ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2023 (33)

KRIMINALISTIKOS MOKSLO INDĖLIS KOVOJANT SU ŠIUOLAIKINIU ORGANIZUOTU NUSIKALSTAMUMU

Povilas KĖŽA
Mykolo Romerio Universitetas, Viešojo Saugumo Akademija
Maironio g. 27, LT-44298 Kaunas, Lithuania
El. paštas pov.keza@gmail.com
ORCID ID: 0009-0009-8833-8332

Jurgita BALTRŪNIENĖ
Mykolo Romerio Universitetas, Viešojo Saugumo Akademija
Maironio g. 27, LT-44298 Kaunas, Lithuania
El. paštas: baltruniene.jurgita@gmail.com
ORCID ID: 0000-0001-8323-0570

DOI: 10.13165/PSPO-23-33-16

Anotacija. *Vienas pagrindinių kriminalistikos mokslo uždavinių yra nusikaltimų tyrimo, atskleidimo bei prevencijos metodų įdiegimas praktinėje veikloje. Socialiniai pokyčiai, mokslo ir technikos pažanga suteikia galimybę efektyviai panaudoti gautus rezultatus kriminalistikos metodų, priemonių bei rekomendacijų išpildymui kovojant su nusikalstamumu. Kriminalistikos mokslo raida rodo, kad naujų poreikių būvimas skatino konkrečių poreikių tenkinimą. Tokiu būdu buvo mažinama takoskyra tarp didėjančios būtinybės ir jos neišpildymo. Kriminalistika, kaip integralus mokslas yra priklausomas nuo kitų mokslų laimėjimų ir jų pritaikymo nusikaltimų tyrimo reikmėms. Ryšys tarp kriminalistikos mokslo ir esamų tendencijų turi būti glaudus ir nenutrūkstamas. Šis procesas, turi leisti ne tik efektyviai kovoti su esamomis grėsmėmis, bet taip pat užbėgti įvykiams už akių ir tokiu būdu didinti piliečių saugumą visuomenėje.*

Organizuotas nusikalstamumas yra viena pagrindinių grėsmių ES saugumui. Informacinėms Technologijoms žengiant į priekį, išvien keičiasi nusikaltimų modus operandi. Technologijos mums atveria lyg šiol nematytas galimybes, bet tuo pačiu suteikia ir beprecedentį lankstumą organizuotoms nusikalstamoms grupuotėms. Šiame straipsnyje apžvelgiamos galima dirbtinio intelekto ir kriminalistikos mokslo sąveika tarpusavyje kovojant su šiuolaikiniu[1] organizuotu nusikalstamumu ir esami iššūkiai tiriant, bei atskleidžiant nusikalstamas veikas. Analizuojamos organizuoto nusikalstamumo tendencijos ir dirbtinio taikymo galimybės tiriant, išaiškinant ir užkardant nusikalstamas veikas. Kovojant su šiuolaikiniu organizuotu nusikalstamumu, reikia naujų ir efektyvių metodų, būtina tobulinti teisėsaugos institucijų pajėgumus ir naudoti naujas technologijas, kurios padėtų atkleisti ir nustatyti nusikalstamų organizacijų veiklą ne tik fizinėje, bet ir virtualioje erdvėje. Reikia suprasti, kad šiame sparčiai besikeičiančiame pasaulyje, efektyvi kova su organizuotu nusikalstamumu yra įmanoma tik sujungiant profesionalaus personalo, pažangių technologijų ir tarptautinio bendradarbiavimo galimybes.

Pagrindinės sąvokos: *Dirbtinis intelektas, Konvoliuciniai neuronų tinklai, kontrabanda, šifruoti komunikacijos tinklai, organizuotas nusikalstamumas.*

Įvadas

Hansas Grosas, norėdamas parodyti kriminalistikos mokslo reikšmę, rašė: „Kokiu būdu mes galim rasti tą ar kitą įrodymą, kaip prie jų prieiti, kaip juos apsaugoti ir panaudoti, visa tai taip pat svarbu, tai tas rezultatas, kurio mes siekiame vykdydami teisingumą. Rasti ir panaudoti nusikaltėlio pėdsakai, kruopščiai nubraižytas nors ir nesudėtingas brėžinys, mikroskopinis preparatas, iššifruotas susirašinėjimas, fotografinės nuotraukos, tatuiruotės, atkurtas apanglėjęs laiškas, koks nors tikslus matmuo ir tūkstančiai panašių realijų – tai ne kas kita, kaip nepaperkami liudytojai, neleidžiantys paneigti ir kartu leidžiantys nuolat tikrinti, liudytojai,

[1] Autorių paaiškinimas: Šiuolaikinis organizuotas nusikalstamumas yra reiškinys, kurio veikimo ir sąveikos su aplinka mechanizmas yra paremtas globalizacijos ir modernių technologijų plėtros naudojimosi galimybėm.

kurių atžvilgiu negalima klaida, vienpusiškas supratimas, pikta valia, šmeižtas ir panašiai. Su kiekvienu kriminalistikos laimėjimu krenta liudytoju parodymų reikšmė ir drauge kyla realių įrodymų reikšmė“.[2]

Kriminalistika yra integralus mokslas, kurio raidai daug įtakos turėjo socialiniai pokyčiai, gamtos ir technikos mokslų laimėjimai. Tai yra mokslas kuris suteikia teisingumo ir saugumo garantą šiame sparčiai besikeičiančiame pasaulyje. Nusikaltėlių paliekami pėdsakai įgauna vis naujas formas, kurių išaiškinimui ir tyrimui nebeužtenka tradicinių kriminalistikos metodų. Naujų būdų ir metodų, kuriuos gali suteikti moderniausios technologijos, integracija į kriminalistinę praktiką yra labai svarbi norint sėkmingai kovoti su šiuolaikiniais nusikaltėliais. Kaip pažymi Doc. Dr. Egidijus Kurapka, „<...> kriminalistikos mokslas nuolat plėtojamas, tobulėja kriminalistinių tyrimų metodikos, didėja kriminalistikos galimybės, į nusikaltimų tyrimo sferą skverbiasi tobuliausios ir veiksmingiausios mokslinės technologijos. Kriminalistų kuriamas rekomendacijas lemia teisėsaugos institucijų poreikiai. Kriminalistikos mokslininkai, ieškodami naujų mokslo laimėjimų taikymo galimybių nusikaltimams tirti, daro tai vykdydami teisėsaugos institucijų užsakymus. Mat gyvenimas nestovi vietoje: nuolat tobulėja nusikaltimų darymo būdai, atsiranda naujos jų rūšys, todėl prireikia naujų tyrimo metodikų <...>“.[3]

Informacinio amžiaus kontekste, pasaulis tampa vis labiau skaitmenizuotas. Progresyvus technologijų tobulėjimas mums suteikia tokias galimybes, kurios sunkiai buvo įsivaizduojamos prieš kelis dešimtmečius. Šis reiškinys yra susijęs su moderniomis technologijomis, tokiomis kaip internetas, mobilieji įrenginiai ar socialiniai tinklai, kurie leidžia keliais mygtukų paspaudimais pasiekti kitą pasaulio kraštą, komunikuoti ir dalintis informacija tarpusavyje. Didelis duomenų kiekis ir šiuolaikinių technologijų pažanga mums leidžia sukurti technologinius instrumentus, kurti naujas technologines architektūras, kurios atveria nematytas galimybes siekiant atlikti tam tikras užduotis.

