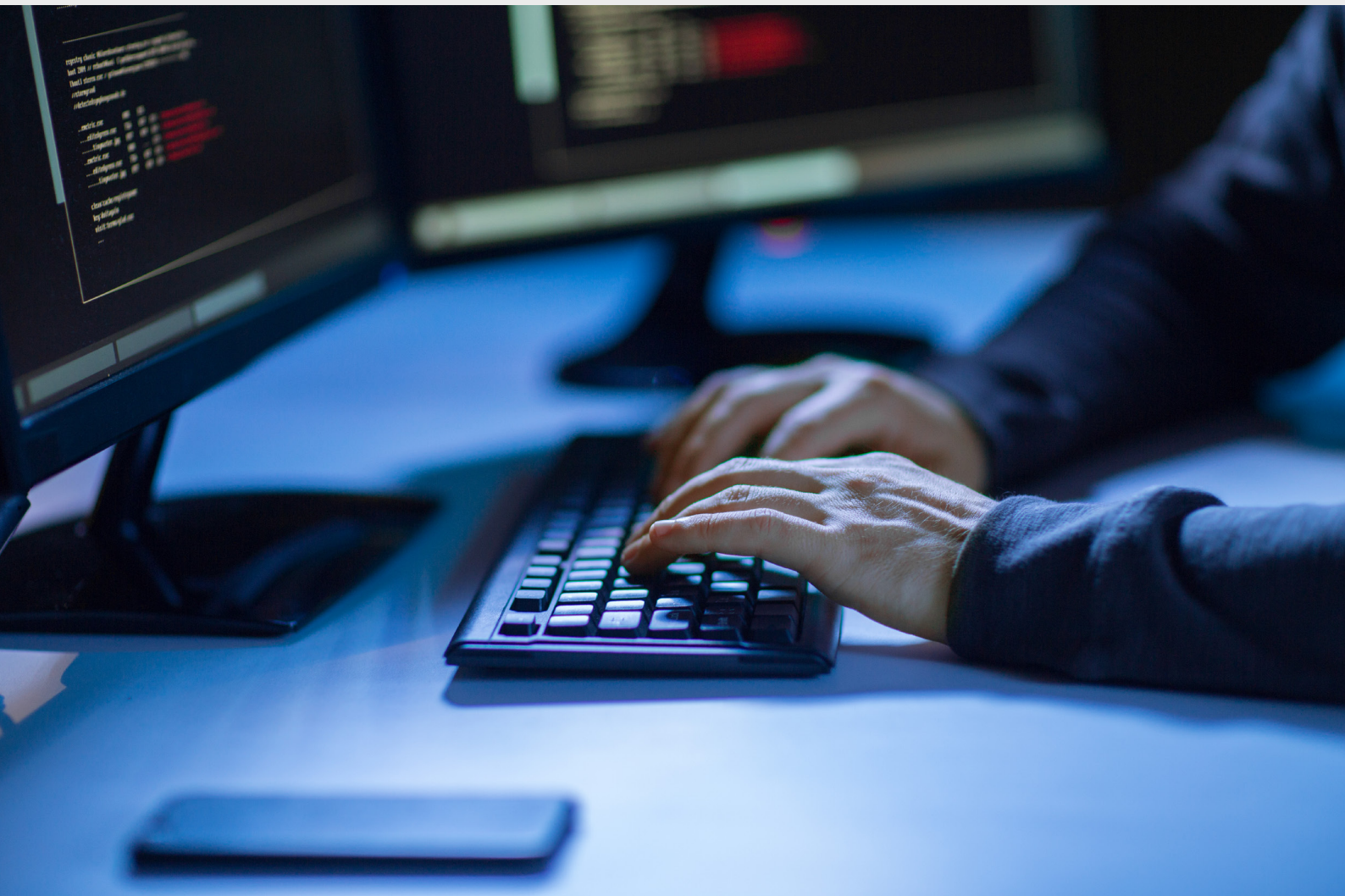
SL

2019

Izzivi za uspešno politiko EU za kibernetsko varnost

Informativni dokument

Marec 2019



O dokumentu:

Namen tega informativnega dokumenta, ki ni revizijsko poročilo, je zagotovitev pregleda kompleksne politike EU za kibernetsko varnost ter opredelitev glavnih izzivov za uspešno izvajanje te politike. V dokumentu so obravnavane varnost omrežij in informacijskih sistemov, kibernetska kriminaliteta, kibernetska obramba in dezinformacije. Poleg tega bo dokument podlaga za morebitne prihodnje revizije tega področja.

Analiza Sodišča temelji na dokumentacijskem pregledu javno dostopnih informacij v uradnih dokumentih, dokumentov o stališču in študij tretjih oseb. Delo na terenu je potekalo med aprilom in septembrom 2018, v dokumentu pa je upoštevan razvoj do decembra 2018. To delo dopolnjujejo anketa nacionalnih revizijskih uradov držav članic ter razgovori s ključnimi deležniki iz institucij EU in predstavniki zasebnega sektorja.

Opredeljeni izzivi so razvrščeni v štiri široke skupine: i) okvir politike; ii) financiranje in poraba; iii) izgradnja kibernetske odpornosti; iv) uspešno odzivanje na kibernetske incidente. Doseganje višje ravni kibernetske varnosti v EU ostaja nujno. Zato Sodišče na koncu vsakega poglavja navaja vrsto zamisli za prihodnji razmislek oblikovalcev politik, zakonodajalcev in strokovnjakov.

Sodišče se zahvaljuje službam Komisije, Evropski službi za zunanje delovanje, Svetu Evropske unije, ENISI, Europolu, Evropski organizaciji za kibernetsko varnost in nacionalnim revizijskim uradom držav članic za konstruktivne povratne informacije.

Vsebina

Povzetek

I Tehnologija ustvarja številne nove priložnosti, novi proizvodi in storitve pa postajajo sestavni del našega vsakodnevnega življenja. S tem se povečuje tudi tveganje, da postanemo žrtve kibernetske kriminalitete ali kibernetskega napada, katerih družbeni in ekonomski učinek se še vedno povečuje. Zagon EU od leta 2017 za povečanje prizadevanj za okrepitev kibernetske varnosti in njene digitalne samostojnosti tako poteka v ključnem trenutku.

II S tem informativnim dokumentom, ki ni revizijsko poročilo in temelji na javno dostopnih informacijah, želi Sodišče zagotoviti pregled zapletene in neenotne politike ter opredeliti glavne izzive za uspešno izvajanje te politike. V dokumentu je obravnavana politika EU za kibernetsko varnost, pa tudi kibernetska kriminaliteta in kibernetska obramba ter prizadevanja za boj proti dezinformacijam. Opredeljeni izzivi so razvrščeni v štiri glavne sklope: i) okvir politike in zakonodajni okvir; ii) financiranje in poraba; iii) izgradnja kibernetske odpornosti ter iv) uspešno odzivanje na kibernetske incidente. V vsakem poglavju je nekaj točk za razmislek o predstavljenih izzivih.

Okvir politike in zakonodajni okvir

III Oblikovanje ukrepov, usklajenih s širokimi cilji strategije EU za kibernetsko varnost, da bi EU postala najvarnejše digitalno okolje na svetu, je izziv, ker ni merljivih ciljev in ker je malo zanesljivih podatkov. Izidi se redko merijo, ocenjenih pa je bilo le malo področij. **Zagotavljanje smiselne odgovornosti in ocenjevanja** s prehodom na kulturo smotrnosti s praksami ocenjevanja je zato eden ključnih izzivov.

IV Zakonodajni okvir je še vedno nepopoln. Zakonodaja EU zaradi **vrzeli in neskladnosti pri njenem prenosu v nacionalne zakonodaje** težko dosega svoj polni potencial.

Financiranje in poraba

V **Uskladitev ravni naložb s cilji** je zahtevna: zanjo ni potrebno samo povečanje splošnih naložb v kibernetsko varnost – ki so bile v EU nizke in razdrobljene – temveč tudi učinka, zlasti z boljšim izkoriščanjem rezultatov porabe za raziskave in zagotavljanjem uspešnega ciljnega usmerjanja in financiranja zagonskih podjetij.

VI **Jasen pregled nad porabo EU** je bistven za to, da EU in njene države članice vedo, katere vrzeli je treba zapolniti za dosego njihovih zastavljenih ciljev. Ker v proračunu

EU ni namenskih sredstev za financiranje strategije za kibernetsko varnost, ni jasno, koliko denarja se porabi za kaj.

VII V času, ko je vedno več političnih prioritet povezanih z varnostjo, bi lahko **nezadostnost virov agencij EU, relevantnih za kibernetsko varnost**, preprečila doseganje ambicij EU. Obravnava tega izziva vključuje iskanje načinov za privabljanje in ohranjanje talentov.

Izgradnja kibernetske odpornosti

VIII Obstaja mnogo slabosti v upravljanju kibernetske varnosti, in sicer tako v javnih in zasebnih sektorjih v EU kot tudi na mednarodni ravni. To omejuje zmožnost svetovne skupnosti za odziv na kibernetske napade in njihovo omejevanje, poleg tega pa otežuje koherenten pristop na ravni EU. Zato je treba **okrepiti upravljanje kibernetske varnosti**.

IX **Usposabljanje in ozaveščanje** v vseh sektorjih in na vseh ravneh družbe je bistveno, saj je na svetovni ravni pomanjkanje znanja v zvezi s kibernetsko varnostjo vedno večje. Zdaj obstajajo omejeni standardi EU za usposabljanje, certificiranje ali ocenjevanje kibernetskega tveganja.

X Zaupanje je bistveno za krepitev splošne kibernetske odpornosti. Komisija sama je ocenila, da je usklajevanje na splošno še vedno nezadostno. **Izboljšanje izmenjave informacij in usklajevanja** med javnimi in zasebnimi sektorji je še vedno izziv.

Uspešno odzivanje na kibernetske incidente

XI Digitalni sistemi so postali tako kompleksni, da je nemogoče preprečiti vse napade. Odziv na ta izziv je **hitro zaznavanje in odzivanje**. Toda kibernetska varnost še ni v celoti vključena v obstoječe mehanizme za usklajevanje odzivanja na krize na ravni EU, kar lahko zmanjšuje zmožnost EU za odziv na velike čezmejne kibernetske incidente.

XII Ključna je **zaščita kritične infrastrukture in družbenih funkcij**. Kritičen izziv so potencialno poseganje v volilne procese in kampanje širjenja dezinformacij.

XIII Zaradi sedanjih izzivov v zvezi s kibernetskimi grožnjami, s katerimi se srečujeta EU in širše globalno okolje, sta potrebna stalna zavezanost temeljnim vrednotam EU in njihovo neomajno uveljavljanje.

Uvod

01 Tehnologija ustvarja številne nove priložnosti, novi proizvodi in storitve pa postajajo sestavni del našega vsakodnevnega življenja. Z vsako novostjo pa se naša odvisnost od tehnologije in z njo pomembnost kibernetske varnosti večata. Več osebnih podatkov ko damo na voljo na spletu in bolj ko smo povezani, večja je verjetnost, da bomo postali žrtev neke vrste kibernetske kriminalitete ali kibernetskega napada.

Kaj je kibernetska varnost?

02 Standardna in splošno sprejeta opredelitev kibernetske varnosti ne obstaja[1]. Na splošno so to vsi zaščitni in drugi ukrepi, sprejeti za obrambo informacijskih sistemov in njihovih uporabnikov pred nepooblaščenim dostopom, napadom in poškodovanjem, da se zagotovi zaupnost, celovitost in razpoložljivost podatkov.

03 Kibernetska varnost obsega preprečevanje in odkrivanje kibernetskih incidentov ter odzivanje nanje in ponovno vzpostavitev prejšnjega stanja. Incidenti so lahko namerni ali nenamerni in zajemajo npr. nenamerno razkritje informacij, napade na podjetja in kritično infrastrukturo, krajo osebnih podatkov in celo poseganje v demokratične procese. Vse to ima lahko obširne škodljive posledice za posameznike, organizacije in skupnosti.

04 Kot izraz, ki se uporablja v zvezi s politiko EU, kibernetska varnost ni omejena na varnost omrežij in informacij. Zajema vse nezakonite dejavnosti, ki vključujejo uporabo digitalnih tehnologij v kibernetskem prostoru. Zato lahko zajema kibernetsko kriminaliteto, kot sta npr. izvedba napada z računalniškim virusom in goljufija z negotovinskim plačevanjem, lahko pa vključuje tudi sisteme in vsebino, kot npr. razširjanje spletnega gradiva o spolni zlorabi otrok. Vključuje lahko tudi kampanje za širjenje dezinformacij za vplivanje na spletne razprave in domnevno poseganje v volilne procese. Poleg tega Europol meni, da se kibernetska kriminaliteta in terorizem zbližujeta[2].

05 Različni akterji, vključno z državami, kriminalnimi združbami in hekerji-aktivisti, izvajajo kibernetske incidente z različnimi motivi. Negativne posledice teh incidentov so občutene na nacionalni, evropski in celo svetovni ravni. Vendar neotipljivost in brezmejnost interneta ter uporabljena orodja in taktike pogosto otežujejo identifikacijo storilca napada (t. i. problem pripisa).

06 Številne vrste groženj za kibernetsko varnost je mogoče razvrstiti glede na to, kaj se pri njih zgodi s podatki – razkritje, spreminjanje, uničenje ali preprečitev dostopa –, ali glede na to, katera temeljna načela varnosti informacij kršijo, kot je prikazano na *sliki 1* spodaj. Nekaj primerov napadov je opisanih v *okviru 1*. Z vedno večjo sofisticiranostjo napadov na informacijske sisteme naši obrambni mehanizmi postajajo manj uspešni[3].

Slika 1 – Vrste groženj in varnostna načela, ki jih ogrožajo

Vir: Evropsko računsko sodišče, prilagojeno po študiji Evropskega parlamenta[4]. Obešanka = varno; klicaj = varnost ogrožena.

Okvir 1

Vrste kibernetskih napadov

Vsakič ko se nova naprava poveže na splet ali z drugimi napravami, se poveča t. i. površina za kibernetske napade. Eksponentno rast interneta stvari, računalništva v oblaku, velepodatkov in digitalizacije industrije spremlja vedno večja izpostavljenost ranljivosti, zaradi česar lahko zlonamerni akterji napadajo vedno več žrtev. Zaradi velikega števila različnih vrst napadov in njihove vse večje sofisticiranosti je resnično težko slediti razvoju[5].

Zlonamerna programska oprema je zasnovana tako, da škoduje napravam ali omrežjem. Vključuje lahko viruse, trojance, izsiljevalsko programje, črve, oglaševalsko in vohunsko programje. **Izsiljevalsko programje** šifrira podatke in s tem uporabnikom preprečuje dostop do njihovih datotek, dokler ne plačajo odkupnine, običajno v kriptovaluti, ali dokler ne izvedejo zahtevanega dejanja. Po podatkih

Europola na splošno prevladujejo napadi z izsiljevalskim programjem, število vrst izsiljevalskega programja pa se je v zadnjih nekaj letih izredno povečalo. Povečuje se tudi število **porazdeljenih napadov za zavrnitev storitve** (DDoS), s katerimi se onemogoči dostop do storitev ali virov s tem, da jih preplavi s toliko zahtevki, da jih ne morejo obdelati. Leta 2017 se je tretjina organizacij srečevala s to vrsto napadov[6].

Uporabniki se lahko z manipulacijo pripravijo do tega, da nevede nekaj storijo ali razkrijejo zaupne informacije. To se lahko uporabi za krajo podatkov ali kibernetsko vohunjenje in se imenuje **socialni inženiring**. Obstajajo različni načini za doseganje tega, običajna metoda pa je **lažno predstavljanje**, pri katerem so elektronska pisma videti, kot da prihajajo iz zanesljivega vira, da se prejemnike zavede, da razkrijejo informacije ali kliknejo na povezave, ki bodo naprave okužile s preneseno zlonamerno programsko opremo. Več kot polovica držav članic je poročala o preiskavah v zvezi z napadi na omrežja[7].

Najbolj škodljiva vrsta groženj pa so verjetno **napredne neprestane grožnje** (APT). Gre za sofisticirane napadalce, ki dolgo spremljajo in kradejo podatke, včasih pa imajo tudi uničevalne cilje. Njihov cilj je, da njihova dejanja čim dlje ostanejo nezaznana. Napredne neprestane grožnje so pogosto povezane z državo in usmerjene v posebej občutljive sektorje, kot so tehnologija, obramba in kritična infrastruktura. Kibernetsko vohunjenje naj bi pomenilo vsaj četrtino kibernetskih incidentov in večino stroškov[8].

Kako resen je problem?

07 Vpliv slabe pripravljenosti na kibernetski napad je težko opisati, ker ni dovolj zanesljivih podatkov. Ekonomski vpliv kibernetske kriminalitete se je v obdobju med letoma 2013 in 2017 povečal za petkrat[9], prizadene pa vlade velikih in majhnih držav ter velika in majhna podjetja. Napovedana rast zneska premij za kibernetsko zavarovanje s 3 milijard EUR leta 2018 na 8,9 milijarde EUR leta 2020 odraža ta trend.

08 Medtem ko finančni vpliv kibernetskih napadov še vedno raste, obstaja zaskrbljujoča razlika med stroški izvedbe napada in stroški preprečevanja, preiskave in vzpostavitve prejšnjega stanja. Izvedba porazdeljenega napada za zavrnitev storitve lahko npr. stane manj kot 15 EUR na mesec, izgube podjetja, ki je tarča napada, vključno z oškodovanjem ugleda, pa so bistveno večje[10].

09 Čeprav je 80 % podjetij v EU leta 2016 izkusilo vsaj en incident, povezan s kibernetsko varnostjo[11], je priznavanje tveganj še vedno zaskrbljujoče nizko. Od podjetij v EU jih 69 % ne pozna svoje izpostavljenosti kibernetskim grožnjam ali pa poznajo le osnove[12], 60 % pa jih še nikoli ni ocenilo potencialnih finančnih izgub[13]. Poleg tega bi po navedbah iz svetovne raziskave tretjina organizacij raje plačala odkupnine hekerjem, kot da bi vložila v varnost informacij[14].

10 Svetovna napada z izsiljevalskim programjem *WannaCry* in zlonamerno programsko opremo za brisanje *NotPetya* leta 2017 sta skupaj prizadela več kot 320 000 žrtev v približno 150 državah[15]. Ti dogodki so privedli do nekakšnega svetovnega prebujenja v zvezi s tem, kako velika grožnja so kibernetski napadi, kar je ustvarilo nov zagon za vključitev kibernetske varnosti v razmišljanje o splošnih politikah. Poleg tega 86 % državljanov EU zdaj meni, da tveganje, da bi postali žrtve kibernetske kriminalitete, narašča[16].

Ukrepi EU na področju kibernetske varnosti

11 EU je leta 2001 postala organizacija opazovalka v Odboru Sveta Evrope za Konvencijo o kibernetski kriminaliteti (Budimpeška konvencija)[17]. Odtlej je EU za izboljšanje kibernetske odpornosti uporabljala politike, zakonodajo in finančna sredstva. Ob vedno večjem številu velikih kibernetskih napadov in incidentov so se dejavnosti od leta 2013 pospešile, kot je prikazano na ***sliki 2***. Hkrati pa so države članice sprejele (nekatere pa tudi že posodobile) svoje prve nacionalne strategije za kibernetsko varnost.

12 Glavni akterji EU z odgovornostjo za kibernetsko varnost so navedeni v ***okviru 2*** in ***Prilogi I***.

Okvir 2

Kdo je vpleten?

Evropska komisija se zavzema za povečanje zmogljivosti in sodelovanja na področju kibernetske varnosti, krepitev vloge EU kot akterja na področju kibernetske varnosti ter vključitev kibernetske varnosti v druge politike EU. Glavna generalna direktorata (GD), odgovorna za politiko za kibernetsko varnost, sta GD **CNECT** (kibernetska varnost) in GD **HOME** (kibernetska kriminaliteta), ki sta odgovorna za enotni digitalni trg oz. varnostno unijo. GD **DIGIT** je odgovoren za varnost IT v sistemih Komisije.

