EVROPSKA
KOMISIJA

Bruselj, 24.7.2020
COM(2020) 605 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, EVROPSKEMU SVETU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

o strategiji EU za varnostno unijo

I. Uvod

V političnih usmeritvah Komisije je poudarjeno, da moramo storiti vse, kar je v naši moči, da bi zaščitili naše državljanke in državljane. Varnost ne pomeni le osebne varnosti, zagotavlja tudi varstvo temeljnih pravic ter osnovo za zaupanje in dinamiko v našem gospodarstvu, družbi in demokraciji. Evropejci in Evropejke se danes soočamo z varnostno krajino, ki se nenehno spreminja, nanjo pa vplivajo spreminjajoče se grožnje in drugi dejavniki, vključno s podnebnimi spremembami, demografskimi trendi in politično nestabilnostjo zunaj naših meja. Globalizacija, prosto gibanje in digitalna preobrazba še naprej prinašajo blaginjo, olajšujejo naša življenja ter spodbujajo inovacije in rast. Vendar pa poleg teh koristi prinašajo tudi tveganja in stroške. Lahko se zlorabljajo za namene terorizma, organiziranega kriminala, nedovoljenega prometa s prepovedanimi drogami in trgovine z ljudmi, ki pomenijo neposredno grožnjo za državljanke in državljane ter evropski način življenja. Kibernetski napadi in kibernetska kriminaliteta so še naprej v porastu. Varnostne grožnje postajajo vse bolj zapletene; uspevajo zaradi svoje čezmejne narave in povezljivosti, poleg tega pa izkoriščajo zabrisane meje med fizičnim in digitalnim svetom, ranljive skupine ter družbene in gospodarske razlike. Napadi so lahko nenadni in ne pustijo praktično nobenih sledi, tako državni kot tudi nedržavni akterji se lahko poslužujejo vrste hibridnih groženj[1], dogodki zunaj EU pa lahko odločilno vplivajo na varnost znotraj EU.

Tudi kriza zaradi COVID-19 je spremenila naše predstave o varnostnih grožnjah in ustreznih politikah. Izpostavila je, da je treba zagotoviti tako varnost v fizičnem kot tudi v digitalnem okolju. Opozorila je tudi na pomen odprte strateške avtonomije za naše dobavne verige, kar zadeva kritične proizvode, storitve, infrastrukture in tehnologije. Okrepila je potrebo po vključitvi vseh sektorjev in vseh posameznikov v skupna prizadevanja, da bi bila EU že v izhodišču bolje pripravljena in odpornejša ter da bi imela na voljo boljša orodja, kadar je potreben odziv.

Državljanov in državljank ni mogoče zaščititi samo s samostojnim ukrepanjem držav članic. Izkoriščanje naših prednosti za sodelovanje še nikoli ni bilo tako pomembno, EU pa še nikoli ni imela take priložnosti, da doseže resnične spremembe. Lahko služi kot zgled, tako da izboljša svoj celotni sistem kriznega upravljanja ter z ukrepanjem znotraj in zunaj svojih meja prispeva k stabilnosti na svetovni ravni. Čeprav so za varnost v prvi vrsti odgovorne države članice, se je v zadnjih letih izkazalo, da je varnost ene države članice pomembna za varnost vseh držav. EU lahko zagotovi multidisciplinaren in celosten odziv ter akterjem na področju varnosti v državah članicah pomaga z orodji in informacijami, ki jih potrebujejo[2].

EU lahko zagotovi tudi, da bo varnostna politika še naprej temeljila na naših skupnih evropskih vrednotah – spoštovanju pravne države, enakosti[3] in temeljnih pravic ter zagotavljanju preglednosti, odgovornosti in demokratičnega nadzora –, da bi bile politike zares vredne zaupanja. Vzpostavi lahko pravo in učinkovito varnostno unijo, v kateri bodo pravice in svoboščine posameznikov dobro varovane. Varnost in spoštovanje temeljnih pravic si ne nasprotujeta, pač pa se ujemata in dopolnjujeta. Podlaga za varnostno politiko

[1] Opredelitve hibridnih groženj se sicer razlikujejo, na splošno pa gre za kombinacijo prisilnih in subverzivnih dejavnosti, konvencionalnih in nekonvencionalnih metod (tj. diplomatskih, vojaških, gospodarskih in tehnoloških), ki jih lahko državni ali nedržavni akterji usklajeno uporabljajo za doseganje specifičnih ciljev (pri čemer razmere ne dosežejo praga za uradno razglasitev vojne). Glej JOIN(2016) 18 final.

[2] Na primer s storitvami v okviru vesoljskega programa EU. Program Copernicus na primer zagotavlja podatke, pridobljene z opazovanjem Zemlje, ki se lahko uporabljajo za varovanje meja, pomorsko varnost, kazenski pregon, preprečevanje piratstva, preprečevanje tihotapljenja drog in ravnanje v izrednih razmerah.

[3] Unija enakosti: strategija za enakost spolov za obdobje 2020–2025 (COM(2020) 152).

morajo biti naše vrednote in temeljne pravice, da se zagotovijo spoštovanje načel nujnosti, sorazmernosti in zakonitosti ter ustrezni zaščitni ukrepi glede odgovornosti in pravnih sredstev, hkrati pa omogoči učinkovit odziv za zaščito posameznikov, zlasti najranljivejših.

Pomembna pravna, praktična in podporna orodja so že na voljo, vendar jih je treba okrepiti in bolje izvajati. Občuten napredek je bil dosežen pri izboljšanju izmenjave informacij in sodelovanja med obveščevalnimi službami držav članic ter omejevanju možnosti za delovanje teroristov in storilcev kaznivih dejanj. Vendar razdrobljenost ostaja.

Prizadevanja morajo preseči meje EU. Zaščita Unije ter njenih državljanov in državljank ne pomeni več le zagotavljanja varnosti znotraj meja EU, temveč tudi obravnavo zunanje razsežnosti varnosti. Pristop EU k zunanji varnosti v okviru skupne zunanje in varnostne politike (SZVP) ter skupne varnostne in obrambne politike (SVOP) bo še naprej bistven del prizadevanj EU za večjo varnost v EU. Sodelovanje s tretjimi državami in na svetovni ravni za obravnavanje skupnih izzivov je ključnega pomena za učinkovit in celovit odziv, pri čemer sta za varnost EU bistveni stabilnost in varnost v sosedstvu EU.

Ta nova strategija, ki temelji na predhodnem delu Evropskega parlamenta[4], Sveta[5] in Komisije[6], kaže, da mora resnična in učinkovita varnostna unija združevati trdno jedro instrumentov in politik, da zagotovi varnost v praksi, pri čemer je treba poudariti, da varnost vpliva na vse dele družbe in vse javne politike. EU mora zagotoviti varno okolje za vse, ne glede na njihovo rasno ali etnično pripadnost, vero, prepričanje, spol, starost ali spolno usmerjenost.

Ta strategija zajema obdobje 2020–2025 in se osredotoča na krepitev sposobnosti in zmogljivosti za zagotovitev varnostnega okolja, ki bo primerno za prihodnost. Določa pristop celotne družbe k varnosti, ki se lahko učinkovito in usklajeno odziva na hitro se spreminjajočo krajino groženj. Opredeljuje strateške prednostne naloge in ustrezne ukrepe za celostno obravnavo digitalnih in fizičnih tveganj v celotnem ekosistemu varnostne unije, pri čemer se osredotoča na področja, na katerih lahko EU zagotovi dodatno vrednost. Njen cilj je zagotoviti varnostno dividendo za zaščito vseh ljudi v EU.

II. Hitro spreminjajoča se krajina varnostnih groženj v Evropi

Varnost, blaginja in dobrobit državljank in državljanov so odvisne od varnosti. Grožnje tej varnosti so odvisne od tega, v kolikšni meri so ranljiva njihova življenja in možnosti za preživljanje. Večja kot je ranljivost, večje je tveganje za njeno izkoriščanje. Ranljivosti in grožnje se stalno razvijajo, zato se mora EU prilagoditi.

V vsakdanjem življenju se poslužujemo številnih storitev, kot so energetika, promet, finance in zdravstvo. Te storitve temeljijo tako na fizični kot tudi na digitalni infrastrukturi, kar še prispeva k ranljivosti in možnostim za motnje. Med pandemijo COVID-19 so nove tehnologije omogočile, da so številna podjetja in javne službe lahko nadaljevale z delom, saj so vzdrževale povezave za delo na daljavo in ohranjale logistiko dobavnih verig. S tem pa so se tudi odprla vrata za izjemno povečanje števila zlonamernih napadov, ki so poskušali

[4] Na primer delo odbora Evropskega parlamenta TERR, ki je poročal novembra 2018.

[5] Od sklepov Sveta iz junija 2015 o prenovljeni strategiji notranje varnosti do novejših sklepov Sveta iz decembra 2019.

[6] Izvajanje evropske agende za varnost z namenom boja proti terorizmu ter utiranja poti k učinkoviti in pravi varnostni uniji (COM(2016) 230 final z dne 20. aprila 2016). Glej nedavno oceno izvajanja zakonodaje na področju notranje varnosti: Implementation of Home Affairs legislation in the field of internal security – 2017–2020 (SWD(2020) 135).

motnje zaradi pandemije in prehod na digitalno delo od doma izkoristiti za kriminalne namene[7]. Zaradi pomanjkanja blaga so nastale nove priložnosti za organizirani kriminal. Posledice bi bile lahko usodne, saj bi lahko nastale motnje osnovnih zdravstvenih storitev v času največjega pritiska.

Zaradi vedno večjih možnosti uporabe digitalnih tehnologij v vsakdanjem življenju je postala **kibernetska varnost** tehnologij strateško pomembna[8]. Kibernetski napadi so velik problem za gospodinjstva, banke, finančne storitve in podjetja (zlasti mala in srednja). Potencialna škoda je še večja zaradi soodvisnosti fizičnih in digitalnih sistemov; vsakršen fizičen učinek bo vplival tudi na digitalne sisteme, kibernetski napadi na informacijske sisteme in digitalne infrastrukture pa lahko zaustavijo bistvene storitve[9]. Vzpon interneta stvari in večja uporaba umetne inteligence bosta prinesla nove koristi in nov sklop tveganj.

Naš svet temelji na digitalnih infrastrukturah, tehnologijah in spletnih sistemih, ki nam omogočajo, da ustvarjamo podjetja, nakupujemo in uporabljamo storitve. Vse to temelji na komunikaciji in interakciji. Odvisnost od spleta je omogočila val **kibernetske kriminalitete**[10]. Kibernetska kriminaliteta kot storitev in neformalna ekonomija kibernetske kriminalitete omogočata enostaven dostop do produktov in storitev kibernetske kriminalitete na spletu. Storilci kaznivih dejanj se hitro prilagajajo uporabi novih tehnologij za svoje namene. V zakonito dobavno verigo farmacevtskih izdelkov so na primer vstopila lažna in ponarejena zdravila[11]. Eksponentna rast količine spletnega gradiva, ki prikazuje spolno zlorabo otrok[12], kaže na družbene posledice spreminjajočih se vzorcev kaznivih dejanj. Nedavna raziskava je pokazala, da je večina ljudi v EU (55 %) zaskrbljenih zaradi morebitnega dostopa storilcev kaznivih dejanj in goljufov do njihovih podatkov[13].

Te grožnje povečuje tudi **svetovno okolje**. Agresivne industrijske politike tretjih držav skupaj z neprekinjeno krajo intelektualne lastnine, ki jo omogočajo kibernetske tehnologije, spreminjajo strateško paradigmo za zaščito in spodbujanje evropskih interesov. To je še bolj poudarjeno zaradi vedno večje uporabe tehnologij z dvojno rabo, zaradi česar je močan civilni tehnološki sektor zelo pomemben za obrambne in varnostne zmogljivosti. Industrijsko vohunjenje ima pomembne posledice za gospodarstvo, delovna mesta in rast v EU; kibernetske kraje poslovnih skrivnosti naj bi po ocenah stale 60 milijard EUR[14]. Zato je treba temeljito razmisliti o tem, kako odvisnost in vse večja izpostavljenost kibernetskim grožnjam vplivata na zmožnost EU, da zaščiti posameznike in podjetja.

---

7 Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (april 2020).

8 Priporočilo Komisije o kibernetski varnosti omrežij 5G (C(2019) 2335), Sporočilo o varni uvedbi tehnologije 5G v EU – izvajanje nabora orodij EU (COM(2020) 50).

9 Univerzitetna bolnišnica v Brnu na Češkem je morala marca 2020 zaradi kibernetskega napada preusmeriti bolnike in odložiti operacije (Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis). Umetna inteligenca se lahko zlorablja za digitalne, politične in fizične napade ter za nadzor. Zbiranje podatkov pri uporabi interneta stvari se lahko uporabi za nadzor posameznikov (pametne ure, govorni pomočniki itd.).

10 Glede na nekatere napovedi naj bi stroški kršitev varstva podatkov do leta 2024 znašali 5 bilijonov USD letno; leta 2015 so znašali 3 bilijone USD (Juniper Research, The Future of Cybercrime & Security).

11 Po ocenah študije iz leta 2016 (Legiscript) le 4 % spletnih lekarn na svetovni ravni deluje zakonito, pri čemer so potrošniki v EU glavna tarča za 30 000–35 000 nezakonitih spletnih lekarn.

12 Strategija EU za učinkovitejši boj proti spolni zlorabi otrok (COM(2020) 607).

13 Agencija Evropske unije za temeljne pravice (2020): Your rights matter: Security concerns and experiences, Fundamental Rights Survey, Luxembourg, Urad za publikacije.

14 The scale and impact of industrial espionage and theft of trade secrets through cyber, 2018.

Kriza zaradi COVID-19 je tudi izpostavila, da so socialne delitve in negotovosti vzrok za ranljivost na področju varnosti. To povečuje možnosti za bolj izpopolnjene in **hibridne napade** državnih in nedržavnih akterjev, ki izkoriščajo ranljivosti s kombinacijo kibernetskih napadov, škode na kritični infrastrukturi[15], dezinformacijskih kampanj in radikalizacije političnega diskurza[16].

Hkrati se že bolj uveljavljene grožnje še naprej razvijajo. V letu 2019 se je število **terorističnih napadov** v EU zmanjšalo. Vendar napadi džihadistov, ki so člani Daiša, Al Kaide in povezanih organizacij ali jih posnemajo, za državljane in državljanke EU še vedno predstavljajo veliko grožnjo[17]. Hkrati se povečuje tudi grožnja nasilnega desničarskega ekstremizma[18]. Zaradi rasističnih napadov bi morali biti resno zaskrbljeni; smrtonosni antisemitski teroristični napad v Halleju služi kot opomin, da je treba okrepiti odziv v skladu z izjavo Sveta iz leta 2018[19]. Ena oseba od petih v EU je zelo zaskrbljena, da bo v naslednjih 12 mesecih prišlo do terorističnega napada[20]. Velika večina nedavnih terorističnih napadov so bili „nizkotehnološki“ napadi, tj. posamezniki, ki so napadli posameznike na javnih mestih, teroristična propaganda na spletu pa je dobila nove razsežnosti z neposrednim prenosom napadov v Christchurchu v živo[21]. Grožnja, ki jo predstavljajo radikalizirani posamezniki, je še vedno velika in jo morda še povečujejo vračajoči se teroristični bojevniki in skrajneži, izpuščeni iz zapora[22].

