EUROPSKA
KOMISIJA

Bruxelles, 24.7.2020.
COM(2020) 605 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, EUROPSKOM VIJEĆU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU TE ODBORU REGIJA

o strategiji EU-a za sigurnosnu uniju

I. Uvod

U političkim smjernicama Komisije jasno je navedeno da trebamo poduzeti sve što možemo kada je riječ o zaštiti naših građana. Sigurnost nije samo osnovni preduvjet osobne sigurnosti, već štiti i temeljna prava i temelj je povjerenja i dinamike u našem gospodarstvu, društvu i demokraciji. Europljani se danas suočavaju s nestabilnim sigurnosnim okruženjem na koje utječu nove prijetnje i drugi čimbenici, među ostalim klimatske promjene, demografska kretanja i politička nestabilnost izvan naših granica. Globalizacija, slobodno kretanje i digitalna transformacija i dalje donose prosperitet, olakšavaju nam živote te potiču inovacije i rast. Međutim, uz te koristi prisutni su i inherentni rizici i troškovi. Njima se može manipulirati u službi terorizma, organiziranog kriminala, trgovine drogom i ljudima, što sve izravno ugrožava građane i europski način života. Kibernapadi i kiberkriminalitet i dalje su u porastu. Sigurnosne prijetnje usto postaju sve složenije: pogoduju im mogućnost prekograničnog rada i međupovezanost, zloupotrebljavaju nestanak granica između fizičkog i digitalnog svijeta i iskorištavaju ranjive skupine te društvene i gospodarske razlike. Do napada može doći u svakom trenutku, uz oskudne ili nikakve tragove, državni kao i nedržavni akteri imaju na raspolaganju niz hibridnih prijetnji[1], a događaji izvan EU-a mogu bitno utjecati na sigurnost u EU-u.

Kriza uzrokovana bolešću COVID-19 izmijenila je i naše poimanje prijetnji sigurnosti i zaštiti kao i relevantne politike te je istaknula potrebu da se sigurnost zajamči i u fizičkom i u digitalnom okruženju. Ta kriza naglasila je važnost otvorene strateške autonomije naših opskrbnih lanaca za ključne proizvode, usluge, infrastrukture i tehnologije. Povećala je i potrebu za uključivanjem svih sektora i pojedinaca kako bismo zajednički osigurali najprije bolju pripremljenost i veću otpornost EU-a, a zatim i bolje alate za odgovor kada to bude potrebno.

Građanima se ne može pružiti zaštita samo samostalnim djelovanjem država članica. Udruživanje naših snaga i razvoj prednosti sada su važniji nego ikad prije, a EU upravo sada ima najveći potencijal za ostvarivanje stvarnih promjena. Jačanjem svojeg cjelokupnog sustava upravljanja krizom te radom na jačanju globalne stabilnosti unutar i izvan svojih granica EU može biti dobar primjer drugima. Iako su za sigurnost u prvom redu odgovorne države članice, posljednjih godina postaje sve jasnije da je pitanje sigurnosti jedne države članice pitanje sigurnosti sviju njih. EU može pružiti multidisciplinaran i integriran odgovor te akterima u području sigurnosti u državama članicama osigurati potrebne alate i informacije[2].

EU usto može zajamčiti da se sigurnosna politika i dalje temelji na našim zajedničkim europskim vrijednostima – poštovanju vladavine prava, ravnopravnosti[3] i temeljnih prava te jamčenju transparentnosti, odgovornosti i demokratskog nadzora – kako bi politike ulijevale potrebno povjerenje. EU može izgraditi učinkovitu i istinsku sigurnosnu uniju u kojoj su prava i slobode pojedinaca dobro zaštićeni. Sigurnost i poštovanje temeljnih prava nisu međusobno proturječni nego dosljedni i komplementarni ciljevi. Naše vrijednosti i temeljna

[1] Iako se definicije hibridnih prijetnji razlikuju, konceptom hibridnih prijetnji nastoji se obuhvatiti kombinacija prisilne i subverzivne aktivnosti te konvencionalnih i nekonvencionalnih metoda (tj. diplomatske, vojne, gospodarske i tehnološke) koje državni ili nedržavni akteri mogu upotrebljavati na koordiniran način kako bi postigli određene ciljeve (a da pritom ne poprimaju razmjere službene objave rata). Vidjeti dokument JOIN(2016) 18 (final).

[2] Na primjer, uslugama koje pruža svemirski program EU-a, kao što je Copernicus, pružanjem podataka o promatranju Zemlje i aplikacija za nadzor granica, pomorsku sigurnost, kazneni progon, borbu protiv piratstva, odvraćanje od krijumčarenja droga i upravljanje kriznim situacijama.

[3] Unija ravnopravnosti: Strategija za rodnu ravnopravnost 2020.–2025.(COM(2020) 152).

prava moraju biti osnova sigurnosnih politika i jamčiti načela nužnosti, proporcionalnosti i zakonitosti, uz odgovarajuće zaštitne mjere u vidu odgovornosti i pravnih lijekova, te istodobno omogućiti učinkovit odgovor za zaštitu pojedinaca, posebno onih najranjivijih.

Već postoje znatni pravni i praktični instrumenti te alati za potporu, ali ih je potrebno ojačati i bolje provoditi. Ostvaren je velik napredak u poboljšanju razmjene informacija i obavještajne suradnje s državama članicama te u ograničavanju prostora za djelovanje terorista i kriminalaca. No rascjepkanost je i dalje prisutna.

Rad na tome ne smije se zaustaviti na granicama EU-a jer zaštita Unije i njezinih građana više nije samo pitanje sigurnosti unutar naših granica, već zahtijeva i sagledavanje vanjske dimenzije sigurnosti. Pristup EU-a vanjskoj sigurnosti u okviru zajedničke vanjske i sigurnosne politike (ZVSP) i zajedničke sigurnosne i obrambene politike (ZSOP) i dalje će biti ključna sastavnica njegova djelovanja u cilju veće sigurnosti u EU-u. Suradnja s trećim zemljama i na globalnoj razini radi suočavanja sa zajedničkim izazovima osnovni je preduvjet za učinkovit i sveobuhvatan odgovor, pri čemu su stabilnost i sigurnost u susjedstvu ključni za sigurnost samog EU-a.

Ova nova strategija nadovezuje se na prethodni rad Europskog parlamenta[4], Vijeća[5] i Komisije[6] te dokazuje da je za istinsku i učinkovitu sigurnosnu uniju potrebno kombinirati snažnu okosnicu instrumenata i politika za sigurnost u praksi sa spoznajom da sigurnost utječe na sve dijelove društva i sve javne politike. EU treba zajamčiti sigurno okruženje svima, bez obzira na njihovo rasno ili etničko podrijetlo, vjeru, uvjerenje, rod, dob ili spolnu orijentaciju.

Ova strategija obuhvaća razdoblje 2020.–2025. i usmjerena je na izgradnju sposobnosti i kapaciteta radi postizanja sigurnosnog okruženja otpornog na promjene u budućnosti. U njoj se utvrđuje pristup sigurnosti na razini cijelog društva kojim se na koordiniran način može učinkovito odgovoriti na brze promjene prijetnji. Definiraju se strateški prioriteti i odgovarajuće mjere za integriran odgovor na rizike u digitalnoj i fizičkoj sferi u cijelom ekosustavu sigurnosne unije, s naglaskom na područjima u kojima EU može donijeti dodatnu vrijednost. Cilj je ove strategije unaprijediti sigurnost u cilju zaštite svih građana u EU-u.

II. Brze promjene sigurnosnih prijetnji EU-u

Sigurnost je preduvjet za osjećaj zaštićenosti, blagostanje i dobrobit građana. Prijetnje toj sigurnosti ovise o tome koliko su njihovi životi i izvori prihoda ranjivi. Što je ta ranjivost veća, veći je rizik od njezina iskorištavanja. Ranjivost kao i prijetnje stalno se razvijaju, a EU se tome mora prilagoditi.

Naš svakodnevni život ovisi o nizu usluga, kao što su energetika, promet, financije i zdravstvo. Te djelatnosti oslanjaju se na fizičku i na digitalnu infrastrukturu, zbog čega su ranjivost i mogućnosti poremećaja još veće. Tijekom pandemije bolesti COVID-19 brojna poduzeća i javne službe nastavili su s radom, bilo da su nam omogućili povezanost

[4] Na primjer, rad odbora TERR Europskog parlamenta, koji je o tome izvijestio u studenome 2018.

[5] Od zaključaka Vijeća iz lipnja 2015.o „obnovljenoj strategiji unutarnje sigurnosti” do novijih rezultata Vijeća iz prosinca 2019.

[6] Provedba Europskog programa sigurnosti za borbu protiv terorizma i stvaranje uvjeta za uspostavu učinkovite i istinske sigurnosne unije, COM(2016) 230 final). Vidjeti nedavnu ocjenu provedbe zakonodavstva u području unutarnje sigurnosti: Provedba zakonodavstva o unutarnjim poslovima u području unutarnje sigurnosti – 2017.–2020. (SWD/2020/135).

zahvaljujući radu na daljinu ili su osiguravali logistiku opskrbnih lanaca. No to je stvorilo prostor i za izvanredni porast zlonamjernih napada kojima se poremećaji izazvani pandemijom i prelazak na rad od kuće nastoje iskoristiti u kriminalne svrhe[7]. Nedostatak robe stvorio je nove prilike za organizirani kriminal. Posljedice su mogle biti smrtonosne i izazvati poremećaje u pružanju osnovnih zdravstvenih usluga u vrijeme najintenzivnijeg pritiska.

Kibersigurnost tehnologija postaje pitanje od strateške važnosti zbog sve većih koristi koje digitalne tehnologije donose u naše živote[8]. Kibernapadi snažno pogađaju domove, banke, financijske usluge i poduzeća (posebno mala i srednja poduzeća). Potencijalna šteta višestruko se povećava zbog međuovisnosti fizičkih i digitalnih sustava: svaki fizički napad vjerojatno će utjecati na digitalne sustave, dok kibernapadi na informacijske sustave i digitalne infrastrukture mogu dovesti do prekida ključnih usluga[9] Razvoj interneta stvari i povećana primjena umjetne inteligencije donijet će nove koristi, ali i novi skup rizika.

Naš svijet oslanja se na digitalnu infrastrukturu, tehnologije i internetske sustave koji nam omogućuju pokretanje poslovanja i korištenje proizvoda i usluga. Svi oni oslanjaju se na komunikaciju i interakciju. Ovisnost o internetu otvorila je put valu **kiberkriminaliteta**.[10] „Kiberkriminalitet kao usluga" i kiberkriminalno gospodarstvo omogućuju jednostavan pristup proizvodima i uslugama kiberkriminaliteta na internetu. Kriminalci se brzo prilagođavaju i nove tehnologije iskorištavaju u vlastite svrhe. Na primjer, krivotvoreni i lažni lijekovi prodiru u zakonit lanac opskrbe farmaceutskim proizvodima[11]. Eksponencijalni rast internetskih sadržaja[12] povezanih sa seksualnim zlostavljanjem djece upućuje na društvene posljedice promjena u obrascu kriminala. Nedavna anketa pokazala je da je većina stanovnika EU-u (55 %) zabrinuta da bi kriminalci i prevaranti mogli pristupiti njihovim podacima[13].

I **globalno okruženje** dodatno pridonosi tim prijetnjama. Agresivne industrijske politike trećih zemalja, u kombinaciji s kontinuiranom krađom intelektualnog vlasništva koju kibertehnologije omogućuju, mijenjaju stratešku paradigmu za zaštitu i promicanje europskih interesa. Tome pridonosi i sve veće korištenje robe s dvojnom namjenom, zbog čega je snažan sektor civilne tehnologije snažan resurs za obrambene i sigurnosne

---

7 Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (Europol: Nakon pandemije. Kako će COVID-19 utjecati na teški i organizirati kriminal u EU-u, travanj 2020).

8 Preporuka Komisije: Kibersigurnost 5G mreža, C(2019) 2335; Komunikacija Komisije: Sigurno uvođenje 5G mreža u EU-u – Provedba paketa instrumenata EU-a, COM(2020) 50.

9 U ožujku 2020. sveučilišna bolnica Brno u Češkoj pretrpjela je kibernapad koji ju je prisilio da preusmjeri pacijente i odgodi operacije, Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis (Europol: Profitiranje od krize. Kako kriminalci iskorištavaju krizu uzrokovanu bolešću COVID-19). Umjetna inteligencija može se zloupotrijebiti za digitalne, političke i fizičke napade te za nadzor. Prikupljanje podataka na internetu stvari može se iskoristiti za nadzor pojedinaca (pametni satovi, virtualni asistenti itd.).

10 Prema nekim prognozama troškovi povreda podataka dosegnut će 5 bilijuna USD godišnje do 2024., u odnosu na 3 bilijuna USD 2015., Juniper Research, The Future of Cybercrime & Security (Juniper Research, Budućnost kiberkriminaliteta i sigurnosti).

11 U jednoj studiji iz 2016. (Legiscript) procijenjeno je da u svijetu samo 4 % internetskih ljekarni posluje zakonito, a od 30 do 35 tisuća nezakonitih internetskih ljekarni primarno je usmjereno na potrošače iz EU-a.

12 Strategija EU-a za učinkovitiju borbu protiv seksualnog zlostavljanja djece, COM(2020) 607.

13 Agencija Europske unije za temeljna prava (2020.), Your rights matter: Security concerns and experiences (Vaša su prava važna: Zabrinutost i iskustva povezani sa sigurnošću), Anketa o temeljnim pravima, Luxembourg, Ured za publikacije.

kapacitete. Industrijska špijunaža ima znatne posljedice na gospodarstvo, radna mjesta i rast EU-a: Procjenjuje se da zbog kiberkrađa poslovnih tajni EU gubi 60 milijardi EUR[14]. Stoga treba temeljito analizirati kako ovisnosti i povećana izloženost kiberprijetnjama utječu na sposobnost EU-a da zaštiti pojedince i poduzeća.