Kartu su inovatyviu pasauliu, neatsiejamai, tobulėja ir organizuotų nusikalstamų grupuočių daromi nusikaltimai. Nusikaltėliai greitai adaptuojasi prie sparčiai besikeičiančios aplinkos ir išradingai pritaiko naujausius technologijų laimėjimus savo veikoms realizuoti.

2011 m. spalio 25 d. Europos Parlamentas rezoliucijoje dėl organizuoto nusikalstamumo Europos Sąjungoje[4], pabrėžė, kad organizuotas nusikalstamumas yra viena pagrindinių grėsmių ES saugumui. Organizuotų nusikalstamų grupuočių daromi nusikaltimai visuomenei kainuoja daug, nes yra pažeidžiamos pamatinės žmogaus teisės ir demokratinės vertybės, nukreipiami ir netikslingai iššvaistomi finansiniai ir darbo ištekliai, iškreipiama laisva bendroji rinka, skatinama korupcija ir tokiu būdu skverbiamasi į politiką, viešąjį administravimą ir teisėtą ekonomiką.

2021 m. balandžio mėn. Europos Komisija priėmė 2021 – 2025 m. ES kovos su organizuotu nusikalstamumu strategiją. Strategijoje pažymėta, kad „ <...> dėl neskaidraus veiklos pobūdžio visuomenei nematomas organizuotas nusikalstamumas kelia didelę grėsmę Europos piliečiams, verslui ir valstybės institucijoms. Reaguojant į realiame gyvenime ir internete veikiančių organizuotų nusikalstamų grupių keliamą tarpvalstybinę grėsmę ir kintantį

[2] Kriminalistika. Teorija ir technika. Mykolo Romerio Universitetas. 2012 m. Šaltinis: https://repository.mruni.eu/handle/007/16854

[3] Doc. Dr. Egidijus Kurapka. Kriminalistikos raidos Lietuvoje tendencijos: mokslas ir praktika. Šaltinis: https://etalpykla.lituanistika.lt/fedora/objects/LT-LDB-0001:J.04~2000~1367178506602/datastreams/DS.002.0.01.ARTIC/content.

[4] Organizuotas nusikalstamumas Europos Sąjungoje 2011 m. spalio 25 d. Europos Parlamento rezoliucija dėl organizuoto nusikalstamumo Europos Sąjungoje (2010/2309(INI)) Šaltinis: (https://www.infolex.lt/teise/default.aspx?id=1929&crd=295363&qi=7006681)

jų veikimo būdą, reikia imtis suderintų, tikslingesnių ir pritaikytų atsakomųjų priemonių.<...>“.[5]

Europos Sąjungoje veikiantis organizuotų nusikalstamų grupių veikimas ir bendradarbiavimas yra nuolat kintantis ir daug sričių apimantis procesas. Nusikalstamų grupuočių tinklai dalyvauja įvairioje nusikalstamoje veikloje, kuri dažnu atveju apima prekybą narkotikais, kontrabandą, sukčiavimą, neteisėtą migrantų gabenimą ar prekybą žmonėmis. Tokių veikų atskleidimas reikalauja daug resursų ir profesionalaus personalo bendradarbiavimo tarptautiniame lygmenyje. Šiuolaikinės organizuotos nusikalstamos grupuotės yra skaitmeninio amžiaus atstovai, todėl technologinių instrumentų, tokių kaip šifruotų ryšių kanalų naudojimas ar kriptovaliutos, kuriomis yra maskuojami finansiniai srautai, sukelia papildomų sunkumų teisėsaugos institucijoms efektyviai su to kovoti. Taip pat svarbu atsižvelgti ir į internetinę dimensiją, nes šiuolaikinis organizuotas nusikalstamumas veikia ne tik realioje, bet ir kibernetinėje erdvėje. Vis intensyvesnis naudojimasis internetu ir internetinėmis paslaugomis, skatina kibernetinių nusikaltimų augimą ir didina riziką vartotojams tapti tokių nusikaltimų aukomis.

Lietuvos Respublikos Seimas 2015 m. gegužės 7 d. nutarime „dėl viešojo saugumo plėtros 2015 – 2025 metų programos patvirtinimo“ pažymėjo, kad organizuotų nusikalstamų grupuočių *modus operandi* būtent dėl modernių technologijų naudojimo tampa vis sudėtingesnė ir įvairesnė. Ryškėja tendencija užsiimti vis labiau pelninga nusikalstama veikla ir mažėja specializacija konkrečių nusikalstamų veikų srityse. Pabrėžiama, kad „<...> augant interneto įtakai mūsų gyvenime, nusikalstamų veikų elektroninėje erdvėje mastas ir galima žala tik didės, o spartūs informacinių ir ryšių technologijų pokyčiai (pvz., debesų kompiuterija) gali lemti ir naujus iššūkius. Todėl nusikalstamos veikos elektroninėje erdvėje vertintos kaip auganti grėsmė viešajam saugumui <...>“.[6]

2021 m. Europolo atliktame ES sunkių ir organizuotų nusikaltimų tyrime (angl. The European Union Serious And Organised Crime Threat Assessment, SOCTA) pažymėta, kad organizuotų nusikalstamų grupių esama visose valstybėse narėse.[7] Organizuotas nusikalstamumas yra iš esmės paveiktas globalizacijos procesų. Daugėja nusikalstamų tinklų, kurie nėra susieti su konkrečia pilietybe ar tautybe ir veikia tarpvalstybiniu mastu. Nusikaltėliai greitai įsisavina ir integruoja naujas technologijas į nusikaltimų schemas, jas tobulina ir kuria naujus intersubjektyvius nusikaltimų tinklus, paremtus modernių technologijų teikiamu beprecedenčiu lankstumu, kuriam įtakos neturi geografiniai ar laiko zonų apribojimai.

Šiuolaikinio organizuoto nusikalstamumo mastas ir sudėtingumas kelia naujus iššūkius kriminalistikos mokslui. Kriminalistikos mokslo atsiradimas ir istorija kilo iš valstybės ir visuomenės socialinio užsakymo: reikėjo kurti naujus įrankius ir metodus nusikaltimų atskleidimui ir tyrimui.[8] Kiekviena idėja ir gautas rezultatas skatina naujų kriminalistinių poreikių augimą ir tų poreikių tenkinimą. Kriminalistika, norėdama tapti šiuolaikine, privalo pasiduoti naujausioms informacinių technologijų ir ryšių tendencijoms, jas priimti ir naudoti tai kaip efektyvų įrankį kovojant su šiuolaikiniu organizuotu nusikalstamumu. Daugeliui, modernių technologijų integraciją kelia nerimą, tačiau manau, kad tai turėtų kelti parengtumo

[5] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui regionų komitetui „2021 – 2025 m. ES kovos su organizuotu nusikalstamumu strategija“. Šaltinis: (https://www-infolex-lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1245030&qi=7007649)

[6] Lietuvos Respublikos Seimo 2015 m. gegužės 7 d. nutarimas Nr. XII-1682 „Dėl viešojo saugumo plėtros 2015-2025 metų programos patvirtinimo“. Šaltinis: (https://www-infolex-lt.skaitykla.mruni.eu/ta/332447)

[7] Serious and Organised Crime Threat Assessment (SOCTA) 2021 m. Šaltinis: (https://www.europol.europa.eu/publications-events/main-reports/socta-report)

[8] Developments of theory of criminalistics and future of forensic expertology. Innovative essence of criminalistics and prospective directions of its development. Viktor Shevchuk. P. 165

lygį. Reikia kovoti ne tik su dabartinėmis grėsmėmis, bet ir atsižvelgti į tai, kad sparčiai tobulėjantis informacinių technologijų sektorius pasauliui siūlo vis naujas galimybes ir tuo pačiu kelia naujus iššūkius kriminalistikos mokslui. Šiuolaikinis organizuotas nusikalstamumas yra globalus ir skaitmenizuotas reiškinys, todėl šiai kovai yra reikalingas tarptautinis bendradarbiavimas, informacijos ir išteklių dalijimasis, naujausių technologijų teikiamų galimybių naudojimas ir bendrų strategijų kūrimas.