Kriza je tudi pokazala, da se lahko obstoječe grožnje v novih okoliščinah še razvijajo. **Organizirane kriminalne združbe** izkoriščajo pomanjkanje blaga, ki omogoča vzpostavljanje novih nezakonitih trgov. Nedovoljen promet s prepovedanimi drogami ostaja največji kriminalni trg v EU in po ocenah dosega najmanj 30 milijard EUR letno[23]. Trgovina z ljudmi se nadaljuje; po ocenah znaša letni dobiček na svetovni ravni za vse oblike izkoriščanja skoraj 30 milijard EUR[24]. Mednarodna trgovina s ponarejenimi farmacevtski izdelki je dosegla 38,9 milijarde EUR[25]. Hkrati pa lahko storilci kaznivih dejanj zaradi majhnega števila zasegov še naprej širijo svoje kriminalne dejavnosti in vdirajo v zakonito gospodarstvo[26]. Storilci kaznivih dejanj in teroristi imajo prek spletnega trga in novih tehnologij, kot je 3D-tiskanje, lažji dostop do strelnega orožja[27]. Uporaba umetne

---

15 Kritična infrastruktura je bistvena za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi, katerih motnje ali uničenje bi imeli resne posledice (Direktiva Sveta št. 114/2008/ES).

16 97 % državljanov in državljank EU se je že srečalo z lažnimi novicami, 38 % se z njimi srečuje dnevno. Glej JOIN(2020) 8 final.

17 13 držav članic EU je poročalo o skupaj 119 izvedenih, neuspešnih in preprečenih terorističnih napadih, ki so povzročili 10 smrtnih žrtev in 27 ranjenih (Europol, European Union Terrorism Situation and Trend Report, 2020).

18 V letu 2019 se je zvrstilo šest skrajno desničarskih terorističnih napadov (v treh državah članicah; eden je bil uspešen, eden je spodletel, štirje pa so bili preprečeni), medtem ko je bil leta 2018 samo en teroristični napad. Nadaljnje smrtne žrtve so povzročili tudi napadi, ki se nišo šteli za teroristične (Europol, 2020).

19 Glej tudi Izjavo Sveta o boju proti antisemitizmu in vzpostavitvi skupnega varnostnega pristopa za boljšo zaščito judovskih skupnosti in ustanov v Evropi.

20 Agencija EU za temeljne pravice: Your rights matter: Security concerns and experiences, 2020.

21 Od julija 2015 do konca leta 2019 je Europol odkril teroristične vsebine na 361 platformah (Europol, 2020).

22 Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism, 2019.

23 Poročilo Evropskega centra za spremljanje drog in zasvojenosti z drogami (EMCDDA) in Europola: EU Drug Markets Report 2019.

24 Poročilo Europola o finančnem poslovnem modelu trgovine z ljudmi (2015).

25 Poročilo Urada EU za intelektualno lastnino in OECD o trgovini s ponarejenimi farmacevtskimi izdelki.

26 Poročilo o povrnitvi in odvzemu sredstev: Zagotavljanje, da se kriminal ne splača (COM(2020) 217).

27 Leta 2017 je bilo v 41 % vseh terorističnih napadov uporabljeno strelno orožje (Europol, 2018).

inteligence, novih tehnologij in robotike bo še povečala tveganje zlonamerne uporabe inovacij s strani storilcev kaznivih dejanj[28].

Te grožnje obsegajo več kategorij in na različne načine ogrožajo različne dele družbe. Vse pa so zelo nevarne za posameznike in podjetja, zato zahtevajo celovit in skladen odziv na ravni EU. Če lahko ranljivost na področju varnosti predstavljajo že majhni medsebojno povezani aparati v gospodinjstvu, na primer hladilnik ali avtomat za kavo, ki sta povezana z internetom, se za zagotavljanje varnosti ne moremo več zanašati le na tradicionalne državne akterje. Gospodarski subjekti morajo prevzeti večjo odgovornost za kibernetsko varnost proizvodov in storitev, ki jih dajo na trg, posamezniki pa morajo poznati vsaj osnove kibernetske varnosti, da se lahko zaščitijo sami.

III. Na ravni EU usklajen odziv za celotno družbo

EU je že pokazala, da lahko zagotovi resnično dodano vrednost. Od leta 2015 je varnostna unija zagotovila nove povezave pri obravnavi varnostnih politik na ravni EU. Vendar je treba storiti več, da se vključi celotna družba, tudi vlade na vseh ravneh, podjetja v vseh sektorjih in posamezniki v vseh državah članicah. Vse večja ozaveščenost o nevarnosti odvisnosti[29] in potreba po močni evropski industrijski strategiji[30] kažeta, da mora imeti EU kritično maso industrije in tehnološke proizvodnje ter odporno dobavno verigo. Moč pomeni tudi polno spoštovanje temeljnih pravic in vrednot EU, ki so pogoj za legitimne, učinkovite in trajnostne varnostne politike. Ta strategija za varnostno unijo določa konkretne delovne tokove, ki so potrebni za nadaljnje delo. Temelji na naslednjih skupnih ciljih:

- ***Krepitev zmogljivosti za zgodnje odkrivanje in preprečevanje kriz ter hitro odzivanje nanje:*** Evropa mora biti odpornejša, da bo lahko preprečevala oziroma vzdržala prihodnje pretrese. Vzpostaviti moramo zmogljivosti za zgodnje odkrivanje varnostnih kriz in hitro odzivanje nanje s celostnim in usklajenim pristopom, tako na splošno kot tudi s sektorskimi pobudami (na primer v finančnem, energetskem, pravosodnem, zdravstvenem, pomorskem in prometnem sektorju ter sektorju kazenskega pregona), in sicer na podlagi obstoječih orodij in pobud[31]. Komisija bo predstavila tudi predloge za obsežen sistem kriznega upravljanja v EU, ki bi bil lahko relevanten tudi za varnost.
- ***Osredotočenost na rezultate***: Strategija, usmerjena v uspešnost, mora temeljiti na skrbni oceni groženj in tveganj, da bi bila naša prizadevanja čim bolj učinkovita. Opredeliti in uporabljati mora ustrezna pravila in orodja. Potrebuje zanesljive strateške obveščevalne podatke kot podlago za varnostne politike EU. Kadar je potrebna zakonodaja EU, jo je treba izvajati v celoti, da bi preprečili razdrobljenost in vrzeli, ki bi jih bilo mogoče izkoriščati. Učinkovito izvajanje te strategije bo odvisno tudi od zagotovitve ustreznih

[28] Francoski in nizozemski organi kazenskega pregona in pravosodni organi so julija 2020 skupaj z Europolom in Eurojustom predstavili skupno preiskavo za razbitje EncroChata, šifriranega telefonskega omrežja, ki so ga uporabljale kriminalne združbe, vpletene v nasilne napade, korupcijo, poskuse umorov in obsežen promet z drogami.

[29] Tveganja zaradi zunanje odvisnosti vključujejo večjo izpostavljenost potencialnim grožnjam, od izkoriščanja ranljivosti infrastrukture IT, ki ogroža kritično infrastrukturo (npr. na področju energetike, prometa, bančništva ali zdravstva), ali prevzema nadzora nad industrijskimi nadzornimi sistemi do večjih možnosti za krajo podatkov ali vohunjenje.

[30] Sporočilo Komisije: Nova industrijska strategija za Evropo (COM(2020) 102).

[31] Na primer enotna ureditev EU za politično odzivanje na krize (IPCR), Center za usklajevanje nujnega odziva, Priporočilo Komisije o usklajenem odzivu na velike kibernetske incidente in krize (C(2017) 6100), operativni protokol EU za preprečevanje hibridnih groženj (SWD(2016) 227).

sredstev v naslednjem programskem obdobju 2021–2027, tudi za povezane agencije EU.

- ***Povezovanje vseh akterjev v javnem in zasebnem sektorju z namenom sodelovanja:*** Ključni akterji v javnem in zasebnem sektorju niso naklonjeni izmenjavi informacij, pomembnih za varnost, in sicer zato, da ne bi ogrozili nacionalne varnosti ali svoje konkurenčnosti[32]. Vendar smo najučinkovitejši takrat, kadar vsi podpiramo drug drugega. To pomeni predvsem tesnejše sodelovanje med državami članicami, vključno z organi kazenskega pregona, pravosodnimi in drugimi javnimi organi, ter z institucijami in agencijami EU, da bi dosegli razumevanje in izmenjavo, ki sta potrebni za skupne rešitve. Ključnega pomena je tudi sodelovanje z zasebnim sektorjem, zlasti zato, ker ima industrija v lasti pomemben del digitalne in nedigitalne infrastrukture, ki je bistvena za učinkovit boj proti kriminalu in terorizmu. Prispevajo lahko tudi posamezniki, na primer z nadgrajevanjem veščin in ozaveščenostjo za boj proti kibernetski kriminaliteti ali dezinformacijam. Skupna prizadevanja morajo prav tako preseči naše meje in vzpostaviti je treba tesnejše vezi s podobno mislečimi partnerji.

IV. Zaščita vseh ljudi v EU: strateške prednostne naloge varnostne unije

EU je v edinstvenem položaju, da se lahko odziva na te nove grožnje in izzive na svetovni ravni. Zgornja analiza groženj kaže na štiri medsebojno odvisne strateške prednostne naloge, ki jim je treba slediti na ravni EU ob polnem spoštovanju temeljnih pravic: (i) varnostno okolje, primerno za prihodnost, (ii) obravnavanje spreminjajočih se groženj, (iii) zaščita Evropejcev in Evropejk pred terorizmom in organiziranim kriminalom (iv) trden evropski varnostni ekosistem.

1. Varnostno okolje, primerno za prihodnost

Zaščita in odpornost kritične infrastrukture

V vsakdanjem življenju, pri potovanjih, delu ali uporabi osnovnih javnih storitev, na primer v zdravstvu, prevozu ali energetiki, ter pri uveljavljanju demokratičnih pravic se zanašamo na ključne infrastrukture. Če te infrastrukture niso dovolj zaščitene in odporne, lahko napadi povzročijo velike motnje – fizične ali digitalne – tako v posameznih državah članicah kot tudi v vsej EU.

Obstoječi okvir EU za zaščito in odpornost kritičnih infrastruktur[33] zaostaja za razvojem tveganj. Vse večja soodvisnost pomeni, da lahko motnje v enem sektorju takoj vplivajo na delovanje drugih sektorjev; napad na proizvodnjo električne energije bi lahko onesposobil telekomunikacije, bolnišnice, banke ali letališča, napad na digitalno infrastrukturo pa bi lahko povzročil motnje v omrežjih za električno energijo ali finančnem sektorju. Ker se naše gospodarstvo in družba vedno bolj selita na splet, so taka tveganja vedno večja. Zakonodajni okvir mora upoštevati to vse večjo medsebojno povezanost in soodvisnost. Potrebni so trdni ukrepi za zaščito in odpornost kritične infrastrukture, tako kibernetske kot tudi fizične. Bistvene storitve, vključno s tistimi, ki temeljijo na vesoljski infrastrukturi, morajo biti ustrezno zaščitene pred sedanjimi in pričakovanimi grožnjami, pa tudi odporne. To pomeni,

[32] Skupno sporočilo o odpornosti, odvračanju in obrambi: okrepitev kibernetske varnosti za EU (JOIN(2017) 450).

[33] Direktiva (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016), Direktiva Sveta (ES) št. 114/2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite.

da mora biti sistem sposoben, da predvidi neželene dogodke, se pripravi nanje, jih nevtralizira, si opomore po njih ter se jim bolje prilagodi.

Hkrati države članice uveljavljajo svojo diskrecijsko pravico, tako da obstoječo zakonodajo izvajajo na različne načine. Posledična razdrobljenost lahko ogrozi notranji trg in oteži čezmejno usklajevanje – najočitneje v obmejnih regijah. Subjekti, ki nudijo bistvene storitve v različnih državah članicah, morajo upoštevati različne režime poročanja. Komisija proučuje, ali bi lahko **novi okviri za fizične in digitalne infrastrukture** zagotovili večjo doslednost in skladnejši pristop k zagotavljanju zanesljivega izvajanja osnovnih storitev. Ta okvir je treba dopolniti s **sektorskimi pobudami** za obravnavanje specifičnih tveganj, s katerimi se soočajo kritične infrastrukture, kot so prometne, vesoljske, energetske, finančne in zdravstvene infrastrukture[34]. Glede na veliko odvisnost finančnega sektorja od storitev IT in njegovo veliko izpostavljenost kibernetskim napadom bo prvi korak pobuda o digitalni operativni odpornosti finančnega sektorja. Zaradi posebnih občutljivih točk in učinka energetskega sistema bo posebna pobuda podpirala večjo odpornost kritične energetske infrastrukture na fizične, kibernetske in hibridne grožnje, s čimer se bodo zagotovili enaki pogoji za energetske operaterje prek meja.

Učinki neposrednih tujih naložb na varnost, ki bi lahko vplivali na kritične infrastrukture ali kritične tehnologije, bodo prav tako predmet ocen, ki jih bodo izvedle države članice EU in Komisija v okviru novega evropskega okvira za pregled neposrednih tujih naložb[35].

EU lahko vzpostavi tudi nova orodja za podporo odpornosti kritičnih infrastruktur. Svetovni splet je doslej pokazal visoko stopnjo odpornosti, zlasti kar zadeva zmožnost podpore povečanemu obsegu prometa. Vendar pa moramo biti pripravljeni na morebitne prihodnje krize, ki bi ogrožale varnost, stabilnost in odpornost interneta. Zagotoviti je treba, da bo internet še naprej deloval in bo odporen na kibernetske incidente in zlonamerne spletne dejavnosti, ter omejiti odvisnost od infrastruktur in storitev, ki se nahajajo zunaj Evrope. Za to bo potrebna kombinacija zakonodaje (s pregledom obstoječih pravil, da se zagotovi visoka skupna raven varnosti omrežij in informacijskih sistemov v EU); dodatnih naložb v raziskave in inovacije ter uvajanja ali utrjevanja ključnih internetnih infrastruktur in virov, zlasti sistema domenskih imen[36].