Kriza izazvana bolešću COVID-19 istaknula je i kako socijalne podjele i nesigurnosti stvaraju sigurnosnu ranjivost. Time se povećava mogućnost za sofisticiranije i **hibridne napade** državnih i nedržavnih aktera, pri čemu se ranjivosti iskorištavaju kombinacijom kibernapada, štete na kritičnoj infrastrukturi[15], kampanja dezinformiranja i radikalizacije političkog diskursa.[16]

Istodobno se i dalje razvijaju neke već dugo prisutne prijetnje. U 2019. zabilježen je silazni trend **terorističkih napada** u EU-u. Međutim, prijetnja od džihadističkih napada Islamske države i Al Qaide njihovih suradnika na građane EU-a i dalje je visoka[17]. Istovremeno raste i prijetnja od nasilnog desničarskog ekstremizma[18]. Napadi motivirani rasizmom razlog su za ozbiljnu zabrinutost: antisemitski teroristički napadi sa smrtnim posljedicama podsjetnik su na potrebu za jačim odgovorom u skladu s Deklaracijom Vijeća iz 2018.[19]. Svaka peta osoba u EU-u vrlo je zabrinuta zbog mogućeg terorističkog napada u sljedećih 12 mjeseci[20]. Velika većina nedavnih terorističkih napada bili su „niskotehnološki" napadi u kojima su pojedinci u javnim prostorima bili meta samostalnih aktera, dok je teroristička propaganda na internetu dobila novu važnost prijenosom uživo napada u Christchurchu[21]. Prijetnja koju radikalizirani pojedinci predstavljaju i dalje je visoka, a potencijalno je pojačana povratkom stranih terorističkih boraca i ekstremista puštenih iz zatvora.[22]

Kriza je pokazala i kako se postojeće prijetnje mogu razvijati u novim okolnostima. Skupine **organiziranog kriminala** iskoristile su nestašice neke robe, što im je otvorilo put za stvaranje novih nezakonitih tržišta. Nezakonita trgovina drogama i dalje je najveće kriminalno tržište u EU-u, čija se maloprodajna vrijednost u EU-u procjenjuje na najmanje 30 milijardi EUR godišnje[23]. Trgovina ljudima i dalje je prisutna: prema procjenama svi oblici iskorištavanja ljudi donose globalni profit od gotovo 30 milijardi EUR godišnje.[24]

---

[14] The scale and impact of industrial espionage and theft of trade secrets through cyber (Opseg i učinci industrijske špijunaže i kiberkrađa poslovnih tajni), 2018.

[15] Kritična infrastruktura neophodna je za održavanje vitalnih društvenih funkcija, zdravlja, sigurnosti, zaštite, gospodarske i socijalne dobrobiti ljudi, a njezini bi poremećaj rada ili uništenje imali znatan učinak (Direktiva Vijeća 2008/114/EC).

[16] 97 % građana EU-a susrelo se s lažnim vijestima, a njih 38 % njih to se događa svakodnevno. Vidjeti JOIN(2020) 8 final.

[17] 13 država članica EU-a prijavilo je ukupno 119 izvršenih, neuspjelih i spriječenih terorističkih napada, u kojima je smrtno stradalo 10 osoba, a 27 ih je ranjeno (Europol, European Union Terrorism Situation and Trend Report (Europol: Izvješće o stanju i kretanjima terorizma), 2020.).

[18] U 2019. zabilježeno je šest desničarskih terorističkih napada (jedan izvršen, jedan neuspješan i četiri spriječena u trima državama članicama), u usporedbi sa samo jednim 2018., uz daljnje smrtne posljedice u slučajevima koji nisu klasificirani kao terorizam (Europol, 2020.).

[19] Vidjeti i Izjavu Vijeća o borbi protiv antisemitizma i razvoju zajedničkog sigurnosnog pristupa za bolju zaštitu židovskih zajednica i institucija u Europi.

[20] Agencija EU-a za temeljna prava: Your rights matter: Security concerns and experiences (Vaša su prava važna: Zabrinutost i iskustva povezani sa sigurnošću), 2020.

[21] Od srpnja 2015.do kraja 2019. Europol je pronašao teroristički sadržaj na 361 platformi (Europol, 2020.).

[22] Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism (Europol: Pregled najboljih praksi s obje strane Atlantika za borbu protiv radikalizacije u zatvorima i terorističkog recidivizma), 2019.

[23] Izvješće EMCDDA-e i Europola: EU Drugs Market Report (Tržište droga u EU-u), 2019.

[24] Izvješće Europola: Trafficking in Human Beings, Financial Business Model (Trgovanje ljudima, model financijskog poslovanja), 2015.

Međunarodna trgovina krivotvorenim farmaceutskim proizvodima dosegnula je vrijednost od 38,9 milijardi EUR[25]. Istovremeno, niske stope oduzimanja imovine kriminalcima dopuštaju da nastave širiti svoje kriminalne aktivnosti i prodirati u zakonito gospodarstvo.[26]. Počiniteljima kaznenih djela i teroristima olakšan je pristup vatrenom oružju, zahvaljujući internetskom tržištu i novim tehnologijama kao što je 3-D tisak.[27] Korištenjem umjetne inteligencije, novih tehnologija i robotike dodatno će povećati rizik od toga da kriminalci iskoriste prednosti inovacija u kriminalne svrhe[28].

Te su prijetnje transverzalne i na različite načine pogađaju razne dijelove društva. Sve one u velikoj mjeri ugrožavaju građane i poduzeća te zahtijevaju sveobuhvatan i dosljedan odgovor na razini EU-a. Ako su čak i mali međusobno povezani kućanski aparati, npr. hladnjak ili uređaj za kavu povezani na internet, izvor sigurnosnih ranjivosti, više se ne možemo oslanjati samo na tradicionalne državne aktere kako bismo zaštitili svoju sigurnost. Gospodarski subjekti moraju preuzeti veću odgovornost za kibersigurnost proizvoda i usluga koje stavljaju na tržište, dok građani trebaju imati barem osnovno poznavanje kibersigurnosti kako bi se mogli zaštititi.

III. Koordinirani odgovor EU-a za obranu na razini društva u cjelini

EU je već pokazao kako može donijeti stvarnu dodanu vrijednost. Sigurnosna unija od 2015. stvara nove poveznice za oblikovanje sigurnosnih politika na razini EU-a. No potrebno je učiniti više kako bi se uključilo cijelo društvo, sve razine vlasti, poduzeća u svim sektorima i stanovnike svih država članica. Sve veća svijest o rizicima ovisnosti[29] i potreba za snažnom europskom industrijskom strategijom[30] ukazuju na EU s kritičnom masom industrije, proizvodnjom tehnologije i otpornošću opskrbnog lanca. Snaga podrazumijeva i puno poštovanje temeljnih prava i vrijednosti EU-a: to je preduvjet za legitimne, učinkovite i održive sigurnosne politike. U ovoj strategiji za sigurnosnu uniju utvrđuju se konkretne smjernice za buduće djelovanje. Strategija se temelji na sljedećim zajedničkim ciljevima:

- ***Izgradnja sposobnosti i kapaciteta za rano otkrivanje, prevenciju i brzi odgovor na krize:*** Kako bi spriječila, zaštitila se i uspješno prevladala buduće šokove, Europa mora biti otpornija. Moramo izgraditi sposobnosti i kapacitete za rano otkrivanje, prevenciju i brzi odgovor na sigurnosne krize s pomoću integriranog i koordiniranog pristupa, općenito i putem inicijativa za pojedinačne sektore (na primjer za financijski sektor, energetiku, pravosuđe, policiju, zdravstvo, pomorstvo i promet) te na temelju postojećih

[25] Izvješće Ureda EU-a za intelektualno vlasništvo i OECD-a: Trade in counterfeit pharmaceutical products (Trgovina krivotvorenim farmaceutskim proizvodima).

[26] Izvješće o povratu i oduzimanju imovine: osiguravanje da se kriminal ne isplati, COM(2020) 217.

[27] U 2017. vatreno oružje upotrijebljeno je u 41 % svih terorističkih napada (Europol, 2018.).

[28] U srpnju 2020. francuska i nizozemska policijska i pravosudna tijela, u suradnji s Europolom i Eurojustom, predstavila su zajedničku istragu o razbijanju šifrirane telefonske mreže EncroChat, kojom se koriste kriminalne mreže povezane s nasilnim napadima, korupcijom, pokušajima ubojstva i masovnim krijumčarenjem droge.

[29] Rizici ovisnosti o inozemnim resursima uključuju povećanu izloženost potencijalnim prijetnjama, od iskorištavanja ranjivosti informatičke infrastrukture, čime se ugrožava kritična infrastruktura (npr. energetika, promet, bankarstvo, zdravstvo) ili preuzimanja kontrole nad industrijskim kontrolnim sustavima do povećanih mogućnosti za krađu podataka ili špijunažu.

[30] Komunikacija Komisije: Nova industrijska strategija za Europu, COM(2020) 102.

instrumenata i inicijativa[31]. Komisija će usto iznijeti prijedloge za sveobuhvatan sustav upravljanja krizama u EU-u, koji će biti relevantan i za sigurnost.

- ***Usmjerenost na rezultate***: Strategija fokusirana na uspješnost mora se temeljiti na pažljivoj procjeni prijetnji i rizika kako bi optimalno usmjerili naše napore. Potrebno ju je definirati i primjenjivati odgovarajuća pravila i odgovarajuće instrumente. Zahtijeva pouzdane strateške obavještajne podatke kao temelj sigurnosnih politika EU-a. Ako je potrebno donijeti zakonodavstvo EU-a, treba ga u potpunosti i provesti kako bi se izbjegla fragmentacija i nedostaci koji bi se mogli iskoristiti. Učinkovita provedba ove strategije ovisit će i o osiguravanju odgovarajućih sredstava u sljedećem programskom razdoblju 2021.–2027., među ostalim za agencije EU-a koje u njoj sudjeluju.
- ***Zajedničko djelovanje svih aktera u javnom i privatnom sektoru:*** Ključni akteri u javnom i privatnom sektoru nisu skloni dijeljenju informacija koje su važne za sigurnost, bilo zbog straha od ugrožavanja nacionalne sigurnosti bilo zbog konkurentnosti.[32]No najviše možemo postići kada smo svi usredotočeni na međusobno pružanje potpore. Kao prvo, to znači intenzivniju suradnju među državama članicama, uključujući policijska, pravosudna i druga javna tijela te s institucijama i agencijama EU-a, kako bi se izgradilo razumijevanje i razmjena koji su potrebni za zajednička rješenja. Ključna je i suradnja s privatnim sektorom, tim više što industrija posjeduje važan dio digitalne i nedigitalne infrastrukture koja je presudna za učinkovitu borbu protiv kriminala i terorizma. I pojedinci mogu dati svoj obol, primjerice izgradnjom vještina i podizanjem svijesti u borbi protiv kiberkriminaliteta ili dezinformacija. Naposljetku, taj zajednički napor mora se proširiti van naših granica kako bismo uspostavili tješnju suradnju s partnerima sličnih stajališta.

IV. Zaštita za sve u EU-u: strateški prioriteti sigurnosne unije

EU je u najboljem položaju da odgovori na nove globalne prijetnje i izazove. Prethodno navedena analiza prijetnji upućuje na četiri međuovisna strateška prioriteta u kojim treba ostvariti napredak na razini EU-a, uz puno poštovanje temeljnih prava: i. sigurnosno okruženje otporno na promjene u budućnosti, ii. suzbijanje novih prijetnji, iii. zaštita Europljana od terorizma i organiziranog kriminala i iv. snažan europski sigurnosni ekosustav.

1. Sigurnosno okruženje otporno na promjene u budućnosti

Zaštita i otpornost kritične infrastrukture

Građani se u svakodnevnom životu oslanjaju na kritičnu infrastrukturu kako bi putovali, radili, koristili osnovne javne usluge, npr. bolnice, prijevoz i opskrbu energijom, ili ostvarili svoja demokratska prava. Ako ta infrastruktura nije dovoljno zaštićena i otporna, napadi mogu uzrokovati velike poremećaje, u fizičkoj ili digitalnoj sferi, u pojedinačnim državama članicama, a potencijalno i cijelom EU-u.

[31] Kao što su integrirani politički odgovor na krizu (IPCR), Koordinacijski centar za odgovor na hitne situacije, Preporuka Komisije o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (C/2017/6100), operativni protokol EU-a za suzbijanje hibridnih prijetnji (EU Playbook) SWD(2016) 227.

[32] Vidjeti Zajedničku komunikaciju o otpornosti, odvraćanju i obrani: jačanje kibersigurnosti EU-a, JOIN(2017) 450.

Postojeći okvir EU-a za zaštitu i otpornost kritične infrastrukture[33] ne ide ukorak s pojavom novih rizika. Sve veća međuovisnost znači da poremećaji u jednom sektoru mogu imati neposredan učinak na operacije u drugima: napad na proizvodnju električne energije može uzrokovati kolaps telekomunikacija, bolnica, banaka ili zračnih luka, dok bi napad na digitalnu infrastrukturu mogao dovesti do poremećaja u elektroenergetskim mrežama ili financijskom sektoru. Kako se naše gospodarstvo i društvo u sve većoj mjeri oslanjaju na internet, takvi rizici sve su veći. Zakonodavnim okvirom potrebno je obuhvatiti tu povećanu međusobnu povezanost i međuovisnost, uz snažne mjere za zaštitu kritične fizičke i kiberinfrastrukture i izgradnju otpornosti. Osnovne usluge, uključujući one koje se temelje na svemirskoj infrastrukturi, moraju biti primjereno zaštićene od aktualnih i očekivanih prijetnji, ali i otporne na njih. To podrazumijeva sposobnost sustava za pripremu, planiranje i apsorpciju štetnih događaja te oporavak i uspješniju prilagodbu na njih.

S druge strane, države članice svoje diskrecijsko pravo koriste tako da postojeće zakonodavstvo provode na različite načine. Rascjepkanost koja iz toga proizlazi može potkopati unutarnje tržište i otežati prekograničnu koordinaciju, posebno u pograničnim regijama. Operateri koji pružaju kritične usluge u različitim državama članicama moraju poštovati različite sustave izvješćivanja. Komisija razmatra bi li **novi okviri za fizičku i digitalnu infrastrukturu** mogli dovesti do veće dosljednosti i usklađenijeg pristupa radi osiguravanja pouzdanog pružanja osnovnih usluga. Taj okvir treba biti popraćen **inicijativama za pojedinačne sektore** kako bi se ublažili specifični rizici s kojima se suočavaju ključne infrastrukture, kao što su prometna, energetska, financijska i zdravstvena[34]. S obzirom na veliku ovisnost financijskog sektora o IT uslugama i njegovu veliku osjetljivost na kibernapade, prvi će korak biti inicijativa za digitalnu operativnu otpornost financijskih sektora. S obzirom na posebnu osjetljivost i učinak energetskog sustava, posebnom inicijativom za potporu otpornosti ključne energetske infrastrukture na fizičke, hibridne i kiberprijetnje osigurat će se ravnopravni prekogranični uvjeti za energetske operatere.