Kriminalistikos mokslo ir dirbtinio intelekto sinergija

Šiandienos realybė reikalauja mokslininkų bendruomenės sukurti ir įdiegti tinkamus įrankius, galinčius patenkinti šiuolaikinių tyrimų ir teisminės praktikos poreikius. Moderniausios technologijos ir naujausios informacijos rinkimo, analizavimo metodologijos yra esminės kriminalistikos mokslo tobulėjimo gairės norint efektyviai kovoti su šiuolaikiniu organizuotu nusikalstamumu. Kriminalistikos mokslininkai ir specialistai, atsižvelgdami į aplinkos pokyčius, nuolat tobulina kriminalistinės teorijos ir praktikos metodikas. Inovatyvūs ir efektyvūs įrankiai yra gyvybiškai svarbūs norint ne tik prisitaikyti prie šiuolaikinių nusikalstamumo tendencijų ir su tuo veiksmingai kovoti, bet taip pat, perspektyviniu požiūriu kriminalistikos mokslas turi tapti dar labiau glaudus su informacinių technologijų sritimi. Technologijos, tokios kaip Web3 aplikacijos, blokų grandinės (angl. Blockchain), NFT, kriptovaliutos, kompiuterių debesija, pažangūs kriptografijos ir informacijos šifravimo metodai, plačiai pasiekiami VPN tinklai ir galiausiai proveržis dirbtinio intelekto (angl. artificial intelligence) srityje galiausiai tapo ne tik plačiai naudojamais kiekvieno žmogaus gyvenime, bet tai taip pat tai yra įrankiai, kuriais naudojasi organizuoto nusikalstamumo tinklai savo veikoms vykdyti ir realizuoti.

Sparčiai vystantis technologijoms didelis dėmesys turi būti skiriamas dirbtinio intelekto technologijai, kuri iki 2023 m. buvo mistifikuojama. Daug dėmesio sulaukusi dirbtinio intelekto technologija yra lyginama su „ugnies atradimu“ [9], kitų ekspertų nuomone tai kelia egzistencinę krizę žmonijai, kadangi šios technologijos vystymo galimybės neturi ribų ir tapo nekontroliuojamu procesu.[10] Tačiau aišku tik viena: dirbtinio intelekto amžius prasidėjo.

Dirbtinis intelektas (DI) yra kompiuterių mokymosi, supratimo ir sprendimo sistema, kuri naudoja daugybę mokslinių disciplinų tokių kaip matematiką, statistiką, informatiką. DI leidžia techninėms sistemoms apdoroti didelius kiekius duomenų ir atlikti analizę, kad priimtu tiksliausiai apskaičiuotus sprendimus. Ši technologija taip pat geba mokytis iš savo patirties, kad gerintų teisingų sprendimų priėmimo gebėjimus ateityje.

Dirbtinis intelektas nėra naujovė, nes kaip idėja ir mokslinio tyrimo objektas egzistuoja jau daugiau kaip pusę amžiaus, tačiau tik paskutiniu metu stipriai pažengus skaitmenizacijos ir informacinių technologijų srityse, dirbtinis intelektas tapo labiau matomu ir plačiai naudojamu įrankiu.[11] Didžiulės duomenų saugyklos, kompiuterių ir didelių skaičiavimo galimybių buvimas suteikia reikiamus resursus duomenų analizei ir modelių kūrimui, kad būtų galima apdoroti milžiniškus informacijos srautus, kurių apdorojimas žmogui būtų nepaprastai sudėtingas ar net neįmanomas. Tai yra galinga ir plačiai naudojama technologija daugelyje sričių, pvz.: medicinoje pasitelkiant dirbtinio intelekto technologija, vėžio prognozavimas

[9] Google CEO: A.I. is more important than fire or electricity. Šaltinis: https://www.cnbc.com/2018/02/01/ google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html
[10] Elon Musk among experts urging a halt to A.I. training. Šaltinis: https://www.bbc.com/news/technology-6511 0030)
[11] The History of Artificial Intelligence. Šaltinis: (https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/)

pacientui pasiekė naujas aukštumas.[12] Švietimo srityje tinkamai pritaikyto dirbtinio intelekto technologija mokytojams suteikė galimybę efektyviau peržiūrėti ir įvertinti mokinių užduotis. Mokymo programos buvo individualizuotos atsižvelgiant į mokinių poreikius. [13] Finansų srityje pritaikytas dirbtinis intelektas padidino sukčiavimo rizikos aptikimą, prekyba paremta kompiuteriniais algoritmais tapo pelningesnė. [14]

Platus galimybių diapazonas, kurį suteikia dirbtinio intelekto technologija, yra potencialus ir kryptingas kelias norint sukurti kriminalistinį „produktą“, kuris efektyviai ir veiksmingai padėtų kovoti su šiuolaikiniu organizuotu nusikalstamumu. Tai gali suteikti daugiau galimybių tiriant ir atskleidžiant nusikalstamas veikas ar identifikuojant nusikaltėlius. Šiuolaikinio organizuoto nusikalstamumo kontekste, nusikaltėliai naudodami modernias technologijas, kuriomis neretu atveju paslepia savo tapatybę, apsunkina tyrėjų darbą, todėl koreliacijų radimas tarp daugybės užmaskuotų ir skirtingų kintamųjų yra labai reikalingas, norint išpildyti kriminalistikos mokslo praktinius uždavinius.

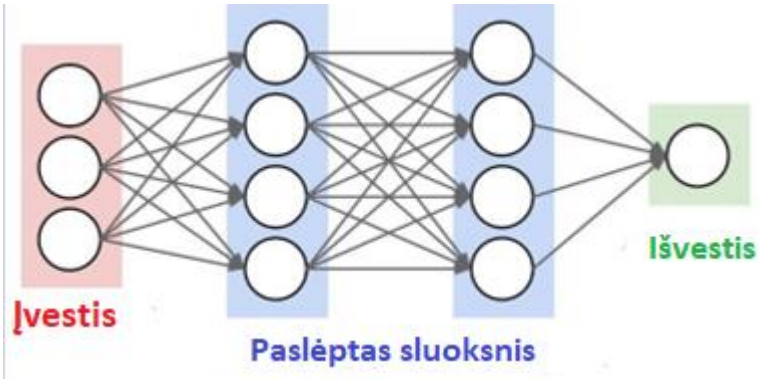
Lietuva, kaip tranzitinė šalis, dažnu atveju tampa didelio mąsto kontrabandos liudininke. Skandalingoje kontrabandos karaliaus byloje atliekant ikiteisminį tyrimą nustatyta, kad per dvejus metus į Lietuvą ir kitas Europos Sąjungos šalis, vilkikais neteisėtai buvo įvežta ir išvežta cigarečių, kurių muitinė vertė viršijo 10 mln. eurų. Nelegaliai per sieną gabenta ar bandyta pergabenti daugiau nei 84,6 mln. vienetų kontrabandinių rūkalų iš Rusijos Federacijos. Šioje byloje, kurioje iš nustatytų aplinkybių matyti, kad nusikalstama veika buvo padaryta pagal kruopščiai parengtą planą – užmaskuotas didelės vertės cigarečių gabenimas į užsienį. *„<...> susitikimo metu sutarė, kad pagamins tuščiavidurį priedangos krovinį iš medienos pakuočių cigarečių kroviniui paslėpti, <...>, paruoš ir perduos nusikaltimo vykdytojui krovinio dokumentus, patvirtinančius, jog iš Rusijos Federacijos į Lietuvos Respublika gabenamas pjautinės medienos krovinys“.*[15]