Ključni element za zaščito ključnih digitalnih dobrin EU in nacionalnih digitalnih dobrin je, da se kritičnim infrastrukturam zagotovi kanal za varno komunikacijo. Komisija sodeluje z državami članicami, da bi vzpostavila certificirano in varno zemeljsko in vesoljsko kvantno infrastrukturo od konca do konca, in sicer v kombinaciji z varnim vladnim satelitskim komunikacijskim sistemom iz uredbe o vesoljskem programu[37].

---

[34] Glede na to, da je med krizo zaradi COVID-19 pod pritiskom zlasti zdravstveni sektor, bo Komisija razmislila tudi o pobudah za okrepitev okvira EU za zdravstveno varnost in pristojnih agencij EU za odzivanje na resne čezmejne zdravstvene grožnje.

[35] Z Uredbo (EU) 2019/452 Evropskega parlamenta in Sveta z dne 19. marca 2019 o vzpostavitvi okvira za pregled neposrednih tujih naložb v Uniji, ki se bo začela v celoti uporabljati 11. oktobra 2020, bo EU dobila nov mehanizem sodelovanja v zvezi z neposrednimi tujimi naložbami iz držav zunaj EU, ki bi lahko vplivale na varnost ali javni red. V skladu z uredbo bodo države članice in Komisija ocenile morebitna tveganja, povezana s takimi neposrednimi tujimi naložbami, in predlagale ustrezne načine za zmanjšanje teh tveganj, če bo to primerno in relevantno za več kot eno državo članico.

[36] Sistem domenskih imen (DNS) je hierarhičen in decentraliziran sistem dodeljevanja imen za računalnike, storitve ali druge vire, ki so povezani z internetom ali zasebnimi omrežji. Domenska imena prevede v naslove IP, ki so potrebni za lociranje in prepoznavanje računalniških storitev in naprav.

[37] Predlog uredbe o vzpostavitvi vesoljskega programa Unije in ustanovitvi Agencije Evropske unije za vesoljski program (COM(2018) 447).

Kibernetska varnost

Število kibernetskih napadov se še naprej povečuje[38]. Ti napadi so bolj izpopolnjeni kot kadar koli prej, prihajajo iz različnih virov v EU in zunaj nje, usmerjeni pa so na najranljivejša področja. Pogosto so udeleženi državni akterji ali akterji, ki imajo podporo države, napade pa usmerjajo v ključne digitalne infrastrukture, kot so veliki ponudniki storitev v oblaku[39]. Kibernetska tveganja so postala pomembna grožnja za finančni sistem. Mednarodni denarni sklad je letno izgubo zaradi kibernetskih napadov ocenil na 9 % neto prihodkov bank v svetovnem merilu oziroma približno 100 milijard USD[40]. Prehod na povezane naprave uporabnikom nudi mnoge prednosti, vendar glede na to, da se manj podatkov hrani in obdeluje v podatkovnih središčih, več pa se jih obdeluje bližje uporabniku („na robu“)[41], kibernetska varnost ne bo mogla biti več osredotočena na zaščito osrednjih točk[42].

EU je leta 2017 predstavila pristop h kibernetski varnosti s krepitvijo odpornosti, hitrim odzivanjem in učinkovitim odvračanjem[43]. Zdaj mora zagotoviti, da bodo njene zmogljivosti na področju kibernetske varnosti v koraku z dejanskimi razmerami, da bo mogoče zagotoviti odpornost in odziv. Zato morajo biti vključeni celotna družba, pri čemer morajo institucije, agencije in organi EU, države članice, industrija, akademski krogi in posamezniki kibernetsko varnost obravnavati prednostno[44]. Ta horizontalni pristop je treba ponovno dopolniti s sektorskimi pristopi h kibernetski varnosti na področjih, kot so energetika, finančne storitve, promet in zdravstvo. Naslednjo fazo prizadevanj EU je treba opredeliti v revidirani strategiji Evropske unije za kibernetsko varnost.

Proučevanje novih in okrepljenih oblik sodelovanja med obveščevalnimi službami, EU INTCEN in drugimi organizacijami s področja varnosti bi moralo biti del prizadevanj za izboljšanje kibernetske varnosti ter boja proti terorizmu, ekstremizmu, radikalizmu in hibridnim grožnjam.

Glede na uvajanje **infrastrukture 5G** v EU in potencialno odvisnost mnogih kritičnih storitev od omrežij 5G bi bile posledice sistemskih in obsežnih motenj še posebej resne. Na podlagi postopka, vzpostavljenega s priporočilom Komisije iz leta 2019 o kibernetski varnosti omrežij 5G[45], so države članice zdaj začele izvajati ključne ukrepe, določene z naborom orodij 5G[46].

Ena od najpomembnejših dolgoročnih potreb je vzpostavitev kulture **vgrajene kibernetske varnosti**, kjer je varnost od samega začetka vgrajena v proizvode in storitve. Pomemben

---

38 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

39 Porazdeljeni napadi za zavrnitev storitve so stalna grožnja; večji ponudniki so utrpeli obsežne tovrstne napade, na primer Amazon Web Service februarja 2020.

40 https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/

41 Računalništvo na robu je porazdeljena odprta arhitektura IT z decentralizirano računalniško močjo, ki omogoča tehnologije mobilnega računalništva in interneta stvari. Pri računalništvu na robu podatke obdeluje sama naprava ali pa lokalni računalnik ali strežnik, namesto da bi se posredovali v podatkovni center.

42 Sporočilo o evropski strategiji za podatke (COM(2020) 66 final).

43 Skupno sporočilo o odpornosti, odvračanju in obrambi: okrepitev kibernetske varnosti za EU (JOIN(2017) 450).

44 Poročilo Skupnega raziskovalnega središča o kibernetski varnosti kot našem digitalnem sidru zagotavlja večrazsežnosten vpogled v razvoj kibernetske varnosti v zadnjih 40 letih.

45 Priporočilo Komisije o kibernetski varnosti omrežij 5G (C(2019) 2335 final). V priporočilu je predviden njegov pregled v zadnjem četrtletju leta 2020.

46 Glej poročilo Skupine za sodelovanje na področju varnosti omrežij in informacij o izvajanju nabora orodij z dne 24. julija 2020.

prispevek k temu bo novi certifikacijski okvir za kibernetsko varnost na podlagi uredbe o kibernetski varnosti[47]. Okvir je že v pripravi, in sicer se pripravljata dve certifikacijski shemi, pozneje letos pa bodo določene prednostne naloge za nadaljnje sheme. Sodelovanje med Agencijo EU za kibernetsko varnost (ENISA), organi za varstvo podatkov in Evropskim odborom za varstvo podatkov[48] je ključnega pomena na tem področju.

Komisija je že ugotovila, da je za strukturirano in usklajeno operativno sodelovanje potrebna **skupna kibernetska enota**. Ta bi lahko vključevala mehanizem vzajemne pomoči v času krize na ravni EU. Skupna kibernetska enota bi lahko na podlagi izvajanja načrta iz priporočila[49] ustvarila zaupanje med različnimi akterji v evropskem ekosistemu kibernetske varnosti in državam članicam nudila ključne storitve. Komisija bo do konca leta 2020 na podlagi razprav z relevantnimi zainteresiranimi stranmi (najprej z državami članicami) določila jasen postopek, mejnike in časovni načrt.

Pomembna so tudi skupna pravila o informacijski in kibernetski varnosti za vse institucije, organe in agencije EU. Cilj bi morala biti vzpostavitev obveznih in visokih skupnih standardov za varno izmenjavo informacij ter varnost digitalnih infrastruktur in sistemov v vseh institucijah, organih in agencijah EU. Ta novi okvir naj bi bil podlaga za močno in učinkovito operativno sodelovanje na področju kibernetske varnosti v institucijah, organih in agencijah EU, osrednjo vlogo pa naj bi imela skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU).

Zaradi globalne narave kibernetskih napadov je za njihovo nadaljnje preprečevanje, odvračanje od njih ter odzivanje nanje ključno vzpostavljanje in vzdrževanje trdnih **mednarodnih partnerstev**. Okvir za skupni diplomatski odziv EU na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“)[50] določa ukrepe v okviru skupne zunanje in varnostne politike, vključno z omejevalnimi ukrepi (sankcijami), ki se lahko uporabijo proti dejavnostim, ki škodijo političnim, varnostnim in gospodarskim interesom EU. EU bi morala tudi poglobiti svoje delo prek skladov za razvoj in sodelovanje, da bi se zagotovila krepitev zmogljivosti za podporo partnerskim državam pri krepitvi njihovih digitalnih ekosistemov, sprejemanju nacionalnih zakonodajnih reform in spoštovanju mednarodnih standardov. To povečuje odpornost celotne skupnosti in njeno sposobnost, da se zoperstavi kibernetskim grožnjam in se nanje učinkovito odziva. To vključuje posebno delo za spodbujanje standardov EU in ustrezne zakonodaje za povečanje kibernetske varnosti partnerskih držav v sosedstvu[51].

Varovanje javnih prostorov

Nedavni teroristični napadi so bili osredotočeni na **javne prostore**, vključno z verskimi objekti in prometnimi vozlišči, pri čemer so izkoristili njihovo odprtost in dostopnost. Zaradi porasta terorizma, ki ga je sprožil politično ali ideološko motiviran ekstremizem, se je grožnja za javne prostore še povečala. Potrebni so tako večja fizična zaščita takih krajev kot

[47] Uredba (EU) 2019/881 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti).

[48] Sporočilo o varstvu podatkov kot stebru krepitve vloge državljanov in pristopa EU k digitalnemu prehodu – dve leti uporabe splošne uredbe o varstvu podatkov (COM(2020) 264).

[49] Priporočilo Komisije (EU) 2017/1584 o usklajenem odzivu na velike kibernetske incidente in krize.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/sl/pdf

[51] Glej smernice EU za krepitev zunanjih kibernetskih zmogljivosti, ki so bile sprejete v sklepih Sveta z dne 26. junija 2018.

tudi ustrezni sistemi odkrivanja, ki ne bi ogrožali svoboščin državljank in državljanov[52]. Komisija bo pri varovanju javnih prostorov okrepila sodelovanje med javnim in zasebnim sektorjem, in sicer s financiranjem, izmenjavo izkušenj in dobrih praks, posebnimi smernicami[53] in priporočili[54]. Del pristopa bodo tudi ozaveščanje, zahteve glede učinkovitosti in testiranje opreme za odkrivanje ter izboljšanje preverjanja preteklosti oseb za obravnavanje notranjih groženj. Pomemben vidik, ki ga je treba upoštevati, je dejstvo, da so lahko manjšine in ranljive osebe nesorazmerno prizadete, vključno z osebami, ki so tarče zaradi veroizpovedi ali spola, zato jim je treba nameniti posebno pozornost. Regionalni in lokalni javni organi imajo pomembno vlogo pri izboljševanju varnosti javnih prostorov. Komisija pomaga tudi pri spodbujanju inovacij mest na področju varnosti javnih prostorov[55]. Začetek novega partnerstva v okviru agende EU za mesta[56] na področju „varnosti javnih prostorov“ novembra 2018 odraža močno zavezanost držav članic, Komisije in mest, da bolje obravnavajo grožnje varnosti v mestih.

Trg za **drone** se še naprej širi, pri čemer imajo ti veliko koristnih in zakonitih možnosti uporabe. Prav tako pa jih lahko zlorabljajo storilci kaznivih dejanj in teroristi, pri čemer so posebej ogroženi javni prostori. Tarče so lahko posamezniki, skupine ljudi, kritična infrastruktura, organi kazenskega pregona, meje ali javni prostori. Znanje o uporabi dronov v konfliktih bi se lahko vračalo v Evropo, in sicer neposredno (z vračanjem tujih terorističnih bojevnikov) ali prek spleta. Pravila, ki jih je že pripravila Evropska agencija za varnost v letalstvu, so pomemben prvi korak na področjih, kot sta registracija upravljavcev dronov in obvezna identifikacija dronov na daljavo. Ker droni postajajo vedno bolj dostopni, cenovno ugodni in zmogljivejši, so potrebni dodatni ukrepi. Ti bi lahko vključevali izmenjavo informacij, smernice in dobre prakse za vse, vključno s kazenskim pregonom, ter več preskušanja protiukrepov za drone[57]. Poleg tega bi bilo treba nadalje analizirati in obravnavati tudi posledice uporabe dronov v javnih prostorih za zasebnost in varstvo podatkov.

Ključni ukrepi
• zakonodaja o zaščiti in odpornosti kritične infrastrukture • revizija direktive o varnosti omrežij in informacijskih sistemov • pobuda o operativni odpornosti finančnega sektorja • zaščita in kibernetska varnost kritične energetske infrastrukture in omrežni kodeks za kibernetsko varnost za čezmejni pretok električne energije • strategija Evropske unije za kibernetsko varnost • nadaljnji ukrepi za vzpostavitev skupne kibernetske enote • skupna pravila o informacijski in kibernetski varnosti za institucije, organe in agencije

[52] Posebno pozornost zaslužijo sistemi za biometrično identifikacijo na daljavo. Začetna stališča Komisije so navedena v njeni beli knjigi z dne 19. februarja 2020 o umetni inteligenci (COM(2020) 65).

[53] Na primer smernice za izbiro ustreznih varnostnih pregrad za varovanje javnih prostorov (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Smernice o dobrih praksah so navedene v dokumentu SWD(2019) 140, vključno z oddelkom o javno-zasebnem sodelovanju. Poseben poudarek financiranja v okviru Sklada za notranjo varnost – policija je na krepitvi javno-zasebnega sodelovanja.

[55] Tri mesta (Pirej v Grčiji, Tampere na Finskem in Torino v Italiji) bodo preskušala nove rešitve v okviru inovativnih urbanističnih ukrepov, ki jih sofinancira Evropski sklad za regionalni razvoj (ESRR).

[56] Agenda EU za mesta predstavlja nov način dela na več ravneh, ki spodbuja sodelovanje med državami članicami, mesti, Evropsko komisijo in drugimi zainteresiranimi stranmi, da bi se spodbujale rast, kakovost življenja in inovacije v evropskih mestih ter prepoznavali in uspešno reševali družbeni izzivi.

[57] Nedavno je bil vzpostavljen večletni program preskušanja za podporo državam članicam pri razvoju skupne metodologije in preskusne platforme na tem področju.

EU
- okrepljeno sodelovanje za varovanje javnih prostorov, vključno z verskimi objekti
- izmenjava najboljših praks za obravnavanje zlorabe dronov

2. Obravnavanje spreminjajočih se groženj

Kibernetska kriminaliteta

Tehnologija prinaša družbi nove priložnosti. Prav tako ponuja nova orodja za pravosodje ter kazenski pregon. Hkrati pa odpira vrata storilcem kaznivih dejanj. Vse pogostejši so uporaba zlonamerne programske opreme, kraja osebnih ali poslovnih podatkov z vdori v računalniške sisteme in prekinitve digitalnih dejavnosti, ki povzročajo finančno škodo ali škodo za ugled. Prva obramba je odporno okolje, ki je rezultat močne kibernetske varnosti. Organi kazenskega pregona morajo biti usposobljeni za digitalne preiskave in imeti jasna pravila za preiskovanje in pregon kaznivih dejanj ter žrtvam zagotoviti potrebno zaščito. To delo bi moralo temeljiti na skupni projektni skupini za ukrepanje proti kibernetski kriminaliteti pri Europolu in protokolu za odzivanje organov kazenskega pregona na izredne razmere, ki je bil vzpostavljen za usklajevanje odzivanja na obsežne kibernetske napade. Ključni so tudi učinkoviti mehanizmi, ki omogočajo javno-zasebna partnerstva in sodelovanje.