Učinci izravnih stranih ulaganja koji su relevantni za sigurnost i koji bi mogli utjecati na ključnu infrastrukturu ili ključne tehnologije također će podlijegati procjenama koje provode države članice EU-a i Komisija u okviru novog europskog okvira za provjeru izravnih stranih ulaganja.[35].

EU može uspostaviti i nove instrumente za jačanje otpornosti kritične infrastrukture. Globalni internet dosad je pokazao visoku razinu otpornosti, posebno kada je riječ o sposobnosti podržavanja povećanog obujma prometa. Međutim, moramo se pripremiti na moguće buduće krize koje ugrožavaju sigurnost, stabilnost i otpornost interneta. Osiguravanje kontinuiranog funkcioniranja interneta podrazumijeva snažne mjere za zaštitu od kiberincidenata i zlonamjernih internetskih aktivnosti te smanjenje ovisnosti o

[33] Direktiva (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL L 194, 19.7.2016. Direktiva Vijeća 2008/114/EZ o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite.

[34] Zbog činjenice da je zdravstveni sektor tijekom krize izazvane bolešću COVID-19 bio pod posebnim opterećenjem, Komisija će razmotriti i inicijative za jačanje okvira EU-a za zdravstvenu sigurnost i za odgovor nadležnih agencija EU-a na ozbiljne prekogranične prijetnje zdravlju.

[35] Kada se 11. listopada 2020. Uredba (EU) 2019/452 Europskog parlamenta i Vijeća od 19. ožujka 2019. o uspostavi okvira za provjeru izravnih stranih ulaganja u Uniji počne u potpunosti primjenjivati, EU će imati na raspolaganju nov mehanizam suradnje u području izravnih stranih ulaganja koja bi mogla utjecati na sigurnost ili javni poredak. U skladu s Uredbom države članice i Komisija procijenit će moguće rizike povezane s takvim izravnim stranim ulaganjima i predložiti odgovarajuće mjere za njihovo ublažavanje ako je to potrebno i relevantno za više od jedne države članice.

infrastrukturi i uslugama izvan Europe. Za to će biti potrebno donijeti kombinaciju zakonodavnih mjera i revidirati postojeće propise kako bi se osigurala visoka zajednička razina sigurnosti mrežnih i informacijskih sustava u EU-u, povećati ulaganja u istraživanje i inovacije, razmotriti uvođenje ili jačanje osnovne internetske infrastrukture i resursa, posebno sustava naziva domena.[36].

Osiguravanje kanala za sigurnu komunikaciju na kritičnoj infrastrukturi najvažniji je element zaštite ključne digitalne imovine na razini EU-a i država članica. Komisija surađuje s državama članicama na uspostavi certificirane cjelokupno sigurne kvantne infrastrukture, zemaljske i svemirske, u kombinaciji sa sigurnim vladinim satelitskim komunikacijskim sustavom predviđenim u Uredbi o svemirskom programu[37].

Kibersigurnost

Broj kibernapada i dalje raste[38]. Ti su napadi sofisticiraniji nego ikad prije, dolaze iz niza izvora unutar i izvan EU-a te su usmjereni na područja najveće ranjivosti. U njima često sudjeluju državni akteri ili akteri s potporom države i usmjereni su na kritičnu digitalnu infrastrukturu, kao što su veliki pružatelji usluga računalstva u oblaku.[39]. Kiberrizici su se pokazali i kao znatna prijetnja financijskom sustavu. Međunarodni monetarni fond procjenjuje da kibernapadi uzrokuju godišnje gubitke od 9 % neto prihoda banaka na globalnoj razini, odnosno oko 100 milijardi USD.[40]. Prelazak na povezane uređaje korisnicima će donijeti brojne prednosti, međutim, s obzirom na to da se manje podataka pohranjuje i obrađuje u podatkovnim centrima, a sve više bliže korisniku „na rubu”[41], kibersigurnost se više neće moći usredotočiti na zaštitu središnjih točaka[42].

EU je 2017. predložio pristup kibersigurnosti koji se temelji na izgradnji otpornosti, brzom odgovoru i učinkovitom odvraćanju.[43] EU sada mora osigurati da njegovi kapaciteti u području kibersigurnosti idu ukorak sa stvarnošću kako bi mu osigurali otpornost i sposobnost za odgovor. To zahtijeva pristup koji je istinski na razini cijelog društva, pri čemu institucije, agencije i tijela EU-a, države članice, industrija, akademska zajednica i pojedinci kibersigurnosti trebaju dati potreban prioritet[44]. Taj horizontalni pristup treba nadopuniti pristupima kibersigurnosti za pojedinačne sektore u područjima kao što su energetika, financijske usluge, promet ili zdravstvo. Sljedeća faza djelovanja EU-a trebala bi se objediniti u revidiranoj Europskoj strategiji za kibersigurnost.

---

[36] Sustav naziva domena hijerarhijski je i decentralizirani sustav određivanja naziva za računala, usluge i druge resurse spojene na internet ili privatne mreže. Taj sustav prevodi nazive domena u IP adrese potrebne za lociranje i identifikaciju računalnih usluga i računala.

[37] Prijedlog Uredbe o uspostavljanju svemirskog programa Unije i Agencije Europske unije za svemirski program. COM(2018) 447.

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

[39] Distribuirani napadi uskraćivanjem usluga i dalje su stalna prijetnja: glavni pružatelji usluga morali su ublažavati posljedice takvih masovnih napada, primjerice napad na Amazonove internetske usluge u veljači 2020.

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

[41] Računalstvo na rubu mreže distribuirana je i otvorena IT arhitektura koja ima decentraliziranu procesnu snagu i omogućuje tehnologije mobilnog računalstva i interneta stvari. U računalstvu na rubu mreže podatke obrađuje sam uređaj, lokalno računalo ili poslužitelj te se oni ne prenose u podatkovni centar.

[42] Komunikacija o Europskoj strategiji za podatke, COM(2020) 66 final.

[43] Vidjeti Zajedničku komunikaciju o otpornosti, odvraćanju i obrani: jačanje kibersigurnosti EU-a, JOIN(2017) 450.

[44] Izvješće Zajedničkog istraživačkog centra pod nazivom „Cybersecurity – our digital Anchor” (Kibersigurnost – naš digitalni temelj) pruža višedimenzionalan uvid u rast kibersigurnosti u posljednjih 40 godina

Istraživanje novih i poboljšanih oblika suradnje obavještajnih službi, EU INTCEN-a i drugih organizacija koje se bave sigurnošću trebalo bi biti dio nastojanja za poboljšanje kibersigurnosti, borbu protiv terorizma, ekstremizma, radikalizma i hibridnih prijetnji.

Budući da je u cijelom EU-u u tijeku uvođenje **5G infrastrukture** i na potencijalnu ovisnost o 5G mrežama mnogih ključnih usluga, posljedice sustavnih i raširenih poremećaja bile bi izuzetno teške. Proces pokrenut Preporukom Komisije iz 2019. o kibersigurnosti 5G mreža[45] sada je rezultirao konkretnim mjerama koje države poduzimaju na temelju skupa mjera za 5G[46].

Jedna od najvažnijih dugoročnih potreba jest razvoj kulture **integrirane kibersigurnosti**, pri čemu se sigurnost od samog početka ugrađuje u proizvode i usluge. Važan doprinos tome bit će nov okvir za kibersigurnosnu certifikaciju u okviru Akta o kibersigurnosti[47]. Na okviru se već radi: dva programa certificiranja već su u pripremi, a prioriteti za daljnje programe bit će definirani krajem godine. Suradnja između Agencije EU-a za kibersigurnost (ENISA), tijela za zaštitu podataka i Europskog odbora za zaštitu podataka[48] od presudne je važnosti u tom području.

Kako bi se osigurala strukturirana i koordinirana operativna suradnja, Komisija je već utvrdila potrebu za uspostavom **zajedničke jedinice za kibersigurnost.** To bi moglo uključivati mehanizam uzajamne pomoći za vrijeme krize na razini EU-a. Nadovezujući se na provedbu preporuka iz Plana[49], zajednička jedinica za kibersigurnost mogla bi izgrađivati povjerenje među različitim akterima u europskom kibersigurnosnom ekosustavu i ponuditi ključne usluge državama članicama. Komisija će pokrenuti rasprave s relevantnim dionicima (počevši s državama članicama) i do kraja 2020. utvrditi jasan postupak, ključne etape i vremenski okvir.

Važna su i zajednička pravila o informacijskoj sigurnosti i kibersigurnosti za sve institucije, tijela i agencije EU-a. Cilj bi trebao biti stvaranje obveznih i visokih zajedničkih standarda za sigurnu razmjenu informacija i sigurnost digitalnih infrastruktura i sustava u svim institucijama, tijelima i agencijama EU-a. Tim novim okvirom trebalo bi poduprijeti snažnu i učinkovitu operativnu suradnju u području kibersigurnosti u svim institucijama, tijelima i agencijama EU-a, a u tome bi središnju ulogu imao tim za hitne računalne intervencije (CERT-EU).

S obzirom na njihovu globalnu prirodu, izgradnja i održavanje snažnih **međunarodnih partnerstava** od ključne su važnosti za daljnje sprečavanje i odvraćanje od kibernapada te odgovor na njih. U okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti („alati za kiberdiplomaciju”)[50] utvrđuju se mjere zajedničke vanjske i sigurnosne politike, uključujući mjere ograničavanja (sankcije), koje se mogu primijeniti protiv aktivnosti koje štete njegovim političkim, sigurnosnim i gospodarskim interesima. EU bi usto trebao intenzivnije djelovati putem fondova za razvoj i suradnju radi izgradnje

---

[45] Preporuka Komisije o kibersigurnosti 5G mreža, COM(2019) 2335 final. Preporuka predviđa njezino preispitivanje u posljednjem tromjesečju 2020.

[46] Vidjeti izvješće Skupine za suradnju u području mrežne i informacijske sigurnosti o provedbi tog skupa mjera od 24. srpnja 2020.

[47] Uredba (EU) 2019/881 o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije (Akt o kibersigurnosti).

[48] Komunikacija o zaštiti podataka kao jedan od stupova jačanja položaja građana i pristupa EU-a digitalnoj tranziciji – dvije godine primjene Opće uredbe o zaštiti podataka, COM(2020) 264.

[49] Preporuka Komisije (EU) 2017/1584 o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera.

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

kapaciteta za potporu partnerskim državama u jačanju njihovih digitalnih ekosustava, donošenju nacionalnih zakonodavnih reformi i pridržavanju međunarodnih standarda. Time se povećava otpornost cijele zajednice i njezina sposobnost borbe protiv kiberprijetnji i učinkovitog odgovora na njih. To uključuje konkretne mjere za promicanje standarda i relevantnog zakonodavstva EU-a u cilju jačanja kibersigurnosti partnerskih zemalja u susjedstvu[51].

Zaštita javnih prostora

Nedavni teroristički napadi bili su usmjereni na **javne prostore**, među ostalim mjesta bogoslužja i prometna čvorišta, iskorištavajući njihovu otvorenost i pristupačnost. Porast terorizma potaknut političkim ili ideološki motiviranim ekstremizmom tu je prijetnju dodatno potencirao. Stoga je potrebna bolja fizička zaštita takvih mjesta i odgovarajućih sustava za otkrivanje, bez ugrožavanja slobode građana[52]. Komisija će financiranjem, razmjenom iskustava i dobre prakse, posebnim smjernicama[53] i preporukama[54] unaprijediti suradnju javnog i privatnog sektora na zaštiti javnih prostora. Dio tog pristupa biti će i informiranje, zahtjevi u pogledu učinkovitosti i ispitivanja opreme za otkrivanje te poboljšanje pozadinskih provjera radi uklanjanja unutarnjih prijetnji. Važan aspekt koji treba uzeti u obzir činjenica je da manjine i ranjivi pojedinci mogu biti nerazmjerno pogođeni, uključujući osobe koje su meta zbog njihove vjere ili roda, zbog čega im je potrebno posvetiti posebnu pozornost. Regionalna i lokalna javna tijela imaju važnu ulogu u poboljšanju sigurnosti javnih prostora. Komisija gradovima pomaže u promicanju inovativnih rješenja za sigurnost javnih prostora[55]. Pokretanje novog partnerstva u studenome 2018. za „sigurnost javnih prostora" u okviru Plana za gradove[56] pokazuje snažnu predanost država članica, Komisije i gradova boljem suzbijanju prijetnji sigurnosti u gradskom prostoru.

Tržište **bespilotnih letjelica** i dalje se širi i one imaju mnoge vrijedne i zakonite namjene. Međutim, kriminalci i teroristi mogli bi ih zloupotrijebiti, pri čemu su javni prostori posebno ugroženi. Među njihovim ciljevima mogu biti pojedinci, javna okupljanja, kritična infrastruktura, policija, granice ili javni prostori. Saznanja o primjeni bespilotnih letjelica u sukobu u Europu bi mogle doći izravno (povratkom stranih terorističkih boraca) ili internetom. Pravila koja je već izradila Europska agencija za sigurnost zračnog prometa važan su prvi korak u tom području i uključuju registraciju operatora i obveznu daljinsku identifikaciju bespilotnih letjelica. Budući da bespilotne letjelice postaju sve dostupnije, pristupačnije i naprednije, potrebno je poduzeti dodatne mjere. To bi moglo uključivati razmjenu informacija, smjernica i dobre prakse za sve sudionike, uključujući tijela kaznenog

---

[51] Vidjeti smjernice za izgradnju vanjskih kiberkapaciteta EU-a iz zaključaka Vijeća od 26. lipnja 2018.)..

[52] Sustavi daljinske biometrijske identifikacije zahtijevaju posebnu kontrolu. Početna stajališta Komisije iznesena su u Bijeloj knjizi Komisije od 19. veljače 2020. o umjetnoj inteligenciji, COM(2020) 65.

[53] Npr. Smjernice za odabir odgovarajućih sigurnosnih barijera za zaštitu javnih prostora (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Smjernice o dobroj praksi navedene su u dokumentu SWD(2019) 140, uključujući odjeljak o javno-privatnoj suradnji. Financiranje u okviru Fonda za unutarnju sigurnost – policija posebno je usmjereno na jačanje javno-privatne suradnje.

[55] Tri grada (Pirej u Grčkoj, Tampere u Finskoj i Torino u Italiji) testirat će nova rješenja u okviru inicijative Inovativne mjere za gradove, koju sufinancira Europski fond za regionalni razvoj (EFRR).