Muitinėje yra naudojamas rentgeno aparatas, kurio bangos gali praeiti pro objektą ir detektoriaus pagalba užfiksuoti praeinančio ir sugerto spindulio intensyvumą. Tai leidžia sukurti vaizdą, kurio pagrindu tokie duomenys yra reikalingi norint pamatyti objekto vidų neardant atskirų jo komponentų.[16] Tačiau bėda ta, kad rentgeno aparatas konkrečioje situacijoje parodys tai kas yra viduje – medienos krovinys.

Pasitelkus rentgeno ir gilaus mokymosi (angl. Deep-Learning)[17] dirbtinio intelekto šakos technologija galima pastebėti daugiau. Įgyvendinant gilaus mokymosi algoritmus, yra naudojami neuroniniai tinklai, kurie yra analogiški žmogaus smegenų veiklai. Gilusis mokymasis yra naudojamas apdorojant duomenis siekiant atpažinti objektus, juos klasifikuoti, prognozuoti arba sugeneruoti naujus turinius. Šis procesas apima įvairius sluoksnius, kurie transformuoja pradinę informaciją. Pradinis sluoksnis (įvestis) gauna duomenis ir transformuoja juos į tinkamą formatą, kuris yra pateikiamas tolimesniems sluoksniams, kiekvienas tolimesnis sluoksnis taip pat atlieka transformacijas ir pateikia juos kitam

[12] Shgiao Huang, Jie Yang, Simong Fong and Qi Zhao. Artificial intelligence in cancer diagnosis and prognosis: Opportunities and challenges. Šaltinis: (https://pubmed.ncbi.nlm.nih.gov/33907522/)
[13] Lijia Chen, Pingping Chen and Zhijan Lin. Artficial Intelligence in Education: A review. Šaltinis: https://iee explore.ieee.org/abstract/document/9069875
[14] The Alan Turing Institute. Artificial intelligence in finance. Bonnie G. Buchanan, PhD, FRSA. Šaltinis: (https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_turing_report_1.pdf)
[15] 2023 m. sausio 17 d. LAT Nutartis. Baudžiamoji byla Nr. 2K-69-788/2023 (Šaltinis: https://www-infolex-lt. skaitykla.mruni.eu/tp/2137004)
[16] Review Article. Recent Development in X-Ray Imaging Technology: Future and Challenges. Xiamgyu Ou, Xue Chen, Xianning Xu, Lilli Xie, Xiaofeng Chen, Zhongzhu Hong, Hua Bai, Xiaowang Liu, Qiushui Chen, Lin Li and Huanghao Yang. Šaltinis: (https://downloads.spj.sciencemag.org/research/2021/9892152.pdf)
[17] Deep Learning for A. I. Šaltinis: (https://dl.acm.org/doi/pdf/10.1145/3448250)

sluoksniui. Proceso pabaigoje yra gauta išvestis, kuri gali būti naudojama sprendžiant konkrečius uždavinius.[18]



1 pav. Konvoliucinių neuronų tinklų iliustracija
Šaltinis: Machine Learning & Big Data Blog. What's Deep Neural Network? Deep Nets Explained. Jonathan Johnson. 2020[19]

Atliktas tyrimas parodė[20], kad pasitelkus Konvoliucinius Neuroninius Tinklus (angl. Convolutional Neuron Network, CNN) kaip gilaus mokymosi modelio tipą ir integruojant į rentgeno aparatą buvo galima aptikti krovininiuose konteineriuose gabenamas „mažas metalines grėsmes" (angl. Small Metallic Threats, SMT's), kurios yra skirtos sprogstamiems užtaisams gaminti. Ši technologija geba aptikti ir atpažinti objektus užimančius mažiau nei 50 pikselių, esančius vaizduose, kuriuose yra daugiau kaip 2 mln. pikselių. Buvo aptikta 90% paslėptų mažų metalinių grėsmių, iš kurių klaidingų indikacijų signalų buvo mažiau nei 6%. Ši technologija turi žmogui nebūdingą darbo našumą, nes krovininio konteinerio apdorojimo t. y. , kelias nuo įvesties iki išvesties ir gauto sistemos atsakymo, laikas buvo 3,5 sekundės. Tai dar kartą parodo, kad dirbtinio intelekto technologija leidžia atlikti sudėtingus analitinius procesus, kurie per daug sudėtingi arba pernelyg dideli, kad juos galėtų atlikti žmogus.

Dirbtinio intelekto gilaus mokymosi neuroninių tinklų veikimas apima daugybę procesų. **Pagrindinis tikslas yra „išmokyti"** sistemą atpažinti ir atskirti tam tikras formas ar objektus vaizdo, garso įraše ar kitame duomenų rinkinyje. Norint išmokinti technologiją atpažinti, pastebėti ar prognozuoti tam tikrus reiškinius, reikia turėti duomenų rinkinį, kuris apimtų ieškomų reikalingų objektų ar formų pavyzdžius. Sistemai suprantama kalba reikia paaiškinti ko mes ieškome ir kas mums reikalinga. Tokio mokymo procesas gali būti pasikartojantis ir reikalaujantis nemažai laiko, tačiau tai leidžia pasiekti labai aukštą tikslumo lygį atpažįstant ir klasifikuojant duomenis ar tam tikrus reiškinius. Kruopščiai parengta duomenų sistema ir tos sistemos pagrindu paruošta dirbtinio intelekto technologija kriminalistikoje gali prisidėti ir išplėsti galimybių ribas kovojant su nusikalstamumu, įskaitant elektroninėje erdvėje, ypač tamsaus interneto platformose. Konvoliucinius neuroninius tinklus galima panaudoti siekiant nustatyti galimus nusikaltimų planus tiek fizinėje, tiek internetinėje erdvėje. Ši technologija gali

[18] What is Deep Learning? How It Works, Techniques and Applications – MATLAB and Simulink. Šaltinis: https://www.mathworks.com/discovery/deep-learning.html
[19] Machine Learning & Big Data Blog. What's Deep Neural Network? Deep Nets Explained. Jonathan Johnson. Šaltinis: https://www.bmc.com/blogs/deep-neural-network/
[20] Automated detection of smuggled high-risk security threats using Deep Learning. N. Jaccard, T.W. Rogers, E.J. Morton, L.D.Griffin. Šaltinis: https://ieeexplore.ieee.org/abstract/document/8267319

analizuoti tekstinius duomenis, kaip pavyzdžiui, pranešimus forumuose ir taip nustatyti galimus bendruomenių ryšius tarp nusikalstamų grupuočių.[21]