Hkrati bi moral postati boj proti kibernetski kriminaliteti strateška prednostna naloga na področju komuniciranja v vsej EU, da bi se Evropejce in Evropejke opozarjalo na tveganja in preventivne ukrepe, ki so jim na voljo. To bi moralo biti del proaktivnega pristopa. Ključen korak je tudi polno izvajanje sedanjega pravnega okvira[58]; Komisija bo pripravljena, da po potrebi uporabi postopke za ugotavljanje kršitev ter pregleda ta okvir, da bi zagotovila, da bo še naprej primeren za svoj namen. Komisija bo skupaj z Europolom in Agencijo EU za kibernetsko varnost (ENISA) proučila tudi, ali je mogoče na ravni EU vzpostaviti sistem zgodnjega opozarjanja na področju kibernetske kriminalitete, ki bi lahko zagotovil pretok informacij in hitro odzivanje pri porastu kibernetske kriminalitete.

Kibernetska kriminaliteta je svetovni izziv in zahteva učinkovito mednarodno sodelovanje. EU podpira Budimpeško konvencijo Sveta Evrope o kibernetski kriminaliteti, ki je učinkovit in dobro uveljavljen okvir, ki vsem državam omogoča, da opredelijo, katere sisteme in komunikacijske kanale morajo vzpostaviti za učinkovito skupno delo.

Skoraj polovica državljank in državljanov EU je zaskrbljena zaradi morebitne zlorabe podatkov[59] in **kraje identitete**[60]. Eden od vidikov zlorabe identitete je pridobitev finančnih koristi, ima pa lahko tudi velik osebni in psihološki učinek, saj lahko nezakonite objave s strani storilca kaznivega dejanja ostanejo na spletu več let. Komisija bo proučila možne praktične ukrepe za zaščito žrtev pred vsemi oblikami kraje identitete, pri čemer bo upoštevala prihodnjo pobudo o evropski digitalni identiteti[61].

---

[58] Direktiva 2013/40/EU o napadih na informacijske sisteme.

[59] Tj. 46 % (raziskava Eurobarometer o odnosu Evropejcev do kibernetske varnosti, januar 2020).

[60] Velika večina vprašanih v raziskavi Eurobarometer iz leta 2018 o odnosu Evropejcev do varnosti na internetu (95 %) je menila, da je kraja identitete hudo kaznivo dejanje, sedem od desetih pa jih je navedlo, da gre za zelo hudo kaznivo dejanje. Raziskava Eurobarometer, ki je bila objavljena januarja 2020, je potrdila zaskrbljenost glede kibernetske kriminalitete, spletnih prevar in kraje identitete; dve tretjini anketirancev sta bili zaskrbljeni zaradi bančnih goljufij (67 %) ali kraje identitete (66 %).

[61] Sporočilo z dne 19. februarja 2020 o oblikovanju digitalne prihodnosti Evrope (COM(2020) 67).

Za boj proti kibernetski kriminaliteti je potrebna usmerjenost v prihodnost. Ker družba uporablja nov tehnološki razvoj za krepitev gospodarstva in družbe, lahko tudi storilci kaznivih dejanj ta orodja izkoriščajo za škodljive namene. Storilci kaznivih dejanj lahko na primer uporabljajo umetno inteligenco za odkrivanje in prepoznavanje gesel ali poenostavitev izdelave zlonamerne programske opreme ter da pridobijo slike ali zvočne posnetke, ki se lahko nato uporabijo za krajo identitete ali goljufijo.

Sodoben pristop h kazenskemu pregonu

Organi kazenskega pregona in pravosodni delavci se morajo prilagoditi novim tehnologijam. Zaradi tehnološkega razvoja in novih groženj morajo imeti organi kazenskega pregona dostop do novih orodij, pridobivati nova znanja in spretnosti ter razvijati alternativne preiskovalne tehnike. Za dopolnitev zakonodajnih ukrepov, namenjenih izboljšanju čezmejnega dostopa do elektronskih dokazov za kazenske preiskave, lahko EU pomaga organom kazenskega pregona pri razvoju potrebnih zmogljivosti za odkrivanje, zavarovanje in branje podatkov, ki so potrebni za preiskovanje kaznivih dejanj, ter uporabo teh podatkov kot dokaznega gradiva na sodišču. Komisija bo proučila ukrepe za **okrepitev zmogljivosti organov kazenskega pregona pri digitalnih preiskavah**, pri čemer bo opredelila, kako čim bolje izkoristiti raziskave in razvoj za vzpostavljanje novih orodij za kazenski pregon ter kako lahko usposabljanje organom kazenskega pregona in pravosodju zagotovi ustrezen nabor znanj in spretnosti. To bo vključevalo tudi zagotavljanje strogih znanstvenih ocen in testnih metod v okviru Skupnega raziskovalnega središča Komisije.

Skupni pristopi lahko tudi zagotovijo, da se **umetna inteligenca**, **vesoljske zmogljivosti**, **velepodatki** in **visokozmogljivostno računalništvo** vključijo v varnostno politiko na način, ki je učinkovit tako v boju proti kaznivim dejanjem kot tudi pri zagotavljanju temeljnih pravic. Umetna inteligenca bi lahko bila močno orodje za boj proti kriminalu, saj bi omogočila ogromne preiskovalne zmogljivosti z analiziranjem velikih količin informacij ter prepoznavanjem vzorcev in anomalij[62]. Prav tako lahko zagotovi konkretna orodja, kot so pomoč pri prepoznavanju spletnih terorističnih vsebin, odkrivanje sumljivih transakcij pri prodaji nevarnih izdelkov ali nudenje pomoči državljankam ali državljanom v nujnih primerih. Uresničitev tega potenciala pomeni povezovanje raziskav, inovacij in uporabnikov umetne inteligence z ustreznim upravljanjem in tehnično infrastrukturo, pri čemer so dejavno vključeni zasebni sektor in akademski krogi. Pomeni tudi zagotavljanje najvišjih standardov spoštovanja temeljnih pravic ob hkratnem zagotavljanju učinkovite zaščite državljank in državljanov. Odločitve, ki vplivajo na posameznike, morajo pregledati ljudje, morajo pa biti tudi skladne z ustrezno veljavno zakonodajo EU[63].

Za približno 85 % preiskav hudih kaznivih dejanj so potrebne elektronske informacije in dokazi, pri čemer je v 65 % preiskav treba vložiti zahtevek pri ponudnikih iz drugih jurisdikcij[64]. Dejstvo, da so se tradicionalne materialne sledi premaknile na splet, še povečuje vrzel med zmogljivostmi na področju kazenskega pregona in zmogljivostmi storilcev kaznivih dejanj. Bistvenega pomena je vzpostavitev jasnih pravil glede čezmejnega dostopa do elektronskih dokazov za kazenske preiskave. Zato je treba hitro sprejeti predloga Evropskega parlamenta in Sveta o elektronskih dokazih, da se preiskovalcem zagotovi učinkovito orodje. Prav tako je za vzpostavitev združljivih pravil na mednarodni ravni

[62] Na primer pri finančnem kriminalu.

[63] To pomeni skladnost z obstoječo zakonodajo, vključno s splošno uredbo o varstvu podatkov ((EU) 2016/679) in direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj ((EU) 2016/680), ki ureja obdelavo osebnih podatkov za namene preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali izvrševanja kazenskih sankcij.

[64] SWD(2018) 118 final.

ključnega pomena čezmejni dostop do elektronskih dokazov prek večstranskih in dvostranskih mednarodnih pogajanj[65].

Dostop do **digitalnih dokazov** je odvisen tudi od razpoložljivosti informacij. Če se podatki izbrišejo prehitro, lahko pomembni dokazi izginejo, z njimi pa možnost identifikacije in izsleditve osumljencev in kriminalnih mrež (kot tudi žrtev). Po drugi strani pa se zaradi sistemov hrambe podatkov porajajo vprašanja glede varstva zasebnosti. Komisija bo na podlagi izida zadev, ki jih trenutno obravnava Evropsko sodišče, ocenila, kateri bodo nadaljnji koraki na področju hrambe podatkov.

Za kazenske preiskave, kibernetsko varnost in varstvo potrošnikov so pomembne informacije o registraciji internetnih domenskih imen (v nadaljnjem besedilu: podatki WHOIS)[66], vendar je dostop do njih vedno težji. Organizacija za dodeljevanje spletnih imen in številk (ICANN) trenutno pripravlja novo politiko za te podatke. Komisija bo še naprej sodelovala z organizacijo ICANN in skupnostjo več zainteresiranih strani, da bi se zagotovilo, da lahko tisti, ki imajo upravičen razlog za to, vključno zaradi kazenskega pregona, dejansko pridobijo dostop do podatkov WHOIS v skladu s predpisi EU in mednarodnimi predpisi o varstvu podatkov. To bo vključevalo presojo možnih rešitev, med drugim tudi to, ali je potrebna zakonodaja, ki bi pojasnjevala pravila za dostop do takih informacij.

Ko bo v EU v celoti vzpostavljena **arhitektura 5G za mobilne telekomunikacije**, bodo morali organi kazenskega pregona ter pravosodni organi prav tako imeti možnost, da pridobijo potrebne podatke in dokaze, ob spoštovanju zaupnosti komunikacij. Komisija bo podprla okrepljen in usklajen pristop k oblikovanju mednarodnih standardov, opredelitvi najboljših praks in postopkov ter vzpostavitvi tehnične interoperabilnosti na ključnih tehnoloških področjih, kot so umetna inteligenca, internet stvari ali tehnologije veriženja blokov.

Dandanes velik del preiskav vseh oblik kaznivih dejanj in terorizma vključuje **šifrirane podatke**. Šifriranje je bistvenega pomena za digitalni svet ter varovanje digitalnih sistemov in transakcij, pa tudi za varstvo vrste temeljnih pravic, vključno s svobodo izražanja, pravico do zasebnosti in pravico do varstva podatkov. Vendar lahko tudi zakrije identiteto storilcev in vsebino njihovih komunikacij, če se uporablja za kazniva dejanja. Komisija bo preučila in podprla uravnotežene tehnične, operativne in pravne rešitve za te izzive ter spodbujala pristop, ki ohranja učinkovitost šifriranja pri varstvu zasebnosti in varnosti komunikacij, obenem pa zagotavlja učinkovit odziv na kriminal in terorizem.

Boj proti nezakonitim spletnim vsebinam

Usklajevanje varnosti spletnega in fizičnega okolja pomeni nadaljnje korake v **boju proti nezakonitim spletnim vsebinam**. Vse več ključnih groženj za državljane in državljanke, kot so terorizem, ekstremizem in spolna zloraba otrok, temelji na digitalnem okolju, zato so potrebni konkretni ukrepi in okvir za zagotavljanje spoštovanja temeljnih pravic. Bistven prvi korak je hiter zaključek pogajanj o predlagani zakonodaji o terorističnih spletnih vsebinah[67] in zagotavljanje njenega izvajanja. Za boj proti zlorabi interneta s strani teroristov, nasilnih skrajnežev in storilcev kaznivih dejanj je ključnega pomena tudi okrepitev prostovoljnega sodelovanja med organi kazenskega pregona in zasebnim

[65] Zlasti Drugi dodatni protokol k Budimpeški konvenciji Sveta Evrope o kibernetski kriminaliteti in sporazum med EU in Združenimi državami Amerike o čezmejnem dostopu do elektronskih dokazov.

[66] Shranjene v zbirkah podatkov, ki jih vzdržuje 2 500 upraviteljev registrov po vsem svetu.

[67] Predlog o preprečevanju razširjanja terorističnih spletnih vsebin (COM(2018) 640 z dne 12. septembra 2018).

sektorjem v okviru **internetnega foruma EU**. Osrednjo vlogo pri spremljanju dejavnosti terorističnih skupin na spletu in ukrepov, ki jih sprejemajo platforme[68], ter pri nadaljnjem razvoju **kriznega protokola EU**[69] bo še naprej imela enota EU za prijavljanje internetnih vsebin v okviru Europola. Poleg tega bo Komisija še naprej sodelovala z mednarodnimi partnerji, tudi z udeležbo v **svetovnem internetnem forumu za boj proti terorizmu**, da bi se ti izzivi obravnavali na svetovni ravni. Nadaljevala se bodo tudi prizadevanja za razvoj alternativnih diskurzov in protinaracij v okviru programa za krepitev vloge civilne družbe[70].

Komisija je leta 2016 za preprečevanje širjenja nezakonitega sovražnega govora na spletu in boj proti njemu predstavila kodeks ravnanja za odpravo nezakonitega sovražnega govora na spletu, ki vključuje prostovoljno zavezo spletnih platform, da bodo odstranjevale vsebine s sovražnim govorom. Najnovejša ocena kaže, da podjetja 90 % označenih vsebin pregledajo v 24 urah in odstranijo 71 % vsebin, ki jih ocenijo kot nezakonit sovražni govor. Vendar morajo platforme nadalje izboljšati preglednost in povratne informacije za uporabnike ter zagotoviti dosledno ocenjevanje označenih vsebin[71].

Internetni forum EU bo tudi olajšal izmenjavo informacij o obstoječih in razvijajočih se tehnologijah za obravnavo izzivov, povezanih s spolno zlorabo otrok na spletu. Boj proti spolni zlorabi otrok na spletu je v središču nove strategije za učinkovitejši **boj proti spolni zlorabi otrok**[72]. Njen namen je čim boljša uporaba orodij, ki so na voljo na ravni EU za boj proti tem kaznivim dejanjem. Podjetja morajo biti sposobna nadaljevati svoje delo za odkrivanje in odstranjevanje spletnega gradiva, ki prikazuje spolno zlorabo otrok. Zaradi škode, ki jo to gradivo povzroča, pa je potreben okvir z jasnimi in trajnimi obveznostmi za reševanje problema. V strategiji bo poleg tega napovedano, da bo Komisija začela pripravljati tudi sektorsko zakonodajo za učinkovitejši boj proti spolni zlorabi otrok na spletu, in sicer ob polnem spoštovanju temeljnih pravic.

Splošneje pa bo tudi prihodnji akt o digitalnih storitvah pojasnil in nadgradil pravila o odgovornosti in varnosti za digitalne storitve ter odpravil dejavnike, ki odvračajo od ukrepov za obravnavanje nezakonitih vsebin, blaga ali storitev.