[56] Plan EU-a za gradove nova je metoda rada na više razina kojom se promiče suradnja država članica, gradova, Europske komisije i drugih dionika radi poticanja rasta, kvalitete života i inovacija u europskim gradovima, utvrđivanja društvenih izazova i uspješnog suočavanja s njima.

progona, kao i više testiranja protumjera za bespilotne letjelice[57]. Osim toga, trebalo bi dodatno analizirati i razmotriti posljedice koje njihova upotreba u javnim prostorima ima na zaštitu privatnosti i podataka.

Ključne mjere
• zakonodavstvo o zaštiti i otpornosti kritične infrastrukture • revizija Direktive o mrežnim i informacijskim sustavima • poboljšanje operativne otpornosti financijskog sektora • zaštita i kibersigurnost kritične energetske infrastrukture te mrežna pravila o kibersigurnosti prekograničnih tokova električne energije • europska strategija za kibersigurnost • sljedeći koraci u stvaranju zajedničke jedinice za kibersigurnost • zajednička pravila o informacijskoj sigurnosti i kibersigurnosti za institucije, tijela i agencije EU-a • pojačana suradnja na zaštiti javnih prostora, uključujući mjesta bogoslužja • razmjena najboljih praksi za suzbijanje zloupotrebe bespilotnih letjelica

2. Suočavanje s novim prijetnjama

Kiberkriminalitet

Tehnologija društvu donosi nove mogućnosti te nudi nove policijske i pravosudne alate. No istovremeno tehnologija otvara vrata i kriminalcima. Sve je više zlonamjernih softvera, krađe osobnih ili poslovnih podataka hakiranjem i slučajeva pada digitalnih sustava koji nanose financijsku štetu ili gubitak ugleda. Otporno okruženje utemeljeno na snažnoj kibersigurnosti pritom je prva linija obrane. Policijska i pravosudna tijela moraju moći provoditi digitalne istraga, s jasnim pravilima za istragu i kazneni progon kaznenih djela te pružanjem potrebne zaštite žrtvama. Taj rad trebao bi se temeljiti na zajedničkoj radnoj skupini za borbu protiv kiberkriminaliteta (u okviru Europola) i protokolu za odgovor tijelâ kazenog progorna EU-a na krizne situacije, koji je donesen radi koordinacije odgovora na kibernapade velikih razmjera. Izuzetno su važni i učinkoviti mehanizmi za javno-privatna partnerstva i suradnju.

Usporedo s tim, borba protiv kiberkriminaliteta trebala bi postati strateški komunikacijski prioritet cijelog EU-a kako bi se Europljane upozorilo na rizike i preventivne mjere koje bi mogli poduzeti. To bi trebalo biti dio proaktivnog pristupa. Bitan je korak i potpuna provedba postojećeg pravnog okvira[58]: Komisija će prema potrebi biti spremna pokrenuti postupke zbog povrede prava, kao i preispitati taj okvir u cilju osiguranja njegove svrsihodnosti. Komisija će usto u suradnji s Europolom i Agencijom EU-a za kibersigurnost istražiti izvedivost EU-ova sustava brzog uzbunjivanja o kiberkriminalitetu, koji bi mogao osigurati protok informacija i brzu reakcija u slučaju naglog rasta kiberkriminaliteta.

Kiberkriminalitet je globalni izazov koji zahtijeva učinkovitu međunarodnu suradnju. EU podupire Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu, koja je učinkovit i dobro uhodan okvir koji svim državama omogućuje da utvrde sustave i komunikacijske kanale potrebne za učinkovitu suradnju.

[57] Nedavno je uspostavljen višegodišnji program ispitivanja za potporu državama članicama u razvoju zajedničke metodologije i platforme za ispitivanje u tom području.

[58] Direktiva 2013/40/EU o napadima na informacijske sustave.

Gotovo polovica građana EU-a zabrinuta je zbog zloupotrebe[59] podataka i **krađe identiteta**[60]. Zloupotreba identiteta radi ostvarivanja financijske dobiti jedan je od aspekata toga, ali može imati i teške osobne i psihološke posljedice, s obzirom na to da nezakonite objave kradljivca identiteta mogu godinama ostati na internetu. Komisija će istražiti moguće praktične mjere za zaštitu žrtava od svih oblika krađe identiteta, uzimajući u obzir predstojeću europsku inicijativu za digitalni identitet[61].

Borba protiv kiberkriminaliteta podrazumijeva da moramo gledati prema budućnosti. Kako koristimo nova tehnološka dostignuća koja donose društveni i gospodarski napredak, tako i kriminalci te alate nastoje iskoristiti u negativne svrhe. Na primjer, kriminalci mogu koristiti umjetnu inteligenciju kako bi otkrili i identificirali lozinke ili pojednostavnili izradu zlonamjernih softvera te iskoristili slike ili audiozapise za krađu identiteta ili prijevaru.

Moderan kazneni progon

Policija i pravosudni organi moraju se prilagoditi novoj tehnologiji. Zbog tehnološkog razvoja i novih prijetnji tijela kaznenog progona moraju imati pristup novim alatima, stjecati nove vještine i razvijati alternativne istražne tehnike. Kako bi se dopunile zakonodavne mjere usmjerene na poboljšanje prekograničnog pristupa elektroničkim dokazima u kaznenim istragama, EU tijelima kaznenog progona može pomoći u razvoju potrebnih kapaciteta za utvrđivanje, zaštitu i tumačenje podataka potrebnih za istrage kaznenih djela i njihovo korištenje kao dokaza na sudu. Komisija će razmotriti mjere za **jačanje kapaciteta za digitalne istrage tijela kaznenog progona** te utvrditi najbolje načine za primjenu istraživanja i razvoja u izradi novih alata kaznenog progona i za razvoj odgovarajućih vještina osposobljavanjem policijskih i pravosudnih tijela. To će uključivati i pružanje strogih znanstvenih evaluacija i metoda ispitivanja Komisijina Zajedničkog istraživačkog centra.

Zajedničkim pristupom može se osigurati i **integracija umjetne inteligencije, svemirskih kapaciteta, velikih podataka i računalstva visokih performansi** u sigurnosnu politiku, na način koji je učinkovit u borbi protiv kriminala i u osiguravanju temeljnih prava. Umjetna inteligencija mogla bi biti moćan alat za borbu protiv kriminala, s obzirom na to da omogućuje analizu velikih količina podataka i utvrđivanje obrazaca i nepravilnosti, čime se stvaraju goleme istražne sposobnosti.[62] Pruža i konkretne alate, kao što je pomoć u prepoznavanju terorističkih sadržaja na internetu i otkrivanju sumnjivih transakcija pri prodaji opasnih proizvoda ili pomoć građanima u hitnim slučajevima. Ostvarivanje tog potencijala podrazumijeva povezivanje istraživanja, inovacija i korisnika umjetne inteligencije s odgovarajućom upravljačkom i tehničkom infrastrukturom, uz aktivno uključivanje privatnog sektora i akademske zajednice. To znači i osiguravanje najviših standarda poštovanja temeljnih prava i istodobne učinkovite zaštite građana. Konkretno,

[59] 46 % (istraživanje Eurobarometra o stavovima Europljana prema kibersigurnosti, siječanj 2020.).

[60] Velika većina ispitanika u istraživanju Eurobarometra iz 2018. o stavovima Europljana prema sigurnosti na internetu (95 %) smatra krađu identiteta teškim kaznenim djelom, a 70 % ih smatra da je to vrlo teško kazneno djelo. Istraživanje Eurobarometra objavljeno u siječnju 2020. potvrdilo je zabrinutost zbog kiberkriminaliteta, prijevara na internetu i krađe identiteta: dvije trećine ispitanika zabrinuto je zbog prijevara u bankarstvu (67 %) ili krađe identiteta (66 %)

[61] Komunikacija od 19. veljače 2020. o izgradnji digitalne budućnosti Europe, COM(2020) 67.

[62] Na primjer, u slučaju financijskih kaznenih djela.

odluke koje utječu na pojedince moraju podlijegati ljudskoj reviziji i biti u skladu s relevantnim primjenjivim pravom EU-a.[63]

Elektroničke informacije i dokazi potrebni su u oko 85 % istraga teških kaznenih djela, a 65 % od ukupnog broja zahtjeva upućuje se pružateljima u drugoj jurisdikciji[64]. Činjenica da su se tradicionalni fizički tragovi preselili na internet dodatno povećava jaz između sposobnosti tijela kaznenog progona i kriminalaca. Od izuzetne je važnosti uspostaviti jasna pravila za prekogranični pristup elektroničkim dokazima za kaznene istrage. Upravo zato je bitno da Europski parlament i Vijeće brzo donesu prijedloge o e-dokazima kako bi se stručnjacima osigurao učinkovit alat. Prekogranični pristup e-dokazima u okviru multilateralnih i bilateralnih međunarodnih pregovora važan je i za uspostavu usklađenih pravila na međunarodnoj razini[65].

Pristup digitalnim dokazima ovisi i o dostupnosti informacija. Ako se podaci prebrzo izbrišu, mogu nestati važni dokazi, a s njima i mogućnost identifikacije i lociranja osumnjičenika i kriminalnih mreža (kao i žrtava). S druge strane, sustavi zadržavanja podataka pokreću pitanja zaštite privatnosti. Ovisno o ishodu predmeta koji su u tijeku pred Sudom Europske unije, Komisija će procijeniti daljnje korake u pogledu zadržavanja podataka.

Pristup informacijama o registraciji naziva internetskih domena („tzv. WHOIS podaci”)[66] važan je za kaznene istrage, kibersigurnost i zaštitu potrošača. Međutim, pristup tim informacijama postaje sve teži jer se čeka da Internetska organizacija za dodijeljene nazive i brojeve (ICANN) donese novu politiku za te podatke. Komisija će nastaviti surađivati s ICANN-om i širom zajednicom dionika kako bi se osiguralo da zakoniti tražitelji pristupa, uključujući tijela kaznenog progona, mogu ostvariti učinkovit pristup WHOIS podacima, u skladu s propisima EU-a i međunarodnim propisima o zaštiti podataka. To će uključivati procjenu mogućih rješenja, među ostalim potrebe za donošenjem propisa kojima bi se pojasnila pravila za pristup takvim informacijama.

Policijska i pravosudna tijela usto moraju biti opremljena za dobivanje potrebnih podataka i dokaza nakon što se u EU-u potpuno uvede **arhitektura 5G za mobilne telekomunikacije**, a da se pritom u potpunosti poštuje povjerljivost komunikacija. Komisija će pružiti podršku poboljšanom i koordiniranom pristupu u izradi međunarodnih standarda, definiranju najbolje prakse, postupaka i tehničke interoperabilnosti u ključnim tehnološkim područjima, npr. umjetna inteligencija, internet stvari ili tehnologije lanaca blokova.

Danas znatan dio istraga svih oblika kaznenih dijela i terorizma uključuje **šifrirane informacije**. Šifriranje ima ključnu ulogu u digitalnom prostoru jer se njime osiguravaju digitalni sustavi i transakcije te štiti niz temeljnih prava, uključujući slobodu izražavanja, privatnost i zaštitu podataka. Međutim, ako se upotrebljava u kriminalne svrhe, njime se može prikriti identitet kriminalaca i sadržaj njihove komunikacije. Komisija će razmotriti i podržati uravnotežena tehnička, operativna i pravna rješenja za te izazove i promicati pristup

[63] To znači usklađenost s postojećim zakonodavstvom, uključujući Opću uredbu (EU) 2016/679 o zaštiti podataka i Direktivu (EU) 2016/680 o obradi osobnih podataka u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija

[64] Radni dokument službi Komisije SWD(2018) 118 final.

[65] Konkretno, drugi protokol uz Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu i sporazum između EU-a i SAD-a o prekograničnom pristupu e-dokazima.

[66] Pohranjuje se u bazama podataka koje održava 2 500 operatera registara i registrara sa sjedištima diljem svijeta.

koji zadržava učinkovitost šifriranja u zaštiti privatnosti i sigurnosti te istodobno pruža učinkovit odgovor na kriminal i terorizam.

Borba protiv nezakonitih sadržaja na internetu

Objedinjavanje sigurnosti internetskog i fizičkog okruženja podrazumijeva daljnje korake u **borbi protiv nezakonitih sadržaja na internetu**. Sve više ključnih prijetnji građanima kao što su terorizam, ekstremizam ili seksualno zlostavljanje djece oslanja se na digitalno okruženje, a to zahtijeva konkretne mjere i okvir kako bi se osiguralo poštovanje temeljnih prava. Za početak je važan brzi dovršetak pregovora o predloženom zakonodavstvu o terorističkim sadržajima na internetu[67] i osiguravanje njegove provedbe. Za borbu protiv zloupotrebe interneta od strane terorista, nasilnih ekstremista i kriminalaca bitno je i jačanje dobrovoljne suradnje tijela kaznenog progona i privatnog sektora u sklopu **internetskog foruma EU-a**. Jedinica za prijavljivanje neprihvatljivog internetskog sadržaja u Europolu i dalje će imati ključnu ulogu u praćenju aktivnosti terorističkih skupina na internetu i mjera koje poduzimaju platforme,[68] kao i u daljnjem razvoju **Protokola EU-a o kriznim situacijama**[69]. Osim toga, Komisija će nastaviti surađivati s međunarodnim partnerima, među ostalim sudjelovanjem u **globalnom internetskom forumu za borbu protiv terorizma** u cilju prevladavanja tih izazova na globalnoj razini. Nastavit će se potpora razvoju alternativnih diskursa i protuargumentacije u okviru Programa za osnaživanje civilnog društva[70].

Kako bi spriječila i suzbila širenje nezakonitog govora mržnje na internetu, Komisija je 2016. uspostavila Kodeks postupanja za borbu protiv nezakonitog govora mržnje na internetu, uz dobrovoljnu obvezu internetskih platformi da uklone sadržaje govora mržnje. Najnovija evaluacija pokazuje da platforme 90 % označenog sadržaja ocjenjuju u roku od 24 sata i uklanjaju 71 % sadržaja koji se smatra nezakonitim govorom mržnje. Međutim, trebaju dodatno poboljšati transparentnost i povratne informacije korisnicima te osigurati dosljednu evaluaciju označenog sadržaja[71].