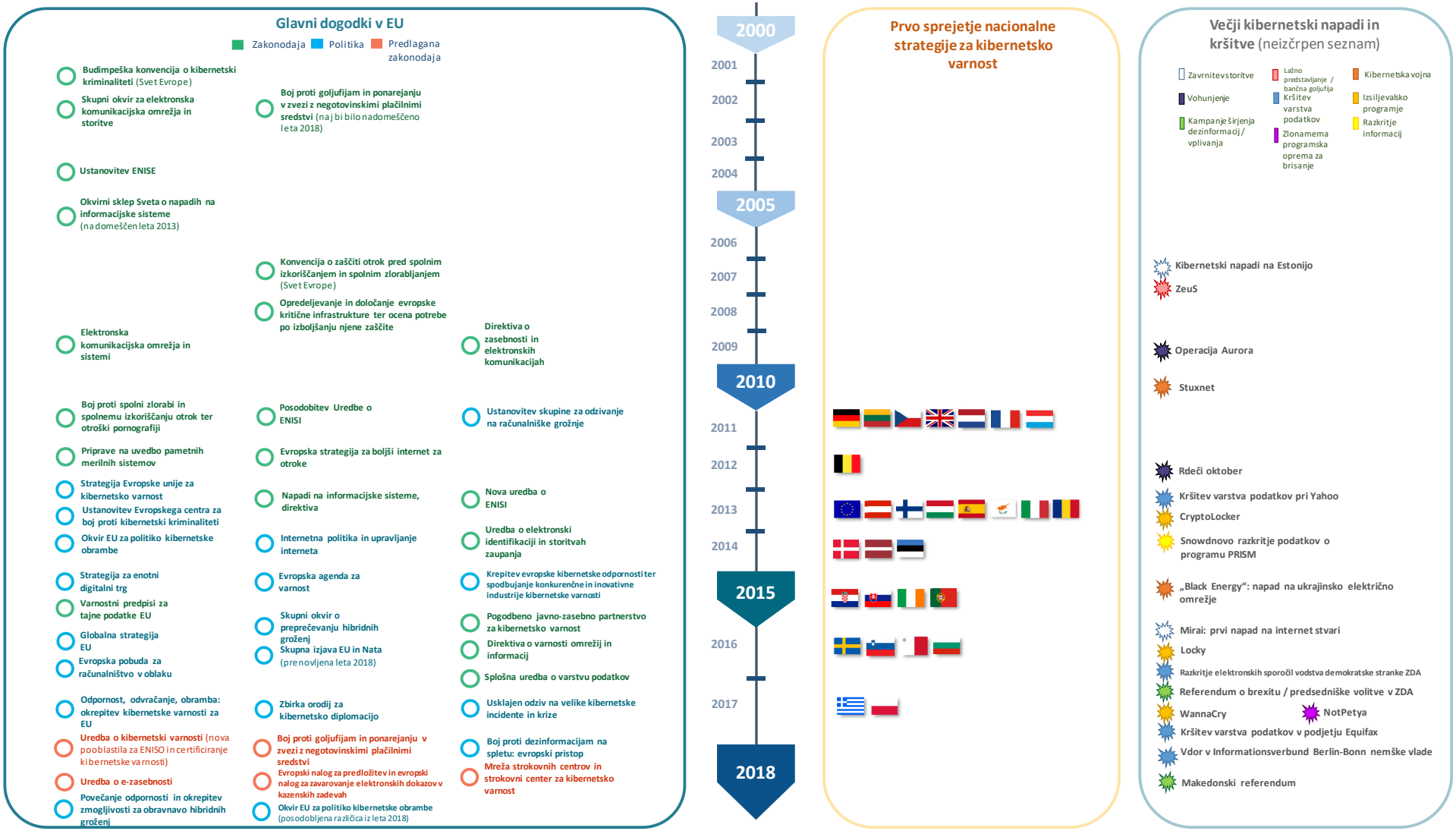
Komisijo podpira več agencij EU, zlasti **ENISA** (Agencija Evropske unije za varnost omrežij in informacij), agencija EU za kibernetsko varnost, ki je v glavnem svetovalni organ in podpira razvoj politik, izgradnjo zmogljivosti in ozaveščanje. Europolov Evropski center za boj proti kibernetski kriminaliteti (**EC3**) je bil ustanovljen za krepitev odziva organov kazenskega pregona EU na kibernetsko kriminaliteto. Komisija gosti skupino za odzivanje na računalniške grožnje (**CERT-EU**), ki podpira vse institucije, organe in agencije Unije.

Evropska služba za zunanje delovanje (ESZD) vodi kibernetsko obrambo, kibernetsko diplomacijo in strateško komuniciranje, poleg tega pa gosti centra za obveščevalne podatke in analize. **Evropska obrambna agencija** (EDA) si prizadeva za razvoj zmogljivosti za kibernetsko obrambo.

Države članice so prve odgovorne za svojo kibernetsko varnost in na ravni EU delujejo prek **Sveta**, ki ima številne organe za usklajevanje in izmenjavo informacij (med njimi tudi Horizontalno delovno skupino za kibernetska vprašanja). **Evropski parlament** deluje kot sozakonodajalec.

Organizacije zasebnega sektorja, vključno z industrijo, organi za upravljanje interneta in akademsko skupnostjo, delujejo kot partnerji v razvoju in izvajanju politike, h katerima prispevajo, tudi s pogodbenimi javno-zasebnimi partnerstvi (**cPPP**).

Slika 2 – Pospešitev razvoja politike in zakonodaje (stanje na dan 31. decembra 2018)



Vir: Evropsko računsko sodišče

Politika

13 Kibernetski ekosistem EU je kompleksen in večplasten, poleg tega pa zadeva različna področja notranje politike, kot so pravosodje, notranje zadeve, enotni digitalni trg in raziskovalne politike. Na področju zunanje politike se s kibernetsko varnostjo ukvarja diplomacija, vedno bolj pa postaja del nastajajoče obrambne politike EU.

14 Temelj politike EU je **strategija za kibernetsko varnost iz leta 2013**[18]. Namen strategije je narediti digitalno okolje EU najvarnejše na svetu, obenem pa zaščititi temeljne vrednote in svoboščine. Ima pet glavnih ciljev: (i) povečevanje kibernetske odpornosti; (ii) zmanjšanje kibernetske kriminalitete; (iii) razvoj politik in zmogljivosti za kibernetsko obrambo; (iv) razvoj industrijskih in tehnoloških virov za kibernetsko varnost in (v) vzpostavitev mednarodne politike o kibernetskem prostoru, ki bi bila skladna s temeljnimi vrednotami EU.

15 Strategija za kibernetsko varnost je povezana s tremi pozneje sprejetimi strategijami:

— Cilj **evropske agende za varnost** (2015) je izboljšanje kazenskega pregona in pravosodnega odziva na kibernetsko kriminaliteto, zlasti s prenavljanjem in posodabljanjem obstoječih politik in zakonodaje[19]. Njen namen je opredelitev ovir za kazenske preiskave v zvezi s kibernetsko kriminaliteto ter okrepitev izgradnje kibernetske zmogljivosti.

— Cilj **strategije za enotni digitalni trg**[20] (2015) je ustvariti boljši dostop do digitalnega blaga in storitev z ustvarjanjem ustreznih pogojev za doseganje največjega mogočega potenciala rasti digitalnega gospodarstva. Krepitev spletne varnosti, zaupanja in vključevanja je za to ključna.

— Cilj **globalne strategije**[21] iz leta 2016 je okrepitev vloge EU v svetu. Z obnovljeno zavezo obravnavi kibernetskih zadev in sodelovanju s ključnimi partnerji ter odločenostjo, da se bodo kibernetske zadeve obravnavale na vseh področjih politike, tudi v okviru ovržbe dezinformacij s strateškimi komunikacijami, je kibernetska varnost postala njen temeljni steber.

16 V zadnjih letih je kibernetski prostor vse bolj militariziran[22] in uporaben kot orožje[23], zato šteje za peto področje vojskovanja[24]. Kibernetska obramba ščiti sisteme, omrežja in kritično infrastrukturo v kibernetskem prostoru pred vojaškimi ali drugačnimi napadi. **Okvir politike za kibernetsko obrambo** je bil sprejet leta 2014 in posodobljen leta 2018[25]. S posodobitvijo leta 2018 je bilo opredeljenih šest prioritet,

vključno z razvojem zmogljivosti za kibernetsko obrambo in varovanjem komunikacijskih in informacijskih omrežij za skupno varnostno in obrambno politiko EU (SVOP). Kibernetska obramba je vključena tudi v okvir za stalno strukturno sodelovanje (PESCO) ter sodelovanje med EU in Natom.

17 S **skupnim okvirom EU o preprečevanju hibridnih groženj** (iz leta 2016) se obravnavajo kibernetske grožnje za kritično infrastrukturo in zasebne uporabnike, pri tem pa je poudarjeno, da se napadi lahko izvajajo s kampanjami za širjenje dezinformacij na družbenih medijih[26]. V njem je poudarjena tudi potreba po izboljšanju ozaveščenosti in krepitvi sodelovanja med EU in Natom, ki je bilo določeno v skupnih izjavah EU in Nata iz let 2016 in 2018[27].

18 Komisija je leta 2017 predstavila nov sveženj o kibernetski varnosti, ki je odražal vse večjo nujnost digitalne zaščite. Vključeval je novo sporočilo Komisije o posodobitvi strategije za kibernetsko varnost iz leta 2013[28], načrt za hiter in usklajen odziv na velik napad ter za hitro izvajanje direktive o varnosti omrežij in informacij[29]. Sveženj poleg tega vsebuje več zakonodajnih predlogov (glej odstavek ***22***).

Zakonodaja

19 Od leta 2002 so bili sprejeti zakonodajni akti z različno relevantnostjo za kibernetsko varnost.

20 Glavni steber strategije za kibernetsko varnost iz leta 2013 je **direktiva o varnosti omrežij in informacij**[30] iz leta 2016, ki je prvi vseevropski zakonodajni akt o kibernetski varnosti. Cilj direktive, ki jo je bilo treba v nacionalne zakonodaje prenesti do maja 2018, je doseči minimalno raven usklajenih zmogljivosti s tem, da se državam članicam naloži obveznost sprejetja nacionalnih strategij za varnost omrežij in informacijskih sistemov ter uvedbe enotnih kontaktnih točk in skupin za odzivanje na incidente na področju računalniške varnosti[31]. Poleg tega so v njej določene varnostne zahteve in zahteve za priglasitev za izvajalce bistvenih storitev v kritičnih sektorjih in ponudnike digitalnih storitev.

21 Leta 2016 je istočasno začela veljati **splošna uredba o varstvu podatkov**[32], ki se je začela uporabljati maja 2018. Njen cilj je varovanje osebnih podatkov evropskih državljanov, in sicer z določitvijo pravil za obdelavo in razširjanje osebnih podatkov. Posamezniki, na katere se nanašajo osebni podatki, so s to direktivo dobili nekatere pravice, upravljavci podatkov (ponudniki digitalnih storitev) pa obveznosti v zvezi z

uporabo in prenosom informacij. Z direktivo so določene zahteve uradne obvestitve v primeru kršitve, v nekaterih primerih pa tudi naložitev globe. Na ***sliki 3*** je prikazano, kako se direktiva o varnosti omrežij in informacij ter splošna uredba o varstvu podatkov dopolnjujeta pri svojih ciljih krepitve kibernetske varnosti in zagotavljanja varstva podatkov.

22 Osnutki zakonodajnih aktov, o katerih se trenutno razpravlja, vključujejo predlagano uredbo o kibernetski varnosti za okrepitev ENISE in uvedbo mehanizma certificiranja za celotno EU[33], predlagano uredbo o nalogu za predložitev in nalogu za zavarovanje elektronskih dokazov[34] ter predlagano direktivo o elektronskih dokazih[35]. Predlog iz leta 2018 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov (v nadaljnjem besedilu: mreža strokovnih centrov za kibernetsko varnost in raziskovalni strokovni center) je del svežnja za kibernetsko varnost iz leta 2017[36].

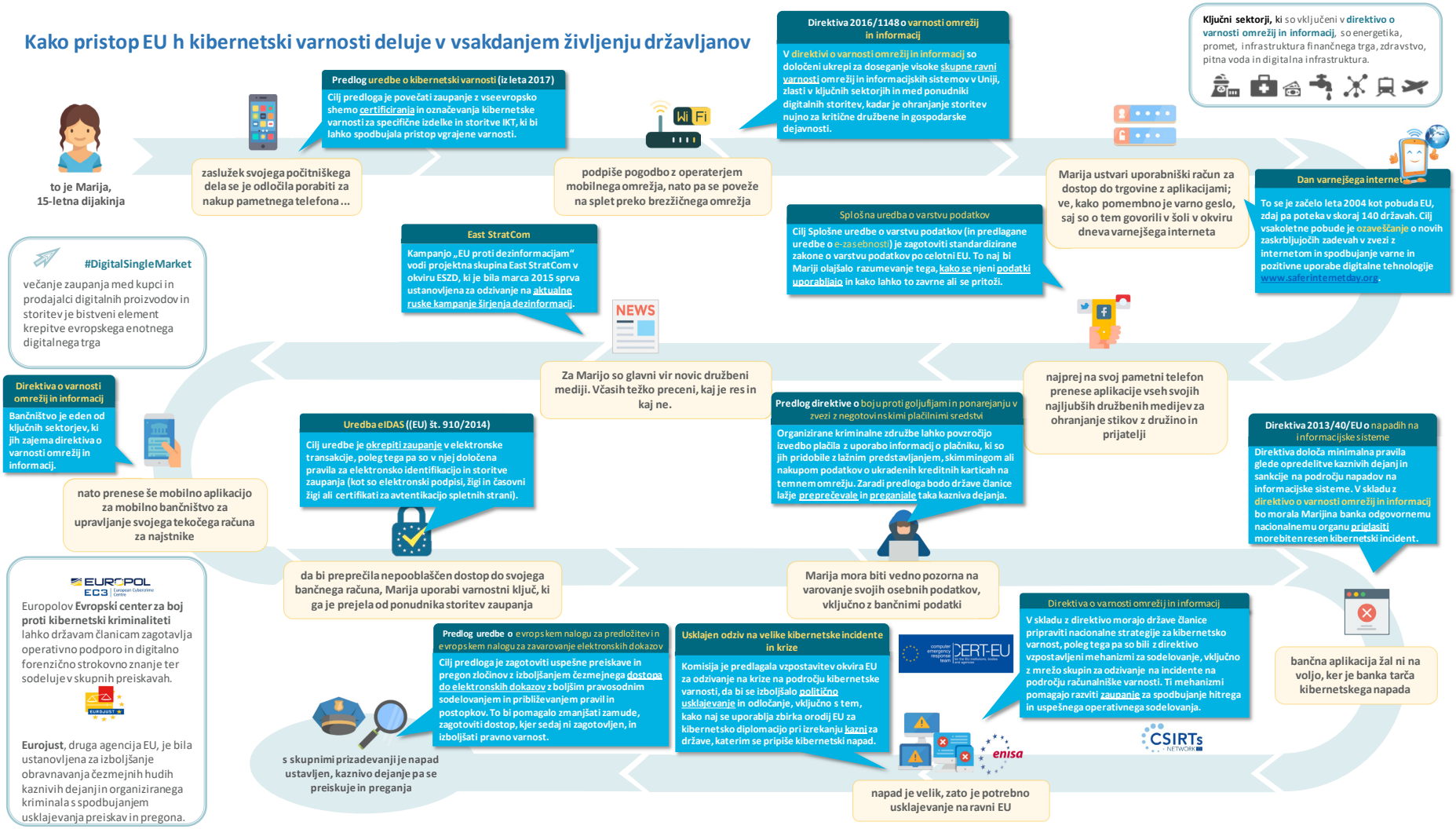
23 Včasih si je težko predstavljati, kako široka sta okvir politike in zakonodajni okvir, ki zadevata kibernetsko varnost, in kako kibernetska varnost vpliva na naš vsakdan.

24 Na ***sliki 4*** je prikazan vpliv različnih zakonodajnih aktov in drugih dejavnosti na življenje fiktivnega evropskega državljana.

Slika 3 – Kako se splošna uredba o varstvu podatkov in direktiva o varnosti omrežij in informacij dopolnjujeta

Vir: Evropsko računsko sodišče

Slika 4 – Kako pristop EU h kibernetski varnosti deluje v vsakdanjem življenju državljanov



Vir: Evropsko računsko sodišče

Priprava okvira politike in zakonodajnega okvira

25 Kibernetski ekosistem EU je kompleksen in večplasten, poleg tega pa vključuje mnogo deležnikov (glej ***Prilogo I***). Združevanje vseh njegovih različnih delov je velik izziv. Od leta 2013 potekajo usklajena prizadevanja za doseganje koherentnosti na področju kibernetske varnosti v EU[37].

Izziv 1: smiselno ocenjevanje in odgovornost

26 Kot je navedla Komisija, je težko vzpostaviti vzročno zvezo med strategijo iz leta 2013 in morebitnimi spremembami. Cilji strategije iz leta 2013 so bili določeni zelo široko in so izražali bolj vizijo kot merljivo ciljno vrednost[38]. Razvijanje ukrepov, usklajenih s temi obsežnimi cilji, je izziv, ker ni merljivih ciljev. Cilj posodobljenega okvira politike za kibernetsko obrambo (2018) bo razvoj ciljev z določeno minimalno ravnjo kibernetske varnosti in zaupanja, ki ga je treba doseči. Toda to bo omejeno na kibernetsko obrambo; cilji v zvezi z želeno ravnjo odpornosti za EU kot celoto še niso bili določeni.

27 Izidi se redko merijo, ocenjenih pa je bilo le malo področij[39]. To je deloma posledica nedavnega izvajanja mnogih ukrepov – zakonodajnih ali drugih –, kar ovira popolno oceno njihovega učinka. Izziv je opredeliti smiselna merila za oceno, s katerimi bi bilo mogoče meriti učinek. Poleg tega strogo ocenjevanje še ni postalo norma za kibernetsko varnost na splošno. Zato je potreben premik v smeri kulture smotrnosti s praksami za ocenjevanje in standardiziranim poročanjem. Sedanja pristojnost ENISE ne zajema ocenjevanja in spremljanja stanja kibernetske varnosti in pripravljenosti v EU.

28 Z dokazi podprto oblikovanje politik je odvisno od razpoložljivosti zadostnih in zanesljivih statističnih in drugih podatkov za lažje spremljanje in analiziranje trendov in potreb. Ker ni obveznega in skupnega sistema spremljanja, je zanesljivih podatkov malo. Kazalniki pogosto niso takoj na voljo, poleg tega pa jih je težko opredeliti[40]. Na nekaterih področjih je bila razvita specifična metrika, kot npr. politični cikel EU, ki se uporablja za boj proti hudim kaznivim dejanjem in organiziranemu kriminalu.

29 Le malo držav članic redno zbira uradne podatke o zadevah, povezanih s kibernetskim prostorom, zato je primerljivost okrnjena. EU do zdaj ni jasno izrazila potrebe po združitvi statističnih podatkov na evropski ravni[41]. Na voljo je tudi le nekaj neodvisnih analiz za celo EU[42], ki obravnavajo ključne teme, kot so: ekonomski vidiki

kibernetske varnosti, vključno z vedenjskimi vidiki (neskladnost spodbud, informacijska asimetrija), razumevanje učinka okvar kibernetske infrastrukture in kibernetske kriminalitete, makrostatistični podatki o kibernetskih trendih in pričakovanih izzivih ter najboljše rešitve za obravnavo groženj.

30 Ker ni specifičnih ciljev in ker je malo zanesljivih podatkov in dobro opredeljenih kazalnikov, je bila do zdaj ocena dosežkov strategije večinoma kvalitativna. V poročilih o napredku so pogosto opisane izvedene dejavnosti ali doseženi mejniki, rezultati pa niso temeljito izmerjeni. Poleg tega še niso bila določena izhodišča za ocenjevanje odpornosti sistemov. Ker ni kodificirane opredelitve kibernetske kriminalitete pa je skoraj nemogoče določiti relevantne evropske kazalnike, s katerimi bi bilo lažje izvajati spremljanje in ocenjevanje.

31 Neodvisen nadzor izvajanja politike kibernetske varnosti se med državami članicami razlikuje. Sodišče je z anketo zbralo podatke o tem, kakšne izkušnje imajo nacionalni revizijski uradi z revidiranjem tega področja. Polovica sodelujočih[43] še nikoli ni revidirala tega področja. Tisti, ki pa so ga že revidirali, so se pri svojih revizijah osredotočali predvsem na: upravljanje informacij, zaščito kritične infrastrukture, izmenjavo informacij in usklajevanje med ključnimi deležniki, pripravljenost na incidente, priglasitev in odziv. Med manj obravnavanimi področji so bili ukrepi za ozaveščanje in vrzel na področju digitalnega znanja. Rezultati teh revizij ali ocen zaradi nacionalne varnosti niso vedno objavljeni. Seznam revizijskih poročil, ki so jih nacionalni revizijski uradi objavili, je v ***Prilogi III***.

32 Omejitve znanja v zvezi s kibernetskim prostorom (glej tudi odstavke ***82 do 90***) ter težave pri ocenjevanju napredka na področju kibernetske varnosti so bili po mnenju sodelujočih glavni izzivi za revidiranje vladnih ukrepov na tem področju.

Izziv 2: odpravljanje vrzeli v zakonodaji EU in neenakomeren prenos zakonodaje EU v nacionalno zakonodajo

33 Pojavljanje novih tehnologij in groženj je veliko hitrejše od zasnove in izvajanja zakonodaje EU. Postopki Unije niso bili zasnovani za digitalno dobo: pomembna prioriteta je razvoj inovativnih in fleksibilnih postopkov za zagotavljanje okvira politike in pravnega okvira, ki ustrezata svojemu namenu[44], za boljše predvidevanje in oblikovanje prihodnosti[45].

34 Kljub prizadevanjem za večjo koherentnost je zakonodajni okvir za kibernetsko varnost še vedno nepopoln (za nekaj primerov glej ***tabelo 1***). Razdrobljenost in vrzeli

ovirajo doseganje splošnih ciljev politike in vodijo do neučinkovitosti. Vrzeli, ki jih je Komisija opredelila v oceni strategije, so vključevale internet stvari, ravnovesje odgovornosti med uporabniki in ponudniki digitalnih izdelkov ter nekatere vidike, ki niso obravnavani v direktivi o varnosti omrežij in informacij. To se poskuša deloma obravnavati s predlagano uredbo o kibernetski varnosti, in sicer s spodbujanjem vgrajene varnosti s certifikacijsko shemo za celotno EU. Po mnenju nekaterih deležnikov še vedno ni jasno opredeljene politike v zvezi s kibernetsko industrijo in skupnega pristopa h kibernetskemu vohunjenju[46].

Tabela 1 – Vrzeli in neenakomeren prenos v zakonodajni okvir (neizčrpen seznam)

Področje	Primeri
Enotni digitalni trg	o Sedanja direktiva o prodaji potrošniškega blaga ne zajema kibernetske varnosti. S predlaganima direktivama o digitalnih vsebinah[47] in spletni prodaji[48] naj bi se ta vrzel odpravila. o Obstajajo omejeni in različni pravni okviri za dolžnosti skrbnega ravnanja v državah članicah EU, kar povzroča pravno negotovost in težave pri uveljavljanju pravnih sredstev[49]. o Politike o razkrivanju ranljivosti programske opreme se v državah članicah razvijajo različno hitro, na ravni EU pa ni splošnega pravnega okvira, ki bi omogočal usklajen pristop[50].
Krepitev varnosti omrežij in informacijskih sistemov	o Države članice lahko vključijo sektorje, ki niso vključeni v direktivo o varnosti omrežij in informacij[51]. Nastanitvena industrija, ki ni vključena, je lahko povezana z drugimi vrstami kriminalitete, vključno s trgovino z ljudmi in drogami ter nezakonitim priseljevanjem[52].
Boj proti kibernetskemu kriminalu	o Številne države članice v svoji zakonodaji niso opredelile elektronskih dokazov[53] (glej tudi odstavek ***22***). o Sedanji okvirni sklep o goljufijah pri negotovinskih plačilih ne vključuje izrecno nefizičnih plačilnih instrumentov, kot so virtualne valute, elektronski denar in mobilni denar, poleg tega pa ne zajema lažnega predstavljanja, skimminga ter posedovanja in posredovanja informacij o plačnikih[54]. o Direktiva o napadih na informacijske sisteme ne obravnava neposredno nezakonitega pridobivanja podatkov od znotraj (npr. kibernetskega vohunjenja), kar ustvarja izzive za organe kazenskega pregona[55]. o Po razsodbi Sodišča Evropske unije o hrambi podatkov[56] so razlike v uporabi pravnega okvira med državami članicami ovirale kazenski pregon, kar bi lahko privedlo do izgube sledi za preiskavo in oviranja uspešnega pregona spletnih kriminalnih dejavnosti[57].