Poleg tega bo Komisija še naprej sodelovala z mednarodnimi partnerji in **svetovnim internetnim forumom za boj proti terorizmu**, tudi prek neodvisnega svetovalnega odbora, da bi prispevala k razpravam o tem, kako bi lahko te izzive obravnavali na svetovni ravni, obenem pa ohranili vrednote EU in temeljne pravice. Obravnavati bi bilo treba tudi nova področja, kot so algoritmi ali spletne igre[73].

Hibridne grožnje

Obseg in raznolikost hibridnih groženj še nikoli nista bila tako velika kot danes. To se je pokazalo tudi med krizo zaradi COVID-19, saj je več državnih in nedržavnih akterjev želelo izkoristiti pandemijo, zlasti z manipuliranjem informacijskega okolja in izrabljanjem temeljnih infrastruktur. To bi lahko oslabilo socialno kohezijo in spodkopalo zaupanje v institucije EU in vlade držav članic.

---

[68] Europol, november 2019.

[69] Evropa, ki varuje – Krizni protokol EU: odziv na teroristične spletne vsebine (oktober 2019).

[70] Povezan z delom programa za ozaveščanje o radikalizaciji, glej oddelek IV.3 spodaj.

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] Strategija EU za učinkovitejši boj proti spolni zlorabi otrok (COM(2020) 607).

[73] Teroristi vse pogosteje uporabljajo sporočilne sisteme platform za spletne igre za komunikacijo, mladi teroristi pa v videoigrah preigravajo nasilne napade.

Pristop EU k hibridnim grožnjam je opredeljen v skupnem okviru iz leta 2016[74] in skupnem sporočilu o okrepitvi odpornosti na hibridne grožnje iz leta 2018[75]. Ukrepe na ravni EU podpira obsežna zbirka orodij, ki zajemajo povezavo med notranjo in zunanjo varnostjo in temeljijo na pristopu, ki vključuje celotno družbo, ter na tesnem sodelovanju s strateškimi partnerji, zlasti Natom in skupino G7. Skupaj s to strategijo je objavljeno poročilo o izvajanju pristopa EU k hibridnim grožnjam[76]. Na podlagi evidentiranja[77], predstavljenega vzporedno s to strategijo, bodo službe Komisije in Evropska služba za zunanje delovanje vzpostavile **spletno platformo z omejenim dostopom**, na kateri bodo države članice lahko preverile orodja in ukrepe, ki so na voljo na ravni EU za preprečevanje hibridnih groženj.

Zaradi tesnih povezav z nacionalnimi varnostnimi in obrambnimi politikami je preprečevanje hibridnih groženj predvsem odgovornost držav članic, vendar so nekatere ranljivosti skupne vsem državam članicam, nekatere grožnje pa segajo prek meja, na primer grožnje za čezmejna omrežja ali infrastrukture. Komisija in visoki predstavnik bosta oblikovala pristop EU k hibridnim grožnjam, ki bo neprekinjeno povezoval zunanjo in notranjo razsežnost ter združeval nacionalna in vseevropska vprašanja. Ta pristop mora zajemati ves spekter ukrepov – od zgodnjega odkrivanja, analize, ozaveščenosti, krepitve odpornosti in preprečevanja do odzivanja na krize in obvladovanja posledic.

Poleg okrepljenega izvajanja bo, glede na nenehen razvoj hibridnih groženj, posebna pozornost namenjena **vključevanju vprašanj hibridnih groženj v oblikovanje politik**, da ostanemo v koraku z dinamičnimi spremembami in zagotovimo, da se ne spregleda nobena morebiti pomembna pobuda. Učinki novih pobud bodo ocenjeni tudi z vidika hibridnih groženj, vključno s pobudami na področjih, ki so bila doslej zunaj okvira za preprečevanje hibridnih groženj, kot so izobraževanje, tehnologija in raziskave. Za ta pristop bi lahko bilo koristno delo, vloženo v konceptualizacijo hibridnih groženj, ki je celovit pregled različnih orodij, ki bi jih lahko uporabili nasprotniki[78]. Prizadevati bi si morali za to, da bo postopek odločanja podpiralo redno, izčrpno in na obveščevalnih podatkih temelječe poročanje o razvoju hibridnih groženj. To bo močno odvisno od obveščevalnih podatkov držav članic in nadaljnjega izboljšanja sodelovanja z njihovimi pristojnimi službami na področju obveščevalnih podatkov prek centra EU INTCEN.

Za razvoj **situacijskega zavedanja** bodo službe Komisije in Evropska služba za zunanje delovanje preučile možnosti za poenostavitev pretoka informacij iz različnih virov, vključno z državami članicami, pa tudi agencijami EU, kot so ENISA, Europol in Frontex. Hibridna fuzijska celica EU bo še naprej informacijska točka EU za ocene ogroženosti zaradi hibridnih groženj. **Krepitev odpornosti** je osrednjega pomena za preprečevanje hibridnih groženj in zaščito pred njimi. Zato je ključno, da se napredek na tem področju sistematično spremlja in objektivno meri. Prvi korak bo opredelitev sektorskih izhodišč za odpornost proti hibridnim grožnjam, tako za države članice kot tudi za institucije in organe EU. Nazadnje bi bilo treba za okrepitev **pripravljenosti za odzivanje na hibridne krize** pregledati obstoječi operativni protokol EU za preprečevanje hibridnih groženj iz leta

[74] Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije (JOIN(2016) 18).

[75] Povečanje odpornosti in krepitev zmogljivosti za obravnavanje hibridnih groženj (JOIN(2018) 16).

[76] Poročilo o izvajanju skupnega okvira o preprečevanju hibridnih groženj iz leta 2016 ter skupnega poročila o povečanju odpornosti in krepitvi zmogljivosti za obravnavanje hibridnih groženj iz leta 2018 (SWD(2020) 153).

[77] Evidentiranje ukrepov za povečanje odpornosti in preprečevanje hibridnih groženj (SWD(2020) 152).

[78] Skupno raziskovalno središče in Evropski center za preprečevanje hibridnih groženj: The Landscape of Hybrid Threats: A conceptual Model, JRC117280.

2016[79], da bi odražal širši pregled in okrepitev sistema EU za odzivanje na krize, ki se trenutno obravnavata[80]. Cilj je čim bolj povečati učinek ukrepanja EU s hitrim združevanjem sektorskih odzivov in zagotavljanjem nemotenega sodelovanja z našimi partnerji, predvsem Natom.

Ključni ukrepi
• zagotavljanje, da se zakonodaja o kibernetski kriminaliteti izvaja in da je primerna za svoj namen • strategija za učinkovitejši boj proti spolni zlorabi otrok • predlogi za odkrivanje in odstranjevanje gradiva, ki prikazuje spolno zlorabo otrok • pristop EU k preprečevanju hibridnih groženj • pregled operativnega protokola EU za preprečevanje hibridnih groženj (EU Playbook) • ocena možnosti za okrepitev zmogljivosti za kazenski pregon pri digitalnih preiskavah

3. Zaščita Evropejcev in Evropejk pred terorizmom in organiziranim kriminalom

Terorizem in radikalizacija

Teroristična grožnja v EU ostaja visoka. Kljub temu, da se je skupno število napadov zmanjšalo, imajo lahko še vedno uničujoč učinek. Radikalizacija lahko tudi širše polarizira in destabilizira socialno kohezijo. Boj proti terorizmu in radikalizaciji je še vedno predvsem odgovornost držav članic, vendar so zaradi vse večje čezmejne/medsektorske razsežnosti grožnje potrebni nadaljnji koraki v smeri sodelovanja in usklajevanja v EU. Prednostna naloga je učinkovito izvajanje zakonodaje EU na področju boja proti terorizmu, vključno z omejevalnimi ukrepi[81]. Še naprej je cilj razširiti mandat Evropskega javnega tožilstva na čezmejna teroristična kazniva dejanja.

Boj proti terorizmu se začne z odpravljanjem temeljnih vzrokov zanj. Polarizacija družbe, dejanska ali zaznana diskriminacija ter drugi psihološki in sociološki dejavniki lahko povečajo dojemljivost ljudi za radikalni govor. S tega vidika je boj proti **radikalizaciji** tesno povezan s spodbujanjem socialne kohezije na lokalni, nacionalni in evropski ravni. V zadnjih desetih letih so bile razvite številne pobude in politike s pomembnim učinkom, zlasti prek mreže za ozaveščanje o radikalizaciji in pobude Mesta v EU proti radikalizaciji[82]. Zdaj je treba razmisliti o ukrepih za racionalizacijo politik, pobud in skladov EU za boj proti radikalizaciji. Takšni ukrepi lahko podprejo razvoj zmogljivosti in spretnosti, izboljšajo sodelovanje, okrepijo dokazno podlago in pomagajo pri oceni napredka z vključevanjem vseh upoštevnih zainteresiranih strani, vključno s strokovnjaki na terenu, oblikovalci politik in akademskimi krogi[83]. Tudi mehke politike, kot so izobraževanje, kultura, mladi in šport,

[79] Operativni protokol EU za preprečevanje hibridnih groženj (EU Playbook) (SWD(2016) 227).

[80] Člani Evropskega sveta so po videokonferenci z dne 26. marca 2020 sprejeli izjavo o ukrepih EU v odziv na izbruh COVID-19 in pozvali Komisijo, naj pripravi predloge za ambicioznejši in obsežnejši sistem kriznega upravljanja v EU.

[81] Svet je s ciljem boja proti terorizmu sprejel omejevalne ukrepe v zvezi z ISIL (Daiš) in Al Kaido ter posebne omejevalne ukrepe proti nekaterim osebam in subjektom. Glej zemljevid sankcij EU (https://www.sanctionsmap.eu/) za pregled vseh omejevalnih ukrepov (https://www.sanctionsmap.eu/#/main).

[82] Dvojni cilj pilotne pobude Mesta v EU proti radikalizaciji je spodbujanje izmenjave strokovnega znanja med mesti EU in zbiranje povratnih informacij o tem, kako bi lahko lokalne skupnosti najbolje podprli na ravni EU.

[83] Na primer financiranje v okviru Evropskega sklada za varnost in programa za državljanstvo.

bi lahko prispevale k preprečevanju radikalizacije ter zagotovile priložnosti za ogrožene mlade in kohezijo v EU[84]. Prednostna področja vključujejo delo pri zgodnjem odkrivanju in obvladovanju tveganja, krepitvi odpornosti, deradikalizaciji ter rehabilitaciji in reintegraciji v družbo.

Teroristi si prizadevajo za pridobitev **kemičnih, bioloških, radioloških in jedrskih** (KBRJ)[85] snovi, da bi jih uporabili kot orožje, ter za razvoj znanja in zmožnosti za njihovo uporabo[86]. Možnost napadov KBRJ je pomemben del teroristične propagande. Glede na veliko potencialno škodo, ki jo lahko povzročijo, je treba tem napadom nameniti posebno pozornost. Komisija bo na podlagi pristopa, ki se uporablja za reguliranje dostopa do predhodnih sestavin za eksplozive, preučila možnost omejitve dostopa do nekaterih nevarnih kemikalij, ki bi se lahko uporabile za izvedbo napadov. Ključnega pomena bo tudi razvoj zmogljivosti za odziv EU na področju civilne zaščite (rescEU) v zvezi z napadi KBRJ. Pomembno je tudi sodelovanje s tretjimi državami, da bi se okrepila skupna kultura varnosti in zaščite pred napadi KBRJ, pri čemer je treba v celoti izkoristiti svetovne centre odličnosti KBRJ EU. To sodelovanje bo vključevalo nacionalne ocene vrzeli in tveganj, podporo nacionalnim in regionalnim akcijskim načrtom KBRJ, izmenjavo dobrih praks in dejavnosti krepitve zmogljivosti na področju KBRJ.

EU je razvila najnaprednejšo zakonodajo na svetu za omejevanje dostopa do **predhodnih sestavin za eksplozive**[87] in odkrivanje sumljivih transakcij z namenom izdelave improviziranih eksplozivnih naprav. Toda grožnja zaradi doma izdelanih eksplozivov je še vedno velika, saj so bili ti eksplozivi uporabljeni v več napadih po EU[88]. Prvi korak mora biti izvajanje pravil in zagotavljanje, da spletno okolje ne omogoča izogibanja nadzoru.

Pomemben element politike za boj proti terorizmu je tudi učinkovit pregon storilcev terorističnih kaznivih dejanj, vključno s **tujimi terorističnimi bojevniki**, ki so trenutno v Siriji in Iraku. Čeprav ta vprašanja v prvi vrsti obravnavajo države članice, jim lahko usklajevanje in podpora na ravni EU pomagata pri reševanju skupnih izzivov. Pomembno vlogo bodo imela tudi tekoča prizadevanja za polno izvajanje zakonodaje na področju varnosti meja[89] in uporabo vseh ustreznih podatkovnih zbirk EU v celoti za izmenjavo informacij o znanih osumljencih. Poleg prepoznavanja posameznikov, ki predstavljajo veliko tveganje, je potrebna politika reintegracije in rehabilitacije. Medpoklicno sodelovanje, tudi z osebjem v zaporih in probacijskimi uslužbenci, bo okrepilo pravosodno razumevanje procesa radikalizacije, ki vodi v nasilni ekstremizem, in pristop pravosodja k izrekanju kazni in alternativam pridržanju.

Izziv tujih terorističnih bojevnikov značilno ponazarja povezavo med notranjo in **zunanjo varnostjo**. Sodelovanje na področju boja proti terorizmu ter preprečevanja radikalizacije in nasilnega ekstremizma ter boja proti njima je osrednjega pomena za varnost znotraj EU[90].

---

[84] Ukrepi EU, kot so virtualne izmenjave Erasmus+ in e-twinning.

[85] V zadnjih dveh letih je bilo na primer v Evropi (Franciji, Nemčiji in Italiji) in drugod (v Tuniziji in Indoneziji) več napadov z biološkimi sredstvi (običajno rastlinskimi toksini).

[86] Svet je sprejel omejevalne ukrepe proti širjenju in uporabi kemičnega orožja

[87] Kemikalije, ki bi se lahko zlorabile za doma izdelane eksplozive. Regulira jih Uredba (EU) 2019/1148 o trženju in uporabi predhodnih sestavin za eksplozive.

[88] Taki uničujoči napadi so bili med drugim izvedeni v Oslu (2011), Parizu (2015), Bruslju (2016) in Manchestru (2017). V napadu z doma izdelanim eksplozivom v Lyonu (2019) je bilo ranjenih 13 ljudi.

[89] Vključno z novimi pooblastili Evropske agencije za mejno in obalno stražo (Frontex).