Internetski forum EU-a olakšat će i razmjenu informacija o postojećim i novim tehnologijama za prevladavanje izazova povezanih sa seksualnim zlostavljanjem djece na internetu. Suzbijanje seksualnog zlostavljanja djece na internetu u središtu je nove strategije za jačanje **borbe protiv seksualnog zlostavljanja djece**[72], kojom će se nastojati u najvećoj mogućoj mjeri iskoristiti alate dostupne na razini EU-a za borbu protiv tih kaznenih djela. Platforme moraju biti u mogućnosti nastaviti otkrivati i uklanjati materijale povezane sa seksualnim zlostavljanjem djece na internetu, a šteta koju takvi materijali uzrokuju zahtijeva okvir u kojem su definirane jasne i trajne obveze radi suočavanja s tim problemom. U toj strategiji će se najaviti i da Komisija počinje pripremu sektorskog zakonodavstva kako bi se učinkovitije suzbilo seksualno zlostavljanje djece na internetu, uz puno poštovanje temeljnih prava.

Općenitije, u sljedećem Aktu o digitalnim uslugama pojasnit će se i nadograditi pravila o odgovornosti i sigurnosti za digitalne usluge te ukloniti čimbenici koji odvraćaju od borbe protiv nezakonitih sadržaja, robe ili usluga.

---

67 Prijedlog Uredbe o sprečavanju širenja terorističkih sadržaja na internetu, COM(2018) 640, 12. rujna 2018.

68 Europol, studeni 2019.

69 A Europe that protects - EU Crisis Protocol: responding to terrorist content online (Europa koja štiti – Protokol EU-a za krizne situacije: odgovor na terorističke sadržaje na internetu). (listopad 2019.).

70 Povezano s radom programa za osvješćivanje o radikalizaciji, vidjeti odjeljak IV.3. u nastavku

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

72 Strategija EU-a za učinkovitiju borbu protiv seksualnog zlostavljanja djece, COM(2020) 607.

Osim toga, Komisija će nastaviti suradnju s međunarodnim partnerima i s **globalnim internetskim forumom za borbu protiv terorizma**, među ostalim u neovisnom savjetodavnom odboru, kako bi se razmotrili načini za prevladavanje tih izazova na globalnoj razini, a da se pritom očuvaju europske vrijednosti i temeljna prava. Trebalo bi sagledati i nove teme kao što su algoritmi ili internetske igre[73].

Hibridne prijetnje

Razmjeri i raznolikost današnjih hibridnih prijetnji veći su nego ikad prije. O tome svjedoči i kriza uzrokovana bolešću COVID-19, tijekom koje je više državnih i nedržavnih aktera pokušalo instrumentalizirati pandemiju, posebno manipuliranjem informacijskog okruženja i podrivanjem temeljne infrastrukture. To ugrožava socijalnu koheziju i narušava povjerenje u institucije EU-a i vlade država članica.

Pristup EU-a hibridnim prijetnjama utvrđen je u Zajedničkom okviru iz 2016.[74] i Zajedničkoj komunikaciji iz 2018.[75] o povećanju otpornosti na hibridne prijetnje. Djelovanje na razini EU-a temelji se na opsežnom paketu instrumenata koji obuhvaća povezanost unutarnje i vanjske sigurnosti, zasnovanom na pristupu na razini cijelog društva i bliskoj suradnji sa strateškim partnerima, osobito s NATO-om i skupinom G-7. Izvješće o provedbi pristupa EU-a hibridnim prijetnjama objavljuje se zajedno s ovom Strategijom[76]. Na temelju pregleda mjera[77] predstavljenog uz ovu Strategiju službe Komisije i Europska služba za vanjsko djelovanje uspostavit će **internetsku platformu s ograničenim pristupom** koja će državama članicama služiti kao referenca za protuhibridna sredstva i mjere na razini EU-a.

Iako zbog intrinzičnih veza s nacionalnim sigurnosnim i obrambenim politikama odgovornost za suzbijanje hibridnih prijetnji prvenstveno imaju države članice, neke su slabosti zajedničke svim državama članicama, a neke se prijetnje šire preko granica, npr. ciljanje na prekogranične mreže ili infrastrukturu. Komisija i Visoki predstavnik utvrdit će pristup EU-a hibridnim prijetnjama kojim se aspekti vanjske i unutarnje sigurnosti spajaju u koherentnu cjelinu i ujedinjuju interesi na nacionalnoj razini i razini EU-a. To mora obuhvaćati cijeli spektar djelovanja – od ranog otkrivanja, analize, osviještenosti, jačanja otpornosti i prevencije do odgovora na krizu i upravljanja posljedicama.

Zbog stalnog razvoja hibridnih prijetnji, uz pojačanu provedbu poseban će naglasak biti na **uključivanju pitanja hibridnih prijetnji u oblikovanje politika**, kako bi se osiguralo da te politike prate dinamične promjene i da se uzmu u obzir relevantne inicijative. Učinci novih inicijativa također će se ocjenjivati u kontekstu hibridnih prijetnji, uključujući inicijative u područjima koja su dosad bila izvan područja primjene protuhibridnog okvira, kao što su obrazovanje, tehnologija i istraživanje. U takvom bi pristupu koristio dosadašnji rad na konceptualizaciji hibridnih prijetnji, koji pruža sveobuhvatan uvid u razna sredstva koja protivnici mogu koristiti[78]. Trebalo bi osigurati da se postupak donošenja odluka temelji na redovitom i sveobuhvatnom izvješćivanju o razvoju hibridnih prijetnji utemeljenom na

[73] Teroristi se sve više služe sustavima za razmjenu poruka u okviru internetskih platformi za videoigre, a mladi teroristi rekreiraju nasilne napade iz videoigara.

[74] Zajednički okvir za suzbijanje hibridnih prijetnji – odgovor Europske unije, JOIN(2016) 18.

[75] Jačanje otpornosti i povećanje sposobnosti za odgovor na hibridne prijetnje, JOIN(2018) 16.

[76] SWD(2020) 153 Izvješće o provedbi Zajedničkog okvira za suzbijanje hibridnih prijetnji iz 2016. i Zajednička komunikacija o jačanju otpornosti i poboljšanju sposobnosti za borbu protiv hibridnih prijetnji iz 2018.

[77] SWD(2020) 152 Pregled mjera za jačanje otpornosti i suzbijanje hibridnih prijetnji.

[78] The Landscape of Hybrid Threats: A conceptual Model (Hibridne prijetnje: konceptualni model), JRC117280, koji su zajednički izradili Zajednički istraživački centar i Centar izvrsnosti za suzbijanje hibridnih prijetnji.

obavještajnim podacima. Pritom će se u velikoj mjeri oslanjati na obavještajne podatke država članica i na daljnje jačanje obavještajne suradnje s nadležnim službama država članica putem EU INTCEN-a.

Radi boljeg **uvida u stanje**, službe Komisije i Europska služba za vanjsko djelovanje razmotrit će mogućnosti pojednostavnjenja protoka informacija iz različitih izvora, uključujući države članice i agencije EU-a, kao što su ENISA, Europol i Frontex. Jedinica EU-a za otkrivanje hibridnih prijetnji i dalje će biti središnja točka EU-a za procjene hibridnih prijetnji. **Izgradnja otpornosti** ključna je za sprečavanje i zaštitu od hibridnih prijetnji. Zato je iznimno važno sustavno pratiti i objektivno mjeriti napredak u tom području. Prvi korak bit će utvrđivanje osnovica sektorske hibridne otpornosti za države članice kao i institucije i tijela EU-a. Na kraju, kako bi se pojačala **pripravnost za odgovor na hibridne krize**, trebalo bi preispitati postojeći protokol definiran u protokolu „EU Playbook" iz 2016.[79], u okviru šireg preispitivanja i jačanja sustava EU-a za odgovor na krizne situacije koji se trenutačno razmatra[80]. Cilj je maksimalno povećati učinak djelovanja EU-a brzim povezivanjem sektorskih odgovora i osiguravanjem nesmetane suradnje s našim partnerima, prvenstveno NATO-om.

Ključne mjere
• osigurati provedbu i svrsishodnost zakonodavstva o kiberkriminalitetu • strategija za učinkovitiju borbu protiv seksualnog zlostavljanja djece • prijedlozi za otkrivanje i uklanjanje materijala povezanog sa seksualnim zlostavljanjem djece • pristup EU-a za suzbijanje hibridnih prijetnji • preispitivanje operativnog protokola EU-a za suzbijanje hibridnih prijetnji („EU Playbook") • procjena načina jačanja policijskih kapaciteta za istrage u području digitalnih tehnologija

3. Zaštita Europljana od terorizma i organiziranog kriminala

Terorizam i radikalizacija

Rizik od terorizma u EU-u i dalje je visok. Iako se njihov ukupan broj smanjio, napadi i dalje mogu imati razorne posljedice. U širem smislu, radikalizacija također može polarizirati i destabilizirati socijalnu koheziju. Države članice i dalje snose primarnu odgovornost u borbi protiv terorizma i radikalizacije. Međutim, zbog širenja prekogranične/međusektorske dimenzije prijetnji potrebne su daljnje mjere u pogledu suradnje i koordinacije na razini EU-a. Prioritet je učinkovita provedba zakonodavstva EU-a u području borbe protiv terorizma[81], uključujući mjere ograničavanja. I dalje je cilj proširiti ovlasti Ureda europskog javnog tužitelja na prekogranična kaznena djela terorizma.

Borba protiv terorizma počinje rješavanjem njegovih uzroka. Polarizacija društva, stvarna ili percipirana diskriminacija te drugi psihološki i sociološki čimbenici mogu povećati

[79] Operativni protokol EU-a za suzbijanje hibridnih prijetnji („EU Playbook"), SWD(2016) 227.

[80] Nakon videokonferencije održane 26. ožujka 2020. članovi Europskog vijeća donijeli su Izjavu o mjerama EU-a kao odgovor na izbijanje bolesti COVID-19, u kojoj su pozvali Komisiju da podnese prijedloge za ambiciozniji i opsežniji sustav za upravljanje krizama unutar EU-a.

[81] Vijeće je donijelo mjere ograničavanja u pogledu ISIL-a (Islamske države) i Al Qaide, kao i posebne mjere ograničavanja protiv određenih osoba i subjekata s ciljem borbe protiv terorizma. Za pregled svih mjera ograničavanja vidjeti kartu sankcija EU-a (https://www.sanctionsmap.eu/#/main).

prijemčivost za radikalni diskurs. U tom je smislu borba protiv **radikalizacije** usko povezana s poticanjem socijalne kohezije na lokalnoj, nacionalnoj i europskoj razini. U zadnjem je desetljeću razvijeno nekoliko učinkovitih inicijativa i politika, posebno u okviru Mreže za osvješćivanje o radikalizaciji i inicijative Gradovi EU-a protiv radikalizacije.[82] Sada treba osmisliti mjere kojima će se povećati učinkovitost politika, inicijativa i sredstava EU-a za borbu protiv radikalizacije. Takvim se mjerama može poduprijeti razvoj sposobnosti i vještina, poboljšati suradnja, ojačati baza dokaza i pridonijeti ocjeni napretka za sve relevantne dionike, uključujući stručnjake, tvorce politika i akademsku zajednicu na prvoj liniji[83]. „Meke" politike kao što su obrazovanje, kultura, mladi i sport mogle bi doprinijeti sprečavanju radikalizacije pružanjem prilika ugroženim mladima i povećanjem kohezije u EU-u[84]. Prioritetna područja uključuju rad na ranom otkrivanju i upravljanju rizikom, izgradnji otpornosti i odustajanju od nasilja te rehabilitaciju i reintegraciju u društvo.

Teroristi su pokušavali nabaviti **kemijski, biološki, radiološki i nuklearni** (KBRN) materijal[85], pretvoriti ga u oružje te steći znanje i kapacitete za njihovu uporabu[86]. Mogućnost KBRN napada vrlo je prisutna u terorističkoj propagandi. S obzirom na veliku potencijalnu štetu takvih napada, potrebno im je posvetiti posebnu pozornost. Oslanjajući se na pristup upotrijebljen za reguliranje pristupa prekursorima eksploziva, Komisija će razmotriti mogućnosti ograničavanja pristupa određenim opasnim kemikalijama koje bi se mogle upotrijebiti za izvršenje napada. Od ključne će važnosti biti i razvoj kapaciteta Mehanizma EU-a za civilnu zaštitu (rescEU) u području KBRN-a. Za jačanje opće kulture zaštite i sigurnosti u području KBRN-a važna je i suradnja s trećim zemljama, pri čemu treba u potpunosti iskoristiti globalne centre izvrsnosti EU-a za KBRN. Ta će suradnja uključivati nacionalne procjene nedostataka i rizika, potporu nacionalnim i regionalnim akcijskim planovima u području KBRN-a, razmjenu dobre prakse i aktivnosti izgradnje kapaciteta u području KBRN-a.

EU ima najnaprednije zakonodavstvo u svijetu za ograničavanje pristupa **prekursorima eksploziva**[87] i otkrivanje sumnjivih transakcija čija je svrha izrada improviziranih eksplozivnih naprava. Međutim, i dalje postoji velika opasnost od eksploziva kućne izrade, korištenih u brojnim napadima diljem EU-a[88]. Prvi korak mora biti provedba propisa i onemogućavanje zaobilaženja kontrola u internetskom okruženju.

Djelotvoran kazneni progon počinitelja kaznenih djela terorizma, uključujući **strane terorističke borce** koji se trenutačno nalaze u Siriji i Iraku, također je važan element politike borbe protiv terorizma. Iako ta pitanja prvenstveno rješavaju države članice, koordinacija i potpora na razini EU-a mogu im pomoći u prevladavanju zajedničkih izazova. Važnu će ulogu imati mjere koje su poduzete za potpunu provedbu zakonodavstva o

[82] Pilot-inicijativa „Gradovi EU-a protiv radikalizacije" ima dvostruki cilj poticanja razmjene stručnog znanja među gradovima EU-a i prikupljanja povratnih informacija o tome kako na najbolji način poduprijeti lokalne zajednice na razini EU-a.

[83] Na primjer, financiranje u okviru Europskog fonda za sigurnost i Programa za građanstvo.

[84] Aktivnosti EU-a kao što su virtualne razmjene u okviru programa Erasmus+, e-twinning.

[85] Na primjer, u posljednje dvije godine bilo je nekoliko slučajeva uporabe bioloških agensa (obično toksini na biljnoj osnovi) u Europi (Francuska, Njemačka, Italija) i drugdje (Tunis, Indonezija).

[86] Vijeće je donijelo mjere ograničavanja u pogledu širenja i uporabe kemijskog oružja.