Vir: Evropsko računsko sodišče

35 Uporaba nekaterih vidikov zakonodaje je še vedno prostovoljna tako za nacionalne organe kot tudi zasebne gospodarske subjekte. V okviru skupine za sodelovanje je npr. ocenjevanje nacionalnih strategij za varnost omrežij in informacijskih sistemov ter uspešnosti skupin za odzivanje na incidente na področju računalniške varnosti prostovoljno. Poleg tega bo v skladu s shemo certificiranja, predlagano v uredbi o kibernetski varnosti, certificiranje izdelkov in storitev IKT prostovoljno.

36 V EU je kibernetska varnost v pristojnosti držav članic. Kljub temu ima EU pomembno vlogo pri ustvarjanju pogojev za izboljšanje zmogljivosti držav članic in za njihovo sodelovanje in doseganje zaupanja. Kljub velikim razlikam v zmogljivosti in angažiranosti med državami članicami[58] bo zagotavljanje občutljivih informacij (v zvezi z nacionalno varnostjo) ostalo prostovoljno.

37 Nedosleden prenos prava EU v nacionalne zakonodaje držav članic lahko privede do pravnih in operativnih neskladnosti ter prepreči doseganje polnega potenciala zakonodaje. Na primer, države članice različno razumejo, kako je treba izvajati nadzor nad izvozom blaga z dvojno rabo[59], zaradi česar nekatera podjetja s sedežem v EU morda izvažajo tehnologije in storitve, ki jih je mogoče uporabiti za kibernetski nadzor in kršenje človekovih pravic s cenzuro ali prestrezanjem. Evropski parlament je v zvezi s tem izrazil zaskrbljenost[60].

38 Poleg tega je zaradi varstva zasebnosti in svobode izražanja potreben prilagojen zakonodajni odziv za dosego potrebnega ravnovesja med varovanjem temeljnih vrednot in doseganjem varnostnih zahtev EU. Na primer, kako zagotoviti šifriranje od konca do konca, hkrati pa poiskati najboljši način za podpiranje kazenskega pregona? Ali, kako doseči cilje splošne uredbe o varstvu podatkov in hkrati razumeti njen vpliv na javno dostopne podatke o prijaviteljih domenskih imen in imetnikih blokov naslovov IP? In kako lahko to negativno vpliva na preiskave organov kazenskega pregona[61]?

39 Samo zakonodaja ne zagotavlja odpornosti. Cilj direktive o varnosti omrežij in informacij je sicer doseganje visoke ravni varnosti v vsej EU, vendar je izrecno osredotočena na doseganje minimalne, ne maksimalne harmonizacije[62]. Z razvojem kibernetskega prostora se bodo še naprej pojavljale nove vrzeli.

Točke za razmislek – okvir politike

- Kateri so ključni ukrepi, potrebni za spodbuditev preusmeritve oblikovalcev politik in zakonodajalcev v močnejšo kulturo smotrnosti na področju kibernetske varnosti, vključno z opredelitvijo splošne odpornosti?
- Kako bi lahko raziskave več prispevale k ustvarjanju potrebnih statističnih in drugih podatkov, ki bi omogočili smiselno oceno?
- Kako bi lahko prilagodili zakonodajne procese EU, da bi bili bolj fleksibilni in da bi bolj upoštevali hitrost razvoja tehnologije in groženj?
- Kako bi lahko prakso razvoja metrike (kazalnikov in ciljnih vrednosti) v političnem ciklu EU prilagodili, okrepili in ponovili na celotnem področju kibernetske varnosti?
- Kaj se lahko nacionalni revizijski uradi naučijo eden od drugega v zvezi s pristopi k revidiranju politik in ukrepov na področju kibernetske varnosti?
- Katere nedoslednosti pri prenosu pravnega okvira EU v nacionalne zakonodaje in njegovem izvajanju ovirajo uspešnejši odziv na vrzeli v kibernetski varnosti in kibernetsko kriminaliteto ter kako bi lahko države članice in institucije EU to najbolje obravnavale?
- Kako učinkovit je nadzor EU nad izvozom kibernetskega blaga in storitev pri preprečevanju kršenja človekovih pravic zunaj EU?

Financiranje in poraba

40 EU želi postati najvarnejše spletno okolje na svetu. Za dosego tega cilja so potrebna velika prizadevanja vseh deležnikov, pa tudi dobra in dobro upravljana finančna podlaga.

Izziv 3: uskladitev ravni naložb s cilji

Povečanje naložb

41 Skupna svetovna poraba za kibernetsko varnost kot odstotek BDP je ocenjena na približno 0,1 %. V Združenih državah Amerike[63] je odstotek višji, in sicer približno 0,35 % (vključno z zasebnim sektorjem). Poraba zvezne vlade ZDA v odstotkih BDP znaša približno 0,1 % ali približno 21 milijard USD, predvidenih v proračunu za leto 2019[64].

42 Poraba v EU je bila v primerjavi z ZDA nizka, razdrobljena in nepodprta z usklajenimi vladnimi programi. Podatke o zneskih je težko pridobiti, vendar javna poraba EU za kibernetsko varnost po ocenah znaša med eno in dvema milijardama EUR na leto[65]. Poraba nekaterih držav članic v odstotkih BDP znaša le desetino porabe ZDA ali celo še manj[66]. EU in njene države članice morajo vedeti, koliko vlagajo skupaj, da lahko ugotovijo, katere vrzeli je treba zapolniti.

43 Težko je oblikovati celovit pregled, ker zaradi medsektorske narave kibernetske varnosti in zato, ker pogosto ni mogoče ločiti porabe za kibernetsko varnost od splošne porabe za IT, ni jasnih podatkov[67]. Z anketo, ki jo je opravilo Sodišče, se je potrdilo, da je težko pridobiti zanesljive statistične podatke o porabi tako v javnem kot tudi v zasebnem sektorju. Tri četrtine nacionalnih revizijskih uradov so poročale, da nimajo centraliziranega pregleda nad vladno porabo za kibernetsko varnost, poleg tega pa nobena država članica ni uvedla obveznosti javnih subjektov, da v svojih finančnih načrtih ločeno poročajo o odhodkih za kibernetsko varnost.

44 Povečanje javnih in zasebnih naložb v evropska podjetja za kibernetsko varnost je poseben izziv. Javni kapital je pogosto na voljo za začetne faze, manj pa za rast in širitev[68]. Obstaja mnogo pobud EU za financiranje, vendar se te predvsem zaradi upravnih ovir ne izkoriščajo[69]. Na splošno podjetja za kibernetsko varnost v EU delujejo manj uspešno kot taka podjetja v drugih državah: v EU je takih podjetij manj, poleg tega pa je povprečen znesek sredstev, ki ga pridobijo, bistveno nižji[70]. Zato je

zagotavljanje uspešne ciljne usmerjenosti in financiranja zagonskih podjetij bistveno za doseganje ciljev digitalne politike EU.

Povečanje učinka

45 Zapolnitev vrzeli v naložbah za kibernetsko varnost mora imeti koristne izide. Na primer, kljub temu, da je sektor za raziskave in inovacije v EU močen, rezultati niso dovolj patentirani, ne tržijo se dovolj ali niso dovolj okrepljeni, da bi lahko pomagali krepiti odpornost, konkurenčnost in digitalno avtonomnost[71]. To velja zlasti v primerjavi z globalnimi tekmeci EU. To, da je ustrezno izkoriščenih rezultatov malo, je posledica različnih dejavnikov[72], vključno s:

- tem, da ni skladne nadnacionalne strategije za okrepitev pristopa, da bi ustrezal širšim digitalnim potrebam EU za konkurenčnost in večjo avtonomijo,
- dolžino ciklusa vrednostne verige, kar pomeni, da orodja hitro zastarijo,
- slabo trajnostnostjo, saj se projekti običajno zaključijo z razpustitvijo projektne ekipe in prenehanjem podpore, vključno s posodobitvami in nameščanjem popravkov.

46 Komisija želi s predlogom za ustanovitev mreže strokovnih centrov za kibernetsko varnost in raziskovalnega strokovnega centra odpraviti razdrobljenost raziskav na področju kibernetske varnosti ter spodbuditi ustrezne naložbe[73]. Skupaj je po vsej EU približno 665 strokovnih centrov.

Izziv 4: jasen pregled nad porabo iz proračuna EU

47 Centraliziran pregled nad porabo je pomemben za transparentnost in boljše usklajevanje. Brez njega oblikovalci politik težko ugotovijo, kako se poraba usklajuje s potrebami za doseganje prednostnih ciljev.

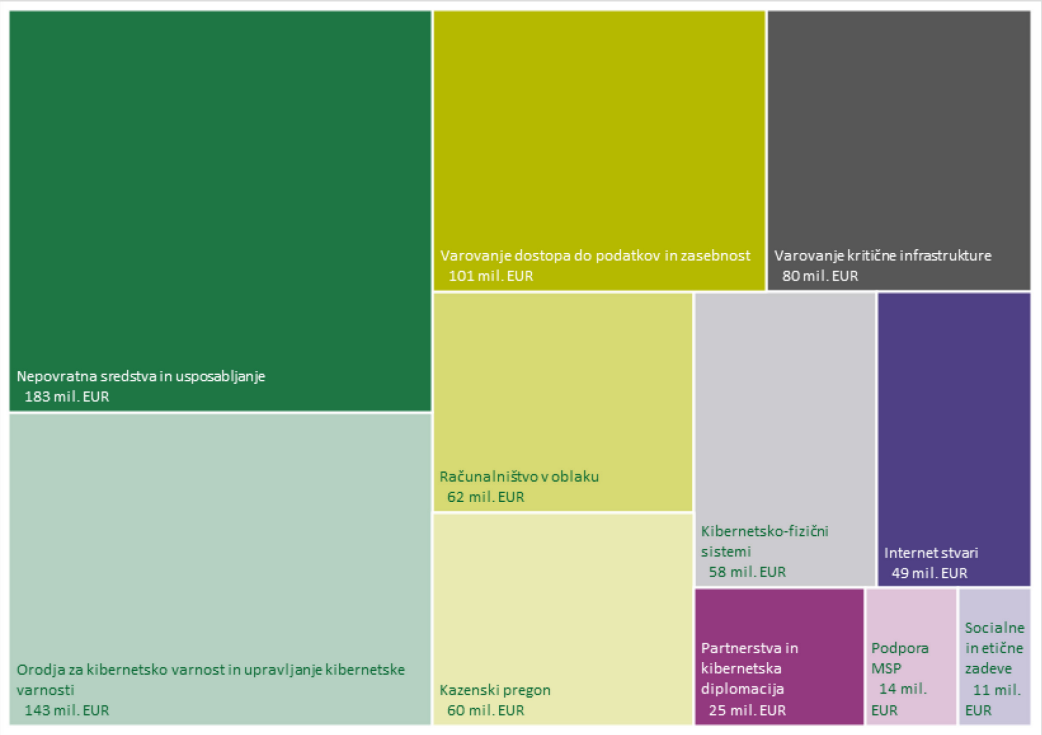
48 Za financiranje strategije za kibernetsko varnost ni namenskega proračuna. Na ravni EU se poraba za kibernetsko varnost financira iz splošnega proračuna EU, države članice pa jo sofinancirajo. Analiza Sodišča je pokazala, da obstaja kompleksna struktura z vsaj desetimi različnimi instrumenti v okviru splošnega proračuna EU, ni pa jasno, koliko denarja se porabi za kaj (glej ***Prilogo II***).

49 Pridobitev jasnega pregleda nad porabo za temo, ki zadeva več področij, je zato velik izziv. Programe porabe upravljajo različne službe Komisije, od katerih ima vsaka svoje cilje, pravila in urnike. Položaj je še bolj zapleten, če se upošteva sofinanciranje držav članic, na primer v okviru Sklada za notranjo varnost (Policija)[74].

Ugotovljiva poraba za kibernetsko varnost

50 V obdobju 2014–2018 je Komisija porabila vsaj 1,4 milijarde EUR za izvajanje strategije[75], največji delež pa je dodelila programu Obzorje 2020[76] (v nadaljnjem besedilu: Obzorje 2020). Financiranje Obzorja 2020 poteka predvsem preko programa izziva varnih družb ter projektov vodilnega položaja na področju omogočitvenih in industrijskih tehnologij[77]. Sodišče je naštelo 279 projektov, povezanih s kibernetsko varnostjo, za katere so bile sklenjene pogodbe do septembra 2018, s skupnim financiranjem EU v višini 786 milijonov EUR[78]. Na ***sliki 5*** je prikazana tipologija teh projektov, ki temelji na tej analizi.

Slika 5 – Raziskovalni projekti na področju kibernetske varnosti, za katere so bile v okviru Obzorja 2020 sklenjene pogodbe (v milijonih EUR)



Vir: Evropsko računsko sodišče

51 Pogodbeno javno-zasebno partnerstvo je bilo vzpostavljeno leta 2016 za spodbujanje evropske industrije kibernetske varnosti. Cilj je bil usmeriti 450 milijonov EUR iz programa Obzorje 2020 v pogodbeno javno-zasebno partnerstvo in do leta 2020

privabiti dodatnih 1,8 milijarde EUR iz zasebnega sektorja. V 18-mesečnem obdobju do 31. decembra 2017 je bilo iz Obzorja 2020 v pogodbeno javno-zasebno partnerstvo usmerjenih 67,5 milijona EUR, zasebni sektor pa je vložil 1 milijardo EUR[79].

52 Boj proti kibernetski kriminaliteti podpira tudi Sklad za notranjo varnost – Policija. Sklad za notranjo varnost – Policija podpira študije, strokovne sestanke in komunikacijske dejavnosti, katerih stroški so med letoma 2014 in 2017 znašali skoraj 62 milijonov EUR. Poleg tega lahko države članice prejmejo nepovratna sredstva za opremo, usposabljanje, raziskave in zbiranje podatkov v okviru deljenega upravljanja. Devetnajst držav članic je prejelo ta nepovratna sredstva v višini 42 milijonov EUR.

53 Sredstva za podporo pravosodnega sodelovanja in delovanja pogodb o medsebojni pravni pomoči s posebnim poudarkom na izmenjavi elektronskih podatkov in finančnih informacij so znašala 9 milijonov EUR v okviru programa Pravosodje, ki ga upravlja GD JUST.

54 V direktivi o varnosti omrežij in informacij je izrecno navedeno, da morajo imeti skupine za odzivanje na incidente na področju računalniške varnosti ustrezne vire, da lahko uspešno opravljajo svoje naloge[80]. Med letoma 2016 in 2018 je bilo vsako leto na voljo 13 milijonov EUR iz instrumenta za povezovanje Evrope, ki so jih države članice lahko uporabile za pomoč pri izvajanju zahtev direktive. Za določitev dejanskih finančnih potreb za doseganje učinka mreže skupin za odzivanje na incidente na področju računalniške varnosti in skupine za sodelovanje ni bila opravljena nobena študija.

55 Operativni stroški več agencij so bili specifično usmerjeni v dejavnosti na področju kibernetske varnosti ali kibernetske kriminalitete. Iz javno dostopnih informacij pa je težko pridobiti natančne podatke o zneskih.

56 Budimpeška konvencija (glej odstavek ***11***) je bistvena za zunanjo porabo EU na področju kibernetske varnosti. EU je za krepitev kibernetske varnosti izven svojih meja v obdobju 2014–2018 porabila približno 50 milijonov EUR. Skoraj polovica tega zneska je bila porabljena preko instrumenta za prispevanje k stabilnosti in miru, glavni projekt pa je bil 13,5 milijona EUR vreden projekt GLACY+, katerega namen je krepitev zmogljivosti za razvoj in izvajanje zakonodaje na področju kibernetske kriminalitete po celem svetu in izboljšanje mednarodnega sodelovanja[81]. Sicer je bila poraba drugih finančnih instrumentov EU osredotočena predvsem na Zahodni Balkan[82] in evropsko sosedstvo, npr. projekt Cybercrime@EaP z državami vzhodnega partnerstva je bil

namenjen izboljšanju mednarodnega sodelovanja na področju kibernetske kriminalitete in elektronskih dokazov.

Druga poraba za kibernetsko varnost

57 V okviru programov EU ni vedno mogoče opredeliti specifične porabe za kibernetsko varnost:

- sredstva Obzorja 2020 so se izvrševala tudi preko Skupnega podjetja Elektronske komponente in sistemi za evropski vodilni položaj (ECSEL) za kibernetsko-fizične sisteme. Vendar Sodišče ni moglo določiti, kateri deli 27 projektov v skupni vrednosti 437 milijonov EUR, izvedeni v letih 2015 in 2016, so bili posebej povezani s kibernetsko varnostjo.

- Do 400 milijonov EUR je na voljo za porabo na področju kibernetske varnosti in storitev zaupanja v okviru evropskih strukturnih in investicijskih skladov. To vključuje naložbe na področju varnosti in varstva podatkov, da se okrepijo interoperabilnost in medsebojna povezanost digitalne infrastrukture, elektronska identifikacija ter storitve zasebnosti in zaupanja.

58 Evropska investicijska banka je v svojem operativnem načrtu za leto 2018 napovedala, da namerava povečati financiranje tehnologij z dvojno rabo ter kibernetske in civilne varnosti na do 6 milijard EUR v triletnem obdobju[83].

Obeti za prihodnost

59 Predlagani novi program za digitalno Evropo[84] ima 2 milijardi EUR vredno komponento za kibernetsko varnost za obdobje 2021–2027, ki je zasnovana za okrepitev industrije kibernetske varnosti v EU in splošno varstvo družbe, vključno s pomočjo za izvajanje direktive o varnosti omrežij in informacij. Predlagana mreža strokovnih centrov za kibernetsko varnost in raziskovalni strokovni center, katerih cilj je uvedba bolj racionaliziranega pristopa, naj bi bila glavni mehanizem za izvajanje porabe EU v okviru programa za digitalno Evropo.

60 Poraba za obrambo iz proračuna EU se je nedavno povečala zaradi evropskega programa za razvoj obrambne industrije, ki mu bo v letih 2019 in 2020 dodeljenih 500 milijonov EUR[85]. Program bo osredotočen na izboljševanje koordinacije in učinkovitosti porabe za obrambo držav članic s spodbudami za skupni razvoj. Njegov cilj je z Evropskim obrambnim skladom ustvariti za skupaj 13 milijard EUR naložb v

obrambne zmogljivosti po letu 2020, od katerih naj bi nekatere zajemale kibernetsko obrambo[86].

Izziv 5: zagotavljanje ustreznih virov za agencije EU

61 Osrednji trije organi, odgovorni za politiko EU za kibernetsko varnost – ENISA, Europolov Evropski center za boj proti kibernetski kriminaliteti in skupina za odzivanje na računalniške grožnje (glej ***okvir 2***) –, se srečujejo z izzivi v zvezi z zagotavljanjem virov v času, ko so politične prioritete vse bolj vezane na zagotavljanje varnosti. Agencije EU zaradi sedanje dodelitve kadrovskih in finančnih virov še vedno težko izpolnjujejo pričakovanja[87].

62 Prošnjam agencij za dodatne vire za izpolnjevanje vse večjih zahtev ni bilo v celoti ugodeno, zaradi česar je morda ogroženo (pravočasno) doseganje ciljev politike. Na primer:

- Omejenost virov je bila eden od dejavnikov, ki je ENISI preprečevala, da bi leta 2017 svoje cilje dosegla v celoti[88]. V svežnju za leto 2017 so bili predlagani dodatni viri, ki ustrezajo novim pooblastilom ENISE.

- Zaposlovanje analitikov in zagotavljanje naložb v zmogljivosti IKT na Europolovem Evropskem centru za boj proti kibernetski kriminaliteti nista dohajala potreb[89]. Poleg tega strokovnjake za projektno skupino za skupno ukrepanje na področju kibernetske kriminalitete v okviru Europolovega Evropskega centra za boj proti kibernetski kriminaliteti, ki podpirajo preiskave na podlagi obveščevalnih podatkov, zagotavljajo države članice in tretje države. Toda večino stroškov zanje krijejo države, ki jih napotijo, zaradi česar ni spodbude za napotitev večjega števila strokovnjakov. S sredstvi Europola ali političnega cikla EU je bila omogočena začasna napotitev za posamezne primere, zaradi česar je lahko sodelovalo več držav.

63 Nekatere omejitve si organi določijo sami. Skupina za odzivanje na računalniške grožnje in ENISA imata mnogo pogodbenih uslužbencev, za katere so postopki zaposlovanja običajno počasni. Druge, kot je privabljanje in ohranjanje talentov, pa izhajajo iz tega, da agencije ne morejo konkurirati plačam v zasebnem sektorju ali da ne ponujajo dobrih možnosti za poklicno napredovanje. ENISA je zato med letoma 2014 in 2016 veliko svojega dela dala v zunanje izvajanje[90].

64 Pomanjkanje uslužbencev in potrebnih orodij lahko pomeni velika tveganja, zlasti v zvezi z zbiranjem obveščevalnih podatkov o grožnjah. Količina podatkov iz odprtih in zaprtih virov še vedno raste, zato obstaja tveganje, da analitiki ne bodo mogli izvajati ustrezne analize groženj. Brez ustreznih zmogljivosti in orodij za uspešno vključevanje in medsebojno povezovanje teh podatkov jih ne bo mogoče uspešno pretvoriti v uporabne obveščevalne podatke o grožnjah, ki bi jih bilo mogoče izmenjevati in analizirati po vsej EU[91].