[90] Svet je v sklepih z dne 16. junija 2020 poudaril, da je treba državljane in državljanke EU zaščititi pred terorizmom in nasilnim ekstremizmom v vseh njunih oblikah, ne glede na izvor, ter nadalje okrepiti zunanje ukrepanje EU v boju proti terorizmu in ukrepanje na nekaterih prednostnih geografskih in tematskih področjih.

Potrebni so nadaljnji ukrepi za razvoj partnerstev za boj proti terorizmu in sodelovanje z državami v sosedstvu in onkraj njega, pri čemer se je treba opreti na strokovno znanje mreže strokovnjakov EU za varnost/boj proti terorizmu. Dober primer takšnega ciljno usmerjenega sodelovanja je Skupni akcijski načrt za boj proti terorizmu za Zahodni Balkan. Zlasti bi si bilo treba prizadevati za podpiranje zmogljivosti partnerskih držav, da identificirajo in izsledijo tuje teroristične bojevnike. EU bo prav tako še naprej spodbujala večstransko sodelovanje z vodilnimi svetovnimi akterji na tem področju, kot so Združeni narodi, Nato, Svet Evrope, Interpol in OVSE. Udejstvovala se bo tudi v Globalnem forumu za boj proti terorizmu in svetovni koaliciji za boj proti Daišu ter sodelovala z ustreznimi akterji civilne družbe. Pri skupnih prizadevanjih s tretjimi državami za preprečevanje terorizma in piratstva imajo pomembno vlogo tudi instrumenti zunanje politike Unije, vključno z razvojem in sodelovanjem. Mednarodno sodelovanje je bistveno tudi za prekinitev vseh virov **financiranja terorizma**, na primer prek Projektne skupine za finančno ukrepanje.

Organizirani kriminal

Organizirani kriminal je povezan z visokimi gospodarskimi stroški in človeškim davkom. Ocenjuje se, da gospodarska izguba zaradi organiziranega kriminala in korupcije znaša od 218 do 282 milijard EUR letno[91]. Leta 2017 se je v Evropi preiskovalo več kot 5 000 organiziranih kriminalnih združb, kar je 50 % več kot leta 2013[92]. Organizirani kriminal vse bolj deluje čezmejno, tudi iz neposrednega sosedstva EU, kar kliče k okrepljenemu operativnemu sodelovanju in izmenjavi informacij s partnerji v sosedstvu.

Pojavljajo se novi izzivi, kriminal pa se seli na splet. Med pandemijo COVID-19 smo bili priča izrazitemu povečanju števila spletnih prevar, osredotočenih na ranljive skupine, zdravstveni in sanitarni izdelki pa so bili tarča vlomov in tatvin[93]. EU mora okrepiti boj proti organiziranemu kriminalu, tudi na mednarodni ravni, z več orodji za razbitje poslovnega modela organiziranega kriminala. Boj proti organiziranemu kriminalu zahteva tudi tesno sodelovanje z lokalnimi in regionalnimi upravami ter civilno družbo, ki so ključni partnerji pri preprečevanju kriminala, pa tudi pri zagotavljanju pomoči in podpore žrtvam, tako sodelovanje pa je najbolj potrebno med upravami v obmejnih regijah. Ta prizadevanja bodo združena v **agendi za boj proti organiziranemu kriminalu**.

Več kot tretjina organiziranih kriminalnih združb, dejavnih v EU, je vpletena v proizvodnjo in distribucijo prepovedanih drog ali nedovoljen promet z njimi. Zasvojenosti z drogami je leta 2019 botrovala več kot osem tisoč smrtim v EU zaradi prevelikega odmerka. Večina **nedovoljenega prometa s prepovedanimi drogami** poteka prek meja, velik del dobička iz njega pa vstopi v zakonito gospodarstvo[94]. Z novo agendo EU za boj proti drogam[95] se bodo okrepila prizadevanja EU in držav članic na področju zmanjševanja ponudbe drog in povpraševanja po njih, opredelili skupni ukrepi za obravnavanje skupnega problema ter izboljšala dialog in sodelovanje med EU in zunanjimi partnerji pri vprašanjih drog. Komisija bo po oceni Evropskega centra za spremljanje drog in zasvojenosti z drogami presodila, ali je treba njegov mandat glede na nove izzive posodobiti.

---

[91] V smislu bruto domačega proizvoda (BDP). Poročilo Europola iz leta 2016: Does crime still pay? – Criminal asset recovery in the EU.

[92] Europolovi oceni ogroženosti zaradi hudih kaznivih dejanj in organiziranega kriminala (SOCTA) iz let 2013 in 2017.

[93] Europol, 2020.

[94] Poročilo Evropskega centra za spremljanje drog in zasvojenosti z drogami (EMCDDA) in Europola iz novembra 2019: EU Drug Markets Report 2019.

[95] Agenda in akcijski načrt EU za boj proti drogam za obdobje 2021–2025 (COM(2020) 606).

Organizirane kriminalne združbe in teroristi so tudi ključni akterji v trgovini z **nezakonitim strelnim orožjem**. Med letoma 2009 in 2018 je v Evropi prišlo do 23 množičnih streljanj, v katerih je umrlo več kot 340 ljudi[96]. Strelno orožje se pogosto pretihotapi v EU prek njenega neposrednega sosedstva[97]. To kaže, da je treba okrepiti usklajevanje in sodelovanje tako znotraj EU kot tudi z mednarodnimi partnerji, zlasti z Interpolom, da bi se uskladila zbiranje informacij in poročanje o zasegih strelnega orožja. Poleg tega je bistveno, da se izboljša sledljivost orožja, vključno na spletu, in zagotovi izmenjava informacij med organi za izdajanje dovoljenj in organi kazenskega pregona. Komisija pripravlja nov **akcijski načrt EU za boj proti nedovoljeni trgovini s strelnim orožjem**[98] in bo prav tako ocenila, ali so pravila o izvoznih dovoljenjih ter uvoznih in tranzitnih ukrepih za strelno orožje še vedno primerna za svoj namen[99].

Kriminalne združbe migrante in ljudi, ki potrebujejo mednarodno zaščito, obravnavajo kot blago. 90 % migrantov brez urejenega statusa pride v EU prek kriminalnih mrež[100]. Tihotapljenje migrantov je pogosto povezano tudi z drugimi oblikami organiziranega kriminala, zlasti trgovino z ljudmi[101]. Poleg visokega človeškega davka, ki ga terja trgovina z ljudmi, Europol ocenjuje, da na svetovni ravni vse oblike izkoriščanja na podlagi trgovine z ljudmi ustvarijo letni dobiček v višini 29,4 milijarde EUR. To je mednarodni kriminal, ki ga omogoča nezakonito povpraševanje znotraj EU in zunaj nje ter vpliva na vse njene države članice. Zaradi slabih rezultatov pri prepoznavanju, pregonu in obsodbah teh kaznivih dejanj je potreben nov pristop k okrepitvi ukrepanja. Nov **celovit pristop k trgovini z ljudmi** bo povezal vsa področja ukrepanja. Poleg tega bo Komisija predstavila **nov akcijski načrt EU za boj proti tihotapljenju migrantov** za obdobje 2021–2025. Oba sklopa ukrepanja bosta osredotočena na boj proti kriminalnim mrežam, izboljšanje sodelovanja in podporo delu organov kazenskega pregona.

Organizirane kriminalne združbe in teroristi iščejo priložnosti tudi na drugih področjih, zlasti tistih, ki ustvarjajo visok dobiček ob nizkem tveganju odkritja, kot je **okoljska kriminaliteta**. Nezakonit lov in trgovina s prostoživečimi vrstami, nezakonito rudarjenje in sečnja ter nezakonito odlaganje in pošiljke odpadkov so postali četrta največja kriminalna dejavnost na svetu[102]. Pojavljajo se tudi zlorabe shem trgovanja z emisijami in shem energijskih izkaznic ter sredstev, namenjenih okoljski odpornosti in trajnostnemu razvoju. Komisija bo poleg spodbujanja ukrepov EU, držav članic in mednarodne skupnosti za okrepitev boja proti okoljski kriminaliteti[103] ocenila, ali je direktiva o okoljski kriminaliteti[104] še vedno primerna za svoj namen. Ena najdonosnejših kriminalnih dejavnosti je postala tudi **nedovoljena trgovina s kulturnimi dobrinami**, ki je vir financiranja teroristov in organiziranega kriminala ter je v porastu. Preučiti bi bilo treba možnosti za izboljšanje spletne in nespletne sledljivosti kulturnih dobrin na notranjem trgu in

[96] Flamski mirovni inštitut: Armed to kill, oktober 2019.

[97] EU od leta 2002 financira boj proti širjenju osebnega in lahkega orožja ter trgovini z njim v regiji; financirala je na primer mrežo strokovnjakov jugovzhodne Evrope za strelno orožje (SEEFEN). Partnerji z Zahodnega Balkana so od leta 2019 v celoti vključeni v prednostno nalogo v zvezi s strelnim orožjem Evropske večdisciplinarne platforme proti grožnjam kriminala (EMPACT).

[98] COM(2020) 608.

[99] Uredba (EU) št. 258/2012 o izvajanju člena 10 Protokola Združenih narodov o nedovoljeni proizvodnji strelnega orožja ter trgovini z njim.

[100] Vir: Europol.

[101] Četrto letno poročilo Europola in Evropskega centra za boj proti tihotapljenju migrantov (EMSC).

[102] UNEP in Interpol: Rapid Response Assessment: The Rise of Environmental Crime, junij 2016.

[103] Glej evropski zeleni dogovor (COM(2019) 640 final).

[104] Direktiva 2008/99/ES o kazenskopravnem varstvu okolja.

sodelovanja s tretjimi državami, v katerih se kulturne dobrine plenijo, ter zagotavljati dejavno podporo organom kazenskega pregona ter akademskim skupnostim.

Gospodarska in finančna kazniva dejanja so izjemno kompleksna, vsako leto pa prizadenejo milijone državljank in državljanov ter tisoče podjetij v EU. Boj proti goljufijam je osrednjega pomena in zahteva ukrepanje na ravni EU. Europol skupaj z Eurojustom, Evropskim javnim tožilstvom in Evropskim uradom za boj proti goljufijam podpira države članice in EU pri varovanju gospodarskih in finančnih trgov ter denarja davkoplačevalcev in davkoplačevalk EU. Evropsko javno tožilstvo bo postalo v celoti operativno konec leta 2020. Njegove naloge bodo preiskovanje, pregon in obtožba storilcev kaznivih dejanj zoper proračun EU, kot so goljufije, korupcija in pranje denarja. Prav tako bo obravnaval čezmejne goljufije na področju DDV, ki davkoplačevalce in davkoplačevalke stanejo vsaj 50 milijard EUR letno.

Komisija bo podpirala tudi razvoj strokovnega znanja in zakonodajnega okvira za nova tveganja, kot so kriptosredstva in novi plačilni sistemi. Zlasti bo preučila odziv na pojav kriptosredstev, kot je bitcoin, in učinek teh novih tehnologij na način izdajanja, izmenjave in delitve finančnih sredstev ter dostopa do njih.

Evropska unija bi morala imeti ničelno toleranco do nezakonitega denarja. EU je v tridesetih letih razvila trden regulativni okvir za preprečevanje **pranja denarja** in financiranja terorizma ter boj proti njima, ki v celoti spoštuje varstvo osebnih podatkov. Kljub temu obstaja vse širše soglasje, da je treba izvajanje sedanjega okvira znatno izboljšati ter obravnavati velike razlike v njegovi uporabi in resne pomanjkljivosti pri izvrševanju pravil. Kot je podrobno opisano v akcijskem načrtu iz maja 2020[105], trenutno poteka delo za oceno možnosti, na katere bi lahko okrepili okvir EU za preprečevanje pranja denarja in boj proti financiranju terorizma. Področja, ki jih je treba preučiti, vključujejo medsebojno povezovanje nacionalnih centraliziranih registrov bančnih računov, s čimer bi se lahko znatno pospešil dostop finančnoobveščevalnih enot in pristojnih organov do finančnih informacij.

Dobiček organiziranih kriminalnih združb v EU se ocenjuje na 110 milijard EUR letno. Trenutni odziv vključuje usklajeno zakonodajo o zaplembi in odvzemu premoženjske koristi[106], da bi se izboljšali zamrznitev in zaplemba sredstev, pridobljenih s kaznivim dejanjem, v EU ter spodbujalo vzajemno zaupanje in učinkovito čezmejno sodelovanje med državami članicami. Vendar pa se zapleni le približno 1 % tega dobička[107], kar organiziranim kriminalnim združbam omogoča, da vlagajo v širitev svojih kriminalnih dejavnosti in vdrejo v zakonito gospodarstvo, ključna tarča za pranje denarja pa so zlasti mala in srednja podjetja, ki imajo težave pri dostopu do posojil. Komisija bo preučila, kako se zakonodaja[108] izvaja in ali so morebiti potrebna nadaljnja skupna pravila, vključno o zaplembi brez kazenske obsodbe. Urade za odvzem premoženjske koristi[109], ki so ključni akterji v postopku odvzema premoženjske koristi, bi bilo mogoče opremiti z boljšimi orodji za hitrejše odkrivanje in sledenje sredstev po vsej EU, da bi se povečale stopnje zaplembe.

[105] Akcijski načrt za preprečevanje pranja denarja in boj proti financiranju terorizma (COM(2020) 2800).
[106] V skladu s pravom EU morajo vse države članice imeti urade za odvzem premoženjske koristi.
[107] Poročilo o povrnitvi in odvzemu sredstev: Zagotavljanje, da se kriminal ne splača (COM(2020) 217 final).
[108] Direktiva 2014/42/EU o začasnem zavarovanju in odvzemu predmetov, ki so bili uporabljeni za kazniva dejanja, in premoženjske koristi, pridobljene s kaznivim dejanjem.
[109] Sklep Sveta 2007/845/PNZ o sodelovanju med uradi za odvzem premoženjske koristi držav članic na področju sledenja in identifikacije premoženjske koristi, pridobljene s kaznivim dejanjem, ali drugega premoženja, povezanega s kaznivimi dejanji.

Organizirani kriminal je močno povezan s **korupcijo**. Ocenjeno je, da samo korupcija gospodarstvo EU stane približno 120 milijard EUR na leto[110]. Preprečevanje korupcije in boj proti njej se bosta še naprej redno spremljala v okviru mehanizma pravne države in evropskega semestra. V okviru evropskega semestra se ocenjujejo izzivi v boju proti korupciji, kot so javna naročila, javna uprava, poslovno okolje ali zdravstveno varstvo. Novo letno poročilo Komisije o stanju pravne države bo zajemalo boj proti korupciji in omogočalo preventivni dialog z nacionalnimi organi in zainteresiranimi stranmi na ravni EU in nacionalni ravni. Tudi organizacije civilne družbe imajo lahko ključno vlogo pri spodbujanju ukrepanja javnih organov na področju preprečevanja organiziranega kriminala in korupcije ter boja proti njima, te skupine pa bi bilo koristno združiti v skupnem forumu. Zaradi čezmejne narave organiziranega kriminala in korupcije je še ena od ključnih razsežnosti sodelovanje s sosednjimi regijami EU in zagotavljanje pomoči na tem področju.

