PRETHODNO PRIOPĆENJE

DOI: 10.59245/ps.34.3.4
UDK: 004.056
Primljeno: veljača 2025.

TONĆI PRODAN*, MARIJA GOMBAR**

Kognitivno-obavještajni model predviđanja sigurnosnih prijetnji

Sažetak

Suvremeni sigurnosni izazovi zahtijevaju sofisticirane metode predviđanja kriminalnih aktivnosti s obzirom na to da su tradicionalne kriminalističke analitičke metode uglavnom retrospektivne i ograničene u anticipaciji prijetnji. Ovaj rad predstavlja Kognitivno-obavještajni model predviđanja sigurnosnih prijetnji (KOMP), razvijen kao konceptualni okvir koji integrira umjetnu inteligenciju, analizu sigurnosno relevantnih informacija i kriminalističku analitiku radi unapređenja procjena rizika i omogućavanja proaktivnog djelovanja. Pojmovi „kognitivno" i „obavještajni" u nazivu modela referiraju se na sposobnost obrade i tumačenja višerazinskih sigurnosnih informacija. Model je razvijen kombinacijom postojećih metoda i novih interpretativnih pristupa, pri čemu se doprinos ne ostvaruje u samim tehničkim komponentama, nego u načinu njihove konceptualne integracije. Cilj istraživanja jest osmisliti i evaluirati model koji povećava točnost predviđanja, smanjuje algoritamsku pristranost i optimizira uporabu sigurnosnih resursa. KOMP se temelji na neuronskim mrežama, strojnom učenju i analizi velikih podataka kako bi se identificirali obrasci kriminalnog ponašanja i detektirale anomalije u financijskim, komunikacijskim i podacima o zemljopisnoj lokaciji. Metodološki okvir obuhvaća simulacijske eksperimente, analizu sintetičkih kriminalističkih podataka i komparativnu evaluaciju s postojećim modelima predviđanja (PredPol, CompStat). Rezultati pokazuju da KOMP postiže veću preciznost u detekciji prijetnji i znatno smanjuje broj lažno pozitivnih rezultata. Model omogućuje dinamičnu prilagodbu sigurnosnih strategija u stvarnom vremenu, no njegova primjena zahtijeva rješavanje etičkih i pravnih pitanja, posebice u području privatnosti podataka i algoritamske transparentnosti. Ovo istraživanje pridonosi kriminalističkoj analitici predviđanja nudeći metodološki utemeljen okvir za razvoj inteligentnih sigurnosnih sustava, s potencijalom primjene u prevenciji kriminala, povećanju operativne učinkovitosti sigurnosnih institucija i strateškom planiranju u borbi protiv organiziranog kriminala, terorizma i kibernetičkih prijetnji.

Ključne riječi: *algoritmi predviđanja, konceptualni model, kriminalistička analitika, KOMP model, sigurnosne prijetnje, umjetna inteligencija.*

* doc. dr. sc. Tonći Prodan, Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti, Hrvatska.

** Marija Gombar, Centar za obrambene i strateške studije „Janko Bobetko", Hrvatsko vojno učilište „Dr. Franjo Tuđman", Hrvatska.