Svarbu paminėti, kad dirbtinio intelekto, kaip ir kitų technologijų, rezultatas priklauso nuo to, kaip ir kokio tikslo siekiant yra naudojama konkreti technologija. 2019 m. vasario 12 d. Europos Parlamentas rezoliucijoje dėl visapusiškos Europos pramonės politikos dirbtinio intelekto ir robotikos srityje, atkreipė dėmesį į tai, kad piktavališkas dirbtinio intelekto naudojimas gali kelti grėsmę skaitmeniniam, fiziniam ir viešajam saugumui.[22] Tai gali tapti įrankiu vykdant iki šiol nematytas dezinformacijos kampanijas, pvz., *DeepFakes*. Taip pat šia technologija gali būti pasinaudota didelio masto atakoms prieš informacines valstybinių institucijų, organizacijų, verslų sistemas ir taip pažeisti kritines kibernetinio saugumo infrastruktūras. Europos Sąjungos policijos biuras (Europol) 2022 m. kovo 10 d. pranešė, jog yra vykdoma nauja iniciatyva skirta užtikrinti, kad dirbtinio intelekto technologija būtų naudojama skaidriu ir atsakingu būdu.[23] Kuriama sistema, kurios tikslas yra užtikrinti, kad dirbtinis intelektas būtų naudojamas pagal nustatytus principus, kurie užtikrintų skaidrumą, atsakomybę ir pagarbą žmogaus teisių apsaugai. Tai yra svarbus žingsnis siekiant teisingo ir atsakingo dirbtinio intelekto naudojimo Europos Sąjungoje.

Svarbios informacijos, tam tikrų tendencijų ir koreliacinių ryšių pastebėjimas yra kriminalistinių tyrimų aspektas, kuris gali būti stipriai patobulintas naudojant dirbtinio intelekto technologijos įrankius. Šios technologijos gali padėti surasti ryšius, kurie yra reikalingi sėkmingai ikiteisminio tyrimo eigai. Tai yra ypač svarbu norint veiksmingai kovoti su vis sudėtingesniu ir įvairesniu organizuotu nusikalstamumu, kuriame dažnai yra pastebimas tam tikras tendencingumas. Visų šių galimybių pagrindu galima teigti, kad dirbtinio intelekto technologija yra nepakeičiamas ir efektyvus įrankis, kuris gali stipriai prisidėti prie kriminalistikos mokslo plėtojimo ir visuomenės saugumo didinimo.

Iššūkiai ir problematika kovojant su šiuolaikiniu organizuotu nusikalstamumu

Kriptografiniai raktai ir šifravimas tapo pagrindinių teisių, skaitmeninio suverenumo ir inovacijų apsaugos elementu. Elektroninių laiškų sistemos, elektroninės bankininkystės, parduotuvės ir daugelio kitų internetinių paslaugų apsaugos sistemos yra paremtos kriptografiniais algoritmais. Tai yra privatumo ir konfidencialumo apsaugos dalis, padedanti užtikrinti, kad tik tam tikri asmenys turėtų prieigą prie tam tikros informacijos, be trečiųjų šalių įsikišimo. Tokios technologijos naudojimas yra būtinas norint išvengti neteisėto priėjimo prie informacijos.[24] Taip pat, dabartinės tendencijos vis labiau skatina interneto vartotojus naudotis programomis arba paslaugomis, kurios didina saugumą naršant internete. Žinoma, iš pažiūros tai nėra blogai, nes pvz., VPN paslaugos apsaugo nuo tapimo aukomis kibernetiniams nusikaltėliams ir mažina asmeninių duomenų nutekinimo riziką. Tačiau, toks tapimas „nematomu“ elektroninėje erdvėje yra kontraversiškas, nes tokių galimybių prieinamumas

[21] Dark Web Data Classification Using Neural Network. Šaltinis: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8979735/

[22] 2019 m. vasario 12 d. Europos Parlamento rezoliucija dėl visapusiškos Europos pramonės politikos dirbtinio intelekto ir robotikos srityje (2018/2088(INI)) Šaltinis: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_LT.html

[23] New Accountability Framework to use artificial intelligence in a transparent and accountable manner. Šaltinis: (https://www.europol.europa.eu/media-press/newsroom/news/new-accountability-framework-to-use-artificial-intelligence-in-transparent-and-accountable-manner)

[24] An Overview of Cryptography. Šaltinis: https://d1wqtxts1xzle7.cloudfront.net/38411944/An_Overview_of_Cryptography.pdf?1438962673=&response-content-disposition=inline%3B+filename%3DAn_Ove_

sukelia riziką ir papildomus iššūkius kriminalistikos mokslui, kai reikia identifikuoti tam tikro žmogaus tapatybę.

Ilgą laiką organizuoto nusikalstamumo pėdsakai internete buvo pastebimi tamsaus interneto (angl. DarkNet) forumuose.[25] Tai yra reiškinys, kuris iš esmės keičia tradicinį nusikalstamų veikų pobūdį ir sudaro naujus iššūkius teisėsaugos institucijoms. Tamsusis internetas yra pasiekiamas per specialias programas, tokias kaip „Tor“, „I2P“, „Freenet“. Tai yra privati tinklų sistema, kuri suteikia vartotojams anonimišką prieigą prie tinklo. Kartu su minėtomis programomis dažnai yra naudojamos papildomos technologijos, kurios yra susijusios su IP ir finansinių srautų maskavimu. Suprantama, kad šios rinkos „dalyviai“ yra technologiškai raštingi, nes priėjimas prie tamsaus interneto nėra indeksuojamas per tradicinius paieškos variklius, tokius kaip „Google“, „Bing“ ar „Yahoo“. Finansiniai srautai dažniausiai maskuojami kriptovaliutomis, kurių transakcijų vykdymas yra greitas ir nereikalauja jokių tarpininku. Ši anonimiškumo savybė, kartu su kriptovaliutų decentralizuotu pobūdžiu, padaro patrauklia alternatyva organizuotų nusikalstamų grupuočių veiklai. Taip pat reikėtų paminėti blokų grandinės (angl. Blockchain) technologiją, kuri yra pagrindinė kriptovaliutų technologinė priemonė. Blokų grandinės yra saugumo ir patikimumo garantas, nes visos kriptovaliutų transakcijos yra saugomos ir sunkiai identifikuojamos, o kriptovaliutų savininko tapatybė yra apsaugota dėl šifruotų kriptografinių kodų naudojimo.