Točke za razmislek – Financiranje in poraba

- Kako bi lahko Komisija in zakonodajalci racionalizirali porabo EU za kibernetsko varnost in jo izrecneje uskladili z jasno opredeljenimi cilji?
- Kako bi bilo mogoče obravnavati primanjkljaj v virih agencij EU na splošno ob upoštevanju potreb in ciljev Unije?
- Kateri ukrepi se opredeljujejo na ravni EU in držav članic za zmanjšanje ovir za MSP pri črpanju naložbenega kapitala za okrepitev njihovih dejavnosti?
- Katere konkretne in trajnostne rezultate dosegajo sredstva Obzorja 2020 v zvezi z rešitvami za kibernetsko varnost?
- Kako so dejavnosti EU za krepitev zmogljivosti izven njenih meja usklajene z vrednotami EU?

Vzpostavitev kibernetsko odporne družbe

65 Upravljanje kibernetske varnosti zajema upravljanje groženj in tveganj, krepitev zmogljivosti in ozaveščenosti ter usklajevanje in izmenjavo informacij, ki temeljita na zaupanju.

Izziv 6: krepitev upravljanja in standardov

Upravljanje varnosti informacij

66 Upravljanje varnosti informacij pomeni vzpostavljanje struktur in politik za zagotavljanje zaupnosti, celovitosti in razpoložljivosti podatkov. Je več kot le tehnično vprašanje, saj zahteva uspešno vodstvo, zanesljive procese in strategije, usklajene z organizacijskimi cilji[92]. Del tega je upravljanje kibernetske varnosti, ki se ukvarja z vsemi vrstami kibernetskih groženj, vključno s ciljno usmerjenimi in kompleksnimi napadi, kršitvami ali incidenti, ki jih je težko odkriti ali upravljati.

67 Modeli upravljanja kibernetske varnosti se med državami članicami razlikujejo, odgovornost za kibernetsko varnost pa je v državah članicah pogosto razdeljena med več subjektov. Te razlike bi lahko ovirale sodelovanje, ki je potrebno za odziv na obsežne čezmejne incidente in izmenjavo obveščevalnih podatkov o grožnjah na nacionalni ravni, še posebej pa na ravni EU. Anketa, ki jo je Sodišče izvedlo med nacionalnimi revizijskimi uradi, je pokazala, da so slabosti v ureditvah javnih organov za upravljanje in obvladovanje tveganj videne kot največje tveganje.

68 Čeprav so lahko posledice za organizacije zasebnega sektorja resne, je slabosti v upravljanju kibernetske varnosti veliko. Skoraj devet od desetih organizacij navaja, da njihove funkcije za kibernetsko varnost ne izpolnjujejo v celoti njihovih potreb[93], uradniki za kibernetsko varnost pa so hierarhično pogosto vsaj dve stopnji pod vodstvom[94].

69 V direktivah EU na področju prava družb niso določene nobene posebne zahteve glede razkrivanja kibernetskih tveganj. V Združenih državah Amerike je komisija Securities and Exchange Commission nedavno izdala nezavezujoče smernice za pomoč javnim družbam pri pripravi razkritij o kibernetskih tveganjih in incidentih[95]. Skupni

odbor evropskih nadzornih organov[96] (ESA) je opozoril na povečanje kibernetskega tveganja in finančne institucije pozval, naj izboljšajo ranljive sisteme IT in preučijo inherentna tveganja za varnost informacij, povezljivost in oddajanje del zunanjim izvajalcem[97].

70 Krepitev upravljanja varnosti informacij v MSP je še posebej zahtevna, saj ta večinoma ne morejo izvajati ustreznih sistemov. MSP nimajo ustreznih smernic o izvajanju zahtev v zvezi z varnostjo in zasebnostjo informacij ter o zmanjševanju tehnoloških tveganj[98]. Ključni izzivi so tako boljše razumevanje njihovih potreb in zagotavljanje potrebnih spodbud in podpore.

71 Ker ni koherentnega mednarodnega okvira za upravljanje kibernetske varnosti, je zmožnost mednarodne skupnosti za odziv na kibernetske napade in njihovo omejevanje okrnjena. Zato je pomembno, da se doseže soglasje o takem okviru upravljanja, ki bo najbolje odražal interese in vrednote EU[99]. Poskusi za določitev zavezujočih mednarodnih norm za kibernetski prostor so čedalje bolj napeti, kot je razvidno iz tega, da leta 2017 ni bilo mogoče doseči soglasja v okviru skupine vladnih strokovnjakov ZN o tem, kako naj se mednarodno pravo uporablja za nacionalne odzive na incidente.

72 EU je za okrepitev svoje agende o upravljanju kibernetskega prostora formalizirala tudi šest kibernetskih partnerstev za vzpostavitev rednega dialoga o politikah za vzpostavitev zaupanja in skupnih področij za sodelovanje[100]. Izidi so različni, vendar na splošno EU na mednarodni ravni še ne more šteti za velikega akterja na področju kibernetske varnosti, čeprav se je njena pomembnost povečala[101].

Varnost informacij v institucijah EU

73 Vsaka institucija EU ima svoja pravila za upravljanje varnosti informacij. Z medinstitucionalnim sporazumom je določeno, da Komisija drugim institucijam in organom zagotavlja pomoč v zvezi z varnostjo informacij. Institucije in organi EU so prepoznali potrebo po koherentnem razvoju lastnih kibernetskih zmogljivosti in pristopov za obvladovanje tveganja. Komisija, Svet in ESZD naj bi Horizontalni delovni skupini za kibernetska vprašanja leta 2020 predstavili poročilo o upravljanju in doseženem napredku pri razjasnjevanju in harmonizaciji upravljanja kibernetske varnosti v institucijah in agencijah EU[102].

74 Znotraj Komisije je za varnost infrastrukture in storitev IT odgovoren Generalni direktorat za informatiko (DIGIT) (glej ***okvir 3***). Glavni cilji varnosti IT iz digitalne strategije Komisije so vključitev varnosti IT v upravljavske procese, zagotovitev

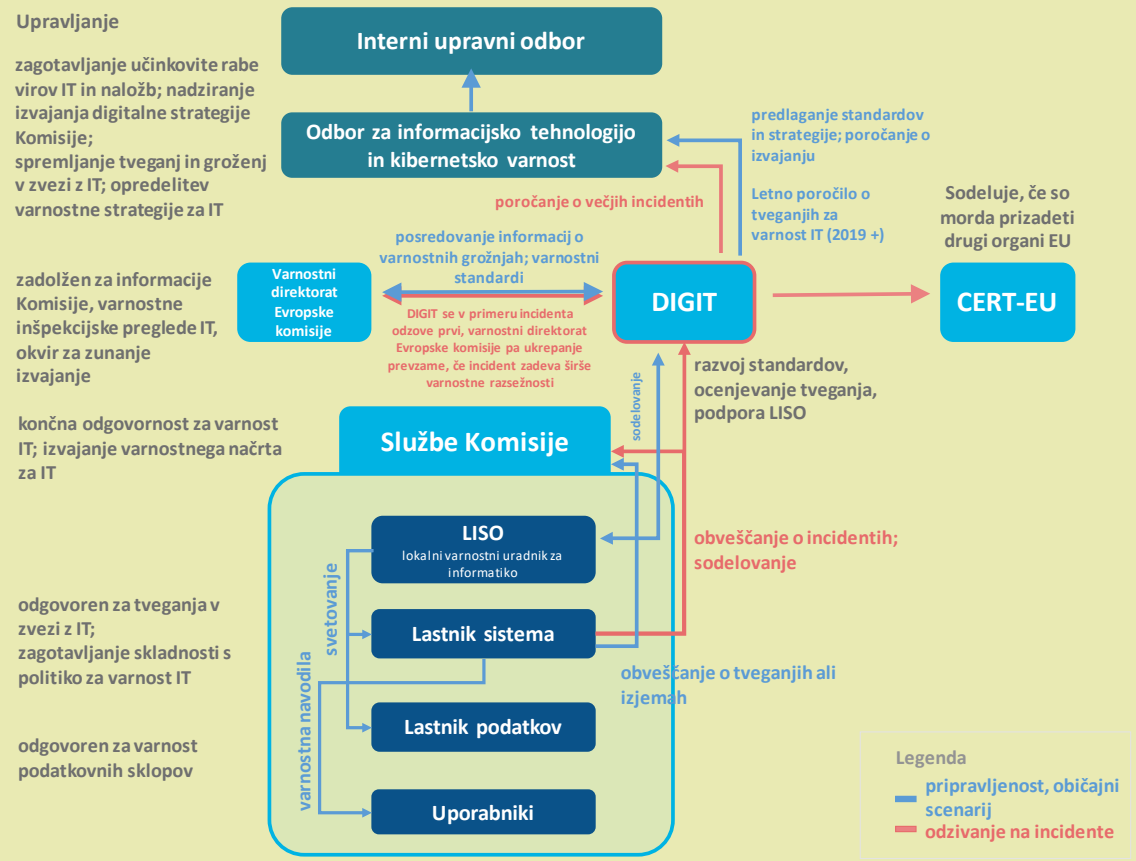
(stroškovno) učinkovite infrastrukture in odpornosti, razširitev obsega zaznavanja incidentov in odzivanja nanje ter povezovanje upravljanja IT in varnosti[103]. Komisija v skladu s svojo pogodbo s ponudnikom zagotavlja, da se skoraj vsa programska oprema dejavno vzdržuje in da se uporablja samo programska oprema s podporo prodajalca[104].

75 Pomembnost zaščite institucij Unije velja tudi za misije in strukture EU SVOP po vsem svetu. Ena od prioritet okvira EU za politiko kibernetske obrambe (posodobitev leta 2018) je okrepitev varstva komunikacijskih in informacijskih sistemov SVOP, ki jih uporabljajo subjekti EU. Zdaj je ustanovljen notranji odbor ESZD za upravljanje kibernetske varnosti, ki se je prvič sestal junija 2017[105].

Okvir 3

Zaščita informacijskih sistemov Komisije

Približno 1 300 sistemov in 50 000 naprav Komisije je nenehno tarča kibernetskih napadov. Odgovornost za IT je decentralizirana, kot je prikazano na sliki spodaj. Varnost informacij in IT temelji na skupnem varnostnem načrtu za IT Generalnega direktorata za informatiko. Odbor za informacijsko tehnologijo in kibernetsko varnost deluje kot dejanski pooblaščenec Komisije za varnost informacij in povezuje operativno stran varnosti IT z višjim vodstvom Komisije, ki ga predstavlja interni upravni odbor.



Vir: Evropsko računsko sodišče na podlagi sklepov Komisije[106]

Glavna naloga Generalnega direktorata za človeške vire in varnost (GD HR DS) je varovanje uslužbencev, informacij in sredstev Komisije. Izvaja tudi varnostne preiskave incidentov, ki presegajo zgolj IT, ter tako prispeva k svojim protiobveščevalnim in protiterorističnim dejavnostim.

Generalni direktorat za informatiko je odgovoren za varnost IT in gosti skupino za odzivanje na računalniške grožnje, ki je bila ustanovljena leta 2011 in ima letni proračun v višini približno 2,5 milijona EUR ter približno 30 uslužbencev. Prva se odzove na vsakršen incident v zvezi z varnostjo informacij, ki zadeva več institucij, vendar ne deluje neprekinjeno. Gosti platformo za izmenjavo informacij. Leta 2018 je podpisala nezavezujoč memorandum o soglasju z ENISO, Evropskim centrom za boj proti kibernetski kriminaliteti in Evropsko obrambno agencijo za okrepitev sodelovanja in usklajevanja. Poleg tega ima tehnični sporazum s službo zveze NATO za odzivanje na incidente na področju računalniške varnosti.

Ocene ogroženosti in tveganja

76 Dobro utemeljene in redne ocene ogroženosti in tveganja so pomembno orodje za javne in zasebne organizacije. Vendar ni standardnega pristopa za klasificiranje in kartiranje kibernetskih groženj ali za ocene tveganja, zato je vsebina ocen zelo različna, kar pomeni izziv za doseganje koherentnega pristopa h kibernetski varnosti v celotni

EU[107]. Poleg tega se pogosto zanašajo na iste vire ali celo na druge ocene ogroženosti, zaradi česar se ugotovitve ponavljajo[108], drugim grožnjam pa morda ni namenjene dovolj pozornosti. Ta položaj poslabšuje tudi to, da organizacije še vedno nerade izmenjavajo informacije in o incidentih ne poročajo dovolj.

77 Hibridna fuzijska celica[109], ki je del ESZD, je bila ustanovljena za izboljšanje situacijskega zavedanja in podporo odločanju z izmenjavo analiz, vendar mora razširiti svoje strokovno znanje, vključno s kibernetsko varnostjo. Skupina za odzivanje na računalniške grožnje institucijam, organom in agencijam EU vzporedno zagotavlja poročila in informacije o kibernetskih grožnjah, ki so usmerjene vanje.

78 ENISA je v preteklosti ugotovila, da mnoge države članice grožnje razumejo kvalitativno in da obstaja potreba po okrepitvi modeliranja kibernetskih groženj[110]. Spremljanje zmogljivosti za strateške analize bo okrepilo splošno razumevanje. Toda ocene ogroženosti bi lahko poleg tehnoloških groženj vključevale tudi socialno-politične in gospodarske grožnje, da bi se zagotovil celovitejši pregled, pa tudi informacije o gibalu groženj in motivih akterjev.

Spodbude

79 Še vedno je premalo pravnih in ekonomskih spodbud, da bi organizacije sporočale in izmenjevale informacije o incidentih. Mnoge organizacije zaradi škode za ugled kibernetske napade še vedno raje obravnavajo diskretno ali pa storilcem plačajo odkupnino. Ni še jasno, kako uspešna bo direktiva o varnosti omrežij in informacij pri izboljšanju priglasitev incidentov. Komisija pričakuje, da bo do izboljšav prišlo predvsem na nacionalni ravni, uredba o kibernetski varnosti pa naj bi dodala razsežnost EU[111].

80 Javni organi lahko z vključitvijo nekaterih standardov v svoja javna naročila kot kupci digitalnih izdelkov in storitev dosežejo pomemben učinek vzvoda pri dobaviteljih z javnim naročanjem ter sredstvi za raziskave in programe (npr. tako, da zahtevajo sprejetje nekaterih tehničnih standardov, kot je internetni protokol IPv6, za lažji boj proti kibernetski kriminaliteti). Toda zdaj ni skupnega okvira za javna naročila na področju infrastrukture za kibernetsko varnost[112]. Komisija v zvezi s tem lahko veliko stori. Cilj predlaganega programa za digitalno Evropo za naslednji večletni finančni okvir je obravnava doslej omejenih naložb javnega sektorja v nakup najnovejše tehnologije za kibernetsko varnost.

81 Komisija lahko s svojo regulativno vlogo zagotovi, da se razvijejo ustrezni standardi za široko uporabo, s čimer bi se okrepila varnost. Komisija in Europol sodelujeta z organi za upravljanje interneta, kot sta ICANN (glej odstavek ***38***) in RIPE-NCC[113], kar je bistveno za vzpostavitev ustrezne strukture za boj proti kibernetski kriminaliteti v podporo organom kazenskega pregona in sodnim organom.

Izziv 7: pridobivanje znanja in ozaveščanje

82 ENISA je opozorila na to, da imajo uporabniki kritično vlogo v boju proti kibernetskim napadom in da so pridobivanje znanja, izobraževanje in ozaveščanje ključni za vzpostavitev kibernetsko odporne družbe[114]. Posamezniki na delovnem mestu ali doma, ki dobro prepoznavajo opozorilne znake in imajo ustrezne tehnike, lahko upočasnijo ali preprečijo napade.

83 Zlasti je zaskrbljujoča vse večja nesorazmernost med znanjem, potrebnim za izvajanje kibernetske kriminalitete in kibernetskih napadov, ter znanjem, potrebnim za obrambo pred njimi. Model kriminala kot storitve je olajšal vstop na trg kibernetske kriminalitete: posamezniki brez tehničnega znanja za programiranje botnetov, orodij za izkoriščanje ranljivosti ali paketov izsiljevalskega programja jih zdaj lahko najamejo.

Usposabljanje, znanje in razvoj zmogljivosti

84 Cel svet se srečuje z vedno večjim primanjkljajem znanj na področju kibernetske varnosti, vrzel v delovni sili pa se je od leta 2015 povečala za 20 %[115]. Tradicionalni načini zaposlovanja ne dohajajo povpraševanja, vključno z vodstvenimi in interdisciplinarnimi položaji[116]. Skoraj 90 % globalne delovne sile na področju kibernetske varnosti predstavljajo moški, stalna neuravnotežena zastopanost spolov pa še dodatno omejuje potencial talentov[117]. Poleg tega je na univerzah na netehničnih programih premalo predmetov, povezanih s kibernetsko varnostjo.

85 Usposabljanje in izobraževanje sta potrebna na vseh ravneh: med javnimi uslužbenci, uradniki organov kazenskega pregona in pravosodnih organov, uslužbenci oboroženih sil in pedagogi. Sodišča morajo biti sposobna obravnavati hitro spreminjajoče se tehnične posebnosti kibernetske kriminalitete in njenih žrtev[118], vendar sedaj na ravni EU ni standardov za usposabljanje in certificiranje[119]. V institucijah EU je pomembno zagotavljanje ustrezne kombinacije znanj. Brez nje institucije morda ne bodo mogle ustrezno opredeliti obsega, ugotoviti, kateri so ustrezni partnerji in kakšne so varnostne potrebe, poleg tega pa ne bodo imele dovolj

zmogljivosti za upravljanje programov. To pa bi lahko ogrozilo uspešnost programov ali razvoj politik EU.

86 Države članice so odgovorne za politike na področju izobraževanja na ravni EU, številne dejavnosti usposabljanja (glej ***tabelo 2***) in vaje (glej ***okvir 4***) pa že potekajo. EU lahko pomaga vključiti standarde EU v učne programe za vsa relevantna področja[120]. Npr. na področju digitalne forenzike so skupni standardi usposabljanja potrebni za omogočanje doseganja dopustnosti dokazov v državah članicah. Zaradi čezmejnosti kibernetske kriminalitete je lahko udeleženih več jurisdikcij, zaradi česar je potrebno usposabljanje na ravni EU. Vendar je CEPOL, agencija EU za usposabljanje na področju kazenskega pregona, ugotovil, da več kot dve tretjini držav članic ne zagotavljata rednega usposabljanja na področju kibernetske varnosti za uradnike organov kazenskega pregona[121]. EU lahko tudi opredeli morebitne načine doseganja sinergij med civilnim in vojaškim izobraževanjem in usposabljanjem[122]. Poleg tega je ENISA ugotovila, da je v kritičnih sektorjih sicer veliko možnosti za usposabljanje, vendar te niso dovolj usmerjene v odpornost kritične infrastrukture[123].

Tabela 2 – Nekatere pobude EU za usposabljanje na področju kibernetske varnosti

Projekti Evropske obrambne agencije, npr. podpora zasebnega sektorja pri vajah in projekt poligonov za kibernetsko varnost.	Mreža Evropske akademije za varnost in obrambo (ki zagotavlja civilno-vojaško usposabljanje), vključno z izobraževanjem na področju kibernetske varnosti, vajami za usposabljanje in ocenjevalno platformo.	ENISA organizira programe usposabljanja za področja, na katerih jih komercialni trg ne zagotavlja.
Programi usposabljanja Europol, CEPOL in Evropske skupine za usposabljanje in izobraževanje na področju kibernetske kriminalitete[124] – vključno z modelom upravljanja usposabljanj in okvirom kompetenc za usposabljanje (vključno s certifikacijo).	(Predlagana) mreža strokovnih centrov in raziskovalni strokovni center.	Ukrepi v zvezi s šifriranjem, predlagani v 11. poročilu o napredku varnostne unije.
Sodelovanje med EU in Natom pri usposabljanju in izobraževanju na področju kibernetske obrambe.	Vojaški program Erasmus.	Evropska mreža institucij za izobraževanje v pravosodju.

Vir: Evropsko računsko sodišče

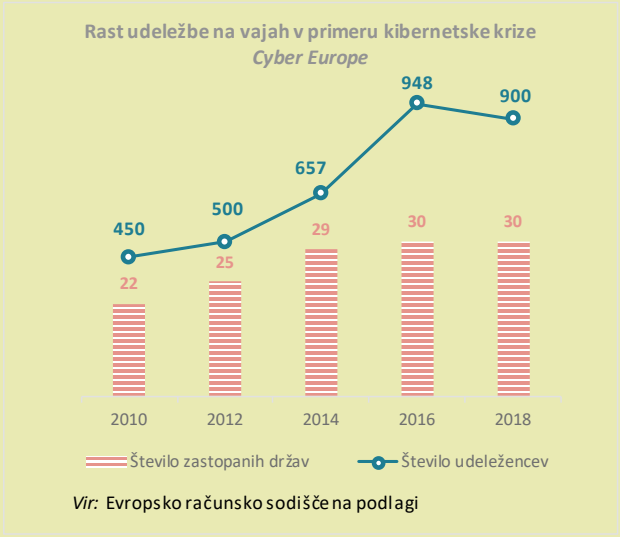
87 EU je zaposlila strokovnjake za boj proti terorizmu in varnost v 17 delegacijah, da bi okrepila povezavo med notranjo in zunanjo varnostjo EU[125]. Boljše znanje na področju kibernetske varnosti bi lahko kljub omejenosti virov pomagalo izbrati in

izvesti ustrezne projekte ter poiskati sinergije z drugimi programi ali viri financiranja[126]. Poleg tega bi lahko to povečalo pomembnost kibernetske varnosti v političnem dialogu, čeprav bi konkurirala mnogim drugim prioritetam, kot so migracije, organizirani kriminal ali bojevniki povratniki.

Okvir 4

Vaje

Vaje so pomemben element izobraževanja in usposabljanja na področju kibernetske varnosti, saj omogočajo odlične priložnosti za krepitev pripravljenosti s preizkušanjem zmogljivosti, dajejo odgovore na resnične scenarije in ustvarjajo mreže službenih stikov. Od leta 2010 jih je čedalje več.