[87] Kemikalije koje bi se mogle zloupotrijebiti za proizvodnju eksploziva kućne izrade. Oni su uređeni Uredbom (EU) 2019/1148 o stavljanju na tržište i uporabi prekursora eksploziva.

[88] Primjeri takvih razornih napada uključuju napade u Oslu (2011.), Parizu (2015.), Bruxellesu (2016.) i Manchesteru (2017.). U napadu eksplozivom kućne izrade u Lyonu (2019.) ranjeno je 13 osoba.

sigurnosti granica[89] i potpuno iskorištavanje svih relevantnih baza podataka EU-a za razmjenu informacija o poznatim sumnjivim osobama. Uz utvrđivanje visokorizičnih pojedinaca, potrebna je i politika reintegracije i rehabilitacije. Suradnja među strukama, među ostalim sa zatvorskim i probacijskim osobljem, pomoći će pravosudnom sustavu da razumije proces radikalizacije koji dovodi do nasilnog ekstremizma i da oblikuje pristup izricanju kazni i alternativama pritvoru.

Izazov koji predstavljaju strani teroristički borci karakterističan je primjer povezanosti između unutarnje i **vanjske sigurnosti**. Suradnja u borbi protiv terorizma te sprečavanju i suzbijanju radikalizacije i nasilnog ekstremizma ključna je za sigurnost unutar EU-a[90]. Potrebno je poduzeti daljnje korake za razvoj protuterorističkih partnerstava i suradnje sa zemljama u susjedstvu i šire, oslanjajući se na stručno znanje mreže stručnjaka EU-a za borbu protiv terorizma i sigurnost. Zajednički akcijski plan EU-a i zapadnog Balkana za borbu protiv terorizma dobra je referenca za takvu ciljanu suradnju. Posebno treba uložiti napore u potporu kapacitetima partnerskih zemalja za identifikaciju i lociranje stranih terorističkih boraca. EU će nastaviti promicati i multilateralnu suradnju, tj. suradnju s vodećim globalnim akterima u tom području, kao što su Ujedinjeni narodi, NATO, Vijeće Europe, Interpol i OESS. Surađivat će i s Globalnim forumom za borbu protiv terorizma i Globalnom koalicijom za borbu protiv Islamske države kao i s relevantnim akterima civilnog društva. Instrumenti vanjske politike Unije, uključujući razvoj i suradnju, također imaju važnu ulogu u suradnji s trećim zemljama na sprečavanju terorizma i piratstva. Međunarodna suradnja ključna je i za ukidanje svih izvora **financiranja terorizma**, primjerice u okviru Stručne skupine za financijsko djelovanje.

Organizirani kriminal

Organizirani kriminal podrazumijeva ogromne gospodarske i ljudske gubitke. Procjenjuje se da gospodarski gubici zbog organiziranog kriminala i korupcije iznose od 218 do 282 milijardi EUR godišnje.[91] U Europi je 2017. pod istragom bilo više od 5 000 skupina organiziranog kriminala, što je porast od 50 % u odnosu na 2013.[92] Organizirani kriminal sve se više odvija prekogranično, uključujući iz neposrednog susjedstva EU-a, zbog čega je potrebna jača operativna suradnja i razmjena informacija s partnerima u susjedstvu.

Pojavili su se novi izazovi koji otvaraju put internetskom kriminalu: tijekom pandemije bolesti COVID-19 zabilježen je golem porast prijevara na internetu čije su žrtve ranjive skupine, kao i zdravstvenih i sanitarnih proizvoda koji su meta krađa i provala.[93] EU se treba intenzivnije boriti protiv organiziranog kriminala, među ostalim na međunarodnoj razini, i na raspolaganju imati više sredstava za razbijanje poslovnog modela organiziranog kriminala. Borba protiv organiziranog kriminala zahtijeva i blisku suradnju s lokalnim i regionalnim upravama te civilnim društvom, koji su ključni partneri u sprečavanju kriminala te pružanju pomoći i potpore žrtvama, posebno uprave u pograničnim regijama. Taj će se rad objediniti u **Agendi za borbu protiv organiziranog kriminala.**

---

89 Uključujući novi mandat Agencije za europsku graničnu i obalnu stražu (Frontex).

90 U zaključcima Vijeća od 16. lipnja 2020. naglašena je potreba za zaštitom građana EU-a od terorizma i nasilnog ekstremizma, u svim njihovim oblicima i neovisno o njihovu podrijetlu, te za daljnjim jačanjem vanjskog angažmana i djelovanja EU-a u borbi protiv terorizma u određenim prioritetnim geografskim i tematskim područjima.

91 U obliku % bruto domaćeg proizvoda (BDP); Izvješće Europola: „Isplati li se još kriminal?” – Oduzimanje imovinske koristi stečene kaznenim djelima u EU-u, 2016.

92 Europol, Procjena prijetnje teškog i organiziranog kriminala (SOCTA), 2013. i 2017.

93 Europol, 2020.

Više od trećine skupina organiziranog kriminala aktivnih u EU-u uključeno je u proizvodnju, trgovinu ili distribuciju droga. U 2019. je od posljedica predoziranja u EU-u umrlo više od osam tisuća ovisnika o drogama. Glavnina **trgovine drogom** obavlja se preko granica, a velik dio profita prodire u zakonito gospodarstvo[94]. Novom Agendom EU-a za borbu protiv droga[95] ojačat će se napori EU-a i država članica u području smanjenja potražnje i ponude droga, definiranja zajedničkih djelovanja kojima se rješava zajednički problem te jačanja dijaloga i suradnje između EU-a i vanjskih partnera u pitanjima povezanima s drogom. Nakon evaluacije Europskog centra za praćenje droga i ovisnosti o drogama Komisija će procijeniti treba li mu zbog novih izazova ažurirati ovlasti.

Skupine organiziranog kriminala i teroristi ključni su akteri i u trgovini **nezakonitim vatrenim oružjem**. Od 2009. do 2018. u Europi se dogodilo 23 masovnih pucnjava u kojima je poginulo više od 340 osoba.[96] Vatreno oružje često nezakonitom trgovinom dospije u EU iz neposrednog susjedstva.[97] To upućuje na potrebu za jačanjem koordinacije i suradnje unutar EU-a i s međunarodnim partnerima, osobito Interpolom, kako bi se uskladilo prikupljanje informacija i izvješćivanje o zapljenama vatrenog oružja. Važno je i poboljšati sljedivost oružja, među ostalim na internetu, te osigurati razmjenu informacija između tijela za izdavanje dozvola i tijela kaznenog progona. Komisija predlaže novi **Akcijski plan EU-a za borbu protiv nezakonite trgovine vatrenim oružjem**[98] te će ocijeniti jesu li pravila o odobrenju izvoza vatrenog oružja te mjerama za uvoz i provoz vatrenog oružja i dalje svrsishodna[99].

Zločinačke organizacije migrante i osobe kojima je potrebna međunarodna zaštita smatraju robom. 90 % nezakonitih migranata u EU je došlo uz pomoć kriminalne mreže.[100] Krijumčarenje migranata često je isprepleteno s drugim oblicima organiziranog kriminala, posebno trgovinom ljudima.[101] Trgovina ljudima uzrokuje goleme ljudske gubitke, a Europol procjenjuje da globalni godišnji profit od svih oblika iskorištavanja u okviru trgovine ljudima iznosi 29,4 milijardi EUR. Riječ je o transnacionalnom kriminalu koji se hrani nezakonitom potražnjom u i izvan EU-a te utječe na sve države članice EU-a. Zbog slabih rezultata u utvrđivanju, kaznenom progonu i osuđivanju tih kaznenih djela potreban je novi pristup i jače djelovanje. Novi **sveobuhvatan pristup trgovini ljudima** objedinit će različita područja djelovanja. Osim toga, Komisija će predstaviti **novi Akcijski plan EU-a za borbu protiv krijumčarenja migranata** za razdoblje 2021.–2025. U oba će slučaja naglasak biti na borbi protiv kriminalnih mreža, jačanju suradnje i potpori radu tijela kaznenog progona.

Skupine organiziranog kriminala, kao i teroristi, prilike traže i u drugim područjima, posebno onima u kojima se može ostvariti veliki profit s niskim rizikom od otkrivanja, kao što su **kaznena djela protiv okoliša**. Nezakoniti lov i trgovina divljom faunom i florom,

---

94 EMCDDA i Europol, Izvješće EU-a o tržištima droga za 2019. (studeni 2019.).

95 Agenda i akcijski plan EU-a za borbu protiv droga 2021.–2025., COM(2020) 606.

96 Flamanski mirovni institut, Armed to kill (Naoružani da ubiju). (listopad 2019.).

97 EU od 2002. financira borbu protiv širenja i nezakonite trgovine malim i lakim oružjem u regiji; primjerice, financirao je Mrežu stručnjaka za vatreno oružje u jugoistočnoj Europi (SEEFEN). Partneri sa zapadnog Balkana su od 2019. potpuno uključeni u prioritet Europske multidisciplinarne platforme za borbu protiv kaznenih djela (EMPACT) u pogledu vatrenog oružja.

98 COM(2020) 608.

99 Uredba (EU) br. 258/2012 o provedbi članka 10. Protokola Ujedinjenih naroda protiv nezakonite proizvodnje i trgovanja vatrenim oružjem.

100 Izvor: Europol.

101 Europol, EMSC, 4. godišnje izvješće.

nezakonito rudarenje, sječa drva te nezakonito odlaganje i otprema otpada postali su četvrta po redu kriminalna djelatnost u svijetu[102]. Nezakonito se iskorištavaju i sustav trgovanja emisijama i sustavi energetskih certifikata te se zloupotrebljavaju sredstva dodijeljena za otpornost okoliša i održivi razvoj. Osim što potiče djelovanje EU-a, država članica i međunarodne zajednice kako bi se pojačali napori u borbi protiv kaznenih djela protiv okoliša[103], Komisija procjenjuje je li Direktiva o kaznenim djelima protiv okoliša[104] još svrsishodna. **Nezakonita trgovina kulturnim dobrima** raste te je postala jedna od najunosnijih kriminalnih aktivnosti i izvor financiranja terorista i organiziranog kriminala. Trebalo bi istražiti kako poboljšati sljedivost kulturnih dobara na internetu i izvan njega na unutarnjem tržištu i suradnju s trećim zemljama u kojima su kulturna dobra ukradena te kako pružiti aktivnu potporu tijelima kaznenog progona i akademskim zajednicama.

Gospodarski i financijski kriminal vrlo je složen te svake godine pogađa milijune građana i tisuće poduzeća u EU-u. Borba protiv prijevara je ključna i zahtijeva djelovanje na razini EU-a. Europol, Eurojust, Ured europskog javnog tužitelja i Europski ured za borbu protiv prijevara podupiru države članice i EU u zaštiti gospodarskih i financijskih tržišta i zaštiti novca poreznih obveznika EU-a. Ured europskog javnog tužitelja bit će sasvim operativan krajem 2020. te će istraživati, kazneno goniti i podizati optužnice protiv kaznenih djela protiv proračuna EU-a, kao što su prijevara, korupcija i pranje novca. Borit će se i protiv prekograničnih prijevara povezanih s PDV-om koji porezne obveznike košta najmanje 50 milijardi EUR godišnje.

Komisija će podupirati razvoj stručnog znanja i zakonodavnog okvira i kad je riječ o novim rizicima, kao što su kriptoimovina i novi sustavi plaćanja. Konkretno, Komisija će razmotriti kako odgovoriti na pojavu kriptoimovine, kao što je Bitcoin, i na učinak te nove tehnologije na izdavanje, razmjenu i pristup financijskoj imovini.

Europska unija ne bi smjela tolerirati nezakonit novac. EU je više od trideset godina razvijao svoj čvrst regulatorni okvir za sprječavanje i suzbijanje **pranja novca** i financiranja terorizma, uz potpuno poštovanje potrebe za zaštitom osobnih podataka. Međutim, sve je veći konsenzus da je potrebno znatno poboljšati provedbu postojećeg okvira. Potrebno je ukloniti velike razlike u načinu na koji se primjenjuje i ozbiljne slabosti u provedbi pravila. Kako je detaljno opisano u Akcijskom planu iz svibnja 2020.[105], u tijeku je rad na procjeni mogućnosti za poboljšanje okvira EU-a za sprječavanje pranja novca i borbu protiv financiranja terorizma. Područja koja treba istražiti uključuju međusobnu povezanost nacionalnih centraliziranih registara bankovnih računa, što bi moglo znatno ubrzati pristup financijskim informacijama za financijsko-obavještajne jedinice i nadležna tijela.

Procjenjuje se da **skupine organiziranog kriminala** u EU-u ostvaruju **profit** od 110 milijardi EUR godišnje. Trenutačni odgovor uključuje usklađeno zakonodavstvo o oduzimanju i povratu imovine[106], kojim se poboljšava zamrzavanje i oduzimanje imovine stečene kaznenim djelima u EU-u i potiče uzajamno povjerenje i učinkovita prekogranična suradnja među državama članicama. Međutim, samo je oko 1 % tih prihoda oduzeto[107], čime se skupinama organiziranog kriminala omogućuje da ulažu u širenje svojih kriminalnih

[102] UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime (Procjena brzog odgovora: porast kaznenih djela protiv okoliša), lipanj 2016.
[103] Vidjeti Europski zeleni plan COM(2019) 640 final.
[104] Direktiva 2008/99/EZ o zaštiti okoliša putem kaznenog prava
[105] Akcijski plan za sprječavanje pranja novca i financiranja terorizma COM(2020) 2800.
[106] Pravom EU-a propisano je da se uredi za oduzimanje imovinske koristi moraju osnovati u svim državama članicama.
[107] Izvješće o povratu i oduzimanju imovine: osiguravanje da se zločin ne isplati, COM(2020) 217 final.

aktivnosti i prodiru u zakonito gospodarstvo, a važna meta za aktivnosti pranja novca su mala i srednja poduzeća, koja imaju poteškoća u pristupu kreditima. Komisija će analizirati provedbu zakonodavstva[108] i potrebu za daljnjim zajedničkim pravilima, među ostalim o oduzimanju bez presude. Osim toga, uredi za oduzimanje imovinske koristi[109], koji su ključni akteri u postupku povrata imovine, mogli bi biti opremljeni boljim sredstva za brže utvrđivanje i praćenje imovine u EU-u, čime bi se povećale stope oduzimanja imovine.