2021-2025 m. ES kovos su organizuotu nusikalstamumu strategijoje yra pažymima, kad didžiausia kliūtis veiksmingai nustatyti šios rūšies nusikaltimus neabejotinai yra nuasmeninimo priemonių naudojimas nusikalstamai veiklai. Šifruotas ryšys naudojant įvairias taikomąsias programas ar internetines pranešimų perdavimo priemones, kuriomis naudojasi nusikaltimų vykdytojai, yra rimta aptikimo proceso problema. Tai, kad teisėsaugos institucijos neturi prieigos prie užšifruotų pranešimų, kuriuos naudoja organizuotos nusikalstamos grupuotės, turėtų būti laikoma vienu didžiausių trūkumų, nes nepakankama prieiga prie informacijos labai trukdo laiku imtis veiksmų.[26]

Didelė teikiamų paslaugų pasiūla ir pažanga skaitmeninio saugumo srityje, nusikalstamas veikas internete leido perkelti ir į viešai ir lengvai prieinamus forumus ar susirašinėjimo platformas. Jeigu prieigai prie tamsiojo interneto platformos reikia suprasti kaip veikia tam tikri netradiciniai paieškos varikliai, kaip apsaugoti savo internetinio ryšio adresą ar jo buvimo vietą, tai dabartinės tendencijos šį faktorių eliminuoja ir visus šiuos procesus padaro žymiai paprastesnius. Pavyzdžiui, „Telegram“ yra populiari komunikacijos programa, kuri leidžia vartotojams siųsti tekstinius, garso ir vaizdo pranešimus, dalintis duomenimis. Apart to, „Telegram“ siūlo paslaptingus pokalbius, kurie išsitrina juos perskaičius arba po nustatyto laiko tarpo. Viena iš svarbiausių savybių, kuri padaro šią aplikaciją labai patrauklia yra „end – to end“ šifravimas. Tai reiškia, kad bet koks susiekimas tarp siuntėjo ir adresato yra matomas tik jiems ir yra nepasiekiamas trečiosioms šalims[27]. Ši galimybė komunikuoti ir tapti sunkiai identifikuojamiems plačiai atveria duris organizuoto nusikalstamumo įvairiems tikslams realizuoti ir vykdyti.

2022 m. duomenimis, „Telegram“ aplikacijos mėnesinių aktyvių naudotojų skaičius buvo 700 mln.[28] Organizuotam nusikalstamumui yra suteikiama galimybė pasiekti plačia auditorija ir anonimiškai dalyvauti įvairiose nelegaliose veiklose, tokiose kaip prekyba narkotikais,

[25] A Mysterious and Darkside of The Darknet: A Qualitative Study. Šaltinis: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4167244
[26] 2021-2025 m. ES kovos su organizuotu nusikalstamumu strategija. Šaltinis https://www-infolex-lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1245030&qi=7007785
[27] https://core.telegram.org/api/end-to-end
[28] Telegram statistika. Šaltinis: https://www.statista.com/statistics/234038/telegram-messenger-mau-users/

ginklais ar žmonėmis. Tai yra didelė problema, su kuria susiduria ne tik teisėsaugos institucijos, bet taip pat tai liečia kiekvieno mūsų gyvenimą, nes lengvai pasiekiamas žmogus gali tapti tam tikros formos nusikaltimo liudininku ar net auka.

Tarptautinio bendradarbiavimo svarba kovojant su šiuolaikiniu organizuotu nusikalstamumu

Šiuolaikinio organizuoto nusikalstamumo globalizacija sudaro poreikį stiprinti tarptautinio bendradarbiavimo galimybes. Nusikaltimų tyrimai, prokuratūrų ir teismų veikla negali būti apribota nacionalinėmis sienomis ir atsiliekančiais teisiniais aspektais. Norint veiksmingai ir optimaliai kovoti prieš organizuotus nusikalstamumo tinklus reikia tobulinti ir supaprastinti teisinius mechanizmus, kurie apima ekstradicijos, tarpvalstybinės teisinės pagalbos, baudžiamųjų proceso perdavimo ir kitus teisiniu aspektu reikalingus klausimus. Vienodų kokybės standartų integracija baudžiamajame procese yra būtina, jog tarptautinio bendradarbiavimo kontekste, kriminalistiniai instrumentai būtų tokie pat efektyvūs kaip ir kitoje ES valstybėje narėje.

2021 m. Europolo sunkaus ir organizuoto nusikalstamumo grėsmės įvertinime yra pažymima, kad beveik 70% nusikalstamų tinklų veikia daugiau nei trejose valstybėse. Šiuolaikinės organizuotos nusikalstamos grupuotės veikia pagal legalaus verslo modelį ir yra labiau nei bet kada suinteresuotas vis didesnių pajamų gavimu, nepriklausomai kokia nusikalstama veikla užsiima. 80% organizuotų nusikalstamų grupuočių veikiančių ES viduje yra dalyvauja tokios nusikalstamose veiklose kaip prekyba narkotikais, ginklais, internetiniai ir kitos formos sukčiavimai, prekyba žmonėmis ir nelegalių migrantų gabenimu. 60% nusikalstamų tinklų pasižymi korupciniais ryšiais.[29] 2021 m. balandžio mėn. 2021–2025 m. ES kovos su organizuotu nusikalstamumu strategijoje pabrėžta, kaip svarbu ardyti organizuotas nusikalstamas struktūras, taikantis į grupes, keliančias didesnį pavojų Europos saugumui, ir į asmenis, esančius aukštesnėje nusikalstamų organizacijų hierarchijos pakopoje.[30]

Kovojant su šiuolaikiniu organizuotu nusikalstamumu yra gyvybiškai svarbu bendradarbiauti ES ir tarptautiniu lygmeniu. Šiai kovai yra reikalingas tarptautinis koordinavimas, informacijos ir išteklių dalijimasis, bendrų strategijų kūrimas. Tarptautinis koordinavimas yra svarbus informacijos dalijimosi ir bendrų strategijų kūrimo atžvilgiu. Informacijos dalijimasis yra kritiškai svarbus, nes organizuotų nusikalstamų grupuočių tinklai veikia skirtingose šalyse ir reikalinga informacija turi būti prieinama kiekvienai Europos Sąjungos narei. Šengeno erdvėje valstybės narės policijos pareigūnai turėtų turėti prieigą prie tokios pat informacijos, kokią gali gauti jų kolegos kitoje valstybėje narėje. Visapusiškas ir veiksmingas bendradarbiavimas turi tapti kasdienybe[31]. Bendros strategijos pagrindu reikia imtis efektyvių veiksmų, kurie apimtų modernių technologijų ir profesionalaus personalo teikiamas galimybes.

„Encrochat“ byloje padedant Europolui ir Eurojustui, Belgijos, Prancūzijos ir Nyderlandų teisminės ir teisėsaugos institucijos bendradarbiaudamos užblokavo šifruoto ryšio kanalą,

[29] 2021. Serious and organised crime threat assessment. Šaltinis: (https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

[30] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui regionų komitetui „2021 – 2025 m. ES kovos su organizuotu nusikalstamumu strategija“. Šaltinis: https://www-infolex-lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1245030&qi=7007649

[31] Komisijos Komunikatas Europos Parlamentui ir Tarybai dėl penktosios ES saugumo sąjungos strategijos įgyvendinimo pažangos ataskaitos. Šaltinis: https://www-infolex-lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1273895&qi=7006916

kuriuo naudojosi stambios organizuotos nusikalstamos grupuotės.[32] Uždarymo metu paslauga naudojosi 60 000 abonentų, iš kurių 90 proc. buvo nusikaltėliai. Užšifruota pranešimų sistema, kurią naudojosi organizuotos grupuotės, vadinosi EncroChat ir buvo labai populiari tarp nusikaltėlių visoje Europoje. Belgijos ir Olandijos teisėsaugos institucijos susipažino su EncroChat sistema 2019 m. vasario mėn., kai buvo pradėtas tyrimas susijęs su tarptautiniu narkotikų kontrabandos tinklu. Per operaciją buvo sulaikyti tūkstančiai nusikaltėlių ir konfiskuoti dešimtys milijonų eurų vertės turto, įskaitant narkotikus, ginklus. Ši operacija leido teisėsaugos institucijoms susipažinti su organizuoto nusikalstamumo struktūra ir veikla, kurios buvo nežinomos anksčiau. EncroChat byla parodė , kad teisėsaugos institucijos gali naudoti naująsias informacines technologijas, kad išaiškintų organizuotų grupuočių tinklus ir veikimo mechanizmus.