Vir: Evropsko računsko sodišče na podlagi

Udeleženci sodelujejo na kraju samem ali na daljavo. Po vajah se izvede ocenjevanje za opredelitev novega znanja, čeprav to morda še ne združuje strateške/politične, operativne in tehnične ravni[127].

Na vodilnih vajah EU in Nata – bienalna vaja Cyber Europe (operativna) in letna vaja Locked Shields (tehnična) – sodeluje več kot 1 000 udeležencev iz približno 30 sodelujočih držav. Obe vaji sta osredotočeni na zaščito in ohranjanje kritične infrastrukture v simulacijah napada. Poglobljenost vaj se je močno povečala in zdaj obe vključujeta medije ter pravne elemente in elemente finančne politike za izboljšanje situacijskega zavedanja strokovnjakov. Z vzporednimi in usklajenimi vajami PACE (strateške) se preizkuša interakcija med EU in Natom v scenariju hibridne grožnje.

To pa niso edine mednarodne vaje. ENISA organizira letni kibernetski izziv, pri katerem ekipe tekmujejo v reševanju izzivov na področju kibernetske varnosti, npr. v zvezi s spletno in mobilno varnostjo, v reševanju kriptosestavljank, obratnem inženiringu, etiki in forenziki. Prva vaja na ministrski ravni EU CYBRID je potekala septembra 2017, osredotočena pa je bila na strateško odločanje. Leta 2018 se je v povezavi z Natom začela izvajati vaja Crossed Swords za izboljšanje ofenzivnih elementov vaje Locked Shields. Nato organizira tudi vaje Cyber Coalition.

Ključni izziv je zagotoviti dejavno sodelovanje vseh pomembnih deležnikov ter usklajenost vseh vaj, da se prepreči podvajanje in zagotovi učinkovita izmenjava pridobljenega znanja.

Ozaveščenost

88 Državljani so pogosto prenašalci napadov in dezinformacij, saj je verjetno, da so nevede izpostavljeni ranljivostim v poceni napravah in programski opremi, ki so zelo razširjene, ali pa so žrtve socialnega inženiringa. Ozaveščanje je zato bistveno za doseganje uspešne kibernetske odpornosti, vendar nikakor ni lahka naloga, saj nestrokovnjaki težko razumejo kompleksnost kibernetske varnosti in z njo povezana tveganja.

89 Primera dejavnosti ozaveščanja sta vsakoletni evropski mesec kibernetske varnosti in dan varnejšega interneta. Evropskemu mesecu kibernetske varnosti se je zdaj pridružilo sedem držav, ki niso članice EU[128]. Europolova kampanja Reci ne! je namenjena zmanjševanju tveganja, da otroci postanejo žrtve spolne prisile in izsiljevanja na spletu. Zmanjševanje tveganja je pomembno, ker sedaj le malo žrtev napadov te zločine prijavi policiji[129]. Komisija priznava, da je bila strategija za kibernetsko varnost le delno uspešna pri ozaveščanju državljanov in podjetij[130]. To je posledica obsega naloge, omejenih virov, neenakomerne angažiranosti držav članic ter tega, da ni znanstvenih dokazov o tem, kako je najbolje ozaveščati in kako meriti ozaveščenost.

90 Izziv za Komisijo in relevantne agencije je zagotoviti, da so ukrepi za ozaveščanje dobro usmerjeni in objavljeni, vključujoči in da upoštevajo vrste groženj, ter preprečevati neželene učinke, kot je prenasičenost z varnostnimi ukrepi[131], in razviti ocenjevalne metode in metriko za ocenjevanje njihove uspešnosti. To bi moralo enako veljati tudi v institucijah EU, v katerih je treba izboljšati kulturo ozaveščenosti[132].

Izziv 8: boljša izmenjava informacij in usklajevanje

91 Za zagotavljanje kibernetske varnosti je potrebno sodelovanje med javnim in zasebnim sektorjem, predvsem si morata izmenjavati informacije in najboljše prakse. Zaupanje je pri ustvarjanju ustreznega okolja za čezmejno izmenjavo občutljivih informacij bistveno na vseh ravneh. Slabo usklajevanje privede do razdrobljenosti, podvajanja prizadevanj ter razpršitve strokovnega znanja. Uspešno usklajevanje pa lahko privede do občutnih uspehov, kot je zaprtje trgovin na temnem spletu[133]. Kljub napredku, doseženemu v zadnjih letih, so ravni zaupanja še vedno nezadostne[134] na ravni EU in v nekaterih državah članicah[135].

Usklajevanje med institucijami EU in z državami članicami

92 Eden od ciljev strategije za kibernetsko varnost in struktur za sodelovanje, uvedenih z direktivo o varnosti omrežij in informacij, je okrepitev zaupanja med deležniki. V oceni strategije je navedeno, da je bil ustvarjen temelj za strateško in operativno sodelovanje na ravni EU[136]. Kljub temu je usklajevanje na splošno ocenjeno kot nezadostno[137]. Izziv je zagotoviti, da izmenjava informacij ni le smiselna, temveč da omogoča tudi popoln pregled nad celotno situacijo. V tem pogledu je doseganje skupnega razumevanja na podlagi sprejete terminologije pomemben dejavnik (glej ***okvir 5***).

93 V oceni ENISE pa je navedeno, da pristop EU h kibernetski varnosti ni dovolj usklajen, zaradi česar ni dovolj sinergij med dejavnostmi ENISE in dejavnostmi drugih deležnikov. Mehanizmi za sodelovanje so še vedno razmeroma nezreli[138], vendar naj bi se to z uredbo o kibernetski varnosti obravnavalo z okrepitvijo usklajevalne vloge ENISE. Želja po okrepitvi sodelovanja je bila razlog za memorandum o soglasju, ki so ga leta 2018 podpisali ENISA, Evropska obrambna agencija, Europolov Evropski center za boj proti kibernetski kriminaliteti in skupina za odzivanje na računalniške grožnje[139]. V prihodnjih letih bo prioriteta Komisije zagotavljanje ustrezne usklajenosti med pobudami politike, potrebami in naložbenimi programi, da bi se odpravila razdrobljenost in ustvarile sinergije[140].

94 Usklajevalne funkcije so vključene v različne institucionalne organe. Delovna skupina za varnostno unijo je bila ustanovljena, da bi prevzela osrednjo vlogo v usklajevanju različnih generalnih direktoratov Komisije za podporo agendi varnostne unije[141]. GD CNECT predseduje podskupini delovne skupine za kibernetsko varnost.

95 V Svetu kibernetsko varnost obravnava Horizontalna delovna skupina za kibernetska vprašanja, ki usklajuje strateška in horizontalna kibernetska vprašanja ter pomaga pripravljati vaje in ocenjevati njihove rezultate. Tesno sodeluje s Političnim in varnostnim odborom, ki ima osrednjo vlogo odločanja v zvezi z vsemi diplomatskimi ukrepi na področju kibernetske varnosti (glej ***okvir 6*** v naslednjem poglavju). Ker je kibernetska varnost medsektorska, usklajevanje vseh relevantnih interesov ni enostavno: v zadnjem času je kibernetska vprašanja obravnavalo kar 24 delovnih skupin in pripravljalnih organov[142].

96 Zadnja zakonodajna predloga o okrepitvi ENISE (iz leta 2017) ter o vzpostavitvi mreže strokovnih centrov za kibernetsko varnost in raziskovalnega strokovnega centra (iz leta 2018) sta zasnovana specifično za obravnavo razdrobljenosti in podvajanja prizadevanj. Spodbuda za mrežo strokovnih centrov za kibernetsko varnost in

raziskovalni strokovni center je bila potreba po zapolnitvi vrzeli, ki je strukture sodelovanja iz direktive o varnosti omrežij in informacij niso zapolnile, ker niso bile zasnovane za podporo razvoja visokotehnoloških rešitev.

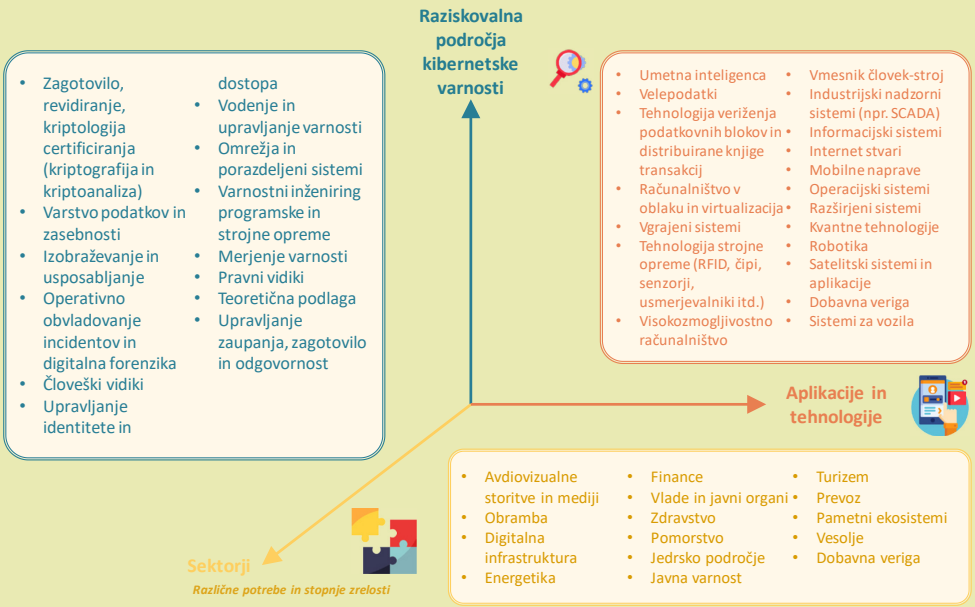
Okvir 5

Prizadevanja za isti kibernetski jezik: *tehnološka koherentnost*

Terminološka jasnost izboljšuje situacijsko zavedanje in usklajevanje[143] ter pomaga ugotoviti, kaj natančno je grožnja in tveganje.

Skupno raziskovalno središče Komisije je nedavno razvilo spremenjeno raziskovalno taksonomijo, ki izhaja iz različnih mednarodnih standardov[144]. Njen cilj je, da postane referenčna točka, ki bi jo raziskovalni subjekti po vsej Evropi uporabljali kot indeks.

Taksonomija na področju kibernetske varnosti



Vir: Evropsko računsko sodišče, prilagojeno po gradivu Evropske komisije

Do nedavnega institucije in agencije EU niso imele skupnih opredelitev. Zdaj se to spreminja. Skupina za sodelovanje je v okviru svojega načrta razvila taksonomijo incidentov, da bi olajšala učinkovito čezmejno sodelovanje.

Sodelovanje in izmenjava informacij z zasebnim sektorjem

97 Sodelovanje med javnimi organi in zasebnim sektorjem je bistveno za povečanje splošne ravni kibernetske varnosti. Komisija je kljub temu v svoji oceni strategije za

kibernetsko varnost iz leta 2017 ugotovila, da izmenjava informacij med zasebnimi deležniki ter med javnim in zasebnim sektorjem še ni optimalna, ker ni dovolj zaupanja vrednih mehanizmov poročanja in spodbud za izmenjavo informacij[145], kar ovira doseganje strateških ciljev. Ugotovila je tudi, da ni učinkovitega mehanizma za sodelovanje, v okviru katerega bi države članice sodelovale za ustrezno strateško okrepitev trajnih industrijskih zmogljivosti[146].

98 Centri za izmenjavo in analizo informacij so organizacije, ustanovljene za zagotavljanje platform in sredstev za olajšanje izmenjave informacij med javnim in zasebnim sektorjem ter zbiranja informacij o kibernetskih grožnjah. Njihov cilj je graditi zaupanje z izmenjavo izkušenj, znanja in analiz, zlasti glede temeljnih vzrokov, incidentov in groženj. Nacionalni in sektorski centri za izmenjavo in analizo informacij že obstajajo v mnogih državah članicah, na evropski ravni pa jih je še vedno razmeroma malo[147]. Srečujejo se s številnimi izzivi (omejenost virov, težave pri ocenjevanju njihove uspešnosti, zagotavljanje ustreznih struktur za vključitev tako javnega kot tudi zasebnega sektorja, vključevanje organov kazenskega pregona), ki jih bo treba premagati, če naj prispevajo k izvajanju direktive o varnosti omrežij in informacij ter izgradnji varnostnih zmogljivosti na evropski ravni[148].

99 Tesno sodelovanje z zasebnim sektorjem je še posebej pomembno za boj proti kompleksni kibernetski kriminaliteti, vendar je njegova učinkovitost v državah članicah različna in odvisna od ravni zaupanja[149]. Europolov Evropski center za boj proti kibernetski kriminaliteti pa je s subjekti zasebnega sektorja, institucijami in agencijami EU ter drugimi mednarodnimi organizacijami ustanovil vrsto svetovalnih skupin za izboljšanje sodelovanja z mreženjem, strateško izmenjavo obveščevalnih podatkov in sodelovanjem. Te skupine delajo v skladu s cilji političnega cikla EU[150]. Kriminalne zlorabe šifriranja so še eno področje, polno izzivov, za katere bo potrebnega več sodelovanja z zasebnim sektorjem. Europolov Evropski center za boj proti kibernetski kriminaliteti sedaj preučuje možnost, da bi skupna projektna skupina za ukrepanje na področju kibernetske kriminalitete v specifičnih primerih kratkoročno gostila strokovnjake iz zasebnega sektorja in akademike (glej odstavek ***62***).

100 To, da ni učinkovitih mehanizmov za sodelovanje je problem tako za civilne kot tudi za obrambne skupnosti – javne in zasebne. Področja, ki predstavljajo skupen izziv, vključujejo kriptografijo, varne vgrajene sisteme, zaznavanje zlonamerne programske opreme, tehnike simulacije, zaščito omrežij in komunikacijskih sistemov ter tehnologije za avtentikacijo. Spodbujanje civilno-vojaškega sodelovanja in podpiranje raziskav in tehnologije (zlasti s podpiranjem MSP) sta dve od prioritet posodobljenega okvira EU za politiko kibernetske obrambe (posodobitev iz leta 2018).

Točke za razmislek – Izgradnja odpornosti

- Kako bi bilo mogoče na ravni EU doseči ustrezno ravnovesje med potrebo po racionalizaciji politike za kibernetsko varnost in po zagotavljanju učinkovitega usklajevanja med različnimi akterji ter razpršenostjo odgovornosti?
- Kako dobro so institucije in agencije EU pripravljene na naslednji velik napad, usmerjen neposredno vanje?
- Kako bi lahko agencije EU, relevantne za kibernetsko varnost, postale privlačnejše za talente?
- Kateri dodatni ukrepi so potrebni za zagotavljanje ustrezne zmogljivosti v vseh institucijah in agencijah EU, da bi te lahko imele koherenten okvir za ocenjevanje tveganj in ogroženosti?
- Kako evropski nadzorni organi (Evropski bančni organ, Evropski organ za vrednostne papirje in trge ter Evropski organ za zavarovanja in poklicne pokojnine) obravnavajo kibernetske ranljivosti v finančnem sektorju in kaj se iz tega lahko naučijo drugi sektorji?
- Kako bi se lahko ob splošnem primanjkljaju strokovnega znanja tehnična pomoč EU za javne organe najbolje uporabila, da bi imela največji mogoč splošen učinek na izboljšanje kibernetske odpornosti?
- Kako lahko EU in države članice zagotovijo smiselno prisotnost v mednarodnih razpravah za oblikovanje upravljanja kibernetskega prostora in standardov ter promocijo vrednot EU?
- Kateri ukrepi za ozaveščanje na ravni EU in držav članic (vključno s prizadevanji za preprečevanje) res dosegajo rezultate in kako jih lahko EU okrepi?
- Kakšno vlogo ima EU pri doseganju uravnotežene zastopanosti spolov na področju kibernetske varnosti?
- Kako lahko EU in države članice izboljšajo sinergije med civilno in obrambno skupnostjo v skladu z okvirom za politiko kibernetske obrambe (posodobitev iz leta 2018)?

Uspešno odzivanje na kibernetske incidente

101 Razvoj uspešnega odzivanja na kibernetske napade je temeljen za njihovo čimprejšnjo popolno zaustavitev. Zlasti je pomembno, da se lahko kritični sektorji, države članice in institucije EU odzovejo hitro in usklajeno. Za to je bistveno zgodnje zaznavanje.

Izziv 9: uspešno zaznavanje in odziv

Zaznavanje in priglasitev

102 Skupna orodja za zaznavanje vsakodnevno pomagajo premagati veliko večino napadov[151]. Vendar so digitalni sistemi postali tako kompleksni, da ni mogoče preprečiti vsakega napada. Napadi zaradi sofisticiranosti pogosto lahko dalj časa ostanejo nezaznani. Strokovnjaki zato menijo, da bi se bilo treba osredotočiti na hitro zaznavanje in obrambo[152]. Vendar nekatera orodja za zaznavanje, kot so avtomatizacija, strojno učenje in vedenjska analitika, ki si prizadevajo za zmanjševanje tveganj ter analizirajo vedenje sistema in se iz njega učijo, podjetja nerada sprejemajo[153]. To je delno posledica ustvarjanja lažnih pozitivnih rezultatov, pri čemer se za dejavnosti, ki ne pomenijo grožnje, zmotno misli, da so zlonamerne.

103 Ko se kršitev odkrije in analizira, sta potrebna hitra priglasitev in poročanje, da lahko drugi javni in zasebni subjekti sprejmejo preventivne ukrepe, zadevni organi pa pomagajo prizadetim. Mnoge organizacije nerade priznajo kibernetske incidente in o njih poročajo[154]. Bistveni sta tudi zgodnja vključenost organov kazenskega pregona v prvem odzivu na domnevno kibernetsko kriminaliteto in proaktivna izmenjava informacij s skupinami za odzivanje na incidente na področju računalniške varnosti.

104 Ker nekdaj ni bilo skupnih zahtev EU glede priglasitve incidentov, je obstajalo tveganje, da bo sporočanje kršitev pozno in da bo odziv oviran, to pa naj bi se odpravilo z uvedbo direktive o varnosti omrežij in informacij (glej odstavek ***20***). Po napadih WannaCry leta 2017 je Komisija ugotovila, da sistem mreže skupin za odzivanje na incidente na področju računalniške varnosti „še ni bil popolnoma operativen“[155]. Izvajanje direktive se nadaljuje, vendar se bo šele pokazalo, ali bodo smernice, ki jih je pripravila skupina za sodelovanje, uspešno odpravile nepripravljenost za poročanje o incidentih[156].

105 Izvajalci bistvenih storitev v nekaterih sektorjih imajo v okviru obstoječih uredb EU več obveznosti za priglasitev (tudi potrošnikom), ki bi lahko ogrozile učinkovitost procesa. Na primer, za izvajalce v finančnem in bančnem sektorju veljajo različna merila, standardi, mejne vrednosti in časovni okviri za priglasitev iz splošne uredbe o varstvu podatkov, direktive o varnosti omrežij in informacij, direktive o plačilnih storitvah, ECB/EMN, TARGET2 in uredbe eIDAS[157]. Zato je pomembno, da se te obveznosti racionalizirajo, saj ne povzročajo samo nepotrebne administrativne obremenitve, temveč zaradi te raznolikosti lahko pride do razdrobljenega poročanja.

Usklajen odziv

106 Evropski okvir za sodelovanje na področju kibernetskih kriz se še vedno razvija. Zato je bil predstavljen z njim povezan načrt[158] (glej odstavek ***18***), da bi se v mehanizem enotne ureditve EU za politično odzivanje na krize (IPCR) vključil še kibernetski vidik, da bi se izboljšalo situacijsko zavedanje in zagotovilo boljše povezovanje z drugimi mehanizmi EU za krizno upravljanje[159]. Načrt vključuje institucije, agencije in države članice EU. V celoti povezati vse te mehanizme za odzivanje na krize je izziv[160]. Velika pomanjkljivost je tudi to, da sedaj ni skupnega varnega komunikacijskega omrežja institucij EU[161].

107 Zmogljivost EU za odzivanje na kibernetske napade na operativni in politični ravni v primeru velikega čezmejnega incidenta je bila označena kot omejena, deloma zato, ker kibernetska varnost še ni vključena v obstoječe mehanizme za usklajevanje odzivanja na krize na ravni EU[162]. V direktivi o varnosti omrežij in informacij to vprašanje ni obravnavano.

108 Nedavno predlagane reforme ENISE, s katero naj bi ta dobila večjo operativno vlogo pri obvladovanju velikih kibernetskih incidentov, države članice niso podprle, saj so želele, da bi agencija podpirala in dopolnjevala njihove lastne operativne ukrepe[163]. Zdaj na ravni držav članic obstaja že mnogo skupin za odzivanje na računalniške grožnje in skupin za odzivanje na incidente na področju računalniške varnosti, vendar se njihove zmogljivosti zelo razlikujejo. To je ovira za uspešno čezmejno sodelovanje, ki je potrebno za odziv na velike incidente[164].

109 Sodišče je poskusilo kartirati vloge različnih akterjev iz načrta, vendar je ugotovilo vrzeli, ki jih bo treba odpraviti v nadaljnjem izvajanju. Področje, ki sprva ni bilo dovolj obravnavano, je kazenski pregon, vendar je decembra 2018 začel veljati protokol EU za odzivanje organov kazenskega pregona na izredne razmere[165]. Za

uspešnost načrta je ključno, da je praktičen in da vsi udeleženci vedo, kaj so njihove naloge. To bo treba v naslednjih letih obsežno preizkusiti.

110 Uspešen odziv je več kot le omejevanje škode, ključno je določanje odgovornosti za napade. Izsledite v in identifikacija storilcev sta predvsem pri hibridnem napadu lahko zelo težka zaradi vedno pogostejše zlorabe orodij za anonimizacijo, kriptovalut in šifriranja. To je znano kot problem pripisa. Odprava tega problema ni samo tehnično vprašanje, ampak tudi izziv za kazensko pravosodje. Pravne in postopkovne razlike med državami lahko ovirajo kazenske preiskave in pregon osumljencev. Za obravnavo problema pripisa bo npr. potrebna bolj formalizirana operativna izmenjava informacij z jasnejšimi postopki z Europolom ali Evropsko pravosodno mrežo Eurojusta za kibernetsko kriminaliteto.