Organizirani kriminal i **korupcija** blisko su povezani. Prema grubim procjenama sama korupcija gospodarstvo EU-a košta 120 milijardi EUR godišnje.[110] Sprečavanje i borba protiv korupcije i dalje će se redovito pratiti u okviru mehanizma vladavine prava i europskog semestra. U okviru europskog semestra ocijenjeni su izazovi u borbi protiv korupcije kao što su javna nabava, javna uprava, poslovno okruženje ili zdravstvena zaštita. Komisijino godišnje izvješće o vladavini prava obuhvaćat će borbu protiv korupcije i omogućiti preventivni dijalog s nacionalnim tijelima i dionicima na razini EU-a i na nacionalnoj razini. Organizacije civilnog društva također mogu bitno potaknuti djelovanje javnih tijela za sprečavanje i suzbijanje organiziranog kriminala i korupcije te bi bilo korisno okupiti te skupine na zajedničkom forumu. Zbog prekogranične prirode organiziranog kriminala i korupcije, suradnja i pomoć u susjednim regijama EU-a još je jedan važan aspekt.

Ključne mjere

- Agenda EU-a za borbu protiv terorizma, uključujući obnovu mjera protiv radikalizacije u EU-u
- nova suradnja s ključnim trećim zemljama i međunarodnim organizacijama u borbi protiv terorizma
- Agenda za borbu protiv organiziranog kriminala, uključujući trgovinu ljudima
- Agenda i akcijski plan EU-a za borbu protiv droga za razdoblje 2021.–2025.
- ocjena Europskog centra za praćenje droga i ovisnosti o drogama
- Akcijski plan EU-a za borbu protiv nezakonite trgovine vatrenim oružjem za razdoblje 2020.–2025.
- revizija zakonodavstva o zamrzavanju i oduzimanju imovine i o uredima za oduzimanje imovinske koristi
- ocjena Direktive o zaštiti okoliša putem kaznenog prava
- Akcijski plan EU-a protiv krijumčarenja migranata za razdoblje 2021.–2025.

4. Snažan europski sigurnosni ekosustav

Istinska i djelotvorna sigurnosna unija mora biti zajednički pothvat svih dijelova društva. Vlade, tijela kaznenog progona, privatni sektor, sektor obrazovanja i građani moraju biti angažirani, opremljeni i na odgovarajući način povezani kako bi se izgradila pripravnost i otpornost cijelog društva, a posebno najranjivijih skupina, žrtava i svjedoka.

[108] Direktiva 2014/42/EU o zamrzavanju i oduzimanju predmeta i imovinske koristi ostvarene kaznenim djelima.

[109] Odluka Vijeća 2007/845/PUP o suradnji između ureda za oduzimanje imovinske koristi država članica u području praćenja i utvrđivanja imovinske koristi ostvarene kaznenim djelom ili druge imovine povezane s kaznenim djelom.

[110] Teško je procijeniti ukupni gospodarski trošak korupcije, iako se na temelju procjena tijela kao što su Međunarodna trgovinska komora, Transparency International, Globalni kompakt UN-a i Svjetski gospodarski forum može zaključiti da korupcija iznosi 5 % svjetskog BDP-a.

Sve politike moraju imati sigurnosnu dimenziju, a EU može dati svoj doprinos na svim razinama. Nasilje u obitelji jedan je od najvećih sigurnosnih rizika. U EU-u je 22 % žena doživjelo nasilje od partnera[111]. Pristupanje EU-a Istanbulskoj konvenciji o sprečavanju i borbi protiv nasilja nad ženama i nasilja u obitelji i dalje je ključan prioritet. Ako pregovori ostanu blokirani, Komisija će poduzeti druge mjere za postizanje ciljeva Konvencije, uključujući prijedlog da se nasilje nad ženama doda na popis kaznenih djela EU-a utvrđenih Ugovorom.

Suradnja i razmjena informacija

EU-a može na bitan način pridonijeti zaštiti građana tako da olakša suradnju onih koji su odgovorni za sigurnost. Suradnja i razmjena informacija najmoćnija su sredstva za borbu protiv kriminala i terorizma i provođenje pravde. Da bi bile djelotvorne, moraju biti ciljane i pravodobne. Da bi bile pouzdane, potrebno je primjenjivati zajedničke zaštitne mjere i kontrole.

Uspostavljen je niz instrumenata EU-a i sektorskih strategija[112] za daljnji razvoj **operativne suradnje u kaznenom progonu** među državama članicama. Schengenski informacijski sustav jedan je od glavnih instrumenata EU-a kojim se potiče suradnja u kaznenom progonu među državama članicama, a upotrebljava se za razmjenu podataka o traženim i nestalim osobama i predmetima u stvarnom vremenu. Ostvareni su vidljivi rezultati kad je riječ o uhićenjima kriminalaca, oduzimanju droga i spašavanju potencijalnih žrtava.[113] Međutim, razina suradnje se još može poboljšati tako da se pojednostave i unaprijede dostupni instrumenti. Veći dio pravnog okvira EU-a na kojem se temelji operativna suradnja u kaznenom progonu oblikovan je prije 30 godina. Postoji rizik od fragmentacije složene mreže bilateralnih sporazuma među državama članicama, od kojih su mnogi zastarjeli ili nedovoljno iskorišteni. U manjim zemljama ili zemljama bez izlaza na more policijski službenici koji rade preko granica za obavljanje operativnih radnji ponekad moraju slijediti do čak sedam različitih skupova pravila. Zato se neke operacije, kao što su potjere osumnjičenika preko unutarnjih granica, jednostavno ne provode. Ni operativna suradnja u području novih tehnologija kao što su bespilotne letjelice nije obuhvaćena postojećim okvirom EU-a.

Operativna djelotvornost može se poduprijeti konkretnom suradnjom u kaznenom progonu, koja može bitno pridonijeti i drugim ciljevima politike, kao što je pružanje sigurnosnih informacija za potrebe nove procjene izravnih stranih ulaganja. Komisija će razmotriti kako to poduprijeti Kodeksom policijske suradnje. Tijela kaznenog progona država članica sve se više koriste potporom i stručnim znanjem na razini EU-a, a EU INTCEN je imao ključnu ulogu u promicanju razmjene strateških obavještajnih podataka među obavještajnim i sigurnosnim službama država članica, pružajući institucijama EU-a uvid u stanje na temelju obavještajnih podataka.[114] **Europol** također može imati važnu ulogu u širenju suradnje s trećim zemljama u borbi protiv kriminala i terorizma u skladu s drugim vanjskim politikama i instrumentima EU-a. No Europol se danas suočava s nizom ozbiljnih ograničenja, posebno u pogledu izravne razmjene osobnih podataka s privatnim stranama, zbog čega ne može učinkovito podupirati države članice u borbi protiv terorizma i kriminala. U tijeku je ocjena

[111] Unija ravnopravnosti: Strategija za rodnu ravnopravnost 2020.–2025.(COM(2020) 152).

[112] Kao što je akcijski plan strategije pomorske sigurnosti EU-a, koji je doveo do važnih postignuća u suradnji relevantnih agencija EU-a u pogledu funkcija obalne straže.

[113] Borba EU-a protiv organiziranog kriminala u 2019. (Vijeće, 2020.).

[114] EU INTCEN je jedini kanal putem kojeg obavještajne i sigurnosne službe država članica EU-u pružaju uvid u stanje na temelju obavještajnih podataka.

ovlasti Europola, čija je svrha utvrditi kako ga poboljšati i osigurati da ta agencija može u potpunosti izvršavati svoje zadaće. Stoga bi i relevantna tijela na razini EU-a (kao što su OLAF, Europol, Eurojust i Ured europskog javnog tužitelja) trebala tješnje surađivati i poboljšati razmjenu informacija.

Ključno je dalje razvijati vezu s **Eurojustom** kako bi se ostvarila što veća sinergija između policijske i pravosudne suradnje. EU-u bi koristila i veća strateška usklađenost: **EMPACT**[115], ciklus politike EU-a za borbu protiv teškog i međunarodnog organiziranog kriminala, nadležnim tijelima pruža kriminalističku obavještajnu metodologiju kako bi se zajednički borila protiv kaznenih djela koja najviše utječu na EU. To je dovelo do važnih operativnih rezultata[116] u proteklom desetljeću. Na temelju praktičnog iskustva, za odgovor na najhitnije i nove prijetnje kriminala u novom ciklusu politike za razdoblje 2022.–2025. potreban je učinkovitiji i jednostavniji mehanizam od postojećeg.

Pravodobne i relevantne **informacije** ključne su za svakodnevni rad u području kaznenog progona. Unatoč razvoju novih baza podataka na razini EU-a za sigurnost i upravljanje granicama, velik dio informacija i dalje je pohranjen u nacionalnim bazama podataka ili se razmjenjuje drugim alatima. Rezultat su znatno dodatno radno opterećenje, kašnjenja i veći rizik od propuštanja ključnih informacija. Bolji, brži i jednostavniji postupci koji uključuju cijelu sigurnosnu zajednicu donijeli bi bolje rezultate. Za uspješnu razmjenu podataka i djelotvornu borbu protiv kriminala nužni su odgovarajući alati te primjena zaštitnih mjera kojima će se osigurati poštovanje propisa o zaštiti podataka i temeljnih prava. S obzirom na tehnološki razvoj, razvoj forenzike i zaštite podataka te promijenjene operativne potrebe, EU bi mogao razmotriti postoji li potreba za modernizacijom instrumenata kao što su **prümske odluke iz 2008.**, kojima se uspostavlja automatizirana razmjena podataka o DNK-u, otiscima prstiju i registraciji vozila kako bi se za potrebe kaznenih istraga omogućila automatizirana razmjena dodatnih kategorija podataka koje su već dostupne u kaznenim ili drugim bazama podataka država članica. Osim toga, Komisija će razmotriti mogućnost razmjene policijskih evidencija radi utvrđivanja je li osoba kažnjavana u drugim državama članicama i olakšavanja pristupa toj evidenciji, uz primjenu svih nužnih zaštitnih mjera.

Informacije o putnicima omogućile su bolje granične kontrole, smanjenje nezakonitih migracija i identifikaciju osoba koje predstavljaju sigurnosni rizik. Unaprijed dostavljene informacije o putnicima biografski su podaci o svakom putniku koje su zračni prijevoznici prikupili tijekom prijave (*check-in*) i unaprijed poslali tijelima granične kontrole na odredištu. Revizija pravnog okvira[117] omogućila bi djelotvornije korištenje informacija u skladu sa zakonodavstvom o zaštiti podataka i lakši protok putnika. Evidencija podataka o putnicima (PNR) podaci su koje putnici dostavljaju pri rezervaciji leta. Provedba Direktive o evidenciji podataka o putnicima[118] od ključne je važnosti i Komisija će je nastaviti podupirati i provoditi. Osim toga, Komisija će kao mjeru na sredini provedbenog razdoblja pokrenuti reviziju trenutačnog pristupa **prijenosu podataka iz PNR-a u treće zemlje**.

Pravosudna suradnja nužna je dopuna radu policije u borbi protiv prekograničnog kriminala. Pravosudna suradnja znatno se promijenila u posljednjih 20 godina. Tijela kao što su **Ured europskog javnog tužitelja** i **Eurojust** moraju imati sredstva za optimalno funkcioniranje ili ih treba ojačati. Mogla bi se poboljšati i suradnja među pravosudnim

[115] EMPACT – Europska multidisciplinarna platforma za borbu protiv kaznenih djela.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.
[117] Direktiva Vijeća 2004/82/EZ o obvezi prijevoznika na dostavljanje podataka o putnicima.
[118] Direktiva 2016/681 o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela.

osobljem poduzimanjem daljnjih mjera u pogledu uzajamnog priznavanja sudskih odluka, pravosudne izobrazbe i razmjene informacija. Cilj bi trebao biti povećanje uzajamnog povjerenja među sucima i tužiteljima, što je ključno za neometano rješavanje prekograničnih postupaka. Upotrebom **digitalnih tehnologija** može se poboljšati i učinkovitost naših pravosudnih sustava. Uz potporu Eurojusta uspostavlja se novi sustav digitalne razmjene za prijenos europskih istražnih naloga te slanje zahtjeva za uzajamnu pravnu pomoć i povezane komunikacije među državama članicama. Komisija će s državama članicama raditi na uvođenju potrebnih IT sustava na nacionalnoj razini.

Međunarodna suradnja ključna je i za djelotvoran kazneni progon i pravosudnu suradnju. Bilateralni sporazumi s ključnim partnerima imaju važnu ulogu u osiguravanju informacija i dokaza izvan EU-a. Važnu ulogu ima **Interpol**, kao jedna od najvećih međuvladinih organizacija kriminalističke policije. Komisija će razmotriti mogućnosti za jačanje suradnje s Interpolom, uključujući pristup Interpolovim bazama podataka, te za jačanje operativne i strateške suradnje. U otkrivanju i istragama kriminalaca i terorista tijela kaznenog progona u EU-u oslanjaju se i na ključne partnerske zemlje. Trebalo bi promicati **sigurnosna partnerstva između EU-a i trećih zemalja** kako bi se povećala suradnja u borbi protiv zajedničkih prijetnji, kao što su terorizam, organizirani kriminal, kiberkriminalitet, seksualno zlostavljanje djece i trgovina ljudima. Takav bi se pristup temeljio na zajedničkim sigurnosnim interesima, postojećoj suradnji i sigurnosnim dijalozima.

Osim informacija, razmjena stručnog znanja može biti posebno korisna za povećanje spremnosti tijela kaznenog progona za **netradicionalne prijetnje.** Uz poticanje razmjene najboljih praksi, Komisija će proučiti mogućnost primjene **koordinacijskog mehanizma za policijske snage na razini EU-a** u slučajevima više sile, kao što su pandemije. Pandemija je pokazala i da će policijski nadzor digitalne zajednice, popraćen pravnim okvirima za olakšavanje policijskog nadzora interneta, imati važnu ulogu u borbi protiv kriminala i terorizma. Partnerstva između policije i zajednice na internetu i izvan njega mogu spriječiti kriminal i ublažiti posljedice organiziranog kriminala, radikalizacije i terorističkih aktivnosti. Povezanost lokalnih i regionalnih policijskih rješenja s policijskim rješenjima EU-a ključan je čimbenik uspjeha sigurnosne unije EU-a u cjelini.