Operacija „Pollino“, kuri prasidėjo 2016 m., kai Nyderlandų policija pradėjo tyrimą dėl didelio kokaino kontrabandos tinklo, kurioje buvo įtraukti „Ndragheta“ nariai. „Ndrangheta“ yra galingiausia ir pavojingiausia Italijos mafija, kuri yra laikoma viena iš didžiausių ir įtakingiausių organizuotų nusikalstamų grupuočių pasaulyje.[33] Tyrimo metu buvo aptiktos 4 tonos kokaino ir šimtai kilogramų kitų narkotinės kilmės medžiagų.[34] Operacijos metu buvo sulaikyta daugiau nei 80 įtariamųjų, įskaitant aukšto rango „Ndrangheta“ mafijos narius. Tai yra didžiausia operacija prieš „Ndrangheta“ mafiją, kuri buvo vykdoma per pastaruosius kelis dešimtmečius. Vykdant ES teisminį ir policijos bendradarbiavimą išardyta didžiulė organizuota nusikalstama grupė. Jungtinė tyrimo grupė sudaryta iš Italijos, Vokietijos ir Nyderlandų teisėsaugos surengė Eurojusto koordinuojamą ir Europolo remiamą reidų dieną, po kurios 34 asmenys buvo nuteisti kalėti iš viso daugiau kaip 400 metų. Vėliau dar 12 asmenų buvo nuteisti kalėti daugiau kaip 173 metus, o keliose valstybėse narėse teismo procesai tebevyksta.[35]

Naujausias Eurojusto operatyvinės veiklos šioje srityje pavyzdys – parama, suteikta SKY ECC bylos tyrėjams ir prokurorams. Tyrėjai stebėjo, kaip nusikaltėliai naudojasi šifruotų ryšių priemone SKY ECC , ir gavo neįkainojamos informacijos apie šimtus milijonų žinučių, kuriomis keitėsi nusikaltėliai.[36] Taip buvo surinkta itin svarbi informacija apie daugiau nei šimtą suplanuotų didelio masto nusikalstamų operacijų, užkertant kelią potencialioms gyvybei pavojingoms situacijoms ir išvengiant galimų aukų. Demaskavus „EncroChat“, daugelis naudotojų perėjo prie populiarios SKY ECC platformos.[37]

Išvados

Šiuolaikinis organizuotas nusikalstamumas yra sudėtingas ir pastoviai kintantis reiškinys, su kuriuo susiduriama daugumoje pasaulio valstybių. Šių nusikalstamų grupuočių veikla apima daug sričių, tokias kaip prekyba žmonėmis, narkotikais, pinigų teisinės padėties keitimas, sukčiavimai. Šis reiškinys dominuoja ne tik realybėje, bet taip pat ir internetinėje erdvėje. Nusikaltėliai vis dažniau kūrybiškai pritaiko modernias technologijas savo nusikalstamoms

[33] Italian organized crime threat assessment. Europol. Šaltinis: https://www.europol.europa.eu/sites/default/files/documents/italian_organised_crime_threat_assessment_0.pdf
[34] Coordinated crackdown on Ndrangheta mafia in Europe. šaltinis: https://www.europol.europa.eu/media-press/newsroom/news/coordinated-crackdown-ndrangheta-mafia-in-europe
[35] KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI dėl penktosios ES saugumo sąjungos strategijos įgyvendinimo pažangos ataskaitos. Šaltinis: https://www-infolex-lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1273895&qi=7006916
[36] New major interventions to block encrypted communications of criminal networks. Šaltinis: https://www.eurojust.europa.eu/news/new-major-interventions-block-encrypted-communications-criminal-networks
[37] 2021 m. Eurojusto metinė ataskaita. Šaltinis: https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2021-lt.pdf

veikoms realizuoti ir taip apsunkina teisėsaugos darbą. Siekiant neatsilikti nuo kitų mokslų plačiai taikančių IT technologijas ir dirbančių su DI galimybių diegimu į savo sritis, kriminalistika privalo ne tik greitai ir sumaniai adaptuoti kitų mokslų pasiekimus ir per savo rekomendacijas pritaikyti juos nusikalstamų veikų aiškinimui, tyrimui ir prevencijai, bet ir parengti ilgalaikes strategijas šių technologijų panaudojimui moksliniams ir taikomiesiems tikslams. Didelės apimties duomenų analizė ir jų naudojimas DI priemonėmis gali padėti nustatyti ryšius tarp nusikaltimų ir juos darančių asmenų, įvertinti nusikaltimų riziką ir prognozuoti galimus ateities scenarijus.

Kriminalistikos mokslo plėtros poreikis į kibernetinę erdvę yra vis aktualesnis, nes vis daugiau nusikaltimo formų pasireiškia internetinėje erdvėje. Tai yra svarbu siekiant apsaugoti Europos Sąjungos piliečius nuo kibernetinių atakų ir kitų elektroninio nusikalstamumo formų variacijų. Reikia kurti naujus metodus, kurie padėtų teisėsaugos institucijoms efektyviai kovoti su kibernetinėje erdvėje esančia nusikalstama veikla. Tai reikalauja aukštos kvalifikacijos specialistų darbo, kurie technologinėmis priemonėmis gebėtų identifikuoti, analizuoti ir atkurti kibernetinius įvykius, susijusius su nusikalstamomis veikomis. Tai reikalauja nuolatinio šios srities specialistų ruošimo ir mokymo, naujų metodų ir technologijų kūrimo bei efektyvaus bendradarbiavimo tarp skirtingų teisėsaugos institucijų, tiek nacionaliniu, tiek tarptautiniu lygmeniu.

Norint veiksmingai kovoti su šiuolaikiniu organizuotu nusikalstamumu, labai svarbu teisminėms ir teisėsaugos institucijoms bendradarbiauti tarptautiniu lygmeniu ir bendromis pastangomis kurti strategijas, bei laikytis vieningos baudžiamojo proceso politikos. Organizuotas nusikalstamumas peržengia valstybių sienas, neturi geografinių apribojimu, todėl tarpvalstybinis bendradarbiavimas visomis įmanomomis galimybėmis yra gyvybiškai svarbus. Tai gali apimti daugybę veiksmų, tokių kaip informacijos mainai, išsamių kriminalinių tyrimų koordinavimas, bendrų standartų ir procedūrų diegimas. Tai reikalauja nuolatinio dialogo ir bendradarbiavimo tarp valstybių, teisminių ir teisėsaugos institucijų.