111 Na politični ravni je bila razvita zbirka orodij za kibernetsko diplomacijo (glej ***okvir 6***) za podporo reševanju mednarodnih sporov v kibernetskem prostoru z miroljubnimi sredstvi. Ustanovitev enot za hitro odzivanje na kibernetske grožnje in pobuda za medsebojno pomoč na področju kibernetske varnosti sta projekta, ki spodbujata okrepljeno izmenjavo informacij in ki se razvijata v skladu z okvirom za stalno strukturno sodelovanje[166].

Okvir 6

Zbirka orodij za kibernetsko diplomacijo

Skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti[167] ali zbirka orodij za kibernetsko diplomacijo izhaja iz sklepov Sveta o kibernetski diplomaciji iz leta 2015[168]. Cilj kibernetske diplomacije je razvoj in izvajanje skupnega in celovitega pristopa h kibernetskemu prostoru na podlagi vrednot EU, pravne države, izgradnje zmogljivosti in partnerstev, spodbujanja modela upravljanja interneta z več deležniki ter odprave groženj za kibernetsko varnost in večje stabilnosti mednarodnih odnosov.

Zbirka orodij EU in njenim državam članicam omogoča skupen diplomatski odziv na zlonamerne kibernetske dejavnosti s celovito uporabo ukrepov v okviru skupne zunanje in varnostne politike. Ti lahko vključujejo preventivne ukrepe (npr. ozaveščanje, izgradnjo zmogljivosti), ukrepe sodelovanja, ukrepe za stabilnost in omejevalne ukrepe (npr. prepoved potovanja, embargo na orožje, zamrznitev sredstev) ali podporo za odzive držav članic[169]. Nadaljnje sodelovanje za ublažitev groženj in to, da se jasno pove, katere so verjetne posledice skupnega odziva, naj bi (potencialno) odvrnilo od napadalnega vedenja.

Skupen odziv EU na zlonamerne kibernetske dejavnosti bi bil sorazmeren z obsegom, stopnjo, trajanjem, intenzivnostjo, kompleksnostjo, sofisticiranostjo in učinkom kibernetske dejavnosti.

Za uspešnost zbirke orodij bo ključno to, kako dobro bo prepletena z načrtom in mehanizmom enotne ureditve EU za politično odzivanje na krize (glej odstavek ***106***), kako dobro bo s hitro in stalno izmenjavo informacij vzpostavljeno situacijsko zavedanje (vključno z elementi pripisa)[170], in nazadnje uspešno sodelovanje. Za uspešno uvedbo zbirke orodij je ključno tudi uspešno in usklajeno komuniciranje. Do zdaj je bila zbirka orodij uporabljena dvakrat: za začetek dialoga z Združenimi državami Amerike po napadu *WannaCry*[171] in za pripravo sklepov Sveta o obsodbi zlonamerne uporabe IKT[172]. Operacionalizacija zbirke orodij še poteka in šele pokazalo se bo, kako uspešna bo pri doseganju svojih ciljev.

Izziv 10: zaščita kritične infrastrukture in družbenih funkcij

Zaščita infrastrukture

112 Večino kritične infrastrukture EU upravljajo industrijski nadzorni sistemi[173]. Mnogi so bili zasnovani kot samostojni sistemi z omejeno povezljivostjo z zunanjim svetom. Ko so bili deli industrijskih nadzornih sistemov povezani z internetom, so postali bolj ranljivi za zunanje poseganje. Vzdrževanje obstoječih sistemov in nameščanje popravkov vanje morda nista več mogoča, njihova nadgradnja pa je dolgotrajen in drag proces. Prizadevanja za okrepitev varnosti kritične infrastrukture morajo zato vključevati nadgradnjo industrijskih nadzornih sistemov.

113 Ker se industrija še vedno digitalizira (znano kot „industrija 4.0“), bi lahko imel obsežen incident v enem industrijskem sektorju posredne učinke tudi v drugih sektorjih. ENISA je opozorila na pomembnost kartiranja vpliva vzajemnih odvisnosti ključnih sektorjev[174]. To je bistveno za razumevanje mogočega širjenja incidenta in temelj dobro usklajenih odzivov.

114 Cilj direktive o varnosti omrežij in informacij je povečanje pripravljenosti v ključnih sektorjih, odgovornih za kritično infrastrukturo. V to pa niso zajeti vsi sektorji (glej ***tabelo 1***)[175], kar zmanjšuje uspešnost strategije[176]: v tem pogledu je zlasti zaskrbljujoča zaščita demokratične integritete volitev pred poseganjem v volilno infrastrukturo in širjenjem dezinformacij (glej ***okvir 7***). Poleg prenove obstoječe

zakonodaje bo zato ključni izziv to, kako te sektorje vključiti v uspešno odzivanje na velike incidente.

115 Kritična infrastruktura pa ni ranljiva samo znotraj Evrope. Poseben izziv za Komisijo je spodbujanje držav kandidatk za članstvo v EU, naj sprejmejo enake standarde kot države članice, na primer na področjih, kot sta zakonodaja na področju kibernetske varnosti ali zaščita kritične infrastrukture.

Okvir 7

Zaščita kritičnih družbenih funkcij: *boj proti poseganju v volitve*

Maja 2019 se bo približno 400 milijonov volivcev udeležilo volitev v Evropski parlament, prvič od začetka veljave splošne uredbe o varstvu podatkov. Te volitve bodo potekale po škandalih v zvezi z zlorabo osebnih podatkov za v posameznike usmerjene politične kampanje in kampanje usklajenega širjenja dezinformacij (lažne novice), kot jih še ni bilo. Komisija je opozorila na to, da bi lahko prišlo do kibernetskega poseganja v te volitve[177], ki ga bo mogoče premagati samo z vsevladnim in vsedružbenim pristopom.

Volilna infrastruktura

Organizacija volitev je kompleksna, zagotavljanje njihove zaščite in integritete pa je odgovornost držav članic. S poseganjem v volitve in volilno infrastrukturo bi se lahko vplivalo na naklonjenost volivcev, volilno udeležbo ali sam volilni proces, vključno z oddajo glasov, tabeliranjem glasov in komunikacijo. Za volitve v Evropski parlament je posebej kritičen izziv zaščita t. i. zadnjega dela (sporočanja rezultatov iz nacionalnih prestolnic v Bruselj), saj za to ne obstaja niti ni bil preizkušen noben skupni varnostni pristop[178].

Nedavni volilni sveženj Komisije je vključeval ukrepe za krepitev volilne kibernetske varnosti, kot je imenovanje nacionalnih kontaktnih točk za usklajevanje in izmenjavo informacij v času pred volitvami. Izmenjava najboljših praks in izkušenj je posebej pomembna[179].

Volilni sistemi ne štejejo za del kritične infrastrukture[180] in niso zajeti v direktivo o varnosti omrežij in informacij. Ne glede na to je skupina za sodelovanje v podporo javnim organom pripravila praktične smernice o varnosti volilne tehnologije. Nacionalne kontaktne točke naj bi se sestale v začetku leta 2019[181]. Države članice se tudi spodbujajo, naj izvedejo ocene tveganja v zvezi s kibernetskimi grožnjami za svoje volilne procese.

Dezinformacije

Dezinformacije so vedno pomembnejši element hibridnih napadov, ki zajemajo kibernetske napade in vdore v omrežja. Lahko se uporabljajo za razdvojitev družb, vzbujanje nezaupanja in spodkopavanje zaupanja v demokratične procese ali druge zadeve (npr. kampanje proti cepljenju ali zanikanje podnebnih sprememb). Dezinformacij je vedno več, poleg tega pa postajajo vedno hitrejše in obsežnejše, zato resnično ogrožajo varnost v EU.

EU je sprejela več ukrepov za obravnavo dezinformacij. Leta 2015 je bila znotraj ESZD ustanovljena projektna skupina East StratCom za boj proti ruskim kampanjam širjenja dezinformacij[182]. Strokovnjaki so pohvalili njeno delo na področju spodbujanja politike EU, podpiranja neodvisnih medijev v sosedstvu in napovedovanja dezinformacij, sledenja dezinformacijam in boja proti njim[183]. Toda viri projektne skupine so glede na količino in kompleksnost kampanj za širjenje dezinformacij relativno skromni[184]. Potrebna sta bolj sistematična interakcija z obstoječimi strukturami EU in boljše sodelovanje na področju strateške komunikacije[185]. Evropski svet je nov akcijski načrt[186] podprl decembra 2018.

Komisija je pred kratkim poleg svojega sporočila o boju proti dezinformacijam na spletu[187] iz aprila 2018 razvila neobvezen samoregulativen kodeks ravnanja[188], ki temelji na obstoječih instrumentih politike, ki so se jim zavezale spletne platforme in oglaševalska industrija[189]. Ukrep zajema pomoč za doseganje tega, da so vsebine bolj vredne zaupanja, in podporo prizadevanjem za povečanje medijske pismenosti in pismenosti v zvezi z novicami. Ustanovljena je bila tudi neodvisna evropska mreža preverjevalcev dejstev.

Komisija je navedla, da bi lahko sledili dodatni regulativni ukrepi, če se kodeks ravnanja ne bi upošteval. Ugotavljanje uspešnosti ukrepov bo ključno, zlasti pri odločanju, kako meriti izboljšanje zaupanja, transparentnosti in odgovornosti.

Dodaten izziv je iskanje načinov za izboljšanje zaznavanja, analize in razkrivanja dezinformacij[190]. Potrebna sta tudi aktivno in strateško spremljanje in analiza odprtih podatkovnih virov[191]. Prizadevanja za boljše razumevanje groženj bi morala zajemati tudi nove trende, kot so t. i. globoki ponaredki (lažni videi, ustvarjeni s pomočjo umetne inteligence in globokega strojnega učenja), pa tudi orodja, potrebna za njihovo odkrivanje.

Krepitev avtonomnosti

116 EU je neto uvoznik izdelkov in storitev za kibernetsko varnost, kar povečuje tveganje tehnološke odvisnosti od izvajalcev izven EU in ranljivosti[192]. To zmanjšuje varnost kritične infrastrukture EU, ki jo tudi podpirajo kompleksne svetovne dobavne

verige. Tveganje se dodatno poveča, kadar izvajalci izven EU kupijo evropska podjetja za kibernetsko varnost. Države članice so odgovorne za pregledovanje neposrednih tujih naložb, na ravni EU pa zdaj ni nobenega mehanizma za pregledovanje[193].

117 Večja strateška avtonomnost je cilj globalne strategije EU in sporočila *Odpornost, odvračanje in obramba* iz leta 2017[194]. Obravnava številnih izzivov, predstavljenih v tem dokumentu, bo pomagala okrepiti želeno avtonomnost. Tega ne more doseči en sam ukrep.

Točke za razmislek – Uspešno odzivanje

- Kako je direktiva o varnosti omrežij in informacij izboljšala priglasitve kibernetskih incidentov v kritičnih sektorjih in izven njih?
- Kako dobro so institucije EU internalizirale usklajevanje odzivanja na krize za velike kibernetske incidente?
- Kako lahko kibernetska diplomacija prevzame vidnejšo vlogo v zunanjem delovanju EU?
- Ali so sedanji strukture in ukrepi EU za boj proti širjenju dezinformacij sorazmerni z obsegom in kompleksnostjo problema?

Zaključne pripombe

118 EU in njene države članice so v zadnjih letih v svoji agendi bolj poudarile kibernetsko varnost, da bi izboljšale splošno kibernetsko odpornost. Vendar je doseganje višje ravni kibernetske varnosti v EU še vedno zelo velika naloga. Sodišče je želelo v tem informativnem dokumentu poudariti nekatere glavne izzive za doseganje ambicije EU, da bi postala najvarnejše digitalno okolje na svetu.

119 Pregled Sodišča kaže, da je potreben premik v smeri kulture smotrnosti s praksami za ocenjevanje, da se zagotovita smiselna **odgovornost in ocenjevanje**. **Zakonodaja ima še vedno** nekaj **vrzeli, poleg tega pa obstoječa zakonodaja ni dosledno prenesena v nacionalne zakonodaje držav članic**, zato težje dosega svoj polni potencial. Drug opredeljen izziv zadeva **uskladitev ravni naložb s strateškimi cilji**, za kar bo potrebno povečanje ravni naložb in njihovega učinka. To je še zahtevnejše, ko EU in države članice nimajo **jasnega pregleda nad porabo EU** za kibernetsko varnost. Poroča se tudi o **nezadostnosti virov agencij EU, relevantnih za kibernetsko varnost**, in o težavah pri privabljanju in ohranjanju talentov.

120 Razpoložljive študije so prišle do zaključka, da **je mogoče upravljanje kibernetske varnosti okrepiti** za povečanje zmožnosti svetovne skupnosti za odzivanje na kibernetske napade in incidente. Hkrati pa je nemogoče preprečiti vse napade. Zato so ključni izzivi, ki jih je treba obravnavati, **hitro zaznavanje in odziv**, **zaščita kritične infrastrukture in družbenih funkcij** ter boljša **izmenjava informacij in usklajevanje** med javnim in zasebnim sektorjem. In nazadnje, vse večji primanjkljaj znanj v zvezi s kibernetsko varnostjo na svetovni ravni pomeni, da sta tudi **pridobivanje znanja in ozaveščanje** v vseh sektorjih in na vseh družbenih ravneh bistven izziv.

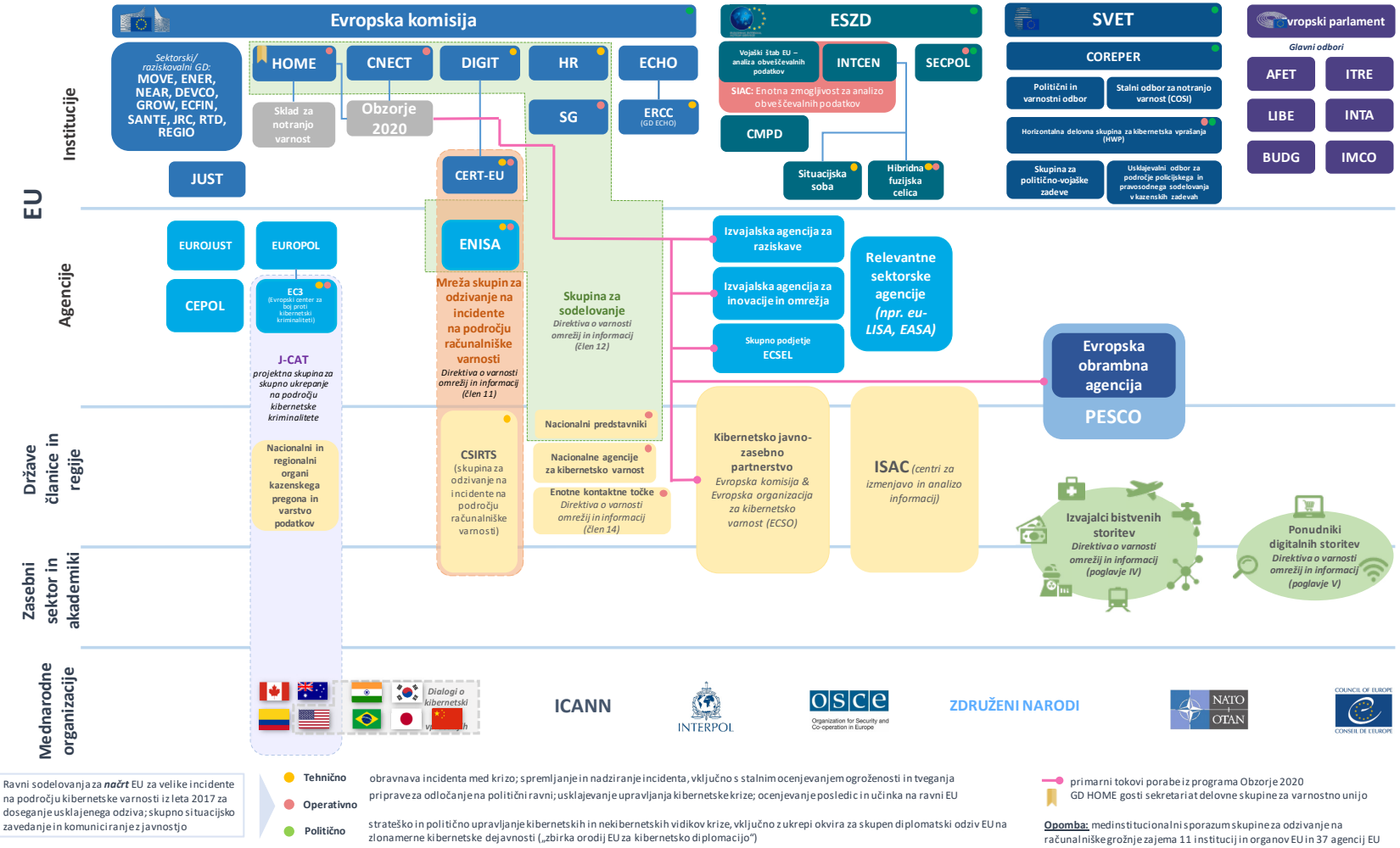
121 Zaradi teh izzivov v zvezi s kibernetskimi grožnjami, s katerimi se srečujeta EU in širše globalno okolje, sta potrebna stalna zavezanost vrednotam EU in njihovo neomajno uveljavljanje.

Ta informativni dokument je sprejel senat III na zasedanju 14. februarja 2019.

Za Evropsko računsko sodišče

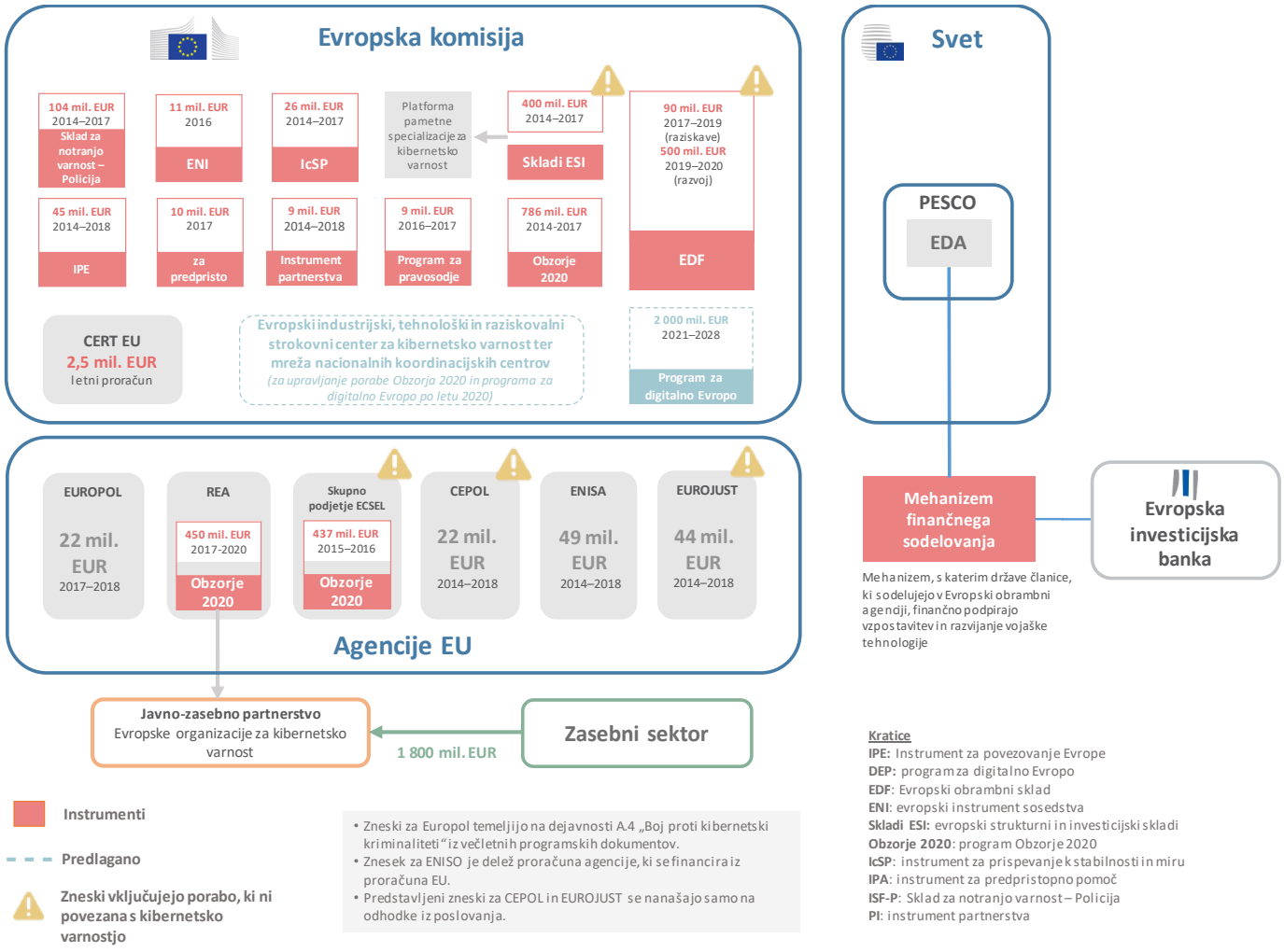
Klaus-Heiner Lehne
Predsednik

Priloga I – Kompleksnost in večplastnost s številnimi akterji



Vir: Evropsko računsko sodišče

Priloga II – Poraba EU za kibernetsko varnost od leta 2014



Vir: Evropsko računsko sodišče na podlagi dokumentov Evropske komisije in agencij EU