Prednost snažnih vanjskih granica

Moderno i djelotvorno upravljanje vanjskim granicama pruža dvostruku korist očuvanja integriteta Schengenskog prostora i pružanja sigurnosti našim građanima. Maksimalno iskorištavanje sigurnosti na granici uključivanjem svih dionika može imati konkretan učinak na sprečavanje prekograničnog kriminala i terorizma. Zajedničkim operativnim aktivnostima nedavno ojačane europske granične i obalne straže[119]pridonosi se sprečavanju i otkrivanju prekograničnog kriminala na **vanjskim granicama** i izvan EU-a. Za borbu protiv prekograničnog kriminala i terorizma ključne su carinske aktivnosti otkrivanja sigurnosnih rizika sve robe prije ulaska u EU i njezina kontroliranja na ulasku u EU. U predstojećem Akcijskom planu o carinskoj uniji najavit će se mjere za jačanje upravljanja rizikom i poboljšanje unutarnje sigurnosti, među ostalim procjenom izvedivosti povezivanja relevantnih informacijskih sustava za analizu sigurnosnih rizika.

Okvir za **interoperabilnost informacijskih sustava EU-a** u području pravosuđa i unutarnjih poslova donesen je u svibnju 2019. Tom novom strukturom nastoji se poboljšati

[119] Sastoji se od Agencije za europsku graničnu i obalnu stražu (Frontex) te tijela graničnog nadzora i obalne straže država članica.

učinkovitost i djelotvornost novih ili nadograđenih informacijskih sustava.[120] To će dovesti do bržeg i sustavnijeg informiranja policijskih službenika, službenika graničnog nadzora i službenika za migracije. Pridonijet će točnom identificiranju i borbi protiv prijevara povezanih s identitetom. Kako bi se to ostvarilo, provedba interoperabilnosti trebala bi biti politički i tehnički prioritet. Bliska suradnja između agencija EU-a i svih država članica bit će ključna za postizanje cilja potpune interoperabilnosti do 2023.

Krivotvorenje putnih isprava među najčešćim je kaznenim djelima. Olakšava nezakonito kretanje kriminalaca i terorista te ima ključnu ulogu u trgovini ljudima i drogom.[121] Komisija će istražiti kako proširiti postojeći rad na sigurnosnim standardima EU-a za boravišne i putne isprave, među ostalim digitalizacijom. Države članice će od kolovoza 2021. početi izdavati osobne iskaznice i boravišne isprave u skladu s usklađenim sigurnosnim standardima, uključujući čip s biometrijskim identifikatorima koje mogu provjeriti sva granična tijela EU-a. Komisija će pratiti provedbu tih novih pravila, uključujući postupnu zamjenu dokumenata koji se trenutačno koriste.

Jačanje istraživanja i inovacija u području sigurnosti

Osiguravanje kibersigurnosti i borba protiv organiziranog kriminala, kiberkriminaliteta i terorizma uvelike ovise o razvoju alata za budućnost: kako bi se stvorile sigurnije nove tehnologije, odgovorilo na izazove koje donose tehnologije i pružila potpora radu tijela kaznenog progona. To pak ovisi o privatnim partnerima i industrijama.

Inovacije bi trebalo smatrati strateškim alatom za suzbijanje trenutačnih prijetnji i predviđanje budućih rizika i prilika. Inovativnim tehnologijama mogu se proizvesti novi alati za pomoć tijelima kaznenog progona i drugim akterima u području sigurnosti. Umjetna inteligencija i analiza velikih podataka mogle bi iskoristiti računalstvo visokih performansi kako bi se omogućilo bolje otkrivanje i brza i sveobuhvatna analiza[122]. Glavni preduvjet za razvoj pouzdanih tehnologija jesu visokokvalitetni skupovi podataka koji su dostupni nadležnim tijelima za razvoj, testiranje i potvrđivanje algoritama[123]. U širem smislu, danas postoji velika opasnost od tehnološke ovisnosti – EU je, na primjer, neto uvoznik proizvoda i usluga za kibersigurnost, uz sve ono što to znači za gospodarstvo i kritičnu infrastrukturu. Kako bi se ovladalo tehnologijom i zajamčio kontinuitet opskrbe i u slučaju nepovoljnih događaja i kriza, Europi su potrebni prisutnost i kapacitet u kritičnim dijelovima relevantnih vrijednosnih lanaca.

Istraživanje, inovacije i tehnološki razvoj u EU-u nude priliku da se sigurnosna dimenzija uzme u obzir pri razvoju tih tehnologija i njihove primjene. Sljedeća generacija prijedloga za financiranje EU-a tomu može biti važan poticaj[124]. U inicijativama za europski podatkovni prostor i infrastrukturu oblaka element sigurnosti se od početka uzimao u obzir. Europski centar za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreža

[120] Sustav ulaska/izlaska (EES), europski sustav za informacije o putovanjima i odobravanje putovanja (ETIAS), prošireni Europski informacijski sustav kaznene evidencije (ECRIS-TCN), Schengenski informacijski sustav, vizni informacijski sustav i budući ažurirani Eurodac.

[121] Veza između krivotvorenja isprava i trgovine ljudima navedena je u Drugom izvješću o napretku u borbi protiv trgovanja ljudima, COM(2018) 777 i pratećem dokumentu SWD(2018) 473 i Izvješću Europola o stanju trgovanja ljudima u EU-u, 2016.

[122] To bi se trebalo temeljiti na strategiji Komisije o umjetnoj inteligenciji.

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

[124] Prijedlozima Komisije za Obzor Europa, Fond za unutarnju sigurnost, Fond za integrirano upravljanje granicama, program InvestEU, Europski fond za regionalni razvoj i program Digitalna Europa poduprijet će se razvoj i uvođenje inovativnih sigurnosnih tehnologija i rješenja u cijelom vrijednosnom lancu sigurnosti.

nacionalnih koordinacijskih centara[125] nastoje uspostaviti učinkovitu i djelotvornu strukturu za udruživanje i dijeljenje istraživačkih kapaciteta i rezultata u području kibersigurnosti. Svemirski program EU-a pruža usluge kojima se podupire sigurnost EU-a, njegovih država članica i pojedinaca[126].

S više od 600 projekata provedenih od 2007. u ukupnoj vrijednosti od približno 3 milijarde EUR, istraživanje u području sigurnosti koje financira EU važan je instrument za poticanje razvoja tehnologije i znanja u području sigurnosnih rješenja. U okviru preispitivanja mandata Europola Komisija će razmotriti uspostavu **Europskog inovacijskog centra za unutarnju sigurnost**[127], koji bi oblikovao opća rješenja za zajedničke sigurnosne izazove i mogućnosti koja države članice možda ne bi mogle samostalno iskorištavati. Suradnja je ključna za optimalno iskorištavanje ulaganja i razvoj inovativnih tehnologija koje koriste i sigurnosti i gospodarstvu.

Jačanje vještina i informiranje

Svijest o sigurnosnim pitanjima i stjecanje vještina za suočavanje s potencijalnim prijetnjama ključni su za izgradnju otpornijeg društva s bolje pripremljenim poduzećima, upravama i pojedincima. Problemi s IT infrastrukturom i e-sustavima pokazali su da je potrebno poboljšati naše kapacitete za pripravnost i odgovor u području kibersigurnosti. Pandemija je iznijela na vidjelo važnost digitalizacije u svim područjima gospodarstva i društva EU-a.

Čak i **osnovno poznavanje sigurnosnih prijetnji** i načina borbe protiv njih može pridonijeti otpornosti društva. U borbi protiv kibernapada mogu se iskoristiti informiranost o rizicima kiberkriminaliteta i zaštita od njega, kao i zaštita pružatelja usluga. Informiranje o opasnostima i rizicima trgovine drogom kriminalcima može otežati posao. EU može poticati širenje najbolje prakse, primjerice putem mreže centara za sigurniji internet[128], te osigurati da se ti ciljevi uključe u programe EU-a.

Budući akcijski plan za digitalno obrazovanje trebao bi sadržavati ciljane mjere za poboljšanje IT vještina cijelog stanovništva u području sigurnosti. Nedavno donesenim Programom vještina[129] podupire se cjeloživotno učenje vještina. Uključuje namjenske mjere za povećanje broja osoba s diplomom u području znanosti, tehnologije, inženjerstva, humanistike i matematike, koje su potrebne u najsuvremenijim područjima kao što je kibersigurnost. Dodatne mjere koje se financiraju u okviru programa Digitalna Europa stručnjacima će omogućiti da prate promjene u području sigurnosnih prijetnji i istovremeno popune manjak radne snage u tom području na tržištu rada EU-a. Njima će se općenito pojedincima omogućiti stjecanje vještina za suočavanje sa sigurnosnim prijetnjama, a poduzećima da pronađu stručnjake koji su im potrebni u tom području. Predstojećom

[125] Prijedlog od 12. rujna 2018. o osnivanju Europskog centra za stručnost u području kibersigurnosti, industrije, tehnologije i istraživanja i Mreže nacionalnih koordinacijskih centara, COM(2018) 630.

[126] Na primjer, u okviru programa Copernicus pružaju se usluge kojima se omogućuje nadzor vanjskih granica EU-a i pomorski nadzor, što pomaže u borbi protiv piratstva i krijumčarenja te podupire kritičnu infrastrukturu. Taj će program biti ključan čimbenik za civilne i vojne misije i operacije kad u cijelosti postane operativan.

[127] To bi funkcioniralo i s EBCGA-om/Frontexom, CEPOL-om, agencijom eu-LISA i Zajedničkim istraživačkim centrom.

[128] Vidjeti www.betterinternetforkids.eu: središnji portal i nacionalni centri za sigurniji internet trenutačno se financiraju u okviru telekomunikacijskog dijela Instrumenta za povezivanje Europe, a buduće financiranje predloženo je u okviru programa Digitalna Europa.

[129] Program vještina za Europu za održivu konkurentnost, socijalnu pravednost i otpornost, COM(2020) 274 final

uspostavom Europskog istraživačkog prostora i Europskog prostora obrazovanja promicat će se i karijere u području znanosti, tehnologije, inženjerstva, humanistike i matematike.

Važno je i da **žrtve** mogu ostvarivati svoja prava – primati pomoć i potporu koje su im potrebne zbog njihovih specifičnih okolnosti. Posebnu pozornost treba posvetiti manjinama i najranjivijim žrtvama, kao što su djeca ili žene kojima se trguje radi seksualnog iskorištavanja ili su izloženi nasilju u obitelji.[130]

Posebno je važno **poboljšati vještine u području kaznenog progona**. Zbog postojećih i novih tehnoloških prijetnji potrebno je više ulagati u usavršavanje policijskih službenika, na početku i tijekom cijele karijere. CEPOL je ključan partner koji pomaže državama članicama u izvršenju te zadaće. Osposobljavanje za kazneni progon rasizma i ksenofobije kao i zaštitu prava građana općenito mora biti temeljna sastavnica kulture sigurnosti EU-a. Nacionalni pravosudni sustavi i pravosudno osoblje također moraju biti opremljeni za prilagodbu i odgovor na nesvakidašnje izazove. Osposobljavanje je ključno kako bi nadležna tijela na terenu u operativnoj situaciji mogla potpuno iskoristiti te alate. Osim toga, svim sredstvima treba promicati rodno osviještenu politiku i sudjelovanje žena u kaznenom progonu.

Ključne mjere
• veće ovlasti Europola • mogućnost uvođenja „Kodeksa policijske suradnje" EU-a i policijske koordinacije u krizama • jačanje Eurojusta radi povezivanja pravosudnih i policijskih tijela • revizija Direktive o unaprijed dostavljenim informacijama o putnicima • Komunikacija o vanjskoj dimenziji evidencije podataka o putnicima • jačanje suradnje između EU-a i Interpola • okvir za pregovore s ključnim trećim zemljama o razmjeni informacija • bolji sigurnosni standardi za putne isprave • mogućnost uspostave Europskog inovacijskog centra za unutarnju sigurnost

V. Zaključci

U sve turbulentnijem svijetu Europska unija općenito se i dalje smatra jednim od najzaštićenijih i najsigurnijih mjesta. No to nije nešto što se može uzeti zdravo za gotovo.

Novom strategijom sigurnosne unije postavljaju se temelji sigurnosnog ekosustava koji obuhvaća cijelo europsko društvo. Temelji se na spoznaji da je sigurnost zajednička odgovornost. Pitanje sigurnosti tiče se svih nas. Sva tijela vlasti, poduzeća, društvene organizacije, institucije i građani moraju ispunjavati svoje zadaće da bi nam društva bila sigurnija.

Sigurnosna pitanja sada treba promatrati s puno šireg gledišta nego prije. Treba prevladati lažne razlike između fizičkih i digitalnih potreba. Strategija EU-a za sigurnosnu uniju objedinjuje cijeli niz sigurnosnih potreba i usredotočuje se na područja koja su u narednim godinama najkritičnija za sigurnost EU-a. U njoj se uzima u obzir činjenica da sigurnosne prijetnje nemaju geografskih granica i sve veća međusobna povezanost unutarnje i vanjske

[130] Vidjeti Strategiju za ravnopravnost spolova, COM(2020) 152, Strategiju za prava žrtava, COM(2020) 258 i Europsku strategiju za bolji internet za djecu, COM(2012) 196.

sigurnosti[131]. Zato je važno da EU radi zaštite svih svojih građana surađuje s međunarodnim partnerima i da ovu Strategiju provodi u bliskoj koordinaciji s vanjskim djelovanjem EU-a.

Naša je sigurnost povezana s našim temeljnim vrijednostima. Svim predloženim mjerama i inicijativama u ovoj Strategiji u potpunosti se poštuju temeljna prava i naše europske vrijednosti. To je temelj našeg europskog načina života i mora ostati polazište našeg rada.

Na kraju, Komisija je i dalje u potpunosti svjesna činjenice da se vrijednost svake mjere ili politike mjeri njihovom provedbom. Stoga je potrebno zadržati stalan naglasak na pravilnoj provedbi i primjeni postojećeg i budućeg zakonodavstva. To će se pratiti putem redovitih izvješća o sigurnosnoj uniji, a Komisija će u potpunosti obavješćivati Europski parlament, Vijeće i dionike i uključivati ih u sve relevantno djelovanje. Osim toga, Komisija je spremna organizirati i sudjelovati u zajedničkim raspravama o Strategiji za sigurnosnu uniju s institucijama kako bi se zajedno sagledao postignuti napredak i pripremilo za buduće izazove.

Komisija poziva Europski parlament i Vijeće da podrže ovu Strategiju za sigurnosnu uniju kao temelj za suradnju i zajedničko djelovanje u području sigurnosti u sljedećih pet godina.

[131] Vidjeti Globalnu strategiju EU-a