Literatūra

1. A Mysterious and Darkside of The Darknet: A Qualitative Study. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4167244
2. Automated detection of smuggled high-risk security threats using Deep Learning. N. Jaccard, T.W. Rogers, E.J. Morton, L.D.Griffin. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/8267319
3. An Overview of Cryptography. Prieiga per internetą: https://d1wqtxts1xzle7.cloudfront.net/38411944/An_Overview_of_Cryptography.pdf?1438962673=&response-content-disposition=inline%3B+filename%3DAn_Ove_)
4. Coordinated crackdown on Ndrangheta mafia in Europe. Prieiga per internetą: https://www.europol.europa.eu/media-press/newsroom/news/coordinated-crackdown-ndrangheta-mafia-in-europe
5. Doc. Dr. Egidijus Kurapka. Kriminalistikos raidos Lietuvoje tendencijos: mokslas ir praktika. Prieiga per internetą: https://etalpykla.lituanistika.lt/fedora/objects/LT-LDB-0001:J.04~2000~1367178506602/datastreams/DS.002.0.01.ARTIC/content
6. Developments of theory of criminalistics and future of forensic expertology. Innovative essence of criminalistics and prospective directions of its development. Viktor Shevchuk. P. 165-170.
7. Deep Learning for A. I. Prieiga per internetą: https://dl.acm.org/doi/pdf/10.1145/3448250

8. Dark Web Data Classification Using Neural Network. Prieiga per internetą: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8979735/
9. Elon Musk among experts urging a halt to A.I. training. Prieiga per internetą: https://www.bbc.com/news/technology-65110030
10. Google CEO: A.I. is more important than fire or electricity. Prieiga per internetą: https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html
11. Italian organized crime threat assessment. Europol. Prieiga per internetą: https://www.europol.europa.eu/sites/default/files/documents/italian_organised_crime_threat_assessment_0.pdf
12. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui regionų komitetui „2021 – 2025 m. ES kovos su organizuotu nusikalstamumu strategija“. Prieiga per internetą: https://wwwinfolex.lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1245030&qi=7007649
13. Komisijos Komunikatas Europos Parlamentui ir Tarybai dėl penktosios ES saugumo sąjungos strategijos įgyvendinimo pažangos ataskaitos. Prieiga per internetą: https://www-infolex-lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1273895&qi=7006916)
14. Lietuvos Respublikos Seimo 2015 m. gegužės 7 d. nutarimas Nr. XII-1682 „Dėl viešojo saugumo plėtros 2015-2025 metų patvirtinimo“. Prieiga per internetą: https://www-infolex-lt.skaitykla.mruni.eu/ta/332447
15. Lijia Chen, Pingping Chen and Zhijan Lin. Artficial Intelligence in Education: A review. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/9069875
16. New Accountability Framework to use artificial intelligence in a transparent and accountable manner. Prieiga per internetą: https://www.europol.europa.eu/media-press/newsroom/news/new-accountability-framework-to-use-artificial-intelligence-in-transparent-and-accountable-manner
17. New major interventions to block encrypted communications of criminal networks. Prieiga per internetą: https://www.eurojust.europa.eu/news/new-major-interventions-block-encrypted-communications-criminal-networks
18. Organizuotas nusikalstamumas Europos Sąjungoje 2011 m. spalio 25 d. Europos Parlamento rezoliucija dėl organizuoto nusikalstamumo Europos Sąjungoje (2010/2309(INI)). Prieiga per internetą: https://www.infolex.lt/teise/default.aspx?id=1929&crd=295363&qi=7006681
19. Review Article. Recent Development in X-Ray Imaging Technology: Future and Challenges. Xiamgyu Ou, Xue Chen, Xianning Xu, Lilli Xie, Xiaofeng Chen, Zhongzhu Hong, Hua Bai, Xiaowang Liu, Qiushui Chen, Lin Li and Huanghao Yang. Prieiga per internetą: https://downloads.spj.sciencemag.org/research/2021/9892152.pdf
20. Shgiao Huang, Jie Yang, Simong Fong and Qi Zhao. Artificial intelligence in cancer diagnosis and prognosis: Opportunities and challenges. Prieiga per internetą: https://pubmed.ncbi.nlm.nih.gov/33907522/
21. The History of Artificial Intelligence. Prieiga per internetą: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/
22. The Alan Turing Institute. Artificial intelligence in finance. Bonnie G. Buchanan, PhD, FRSA. Prieiga per internetą: https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_turing_report_1.pdf

23. Telegram šifravimas. Prieiga per internetą: https://core.telegram.org/api/end-to-end
24. Telegram statistika. Prieiga per internetą: https://www.statista.com/statistics/234038/telegram-messenger-mau-users/
25. Vidmantas Egidijus Kurapka, Snieguolė Matulienė, Eglė Bilevičiūtė, Janina Juškevičiūtė, Lina Novikovienė, Raimundas Jurka, Renata Valūnė. Kriminalistika. Teorija ir Technika. Mykolo Romerio Universitetas. 2012 m. Vilnius. Prieiga per internetą: https://repository.mruni.eu/handle/007/16854
26. What is Deep Learning? How It Works, Techniques and Applications – MATLAB and Simulink. Prieiga per internetą: https://www.mathworks.com/discovery/deep-learning.html
27. 2019 m. vasario 12 d. Europos Parlamento rezoliucija dėl visapusiškos Europos pramonės politikos dirbtinio intelekto ir robotikos srityje (2018/2088(INI)) Prieiga per internetą: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_LT.html
28. 2021 m. Europolo atliktame ES sunkių ir organizuotų nusikaltimų tyrime (angl. The European Union Serious And Organised Crime Threat Assessment, SOCTA) Prieiga per internetą: https://www.europol.europa.eu/publications-events/main-reports/socta-report
29. 2021 m. Eurojusto metinė ataskaita. Prieiga per internetą: https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2021-lt.pdf
30. 2021-2025 m. ES kovos su organizuotu nusikalstamumu strategija. Prieiga per internetą https://www.infolex.lt.skaitykla.mruni.eu/tp/default.aspx?id=1929&crd=1245030&qi=7007785)
31. 2023 m. sausio 17 d. LAT Nutartis. Baudžiamoji byla Nr. 2K-69-788/2023. Prieiga per internetą: https://www-infolex-lt.skaitykla.mruni.eu/tp/2137004

THE CONTRIBUTION OF FORENSIC SCIENCE TO THE FIGHT AGAINST ORGANIZED CRIME

Jurgita BALTRŪNIENĖ, Povilas KĖŽA
Mykolas Romeris University

Summary

One of the main tasks of forensic science is the implementation of crime investigation, detection and prevention methods in practical activities. Social changes, scientific and technical progress provide an opportunity to effectively use the obtained results for the implementation of forensic methods, tools, and recommendations in the fight against crime. The development of forensic science shows that the existence of new needs encouraged the satisfaction of specific needs. In this way, the divide between the increasing necessity and its non-fulfillment was reduced. Criminology, as an integral science, is dependent on the achievements of other sciences and their application to the needs of crime investigation. The connection between forensic science and current trends must be close and continuous. This process must allow not only to effectively fight against existing threats, but also to prevent events from happening and thus increase the safety of citizens in society.

Organized crime is one of the main threats to EU security. As Information Technology advances, the modus operandi of crimes is constantly changing. Technology opens unprecedented possibilities for us, but at the same time it also gives unprecedented flexibility to organized criminal groups. This article reviews the possible interactions between artificial intelligence and forensic science in the fight against modern organized crime and the current challenges in investigating and uncovering criminal acts. The

trends of organized crime and the possibilities of artificial application in investigating, solving, and preventing criminal acts are analyzed. In the fight against modern organized crime, new and effective methods are needed, it is necessary to improve the capabilities of law enforcement institutions and use new technologies that would help uncover and identify the activities of criminal organizations not only in the physical, but also in the virtual space. It must be understood that in this rapidly changing world, an effective fight against organized crime is possible only by combining the capabilities of professional personnel, advanced technologies, and international cooperation.