Priloga III – Poročila revizijskih uradov držav članic EU

Vrsta	Naslov (s povezavo)	Leto	Država članica
Revizije skladnosti	Dokument o oceni notranjih kontrol	2014	FR
	Poročilo o potrditvi zaključnega računa splošne sheme socialne varnosti (obramba, zunanje zadeve)	2016	FR
	Potrditev državnih računov	2016	FR
	Zagotavljanje varnosti in ohranjanja kritičnih estonskih nacionalnih podatkovnih zbirk	Dokončano leta 2018/še ni objavljeno	EE
	Uspešnost notranjih kontrol pri varovanju osebnih podatkov v nacionalnih podatkovnih zbirkah	2008	EE
Revizije smotrnosti poslovanja / stroškovne učinkovitosti	Poročilo o blaženju kibernetskih napadov	2013	DK
	RiR 2014:23, Varnost informacij v civilni javni upravi	2014	SE
	Poročilo o tem, kako vlada obdeluje zaupne podatke o posameznikih in podjetjih	2014	DK
	Nacionalni program za kibernetsko varnost	2014	UK
	Poročilo proračunskemu odboru nemškega zveznega parlamenta v skladu z drugim odstavkom § 88 zveznega proračunskega zakonika – konsolidacija IT, zvezna vlada	2015	DE
	Poročilo o dostopu do sistemov IT, ki podpirajo zagotavljanje bistvenih storitev danski družbi	2015	DK
	Javni organ za načrtovanje Plaine de France	2015	FR
	Kibernetska varnost v Litvi litovska verzija povzetek v angleščini	2015	LT
	Kako javni organi na Poljskem opravljajo naloge na področju kibernetske varnosti (v poljščini)	2015	PL
	RiR 2015:21, Kibernetska kriminaliteta – policija in tožilstvo bi bila lahko učinkovitejša	2015	SE
	Vrzel v digitalnem znanju v vladi (anketa)	2015	UK
	Poročilo zveznemu parlamentu: Zvezne finance: pobiranje davka na dediščino	2016	BE
	Poročilo o upravljanju varnosti IT v sistemih, ki je oddano v izvajanje zunanjim izvajalcem	2016	DK
	Revizijsko poročilo o posojilnih dejavnostih inštituta za posojila za leto 2016	2016	ES
	Usmerjanje vladne varnostne mreže	2016	FI
	Zagotavljanje varnosti sistemov IT, uporabljenih za javne naloge	2016	PL
	Preprečevanje kibernetskega ustrahovanja med otroki in mladimi ter boj proti njemu	2016	PL
	Delo na področju varnosti informacij v devetih agencijah – Še ena revizija o varnosti informacij v državi. RiR 2016:8	2016	SE

Vrsta	Naslov (s povezavo)	Leto	Država članica
	Varovanje informacij v celotni vladi	2016	UK
	Poročilo o zaščiti sistemov IT in zdravstvenih podatkov v treh danskih regijah	2017	DK
	Dokument o rezultatih mednarodne vzporedne revizije: uspešnost notranjih kontrol pri varovanju osebnih podatkov v nacionalnih podatkovnih zbirkah	2017	EE
	Ureditve za kibernetsko zaščito	2017	FI
	Usmerjanje operativne zanesljivosti elektronskih storitev	2017	FI
	Zbornice kmetijske mreže (povzetek)	2017	FR
	Gospodarska in industrijska zbornica Vaucluse (pripravil regionalni revizijski senat PACA)	2017	FR
	Zagotavljanje varnosti in ohranjanja kritičnih estonskih nacionalnih podatkovnih zbirk	Dokončano leta 2018/še ni objavljeno	EE
	Razvoj državne infrastrukture za elektronsko komunikacijo litovska verzija povzetek v angleščini	2017	LT
	Revizija informacijske tehnologije: kibernetska varnost v vladnih subjektih	2017	MT
	Sistem nacionalnih registrov: varnost, smotrnost in uporabnost	2017	PL
	Incident WannaCry	2017	UK
	Spletne goljufije	2017	UK
	Poročilo o zaščiti pred napadi z izsiljevalskim programjem	2018	DK
	Arpajon Hospital (pripravil regionalni revizijski senat Île-de-France)	2018	FR
	Upravljanje kritičnih državnih virov informacij	2018	LT
	Elektronska kriminaliteta	2019	LT
	Varnost informacij na Poljskem	2019	PL
Drugo	Podatkovne zbirke javnih organov	ni relevantno	BE
	Vprašalnik o politiki na področju varnosti in analize tveganja (poteka)	ni relevantno	BE

Kratice in okrajšave

CERT -EU: skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije

cPPP: pogodbeno javno-zasebno partnerstvo

DDoS: porazdeljena zavrnitev storitev

DEP: program za digitalno Evropo

DIGIT: Generalni direktorat za informatiko

Direktiva NIS: direktiva o varnosti omrežij in informacij

EC3: Europolov Evropski center za boj proti kibernetski kriminaliteti

ECA: Evropsko računsko sodišče

ECSEL: Skupno podjetje Elektronske komponente in sistemi za evropski vodilni položaj

ECSM: evropski mesec kibernetske varnosti

ECSO: Evropska organizacija za kibernetsko varnost

EDA: Evropska obrambna agencija

ENISA: Agencija Evropske unije za varnost omrežij in informacij

ESA: evropski nadzorni organ

ESZD: Evropska služba za zunanje delovanje

EU: Evropska unija

FDI: tuji neposredni instrumenti

GD CONNECT: Generalni direktorat za komunikacijska omrežja, vsebine in tehnologijo

GD HOME: Generalni direktorat za migracije in notranje zadeve

GD JUST: Generalni direktorat za pravosodje in potrošnike

GDPR: Splošna uredba o varstvu podatkov

HWPCI: Horizontalna delovna skupina za kibernetska vprašanja

ICS: industrijski nadzorni sistemi

ISF - P: Sklad za notranjo varnost – Policija

ISSB: Usmerjevalni odbor za varnost informacij

JRC: Skupno raziskovalno središče

LISO: lokalni varnostni uradnik za informatiko

MSP: mala in srednja podjetja

NAO: nacionalni revizijski urad

NCIRC: služba zveze NATO za odzivanje na incidente na področju računalniške varnosti

PESCO: stalno strukturno sodelovanje

Sklad ESI: Evropski strukturni in investicijski skladi

Skupina CSIRT: skupina za odzivanje na incidente na področju računalniške varnosti

SVOP: skupna varnostna in obrambna politika

Glosar

Botnet: Omrežje računalnikov, ki so okuženi z zlonamerno programsko opremo in se upravljajo na daljavo brez vednosti njihovih uporabnikov za pošiljanje neželene elektronske pošte, krajo podatkov ali izvajanje usklajenih kibernetskih napadov.

Celovitost: Varovanje pred neustreznim spreminjanjem ali uničenjem informacij in zagotavljanje njihove verodostojnosti.

Dezinformacije: Dokazljivo napačne ali zavajajoče informacije, ki so ustvarjene, predstavljene in se razširjajo za pridobivanje gospodarske koristi ali za namerno zavajanje javnosti ter lahko povzročijo javno škodo.

Digitalne vsebine: Kakršni koli podatki, kot so besedilo, zvok, slike ali video, shranjeni v digitalni obliki.

Heker-aktivist: Posamezniki ali skupine, ki pridobijo nedovoljen dostop do informacijskih sistemov ali omrežij za doseganje socialnih ali političnih ciljev.

Hibridna grožnja: Oznanitev sovražnega naklepa nasprotnikov s kombinacijo konvencionalnih in nekonvencionalnih vojnih tehnik (tj. vojaške, politične, ekonomske in tehnološke metode) za nasilno uresničevanje njihovih ciljev.

Internet stvari: Mreža vsakdanjih predmetov, ki so opremljeni z elektroniko, programsko opremo in senzorji, da lahko komunicirajo in izmenjavajo podatke preko interneta.

Izsiljevalsko programje: Zlonamerna programska oprema, ki žrtvam onemogoči dostop do računalniškega sistema ali povzroči, da datoteke niso berljive, običajno s šifriranjem. Napadalec nato običajno žrtev izsiljuje tako, da noče ponovno vzpostaviti dostopa, dokler mu žrtev ne plača odkupnine.

Kibernetska kriminaliteta: Različne kriminalne dejavnosti, katerih glavno orodje ali glavna tarča so računalniški sistemi in sistemi IT. Te dejavnosti vključujejo: klasična kazniva dejanja (npr. goljufijo, ponarejanje in krajo identitete), kazniva dejanja v zvezi z vsebino (npr. razširjanje otroške pornografije na spletu ali spodbujanje k rasnemu sovraštvu) in kazniva dejanja na področju računalnikov in informacijskih sistemov (npr. napade na informacijske sisteme, napade za zavrnitev storitve in zlonamerno programsko opremo).

Kibernetska obramba: Del kibernetske varnosti, namenjen obrambi kibernetskega prostora z vojaškimi in drugimi ustreznimi sredstvi za doseganje vojaško-strateških ciljev.

Kibernetska odpornost: Zmožnost, da se kibernetski napadi in incidenti preprečijo, da se nanje pripravi, da se jih prestane in da se ponovno vzpostavi prejšnje stanje.

Kibernetska varnost: Vsi zaščitni in drugi ukrepi, sprejeti za obrambo informacijskih sistemov in njihovih podatkov pred nepooblaščenim dostopom, napadom in poškodovanjem, da se zagotovi njihova razpoložljivost, zaupnost in celovitost.

Kibernetski ekosistem: Kompleksna skupnost naprav, ki med seboj sodelujejo, podatkov, omrežij, ljudi, procesov in organizacij ter okolje procesov in tehnologij, ki delujejo na to sodelovanje in ga podpirajo.

Kibernetski incident: Dogodek, ki neposredno ali posredno škoduje odpornosti in varnosti nekega sistema IT in podatkov, ki jih obdeluje, hrani ali prenaša, ali ju ogroža.

Kibernetski napad: Poskus oslabitve ali uničenja zaupnosti, celovitosti in razpoložljivosti podatkov ali računalniškega sistema preko kibernetskega prostora.

Kibernetski prostor: Nesnovno svetovno okolje, v katerem poteka spletna komunikacija med ljudmi, programska oprema in storitve prek računalniških omrežij in tehnoloških naprav.

Kibernetsko pogojena kriminaliteta: Kriminaliteta, ki se lahko izvede samo z uporabo naprav IT.

Kriminaliteta, ki jo omogoča kibernetski prostor: Klasična kriminaliteta, storjena v večjem obsegu z uporabo sistemov IT.

Kriptovaluta: Digitalno sredstvo, ki se izda in menja z uporabo tehnik za šifriranje, neodvisno od centralnih bank. Kot plačilno sredstvo je sprejeta med člani virtualne skupnosti.

Kritična infrastruktura: Fizični viri, storitve in objekti, katerih motnje ali uničenje bi resno vplivali na delovanje gospodarstva in družbe.

Lažno predstavljanje: Pošiljanje elektronskih sporočil, ki so videti, kot da prihajajo iz zanesljivega vira, da se prejemnike zavede, da kliknejo na zlonamerne povezave ali da posredujejo osebne podatke.

Model kriminala kot storitve (CaaS): Kriminalen poslovni model, ki je gonilo digitalne sive ekonomije in zagotavlja mnogo različnih komercialnih storitev in orodij, ki nekvalificiranim kibernetskim kriminalcem začetnikom omogoča izvajanje kibernetske kriminalitete.

Nameščanje popravkov: Uvajanje sklopa sprememb ali posodabljanje, popravljanje ali izboljševanje programske opreme, vključno z odpravo šibkih točk na področju varnosti.

Obstoječi sistem: Zastarel računalniški sistem, aplikacija ali programski jezik, ki je še vedno v uporabi, vendar zanj posodobitve in podpora ponudnika morda niso na voljo, vključno s podporo za varnost.

Oglaševalsko programje: Zlonamerna programska oprema, ki prikazuje oglasne pasice ali pojavna okna s kodami za sledenje ravnanju žrtev na spletu.

Orodje za izkoriščanje ranljivosti: Vrsta zbirke orodij, ki jo kibernetski kriminalci uporabljajo za napad na ranljivosti v omrežju in informacijskih sistemih, da lahko razširijo zlonamerno programsko opremo ali izvajajo druge zlonamerne dejavnosti.

Osebni podatki: Informacije, ki se nanašajo na določljivega posameznika.

Podatki o dostopu: Informacije o uporabnikovih prijavah v storitev in odjavah iz nje, kot so čas, datum in naslov IP.

Porazdeljena zavrnitev storitev (DDoS): Kibernetski napad, ki legitimnim uporabnikom preprečuje dostop do spletnih storitev ali virov s tem, da jih preplavi s toliko zahtevki, da jih ne morejo obdelati.

Računalništvo v oblaku: Zagotovitev virov IT na zahtevo, npr. shranjevanja, računalniške zmogljivosti ali zmogljivosti za souporabo podatkov prek interneta z gostovanjem na oddaljenih strežnikih.

Razpoložljivost: Zagotavljanje pravočasnega in zanesljivega dostopa do informacij in njihove uporabe.

Skimming: Kraja podatkov kreditne ali debetne kartice, ko se ti podatki vnesejo na spletu.

Socialni inženiring: Na področju varnosti informacij je to psihološka manipulacija, s katero se ljudi zavede, da nekaj storijo ali razkrijejo zaupne informacije.

Storitve zaupanja: Storitve, ki povečujejo pravno veljavnost elektronskih transakcij, kot so elektronski podpisi, pečati, časovni žigi, priporočena dostava in avtentikacija spletišč.

Šifriranje: Preoblikovanje berljive informacije v neberljivo kodo za njeno zaščito. Za branje informacij mora imeti uporabnik dostop do tajnega ključa ali gesla.

Upravljanje ranljivosti: Sestavni del računalniške varnosti in varnosti omrežij za proaktivno zmanjševanje ali preprečevanje izkoriščanja šibkih točk sistema in programske opreme z opredelitvijo, klasifikacijo in sanacijo teh šibkih točk.

Varnost informacij: Sklop procesov in orodij za zaščito fizičnih in digitalnih podatkov pred nepooblaščenim dostopom, uporabo, razkritjem, motnjo, spreminjanjem, evidentiranjem ali uničenjem.

Varnost omrežij: Del kibernetske varnosti za varstvo podatkov, poslanih preko naprav v istem omrežju, s katerim se zagotavlja, da se informacije ne prestrežejo ali spremenijo.

Vektorizacija besedila: Pretvarjanje besed, stavkov ali celih dokumentov v numerične vektorje, da jih lahko uporabljajo algoritmi za strojno učenje.

Volilna infrastruktura: To vključuje sisteme IT in podatkovne zbirke za kampanje, občutljive informacije o kandidatih, registracijo volivcev in sisteme upravljanja.

Zaupnost: Varstvo informacij, podatkov ali drugih sredstev pred nedovoljenim dostopom ali razkritjem.

Zlonamerna programska oprema za brisanje: Vrsta zlonamerne programske opreme, katere namen je izbrisati trdi disk računalnika, ki ga je okužila.

Zlonamerna programska oprema: Zlonamerna programska oprema je računalniški program, zasnovan za poškodovanje računalnika, strežnika ali omrežja.

[1] V predlogu za uredbo EU o kibernetski varnosti je bila opredeljena kot „vse dejavnosti, ki so potrebne za zaščito omrežij in informacijskih sistemov, njihovih uporabnikov in prizadetih oseb pred kibernetskimi grožnjami“. Evropski parlament in Svet naj bi uredbo sprejela na začetku leta 2019.

[2] Europol, *Internet Organised Crime Threat Assessment 2017*.

[3] Evropska organizacija za kibernetsko varnost (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, junij 2016.

[4] Evropski parlament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, študija za Odbor za državljanske svoboščine, pravosodje in notranje zadeve (LIBE), september 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18. januar 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018*.

[7] Europol, *Ibid.*, 2018.

[8] Evropsko središče za politično ekonomijo, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, priložnostni dokument št. 2/18, februar 2018.

[9] Evropska komisija, predsednikov govor Stanje v Uniji 2017.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, obvestilo za javnost, 25. april 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017*.

[12] Informativno gradivo Evropske komisije o kibernetski varnosti, september 2017.

[13] Stroški bi lahko vključevali: izgubljene prihodke, stroške popravila poškodovanih sistemov, potencialne obveznosti zaradi ukradenega premoženja ali informacij, spodbude za zadržanje strank, višje zavarovalne premije, višji stroški varovanja (novi sistemi, uslužbenci, usposabljanje), potencialna poravnava stroškov izpolnjevanja obveznosti ali sodnih postopkov.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] Izsiljevalsko programje *WannaCry* je izkoriščalo ranljivosti v protokolu Microsoft Windows, s čimer je lahko na daljavo prevzelo nadzor nad katerim koli računalnikom. Microsoft je po odkritju ranljivosti namestil popravek. Vendar stotisoči računalnikov še niso bili posodobljeni in mnogi od njih so bili nato okuženi. Vir: A. Greenberg, *Hold North Korea Accountable For WannaCry—and the NSA, too*, WIRED, 19. december 2017.

[16] Evropska komisija, *Europeans' attitudes towards cybersecurity*, Posebna raziskava Eurobarometer št. 464a, september 2017. Naknadna raziskava naj bi bila objavljena na začetku leta 2019.

[17] Budimpeška konvencija je zavezujoča mednarodna smernica za države pri razvijanju zakonodaje za boj proti kibernetski kriminaliteti. Zagotavlja okvir za mednarodno

sodelovanje med državami pogodbenicami. Komisija, Svet Evropske unije, Europol, ENISA in Eurojust trenutno zastopajo EU.

[18] Evropska komisija, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final, 7. februar 2013.

[19] Evropska komisija, *The European Agenda on Security*, COM(2015) 185 final, 28. april 2015.

[20] Evropska komisija, *Strategija za enotni digitalni trg za Evropo*, COM(2015) 192 final, 6. maj 2015.

[21] ESZD, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, junij 2016.

[22] Center za evropske politične študije, *Strengthening the EU's Cyber Defence Capabilities – poročilo delovne skupine Centra za evropske politične študije*, november 2018.

[23] Zlonamerno programsko opremo, ki je bila uporabljena za napad z izsiljevalskim programjem WannaCry, ki so ga Združene države Amerike, Združeno kraljestvo in Avstralija pripisali Severni Koreji, je sprva razvila in hranila agencija ZDA za nacionalno varnost, da bi lahko izkoriščala ranljivosti v sistemu Windows. Vir: A. Greenberg, ibid., WIRED, 19. december 2017. Ob napadih je Microsoft obsodil to, da vlade hranijo podatke o ranljivostih programske opreme, in ponovil, da je po njegovem mnenju potrebna digitalna ženevska konvencija.

[24] Poleg kopnega, morja, zraka in vesolja.

[25] Okvir EU za politiko kibernetske obrambe (posodobljen leta 2018), 14413/18, 19. november 2018.

[26] Evropska komisija/Evropska služba za zunanje delovanje, *Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije*, JOIN(2016) 18 final, 6. april 2016.

[27] Skupna izjava predsednika Evropskega sveta, predsednika Evropske komisije in generalnega sekretarja Organizacije Severnoatlantske pogodbe, 8. julij 2016 in 10. julij 2018.

[28] Evropska komisija/Evropska služba za zunanje delovanje, *Odpornost, odvračanje in obramba:okrepitev kibernetske varnosti za EU*, JOIN(2017) 450 final z dne 13. septembra 2017.

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

[30] Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

[31] Te so povezane v strukturo za sodelovanje, uvedeno z direktivo, in sicer mrežo skupin za odzivanje na incidente na področju računalniške varnosti (mreža, sestavljena iz skupin za odzivanje na incidente na področju računalniške varnosti, ki jih imenujejo države članice EU, in skupine za odzivanje na računalniške grožnje; ENISA gosti sekretariat) in skupino za sodelovanje (podpira in olajšuje strateško sodelovanje in izmenjavo informacij med državami članicami; Komisija gosti sekretariat).

[32] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

[33] Evropska komisija, *Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*, COM(2017) 477 final, 13. september 2017.

[34] Evropska komisija, *Predlog uredbe Evropskega parlamenta in Sveta o evropskem nalogu za predložitev in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih zadevah*, COM(2018) 225 final, 17. april 2018.

[35] Evropska komisija, *Predlog direktive Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o imenovanju pravnih zastopnikov za namene zbiranja dokazov v kazenskih postopkih*, COM(2018) 226 final, 17. april 2018.

[36] Evropska komisija, *Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov,* COM(2018) 630 final, 12. september 2018.

[37] H. Carrapico and A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, zvezek 55, št. 6, 2017.

[38] Evropska komisija, ibid., SWD(2017) 295 final, 13. september 2017.

[39] Služba Evropskega parlamenta za raziskave, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, december 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27. november 2014.

[41] Izjema je člen 14 (Spremljanje in statistika) Direktive 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.

[42] Evropski ekonomsko-socialni odbor, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, marec 2018. Projektna skupina Centra za evropske politične študije in European Credit Research Institute, *Cybersecurity in Finance: Getting the policy mix right!*, junij 2018.

[43] Na anketo Sodišča je odgovorilo 24 od 28 nacionalnih revizijskih uradov.

[44] To pomeni, da temeljita na načelih in sta tehnološko čim bolj nevtralna.

[45] Mehanizem Evropske komisije za znanstveno svetovanje Znanstveno mnenje 2/2017, 24. marec 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, september 2018. Evropsko središče za politično ekonomijo, ibid., priložnostni dokument št. 2/18, februar 2018.

[47] Evropska komisija, *Predlog direktive Evropskega parlamenta in Sveta o nekaterih vidikih pogodb o dobavi digitalnih vsebin*, COM(2015) 634 final, 9. december 2015.

[48] Evropska komisija, *Predlog direktive Evropskega parlamenta in Sveta o nekaterih vidikih pogodb o spletni in drugi prodaji blaga na daljavo*, COM(2017) 635 final, 9. december 2015.

[49] Nizozemski svet za kibernetsko varnost, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Center za evropske politične študije, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force*, junij 2018.

[51] Evropska komisija, *Kako kar najbolje izkoristiti direktivo o varnosti omrežij in informacij – za učinkovito izvajanje Direktive (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji*, COM(2017) 476 final/2, 4. oktober 2017.

[52] Europol, ibid., 2017.

[53] Svet Evropske unije, *Končno poročilo o sedmem krogu vzajemnega ocenjevanja z naslovom „Praktično izvajanje in delovanje evropskih politik za preprečevanje in zatiranje kibernetske kriminalitete"*, 12711/1/17 REV 1, 9. oktober 2017.