Ključni ukrepi
• agenda EU za boj proti terorizmu, vključno s prenovljenimi ukrepi proti radikalizaciji v EU • novo sodelovanje s ključnimi tretjimi državami in mednarodnimi organizacijami za boj proti terorizmu • agenda za boj proti organiziranemu kriminalu, vključno s trgovino z ljudmi • agenda in akcijski načrt EU za boj proti drogam za obdobje 2021–2025 • ocena Evropskega centra za spremljanje drog in zasvojenosti z drogami • akcijski načrt EU za boj proti nedovoljeni trgovini s strelnim orožjem za obdobje 2020–2025 • pregled zakonodaje o zamrznitvi in zaplembi ter o uradih za odvzem premoženjske koristi • ocena direktive o okoljski kriminaliteti • akcijski načrt EU za boj proti tihotapljenju migrantov za obdobje 2021–2025

4. Trden evropski varnostni ekosistem

Prava in učinkovita varnostna unija mora biti skupni cilj vseh delov družbe. Vlade, organi kazenskega pregona, zasebni sektor, izobraževalne ustanove ter državljanke in državljani sami morajo biti dejavni, opremljeni in ustrezno povezani, da bi se povečala pripravljenost in odpornost vseh, zlasti najranljivejših, žrtev in prič.

Varnostna razsežnost mora biti vključena v vse politike in EU lahko prispeva na vseh ravneh. V domačem okolju je med najresnejšimi varnostnimi tveganji nasilje v družini. V EU je nasilje intimnega partnerja doživelo 22 % žensk[111]. Ključna prednostna naloga je še vedno pristop EU k Istanbulski konvenciji o preprečevanju nasilja nad ženskami in nasilja v družini ter o boju proti njima. Če bodo pogajanja še naprej blokirana, bo Komisija sprejela druge ukrepe z istimi cilji, kot so zastavljeni v konvenciji, vključno s predlogom, da se nasilje nad ženskami doda na seznam kaznivih dejanj EU, opredeljenih v Pogodbi.

Sodelovanje in izmenjava informacij

[110] Skupne gospodarske stroške korupcije je težko oceniti, vendar si za to prizadevajo različne organizacije, vključno z Mednarodno trgovinsko zbornico, Transparency International, Globalnim dogovorom ZN in Svetovnim gospodarskim forumom, katerih podatki kažejo, da korupcija znaša 5 % svetovnega BDP.

[111] Unija enakosti: strategija za enakost spolov za obdobje 2020–2025 (COM(2020) 152).

Eden od najpomembnejših načinov, na katerega lahko EU prispeva k zaščiti državljank in državljanov, je s pomočjo tistim, ki so odgovorni za varnost, da dobro sodelujejo. Sodelovanje in izmenjava informacij sta najmočnejši orodji za boj proti kriminalu in terorizmu ter uveljavljanje pravice. Da bi bila učinkovita, morata biti ciljno usmerjena in hitra. Da bi bila zaupanja vredna, ju je treba izvajati z uporabo skupnih zaščitnih ukrepov in kontrol.

Vzpostavljenih je bilo več instrumentov EU in sektorskih strategij[112] za nadaljnji razvoj **operativnega sodelovanja** med državami članicami na področju **kazenskega pregona**. Eden od glavnih instrumentov EU za podporo sodelovanju med državami članicami na tem področju je schengenski informacijski sistem, ki se uporablja za izmenjavo podatkov o iskanih in pogrešanih osebah in predmetih v realnem času. Rezultati so vidni pri prijetjih storilcev kaznivih dejanj, zasegih drog in rešitvah potencialnih žrtev[113]. Vendar bi se sodelovanje lahko še izboljšalo z racionalizacijo in nadgradnjo razpoložljivih instrumentov. Večji del pravnega okvira EU, ki je podlaga za operativno sodelovanje na področju kazenskega pregona, je bil zasnovan pred 30 leti. Zapletena mreža dvostranskih sporazumov med državami članicami, od katerih so številni zastareli ali se ne uporabljajo v zadostni meri, povzroča tveganje razdrobljenosti. V manjših ali neobalnih državah morajo uslužbenci organov kazenskega pregona, ki delujejo čezmejno, v nekaterih primerih operativne akcije izvajati ob upoštevanju do sedmih različnih sklopov pravil. Posledica tega je, da se nekatere operacije, kot je zasledovanje osumljencev onstran notranjih meja, preprosto ne izvajajo. Sedanji okvir EU prav tako ne vključuje operativnega sodelovanja z novimi tehnologijami, kot so droni.

Operativno učinkovitost je mogoče podpreti s posebnim sodelovanjem na področju kazenskega pregona, kar lahko prispeva tudi k zagotavljanju ključne podpore drugim ciljem politike, kot so prispevanje informacij o varnosti za novo oceno neposrednih tujih naložb. Komisija bo preučila, kako bi lahko to podprl kodeks policijskega sodelovanja. Organi kazenskega pregona v državah članicah vse pogosteje uporabljajo podporo in strokovno znanje na ravni EU. Ključno vlogo pri spodbujanju izmenjave strateških obveščevalnih podatkov med obveščevalnimi in varnostnimi službami držav članic ima Obveščevalni in situacijski center EU (EU INTCEN), ki zagotavlja informacije o situacijskem zavedanju na podlagi obveščevalnih podatkov v korist institucij EU[114]. Odločilno vlogo ima lahko tudi **Europol**, in sicer s širjenjem svojega sodelovanja s tretjimi državami v boju proti kriminalu in terorizmu ob upoštevanju drugih zunanjih politik in orodij EU. Vendar se Europol danes sooča s številnimi resnimi omejitvami, zlasti kar zadeva neposredno izmenjavo osebnih podatkov z zasebnimi subjekti, kar ga ovira pri učinkovitem podpiranju držav članic v boju proti terorizmu in kriminalu. Trenutno se ocenjuje, kako bi se lahko pooblastila Europola izboljšala, da bi lahko v celoti opravljal svoje naloge. S tega vidika bi morali tudi ustrezni organi na ravni EU (kot so OLAF, Europol, Eurojust in Evropsko javno tožilstvo) tesneje sodelovati in izboljšati izmenjavo informacij.

Druga ključna povezava je **Eurojust**. Z njegovim nadaljnjim razvojem bi bilo mogoče kar najbolj povečati sinergijo med sodelovanjem na področju kazenskega pregona in pravosodnim sodelovanjem. EU bi koristila tudi večja strateška usklajenost. **EMPACT**[115],

[112] Kot je akcijski načrt za strategijo EU za pomorsko varnost, ki je prinesel pomembne dosežke s sodelovanjem na področju nalog obalne straže med ustreznimi agencijami EU.
[113] Boj EU proti organiziranemu kriminalu leta 2019 (Svet, 2020).
[114] EU INTCEN je edini kanal, prek katerega obveščevalne in varnostne službe držav članic zagotavljajo informacije o situacijskem zavedanju na podlagi obveščevalnih podatkov za EU.
[115] Evropska večdisciplinarna platforma proti grožnjam kriminala.

cikel politike EU proti mednarodni organizirani kriminaliteti in hudim oblikam mednarodne kriminalitete, zagotavlja kazensko metodologijo na podlagi obveščevalnih podatkov za organe, ki se skupaj borijo proti najpomembnejšim grožnjam kriminala za EU. V zadnjih desetih letih je prinesel pomembne operativne rezultate[116]. Na podlagi izkušenj strokovnih delavcev bi bilo treba obstoječi mehanizem za novi cikel politike za obdobje 2022–2025 racionalizirati in poenostaviti, da bi bolje obravnaval najbolj pereče in spreminjajoče se grožnje.

Hitre in ustrezne **informacije** so ključnega pomena za vsakodnevno delo v boju proti kaznivim dejanjem. Kljub razvoju novih podatkovnih zbirk za varnost in upravljanje meja na ravni EU je veliko informacij še vedno shranjenih v nacionalnih podatkovnih zbirkah ali pa se izmenjujejo brez uporabe teh orodij. To pomeni precejšnjo dodatno delovno obremenitev, zamude in večje tveganje, da se ključne informacije spregledajo. Boljši, hitrejši in poenostavljeni postopki, ki bi vključevali vso varnostno skupnost, bi prinesli boljše rezultate. Prava orodja so bistvenega pomena, če želimo, da bo izmenjava informacij dosegla svoj potencial pri učinkovitem boju proti kriminalu, prav tako pa so potrebni zaščitni ukrepi, da se pri izmenjavi podatkov spoštujejo zakoni o varstvu podatkov in temeljne pravice. Glede na razvoj na področju tehnologije, forenzike in varstva podatkov ter spremenjene operativne potrebe bi lahko EU razmislila, ali bi bilo treba posodobiti instrumente, kot sta **Prümska sklepa iz leta 2008**, s katerima je bila vzpostavljena avtomatizirana izmenjava podatkov o DNK, prstnih odtisih in registraciji vozil, da se omogoči avtomatizirana izmenjava dodatnih kategorij podatkov, ki so že na voljo v kazenskih ali drugih podatkovnih zbirkah držav članic za namene kazenskih preiskav. Poleg tega bo Komisija preučila možnost izmenjave kazenskih evidenc, kar naj bi pomagalo pri preverjanju, ali oseba že ima kazensko evidenco v drugih državah članicah, in možnost olajšanja dostopa do teh evidenc, ko se odkrijejo, pri čemer bi se uporabljali vsi potrebni zaščitni ukrepi.

Informacije o potnikih so pomagale izboljšati mejne kontrole in prispevajo k zmanjšanju nedovoljenih migracijskih tokov ter prepoznavanju oseb, ki predstavljajo tveganje za varnost. Predhodne informacije o potniku so biografski podatki potnika, ki jih zberejo letalski prevozniki med prijavo na let in vnaprej pošljejo organom za nadzor meje v namembnem kraju. Revizija pravnega okvira[117] bi lahko omogočila učinkovitejšo uporabo informacij, hkrati pa zagotovila skladnost z zakonodajo o varstvu podatkov in olajšala pretok potnikov. Evidence podatkov o potnikih (PNR) so podatki, ki jih navedejo potniki pri rezervaciji letov. Izvajanje direktive o PNR[118] je ključnega pomena, zato ga bo Komisija še naprej podpirala in uveljavljala. Poleg tega bo Komisija kot srednjeročni ukrep začela pregled sedanjega pristopa k **prenosu podatkov PNR tretjim državam**.

Pravosodno sodelovanje je nujno za dopolnitev prizadevanj policije v boju proti čezmejnemu kriminalu. To sodelovanje se je v zadnjih 20 letih korenito spremenilo. Organi, kot sta **Evropsko javno tožilstvo** in **Eurojust**, morajo imeti sredstva za polno delovanje ali pa jih je treba okrepiti. Okrepiti bi bilo mogoče tudi sodelovanje med delavci v pravosodju z nadaljnjimi ukrepi za vzajemno priznavanje sodnih odločb, izobraževanje v pravosodju in izmenjavo informacij. Cilj bi moral biti povečanje vzajemnega zaupanja med sodniki in tožilci, kar je osrednjega pomena za nemotene čezmejne postopke. Tudi uporaba **digitalnih tehnologij** lahko izboljša učinkovitost naših pravosodnih sistemov. S podporo Eurojusta se

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf
[117] Direktiva Sveta 2004/82/ES o obveznosti prevoznikov, da sporočajo podatke o potnikih.
[118] Direktiva (EU) 2016/681 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj.

vzpostavlja nov digitalni sistem izmenjave za pošiljanje evropskih preiskovalnih nalogov, prošenj za medsebojno pravno pomoč in povezanih sporočil med državami članicami. Komisija bo sodelovala z državami članicami, da bi se pospešilo uvajanje potrebnih sistemov IT na nacionalni ravni.

Za učinkovito sodelovanje na področju kazenskega pregona ter pravosodno sodelovanje je ključno tudi mednarodno sodelovanje. Dvostranski sporazumi s ključnimi partnerji so odločilni pri pridobivanju informacij in dokazov iz držav zunaj EU. Pomembno vlogo ima **Interpol**, ena največjih medvladnih organizacij kriminalistične policije. Komisija bo preučila možnosti za okrepitev sodelovanja z Interpolom, vključno z morebitnim dostopom do Interpolovih podatkovnih zbirk in izboljšanjem operativnega in strateškega sodelovanja. Organi kazenskega pregona v EU se pri odkrivanju in preiskovanju storilcev kaznivih dejanj in teroristov opirajo tudi na ključne partnerske države. **Varnostna partnerstva med EU in tretjimi državami** bi se lahko okrepila, da bi se izboljšalo sodelovanje v boju proti skupnim grožnjam, kot so terorizem, organizirani kriminal, kibernetska kriminaliteta, spolna zloraba otrok in trgovina z ljudmi. Tak pristop bi temeljil na skupnih varnostnih interesih in nadgrajeval uveljavljeno sodelovanje in varnostne dialoge.

Poleg izmenjave informacij je lahko tudi izmenjava strokovnega znanja posebej koristna za povečanje pripravljenosti organov kazenskega pregona na **netradicionalne grožnje**. Komisija bo poleg spodbujanja izmenjave najboljših praks preučila možnost **usklajevalnega mehanizma na ravni EU za policijske organe** za dogodke višje sile, kot je pandemija. Med pandemijo se je prav tako izkazalo, da bo pri boju proti kriminalu in terorizmu ključnega pomena v digitalno skupnost usmerjeno policijsko delo, ki ga bodo spremljali pravni okviri za olajšanje policijskega dela na spletu. Partnerstva med policijo in skupnostmi, tako spletna kot nespletna, lahko preprečujejo kriminal in ublažijo učinek organiziranega kriminala, radikalizacije in terorističnih dejavnosti. Povezave med lokalnimi in regionalnimi rešitvami na področju policije do nacionalnih rešitev in rešitev na ravni EU so osrednji dejavnik za uspeh varnostne unije EU kot celote.

Prispevek trdnih zunanjih meja

Sodobno in učinkovito upravljanje zunanjih meja ima dvojno korist, in sicer ohranjanje celovitosti schengenskega območja in zagotavljanje varnosti naših državljank in državljanov. Vključevanje vseh ustreznih akterjev za kar največjo varnost na mejah ima lahko resničen učinek pri preprečevanju čezmejnega kriminala in terorizma. Skupne operativne dejavnosti nedavno okrepljene evropske mejne in obalne straže[119] prispevajo k preprečevanju in odkrivanju čezmejnega kriminala na **zunanjih mejah** in zunaj EU. Carinske dejavnosti pri odkrivanju varnostnih tveganj vsega blaga, preden prispe v EU, in kontroli blaga, ko prispe v EU, so odločilne za boj proti čezmejnemu kriminalu in terorizmu. V bodočem akcijskem načrtu za carinsko unijo bodo napovedani ukrepi za izboljšanje obvladovanja tveganja in notranje varnosti, zlasti bo ocenjena izvedljivost medsebojnega povezovanja ustreznih informacijskih sistemov za analizo varnostnih tveganj.

