Povzetek

Boj proti kibernetski kriminaliteti je edinstven in zahteven zaradi več dejavnikov. Kibernetska kriminaliteta po svoji naravi nima meja in se hitro razvija, včasih celo hitreje, kot se lahko odzovejo nacionalni organi. Dodatna raven kompleksnosti je horizontalna narava kibernetske kriminalitete: skoraj vse vrste kaznivih dejanj se lahko danes zgodijo prek interneta. Zaradi nestanovitnosti podatkov je morda težko zbrati elektronske dokaze o tovrstnih kaznivih dejanjih, poleg tega pa je potrebno tudi posebno strokovno znanje. Pravosodno sodelovanje je bistveno za pravočasno zavarovanje elektronskih dokazov, s čimer za zajamči njihova dopustnost v sodnih postopkih. Mednarodno pravosodno sodelovanje lahko ovirajo precejšnje razlike v nacionalnih pravnih okvirih (npr. z vidika inkriminacije določenega ravnanja ali zakonodaje o hrambi podatkov) in spori o pristojnosti. Zaradi nadnacionalne narave dokazov, potrebnih za uspešen pregon kibernetskih kriminalcev, je celoten pojav kibernetske kriminalitete preoblikoval tradicionalni pravni pojem načela teritorialnosti.

Zato je za učinkovit odziv na kibernetsko kriminaliteto na nacionalni ravni pogosto potrebno sodelovanje na več ravneh. Okrepljeno mednarodno sodelovanje je ključnega pomena, saj je kibernetski prostor mednarodni in čezmejni. „Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor“ se na eni strani osredotoča na oblikovanje kibernetskega prostora, ki spodbuja dostop do interneta in zagotavlja rast trga, ter na drugi strani želi zagotoviti kibernetsko odpornost in se boriti proti kibernetski kriminaliteti ter vzpostaviti pravo ravnovesje med temeljnimi pravicami državljanov in pravno državo ([1]). Poleg tega spodbuja uporabo orodij za mednarodno sodelovanje v boju proti kibernetski kriminaliteti ter s tem povezano policijsko in pravosodno sodelovanje v tretjih državah, iz katerih delujejo organizacije, ki se ukvarjajo s kibernetskim kriminalom ([2]).

Sklepi Sveta z naslovom „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“ ([3]) dopolnjujejo strategijo EU za kibernetsko varnost s poudarjanjem potrebe po preprečevanju zlonamernih kibernetskih dejavnosti, odvračanju od njih, njihovem odkrivanju in odzivanju nanje. V njih je poudarjeno, da je treba javnim organom zagotoviti orodja za odkrivanje, preiskovanje in pregon kibernetske kriminalitete.

Eurojust se osredotoča na boj proti kibernetski kriminaliteti in si prizadeva za okrepljeno pravosodno sodelovanje na tem področju, zlasti z omogočanjem hitre obravnave sodnih zaprosil, kar je ključni dejavnik pri obravnavanju vprašanja nestanovitnosti podatkov in zapolnjevanja vrzeli, ki izhajajo iz uporabe različnih nacionalnih predpisov o hrambi podatkov, ter z zgodnjim vključevanjem sodstva v operacije zoper kibernetsko kriminaliteto za zagotovitev, da se podatki že med preiskavo zberejo v skladu z veljavnimi pravili in se lahko zato predložijo kot dopustni elektronski dokazi v nadaljnjih sodnih postopkih. Poleg tega pripravlja ali pomembno prispeva k pripravi strateških dokumentov na področju kibernetske kriminalitete, s čimer pravosodnim delavcem pomaga pri nadaljnjem razvoju njihovih znanj in spretnosti, potrebnih za delo na področju kibernetske varnosti ([4]).

Namen tega poročila je podati pregled dela Eurojusta na področju kibernetske kriminalitete. Eurojust namreč s svojim operativnim delovanjem ponuja odličen vpogled v skupne izzive, s katerimi se srečujejo pravosodni delavci, ter predstavlja primere dobre prakse za premagovanje teh izzivov. Njegovi primeri obravnave zadev so koristen vir informacij o posebnih ovirah na področju pravosodnega sodelovanja in o možnih rešitvah za njihovo premagovanje, s čimer se prispeva k razpravam o najboljših načinih spopadanja s kibernetsko kriminaliteto. V poglavju v nadaljevanju so

([1]) Svet Evropske unije, Sklepi Sveta o Skupnem sporočilu Komisije in visoke predstavnice Evropske unije za zunanje zadeve in varnostno politiko o Strategiji Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor, Bruselj, 22.7.2013 (12109/13)

([2]) Eurojust je zavezan več projektom za krepitev zmogljivosti na področju kibernetske kriminalitete, kot so projekt Sirius (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), projekt EuroMed Justice (https://www.euromed-justice.eu/) in projekt GLACY+ (https://www.coe.int/en/web/cybercrime/glacyplus).

([3]) Svet Evropske unije, Sklepi Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu: Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU, Bruselj, 20.11.2017 (14435/17).

([4]) Več informacij je na voljo v poglavju „Publikacije in projekti Eurojusta na področju kibernetske kriminalitete“ tega dokumenta.

navedeni konkretni sodni primeri. Na koncu poročila je naveden seznam Eurojustovih publikacij in projektov, ki so zanimivi z vidika kibernetske kriminalitete.