[54] Evropska komisija, ocena učinka, priložena Predlogu direktive Evropskega parlamenta in Sveta o boju proti goljufijam in ponarejanju v zvezi z negotovinskimi plačilnimi sredstvi, SWD/2017/0298 final, 13. september 2017. Politično soglasje o novi zakonodaji je bilo doseženo decembra 2018, zakonodaja pa naj bi bila sprejeta na začetku leta 2019.

[55] Europol, ibid., 2017.

[56] C-362/14: Maximillian Schrems proti Data Protection Commissioner (Irska), 6. oktober 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime*, 7021/17, 13. marec 2017.

[58] Evropska komisija, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD (2017) 295 final, 13. september 2017.

[59] Služba Evropskega parlamenta za raziskave, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, *PE589.832*.

[60] Resolucija Evropskega parlamenta, *Človekove pravice in tehnologija: učinek sistemov za odkrivanje vdorov in sistemov nadzora na človekove pravice v tretjih državah*, (2014/2232(INI)), 8. september 2015. Blago in storitve z dvojno rabo, ki vključujejo programsko opremo in tehnologijo, se lahko uporabljajo v civilne in vojaške namene.

[61] Javno dostopne informacije se hranijo v podatkovni zbirki WHOIS, ki jo upravlja ICANN (Internet Corporation for Assigned Names and Numbers). ICANN vzdržuje sistem domenskih imen. Napačna uporaba domenskih imen omogoča kibernetsko kriminaliteto.

[62] Člen 3 direktive o varnosti omrežij in informacij, ibid.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10. september 2015.

[64] Bela hiša, *Cybersecurity spending fiscal year 2019*.

[65] Evropska komisija, *Delovni dokument služb Komisije: Ocena učinka, spremni dokument k predlogu uredbe Evropskega parlamenta in sveta o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027'*, SWD(2018) 305 final, 6. junij 2018.

[66] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, december 2016.

[67] Evropska komisija, ibid., COM(2018) 630 final, 12. september 2018.

[68] Služba Evropskega parlamenta za raziskave, Oddelek za znanstvene napovedi, *Achieving a sovereign and trustworthy ICT industry in the EU*, december 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31. julij 2017.

[70] Služba Evropskega parlamenta za raziskave, Oddelek za znanstvene napovedi, ibid., december 2017.

[71] Ibid.

[72] Evropska komisija, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 final (del 1/4), 12. September 2018.

[73] Evropska komisija, ibid., COM(2018) 630 final, 12. september 2018.

[74] Posebno poročilo Evropskega računskega sodišča št. 13/2018 – Radikalizacija, ki vodi v terorizem.

[75] Zneski, navedeni v tem oddelku, izhajajo iz javno dostopnih dokumentov Komisije, razen 42 milijonov EUR iz odstavka ***51***, o katerih je Komisija neposredno obvestila Sodišče.

[76] Obzorje 2020 je program EU za raziskave in inovacije, vreden 80 milijard EUR in namenjen podpori Uniji inovacij, katere cilj je zagotoviti konkurenčnost EU na svetovni ravni.

[77] Obzorje 2020 – Družbeni izziv 7 „Varne in inovativne družbe: varovanje svobode in varnosti Evrope in njenih državljanov".

[78] Sodišče je analiziralo projekte Obzorja 2020 iz podatkovnega nabora CORDIS. Sodišče je opravilo vektorizacijo besedila opisov vseh projektov z uporabo taksonomije Skupnega raziskovalnega središča za kibernetsko varnost (glej ***okvir 5*** v naslednjem poglavju), da bi ugotovilo, za katere projekte je verjetno, da so povezani s kibernetsko varnostjo. Nato pa je ročno preverilo in analiziralo rezultate.

[79] Evropska organizacija za kibernetsko varnost, *ECS cPPP Progress Monitoring Report 2016-2017*, 29. oktober 2018.

[80] Člen 9(2) direktive o varnosti omrežij in informacij, ibid.

[81] GLACY+ (Global Action on Cybercrime+ (ukrepanje na svetovni ravni proti kibernetski kriminaliteti)) je skupen projekt s Svetom Evrope. Podpira dvanajst držav v Afriki, azijsko-pacifiški regiji ter Latinski Ameriki in karibski regiji, ki lahko potem služijo kot zvezdišča za izmenjavo izkušenj v svojih regijah.

[82] Evropsko središče za politično strategijo, ki je možganski trust Komisije, je navedlo pripombo o tveganju digitalnega mrtvega kota, do katerega bi lahko prišlo, če bi vrzel med EU in Zahodnim Balkanom še naprej rasla. Države, kot sta npr. Kitajska in Rusija, v to regijo vlagajo velike zneske, zaradi česar bi bila lahko EU kot akter na področju kibernetske varnosti v tej regiji potisnjena v ozadje. Vir: Evropsko središče za politično strategijo, *Engaging with the Western Balkans: an investment in Europe's security*, 17. maj 2018.

[83] Evropska investicijska banka, *The EIB Group Operating Framework and Operational Plan 2018*, 12. december 2017. V času priprave tega informativnega dokumenta dodatne informacije niso bile na voljo.

[84] Evropska komisija, *Predlog uredbe Evropskega parlamenta in sveta o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027*, COM(2018) 434 final, 6. junij 2018.

[85] Evropska komisija, *Uredba (EU) 2018/1092 Evropskega parlamenta in Sveta z dne 18. julija 2018 o vzpostavitvi evropskega programa za razvoj obrambne industrije v podporo konkurenčnosti in inovacijski zmogljivosti obrambne industrije Unije* (UL L 200, 7.8.2018, str. 30). Poleg tega je bil leta 2017 uveden pripravljalni ukrep za raziskave na področju obrambe v skupni vrednosti 90 milijonov EUR za obdobje 2017–2019, ki se bo financiral iz Obzorja 2020. Ni jasno, ali to vključuje tudi porabo za kibernetsko varnost.

[86] Sodišče namerava v letu 2019 objaviti poseben informativni dokument o obrambi EU.

[87] Europolov Evropski center za boj proti kibernetski kriminaliteti, ENISA, ESZD, Evropska obrambna agencija in skupina za odzivanje na računalniške grožnje imajo skupaj 159 uslužbencev. Ta številka ne vključuje uslužbencev, ki opravljajo naloge na področju kibernetske varnosti v Evropski komisiji ali v državah članicah. Vir: Center za evropske politične študije, ibid., november 2018.

[88] *Ocena ENISE*, 2017.

[89] Europol je v svojem večletnem načrtu za obdobje 2018–2020 zahteval povečanje števila zaposlenih za 70 začasnih uslužbencev na leto, vendar je bilo leta 2018 odobrenih le 26. V osnutku naslednjega večletnega načrta za obdobje 2019–2021 je Europol zahteval skromno povečanje, saj meni, da večjim zahtevam za vire ne bi bilo ugodeno. Vir: posvetovanje o osnutku večletnega programskega načrta za obdobje 2019–2021, ki je bil posredovan skupini za skupni parlamentarni nadzor, A 000834, 1. februar 2018.

[90] *Ocena ENISE*, 2017. Med letoma 2014 in 2016 je bilo približno 80 % operativnega proračuna ENISE porabljenega za naročila študij.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, december 2017.

[92] ISACA (nekdaj imenovana Združenje za revizijo in kontrolo informacijskih sistemov), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2. izdaja, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017*, str. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy in H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, julij 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21. februar 2018.

[96] Forum za sodelovanje med Evropskim bančnim organom, Evropskim organom za vrednostne papirje in trge ter Evropskim organom za zavarovanja in poklicne pokojnine.

[97] Evropski organ za vrednostne papirje in trge, *Joint Committee report on risks and vulnerabilities in the EU financial system*, april 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, december 2015.

[99] Mehanizem Komisije za znanstveno svetovanje se sklicuje na države članice EU, ko ugotavlja, da obstaja visoka in edinstvena raven strinjanja o temeljnih načelih in vrednotah, pa tudi skupni strateški interes, ki je lahko v središču uspešnega upravljanja kibernetske varnosti EU. Vir: Znanstveno mnenje 2/2017, 24. marec 2017.

[100] Združene države Amerike, Kitajska, Japonska, Južna Koreja, Indija in Brazilija.

[101] Evropska akademija za varnost in obrambo (T. Renard in A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 23. november 2018.

[102] Svet Evropske unije, *Akcijski načrt za izvajanje sklepov Sveta o skupnem sporočilu Evropskemu parlamentu in Svetu: Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU*, 15748/17, 12. december 2017.

[103] Evropska komisija, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final, 21. november 2018.

[104] Odgovor komisarke Marije Gabriel na pisno parlamentarno vprašanje (E-004294–17) z dne 28. junija 2017.

[105] Svet Evropske unije, *Annual Report on the Implementation of the Cyber Defence Policy Framework*, 15870/17, 19. december 2017.

[106] Sklepi 2015/443, 2015/444 in 2017/46 urejajo varnost komunikacijskih in informacijskih sistemov Komisije. S Sklepom Komisije C(2018) 7706 z dne 21. novembra 2018 je bil ustanovljen odbor za informacijsko tehnologijo in kibernetsko varnost, ki združuje nekdanji odbor za IT in Usmerjevalni odbor za varnost informacij.

[107] Evropski ekonomsko-socialni odbor, ibid., marec 2018.

[108] Evropski parlament, ibid., september 2015.

[109] Hibridna fuzijska celica je bila ustanovljena leta 2016 v okviru Obveščevalnega in situacijskega centra EU v okviru ESZD. Od različnih deležnikov prejema in analizira tajne informacije in informacije iz odprtih virov o hibridnih grožnjah.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, november 2013.

[111] Evropska komisija, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final (Del 1/6), 13. september 2017.

[112] Evropska komisija, ibid., SWD(2018) 403 final, 12. september 2018.

[113] Résaux IP Européens Network Coordination Centre, regionalni internetni register za Evropo, ki nadzira dodeljevanje in registracijo virov internetnih številk.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs*, november 2012.

[115] The Centre for Cyber Safety and Education v partnerstvu z Booz Allen Hamilton, Alta Associates in Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] Evropski ekonomsko-socialni odbor, ibid., marec 2018.

[117] Zgornji dom parlamenta Združenega kraljestva, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19*, 16. julij 2018.

[118] Europol/Eurojust, *Common challenges in combating cybercrime*, 7021/17, 13. marec 2017.

[119] Europol/Eurojust, ibid., 7021/17, 13. marec 2017.

[120] Evropska komisija, ibid., SWD(2018) 403 final, 12. september 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022*, 20. november 2018.

[122] Na primer sodelovanje med ESZD, državami članicami, agencijami in organi, kot so CEPOL, Evropska skupina za usposabljanje in izobraževanje na področju kibernetske kriminalitete ali Evropska akademija za varnost in obrambo.

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, december 2017.

[124] Evropska skupina za usposabljanje in izobraževanje na področju kibernetske kriminalitete.

[125] Evropska komisija, Trinajsto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije, COM(2018) 46 final z dne 24. januarja 2018.

[126] Na podlagi ugotovitev v Posebnem poročilu št. 14/2018, ibid.

[127] Resolucija Evropskega parlamenta z dne 13. junija 2018 o kibernetski obrambi (2018/2004(INI)). Svet Evropske unije, ibid., 15870/17, 19. december 2017.

[128] Švica, nekdanja jugoslovanska republika Makedonija, Ukrajina, Bosna in Hercegovina, Kosovo (to poimenovanje ne posega v stališča glede statusa ter je v skladu z RVSZN 1244/1999 in mnenjem Meddržavnega sodišča o razglasitvi neodvisnosti Kosova), Turčija in Združene države Amerike.

[129] Europol, *Internet Organised Crime Threat Assessment 2018*.

[130] Evropska komisija, ibid., SWD(2017) 295 final, 13. september 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman in S. Furman, *Security Fatigue*, "IT Professional", zvezek 18, št. 5, 2016, str. 26–32. Glej tudi NIST.

[132] Evropska Komisija/Evropska služba za zunanje delovanje, *Povečanje odpornosti in krepitev zmogljivosti za obravnavanje hibridnih groženj*, JOIN(2018) 16 final, 13. junij 2018.

[133] Npr. zaprtje AlphaBay in Hansa po skupnih operacijah ameriškega zveznega preiskovalnega urada in nizozemske nacionalne policije s podporo Europola. To sta bili največji trgovini za preprodajo prepovedanega blaga, kot so droge, strelno orožje in orodje za izvajanje kibernetske kriminalitete, kot je zlonamerna programska oprema. Vir: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, Sporočilo za javnost, 29. maj 2018.

[134] Evropska komisija, ibid., SWD(2018) 403 final, 12. september 2018.

[135] Svet Evropske unije, ibid., 12711/1/17 REV 1, 9. oktober 2017.

[136] Evropska komisija, ibid., SWD(2017) 295 final, 13. september 2017.

[137] Evropska komisija/Evropska služba za zunanje delovanje, ibid., JOIN(2018) 16, 13. junij 2018.

[138] Evropska komisija, SWD(2017) 500 final, 13. september 2017.

[139] *Memorandum of Understanding – ENISA, EDA, Europol EC3, and CERT-EU*; 23. maj 2018.

[140] Evropska komisija, javni razpis: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*, 27. oktober 2017.

[141] Jean-Claude Juncker, poslanica komisarju za varnostno unijo, 2. avgust 2016. Obramba ni v pristojnosti delovne skupine.

[142] Svet Evropske unije, *EU cybersecurity roadmap*, 8901/17, 11. maj 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues, 5. izdaja*, november 2017.

[144] Tehnična poročila Skupnega raziskovalnega središča, European Cybersecurity Centres of Expertise Map: *Definitions and Taxonomy*. Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres, SWD(2018) 403 final, 12. september 2018.

[145] Evropska komisija, ibid., SWD(2017) 295 final, 13. september 2017.

[146] Evropska komisija, ibid., SWD(2018) 403 final, 12. september 2018.

[147] Na primer center za izmenjavo in analizo informacij evropskih finančnih ustanov vključuje predstavnike finančnega sektorja, nacionalnih skupin za odzivanje na računalniške grožnje, organov kazenskega pregona, ENISE, Europola, Evropske centralne banke, Evropskega sveta za plačila in Evropske komisije.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14. februar 2018.

[149] Svet Evropske unije, ibid., 12711/1/17 REV 1, 9. oktober 2017.

[150] https://www.europol.europa.eu/empact.

[151] S študijo, ki jo je podjetje Accenture leta 2018 izvedlo v 15 državah, je bilo ugotovljeno, da se preprečuje 87 % usmerjenih kibernetskih napadov: *2018 State of Cyber Resilience*, 10. april 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, Oxford University Politics Blog, 14. september 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14. julij 2017.

[154] Evropski ekonomsko-socialni odbor, *ibid.*, marec 2018.

[155] Evropska komisija, *Osmo poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije*, COM(2017) 354 final, 29. junij 2017.

[156] Glej različne publikacije skupine za sodelovanje, ustanovljene v skladu z direktivo o varnosti omrežij in informacij.

[157] PSD2: revidirana direktiva o plačilnih storitvah; ECB/EMN: Evropska centralna banka/enotni mehanizem nadzora; TARGET2: transevropski sistem bruto poravnave v realnem času (2. generacija); Uredba (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu. Vir: Projektna skupina Centra za evropske politične študije in European Credit Research Institute, ibid., junij 2018.

[158] Evropska komisija, *Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises*, C(2017) 6100 final, 13. september 2017.

[159] Evropska komisija, ibid., SWD(2017) 295 final, 13. september 2017. Obstaja več mehanizmov za krizno upravljanje, vključno z mehanizmom enotne ureditve EU za politično odzivanje na krize, Argus (mehanizem Komisije za odzivanje na krize), mehanizmom ESZD za odzivanje na krize, mehanizmom Unije na področju civilne zaščite in protokolom EU za odzivanje organov kazenskega pregona na izredne razmere.

[160] Poleg tega bi se zato lahko sklicevali tudi na člen 42(7) Pogodbe o Evropski uniji (klavzula o vzajemni pomoči) ali člen 222 Pogodbe o delovanju Evropske unije (solidarnostna klavzula).

[161] Evropska komisija/Evropska služba za zunanje delovanje, ibid., JOIN(2018) 16, 13. junij 2018. Decembra 2018 se je v medijih poročalo o vdoru v diplomatsko komunikacijsko omrežje ESZD, t. i. omrežje COREU (vir: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*; 18. december 2018). Ta zadeva se sedaj preiskuje.

[162] Dodatno je treba razviti tudi sodelovanje na področju zgodnjega opozarjanja in vzajemne pomoči: *Sklep Sveta o usklajenem odzivu EU na velike kibernetske incidente in krize*, 10085/18, 26. junij 2018.

[163] Služba Evropskega parlamenta za raziskave, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, september 2018.

[164] Evropski ekonomsko-socialni odbor, ibid., marec 2018.

[165] Svet Evropske unije, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, 14893/18. december 2018.

[166] Enote za hitro odzivanje na kibernetske grožnje in medsebojna pomoč na področju kibernetske varnosti; platforma za izmenjavo informacij v zvezi s kibernetskimi grožnjami in odzivanjem na incidente. Vir: Svet Evropske unije, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*, 19. november 2018.

[167] Svet Evropske unije, Sklepi Sveta o okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti, 9916/17, 7. junij 2017.

[168] Svet Evropske unije, *Sklepi Sveta o kibernetski diplomaciji*, 6122/55, 11. februar 2015.

[169] Svet Evropske unije, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.

[170] Pripis odgovornosti za incident ostaja suverena politična odločitev držav članic, za vse ukrepe zbirke orodij pa pripis ni potreben.

[171] Zbirka orodij ni privedla do skupnega ukrepanja; posamezne države članice so prevzele stališče ZDA.

[172] Svet Evropske unije, *Sklepi Sveta o zlonamernih kibernetskih dejavnostih*, 7925/18, 16. april 2018.

[173] Računalniški sistemi, ki se uporabljajo za nadzor procesov v različnih industrijah, kot so javne službe, proizvodnja kemikalij in industrijska proizvodnja, predelava hrane, prometni sistemi in središča ter logistične storitve.

[174] ENISA, ibid., december 2017.

[175] Na primer, javna uprava, kemijska in jedrska industrija, proizvodnja, predelava hrane, turizem, logistika in civilna zaščita.

[176] Evropska komisija, ibid., SWD(2017) 295 final, 13. september 2017.

[177] Govor komisarke Jourove na plenarnem zasedanju Evropskega parlamenta o *krepitvi odpornosti EU na vplive tujih akterjev na skorajšnjo kampanjo za volitve v Evropski parlament*, 14. november 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23. maj 2018.

[179] Evropsko središče za politično strategijo (L. Past), Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses, v publikaciji: "Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts", 2018.

[180] V skladu z Direktivo Sveta (ES) št. 114/2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite.

[181] Evropska komisija, *Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, C(2018) 5949 final, 12. september 2018.

[182] Sklepi Evropskega sveta, EUCO 11/15, 20. marec 2015. Od takrat sta bili ustanovljeni še dve projektni skupini, in sicer za Zahodni Balkan in južno sosedstvo.

[183] V poročilu Atlantic Council je poziv, naj EU od vseh držav članic zahteva, naj v projektno skupino napotijo nacionalne strokovnjake. Glej: D. Fried in A. Polyakova, *Democratic Defense Against Disinformation*, 5. marec 2018.

[184] Sprva ni imela lastnega proračuna, leta 2018 pa ji je Evropski parlament dodelil 1,1 milijona EUR za pripravljalni ukrep StratCom Plus.

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), ibid., 23. maj 2018.

[186] Evropska komisija, visoka predstavnica Unije za zunanje zadeve in varnostno politiko, *Akcijski načrt proti dezinformacijam*, JOIN (2018) 36 final. Načrt je osredotočen na: izboljšanje zmožnosti institucij EU za odkrivanje, analiziranje in razkrivanje dezinformacij; krepitev usklajenih in skupnih odzivov; mobilizacijo zasebnega sektorja; ozaveščanje in izboljšanje družbene odpornosti.

[187] Evropska komisija, *Boj proti dezinformacijam na spletu: evropski pristop*, COM(2018) 236 final, 26. april 2018.

[188] To ni kodeks ravnanja na področju boja proti nezakonitemu sovražnemu govoru na spletu.

[189] Skupno raziskovalno središče, *The digital transformation of news media and the rise of disinformation and fake news*, tehnična poročila Skupnega raziskovalnega središča, delovni dokument Skupnega raziskovalnega središča o digitalnem gospodarstvu 2018-02, april 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")*, april 2018.

[191] Evropsko središče za politično strategijo (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, v: ibid, 2018.

[192] Evropska komisija, ibid., SWD(2018) 403 final, 12. september 2018.

[193] Predlog uredbe (COM(2017) 487 final, 13. september 2017) za pregledovanje neposrednih tujih naložb, predložen septembra 2017, je sedaj v zakonodajnem postopku. Vanj so specifično vključene kritične tehnologije, ki vključujejo umetno inteligenco, kibernetsko varnost in aplikacije z dvojno rabo.

[194] Evropska komisija/Evropska služba za zunanje delovanje, ibid., JOIN(2017) 450 final, 13. september 2017.

Ekipa Evropskega računskega sodišča

Ta informativni dokument z naslovom Izzivi za uspešno politiko EU za kibernetsko varnost je sprejel senat III – zunanji ukrepi, varnost in pravica –, ki mu predseduje članica Evropskega računskega sodišča Bettina Jakobsen. Nalogo je vodil član Evropskega računskega sodišča Baudilio Tomé Muguruza, pri tem pa so mu pomagali vodja njegovega kabineta Daniel Costa de Magalhaes in ataše v njegovem kabinetu Ignacio Garcia de Parada, vodilni upravni uslužbenec Alejandro Ballester-Gallardo, vodja naloge Michiel Sweerts ter revizorji Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha in pripravnik Johannes Bolkart. Jezikovno pomoč je zagotovila Hannah Critoph.

Od leve proti desni: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

EVROPSKO RAČUNSKO SODIŠČE

Urad za publikacije

EVROPSKO RAČUNSKO SODIŠČE
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel. +352 4398-1

Vprašanja: eca.europa.eu/sl/Pages/ContactForm.aspx
Spletišče: eca.europa.eu
Twitter: @EUAuditors