Okvir za **interoperabilnost informacijskih sistemov EU** na področju pravosodja in notranjih zadev je bil sprejet maja 2019. Namen te nove arhitekture je izboljšati učinkovitost in uspešnost novih ali posodobljenih informacijskih sistemov[120]. Omogočila bo hitrejše in

[119] Sestavljena iz Evropske agencije za mejno in obalno stražo (Frontex) ter mejne policije in organov za obalno stražo držav članic.

[120] Sistema vstopa/izstopa (SVI), evropskega sistema za potovalne informacije in odobritve (ETIAS), razširjenega evropskega informacijskega sistema kazenskih evidenc (ECRIS-TCN), schengenskega

bolj sistematične informacije za uslužbence organov kazenskega pregona, mejne policiste in uradnike za migracije. Prav tako bo prispevala k pravilni identifikaciji in boju proti identitetnim prevaram. Da bi interoperabilnost postala resničnost, bi moralo njeno izvajanje biti prednostna naloga tako na politični kot na tehnični ravni. Za dosego cilja popolne interoperabilnosti do leta 2023 bo poglavitnega pomena tesno sodelovanje med agencijami EU in vsemi državami članicami.

Goljufije v zvezi s potovalnimi dokumenti so eno najpogostejših kaznivih dejanj. Omogočajo nezakonito gibanje storilcev kaznivih dejanj in teroristov ter imajo ključno vlogo pri trgovini z ljudmi in nedovoljenem prometu s prepovedanimi drogami[121]. Komisija bo preučila, kako bi se obstoječe delo v zvezi z varnostnimi standardi, ki veljajo za dokumente za prebivanje in potovalne dokumente EU, lahko razširilo, vključno z digitalizacijo. Države članice bodo od avgusta 2021 naprej izdajale osebne izkaznice in dokumente za prebivanje v skladu z usklajenimi varnostnimi standardi. Ti vključujejo čip z biometričnimi identifikatorji, ki jih lahko preverijo vsi mejni organi EU. Komisija bo spremljala izvajanje teh novih pravil, tudi postopno zamenjavo dokumentov, ki so trenutno v obtoku.

Krepitev raziskav in inovacij na področju varnosti

Prizadevanja za zagotovitev kibernetske varnosti in boj proti organiziranemu kriminalu, kibernetski kriminaliteti in terorizmu so v veliki meri odvisni od prihodnjega razvoja orodij v ta namen, da bi se lahko razvile varnejše in bolje varovane nove tehnologije, reševali izzivi, ki jih prinašajo tehnologije, in podprlo delo na področju kazenskega pregona. To pa je po drugi strani odvisno od zasebnih partnerjev in industrije.

Inovacije bi bilo treba obravnavati kot strateško orodje za boj proti sedanjim grožnjam in predvidevanje prihodnjih tveganj in priložnosti. Inovativne tehnologije lahko prinesejo nova orodja za pomoč organom kazenskega pregona ter drugim akterjem na področju varnosti. Umetna inteligenca in analitika velepodatkov bi lahko izkoriščali visokozmogljivostno računalništvo, s čimer bi se zagotovila boljše odkrivanje ter hitra in celovita analiza[122]. Prvi pogoj za razvoj zanesljivih tehnologij so visokokakovostni nabori podatkov, ki so na voljo pristojnim organom za učenje, preskušanje in potrjevanje algoritmov[123]. Na splošno je tveganje tehnološke odvisnosti danes veliko – EU je na primer neto uvoznica proizvodov in storitev kibernetske varnosti, kar ima posledice za gospodarstvo in kritično infrastrukturo. Evropa potrebuje prisotnost in zmogljivosti v kritičnih delih zadevnih vrednostnih verig, da bi lahko obvladovala tehnologije in zagotovila neprekinjeno dobavo, tudi v primeru neželenih dogodkov in kriz.

Raziskave, inovacije in tehnološki razvoj v EU so priložnost, da se že med razvojem teh tehnologij upošteva varnostna razsežnost. Naslednja generacija predlogov za financiranje EU lahko deluje kot pomembna spodbuda[124]. Pri pobudah za evropske podatkovne prostore

---

informacijskega sistema, vizumskega informacijskega sistema in prihodnjega posodobljenega sistema Eurodac.

[121] Povezava med goljufijami v zvezi z dokumenti in trgovino z ljudmi je opisana v drugem poročilu o napredku v boju proti trgovini z ljudmi (COM(2018) 777) in spremnem delovnem dokumentu (SWD(2018) 473) ter v poročilu Europola iz leta 2016: Situation Report Trafficking in human beings in the EU.

[122] Na podlagi strategije Komisije za umetno inteligenco.

[123] Evropska strategija za podatke (COM(2020) 66 final).

[124] Predlogi Komisije za program Obzorje Evropa, Sklad za notranjo varnost, Sklad za integrirano upravljanje meja, program InvestEU, Evropski sklad za regionalni razvoj in program za digitalno Evropo bodo vsi

in infrastrukture oblaka se varnost upošteva že na samem začetku. Cilj Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov[125] je vzpostaviti učinkovito in uspešno strukturo za združevanje in skupno uporabo raziskovalnih zmogljivosti in rezultatov na področju kibernetske varnosti. Vesoljski program EU zagotavlja storitve, ki podpirajo varnost EU, njenih držav članic in posameznikov[126].

Varnostne raziskave, ki jih financira EU, so z več kot 600 uvedenimi projekti od leta 2007 v skupni vrednosti skoraj 3 milijarde EUR poglavitno gonilo za tehnologije in znanja, ki podpirajo varnostne rešitve. Komisija bo v okviru pregleda pooblastil Europola preučila možnost vzpostavitve **evropskega inovacijskega vozlišča za notranjo varnost**[127], ki bi si prizadevalo najti skupne rešitve za skupne varnostne izzive in priložnosti, ki jih države članice morda ne bi mogle izkoristiti same. Sodelovanje je bistvenega pomena za osredotočanje naložb tja, kjer bo dosežen najboljši učinek, in razvoj inovativnih tehnologij z varnostnimi in gospodarskimi koristmi.

Znanja in spretnosti ter ozaveščanje

Ozaveščenost o varnostnih vprašanjih in pridobivanje znanj in spretnosti za obravnavanje morebitnih groženj sta bistvenega pomena za izgradnjo odpornejše družbe z bolje pripravljenimi podjetji, upravami in posamezniki. Izzivi, povezani z infrastrukturo IT in e-sistemi, so pokazali, da moramo izboljšati človeške zmogljivosti za pripravljenost in odzivanje na področju kibernetske varnosti. Pandemija je opozorila tudi na pomen digitalizacije na vseh področjih gospodarstva in družbe EU.

Že **osnovno znanje o varnostnih grožnjah** in o tem, kako se boriti proti njim, lahko resnično vpliva na odpornost družbe. Zavedanje o nevarnostih kibernetske kriminalitete in o tem, da se moramo pred njimi zaščititi, se lahko povezuje z zaščito ponudnikov storitev proti kibernetskim napadom. Informacije o nevarnostih in tveganjih, povezanih z nedovoljenim prometom s prepovedanimi drogami, lahko storilcem kaznivih dejanj otežijo uspešno delovanje. EU lahko spodbudi širjenje najboljših praks, na primer prek mreže centrov za varnejši internet[128], in zagotovi, da so ti cilji vključeni v njene programe.

Prihodnji akcijski načrt za digitalno izobraževanje bi moral vključevati ciljno usmerjene ukrepe za pridobivanje znanj IT na področju varnosti za vse prebivalstvo. Nedavno sprejeti program znanj in spretnosti[129] podpira pridobivanje znanj in spretnosti skozi vse življenje. Vključuje namenske ukrepe za povečanje števila diplomantk in diplomantov na področju znanosti, tehnologije, inženirstva, umetnosti in matematike, saj so ta znanja potrebna na najnovejših področjih, kot je kibernetska varnost. Dodatni ukrepi, ki se financirajo iz

podpirali razvoj in uvajanje inovativnih varnostnih tehnologij in rešitev vzdolž vrednostne verige na področju varnosti.

[125] Predlog o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov (COM(2018) 630 z dne 12. septembra 2018).

[126] Program Copernicus na primer zagotavlja storitve, ki omogočajo varovanje zunanjih meja EU in pomorski nadzor ter s tem pomagajo pri ukrepanju proti piratstvu in tihotapljenju ter podpirajo kritično infrastrukturo. Ko bo v celoti operativen, bo ključnega pomena za omogočanje civilnih in vojaških misij in operacij.

[127] Vozlišče bi prav tako sodelovalo z Evropsko agencijo za mejno in obalno stražo/agencijo Frontex, agencijo CEPOL, agencijo eu-LISA in Skupnim raziskovalnim središčem.

[128] Glej www.betterinternetforkids.eu: osrednji portal in nacionalni centri za varnejši internet se trenutno financirajo v okviru Instrumenta za povezovanje Evrope za področje telekomunikacij. Predlagano je bilo, da se v prihodnje financirajo v okviru programa za digitalno Evropo.

[129] Program znanj in spretnosti za Evropo za trajnostno konkurenčnost, socialno pravičnost in odpornost (COM(2020) 274 final).

programa za digitalno Evropo, bodo strokovnjakom omogočili, da sledijo razvoju krajine varnostnih groženj in hkrati zapolnijo pomanjkanje na tem področju na trgu dela EU. Skupni učinek bo omogočanje posameznikom, da pridobijo znanja in spretnosti za soočanje z varnostnimi grožnjami, in podjetjem, da najdejo strokovnjake, ki jih potrebujejo na tem področju. Tudi prihodnji evropski raziskovalni prostor in evropski izobraževalni prostor bosta spodbujala poklicno pot na področju znanosti, tehnologije, inženirstva, umetnosti in matematike.

Prav tako je pomembno, da lahko **žrtve** uveljavljajo svoje pravice. Prejeti morajo potrebno pomoč in podporo, ki ju potrebujejo glede na posebne okoliščine. Posebna prizadevanja so potrebna pri manjšinah in najranljivejših žrtvah, kot so otroci ali ženske, ki so žrtve trgovine z ljudmi za namene spolnega izkoriščanja ali izpostavljeni nasilju v družini[130].

Posebno vlogo imajo okrepljene **spretnosti in znanja na področju kazenskega pregona**. Trenutne in nove tehnološke grožnje zahtevajo več naložb v strokovno izpopolnjevanje uslužbencev organov kazenskega pregona v najzgodnejši fazi in nato skozi celotno poklicno pot. Ključni partner za pomoč državam članicam pri tej nalogi je CEPOL. Usposabljanje na področju kazenskega pregona, povezano z rasizmom, ksenofobijo ter pravicami državljanov v širšem smislu, mora biti nujni sestavni del evropske kulture varnosti. Tudi nacionalni pravosodni sistemi in pravosodni delavci morajo imeti orodja, da se lahko prilagodijo in odzovejo na nove izzive. Usposabljanje je bistvenega pomena, da lahko organi na terenu ta orodja izkoristijo v operativnih razmerah. Poleg tega bi bilo treba storiti vse, da bi se okrepilo vključevanje načela enakosti spolov na področju kazenskega pregona ter okrepilo sodelovanje žensk pri njem.

Ključni ukrepi
• okrepitev pooblastil Europola • preučitev možnosti priprave „kodeksa policijskega sodelovanja“ EU in usklajevanja policije v krizah • okrepitev Eurojusta, da se povežejo pravosodni organi in organi kazenskega pregona • revizija direktive o predhodnih informacijah o potniku • sporočilo o zunanji razsežnosti evidenc podatkov o potnikih • krepitev sodelovanja med EU in Interpolom • okvir za pogajanja s ključnimi tretjimi državami o izmenjavi informacij • boljši varnostni standardi za potovalne dokumente • preučitev možnosti vzpostavitve evropskega inovacijskega vozlišča za notranjo varnost

V. Zaključek

V vse nemirnejšem svetu Evropska unija v veliki meri še vedno velja za eno najvarnejših in najbolje varovanih območij. Vendar tega ne smemo jemati za samoumevno.

Nova strategija za varnostno unijo postavlja temelje za varnostni ekosistem, ki zajema vso evropsko družbo. Osnovana je na zavedanju, da je varnost skupna odgovornost. Varnost zadeva vse. Vsi vladni organi, podjetja, družbene organizacije, institucije ter državljanke in državljani morajo prevzeti svojo odgovornost, da bi naše družbe postale varnejše.

[130] Glej strategijo za enakost spolov (COM(2020) 152), strategijo o pravicah žrtev (COM(2020) 258) in evropsko strategijo za boljši internet za otroke (COM(2012) 196).

Na varnostna vprašanja moramo zdaj gledati veliko širše kot v preteklosti. Odpraviti moramo napačno razlikovanje med fizičnim in digitalnim. Strategija EU za varnostno unijo združuje celoten razpon varnostnih potreb in se osredotoča na področja, ki so najpomembnejša za varnost EU v prihodnjih letih. Prav tako priznava, da varnostne grožnje ne spoštujejo geografskih meja, pa tudi to, da sta notranja in zunanja varnost vedno bolj povezani[131]. V tem okviru bo pomembno, da EU za zaščito vseh svojih državljank in državljanov sodeluje z mednarodnimi partnerji ter da se izvajanje te strategije še naprej tesno usklajuje z zunanjimi ukrepi EU.

Naša varnost je povezana z našimi temeljnimi vrednotami. Vsi v tej strategiji predlagani ukrepi in pobude bodo v celoti spoštovali temeljne pravice in naše evropske vrednote. Te so temelj evropskega načina življenja in morajo ostati v središču vsega našega dela.

Komisija se še vedno v celoti zaveda, da je vsaka politika ali ukrep dober le toliko, kolikor dobro se izvaja. Zato je treba nenehno poudarjati ustrezno izvajanje in izvrševanje obstoječe in prihodnje zakonodaje. To se bo spremljalo z rednimi poročili o varnostni uniji, Komisija pa bo Evropski parlament, Svet in zainteresirane strani v celoti obveščala ter jih vključevala v vse ustrezne ukrepe. Poleg tega je Komisija pripravljena sodelovati z institucijami in organizirati skupne razprave o strategiji za varnostno unijo, da bi skupaj spremljale doseženi napredek in prihodnje izzive.

Komisija poziva Evropski parlament in Svet, naj podpreta to strategijo za varnostno unijo kot osnovo za sodelovanje in skupne ukrepe na področju varnosti v naslednjih petih letih.

[131] Glej globalno strategijo EU.