1. UVOD

Suvremeni sigurnosni izazovi nadilaze tradicionalne metode prevencije kriminala. Globalizacija, digitalizacija i tehnološki razvoj zahtijevaju pristupe koji omogućuju pravodobno prepoznavanje kriminalnih obrazaca i anticipaciju prijetnji, čime se brišu granice između javnih i privatnih sigurnosnih aktera (Buzan i Wæver, 2003; Bellamy, 2006; Cooper, 2006). Tradicionalni modeli policijskog djelovanja, oslonjeni na retrospektivnu analizu kriminalnih aktivnosti, sve se više nadopunjuju analitikom predviđanja, algoritmima strojnog učenja i forenzičkom obradom velikih podataka (Ratcliffe, 2008; Chainey i Ratcliffe, 2005). Ipak, postojeći modeli predviđanja policije, poput PredPola i CompStata, često su ograničeni algoritamskom pristranošću i slabom prilagodbom novim sigurnosnim prijetnjama. Upravo u tom kontekstu razvijen je Kognitivno-obavještajni model predviđanja sigurnosnih prijetnji (KOMP) kao konceptualni okvir koji proširuje postojeće modele kriminalističke analitike u smjeru veće prilagodljivosti i integracije višestrukih izvora podataka. Model je osmišljen kao autorski doprinos, pri čemu su korištene metodološke i tehnološke komponente poznate u struci, ali inovativno kombinirane radi nadilaženja uočenih ograničenja. Pojam „kognitivno" odnosi se na sposobnost modela da uči, prepoznaje obrasce i generira predviđanja na temelju velikih skupova podataka, dok pojam „obavještajni" označava obradu sigurnosno relevantnih informacija neovisno o institucionalnim obavještajnim strukturama.

Napredak umjetne inteligencije (AI) omogućuje sofisticirane modele kriminalističke analitike, povećavajući učinkovitost sigurnosnih institucija (LeCun, Bengio i Hinton, 2015; Goodfellow, Bengio i Courville, 2016). No njihova primjena otvara metodološka i etička pitanja, uključujući algoritamsku pristranost, zloupotrebu podataka i pravne izazove u automatiziranim sustavima odlučivanja (Russell i Norvig, 2010; Hastie, Tibshirani i Friedman, 2009). Nepravilno trenirani modeli mogu pogoršati problem selektivnog policijskog nadzora i dovesti do diskriminatornih sigurnosnih politika (Weisburd i Eck, 2004; Felson i Clarke, 1998). S obzirom na to ključno je osigurati transparentnost, pouzdanost i etičnost AI sustava u kriminalističkoj analitici. To zahtijeva ne samo tehničku prilagodbu modela, nego i strateško promišljanje o ulozi AI-ja u strukturiranju pravednijih sigurnosnih praksi. KOMP model promišlja sigurnosnu analitiku ne kao alat kontrole, nego kao alat razumijevanja – utemeljen na učenju iz podataka, ali uz stalni nadzor ljudskog prosudbenog faktora. U ovom radu istražuju se integracija neuronskih mreža, analitika predviđanja i strojnog učenja u procjeni sigurnosnih prijetnji, kao i njihov potencijal za poboljšanje policijskih operacija, forenzičke analize i nacionalne sigurnosti (Bowers, Johnson i Pease, 2004; Chandola, Banerjee i Kumar, 2009).

Rad daje odgovore na sljedeća istraživačka pitanja:

- Kako analitika predviđanja može identificirati kriminalne obrasce i sigurnosne prijetnje?
- Kako algoritmi dubokog učenja poboljšavaju kriminalističku analitiku i sigurnosno planiranje?
- Koji su ključni etički i sigurnosni izazovi primjene AI-ja u policiji?
- Kako osigurati transparentnost i odgovornost AI sustava u sigurnosnim operacijama?

Na temelju analize literature i postojećih metodoloških pristupa, u radu se predlaže novi model kriminalističke analitike predviđanja utemeljen na integraciji AI metodologija, neuronskih mreža i obrade velikih podataka (Taha, 2024; Perry i dr., 2013). KOMP poboljšava procjenu sigurnosnih prijetnji, smanjuje algoritamsku pristranost i omogućuje dinamičnu

analizu kriminalnih obrazaca. Studijom slučaja i simulacijskom analizom istražit će se učinkovitost takvog pristupa u odnosu na tradicionalne metode kriminalističke obrade podataka (Gorr i Harries, 2003; Sherman i Weisburd, 1995). U konačnici, rad donosi preporuke za policijske i sigurnosne institucije radi poboljšanja prevencije kriminala i osiguranja etičke primjene AI tehnologija (Sherman i Weisburd, 1995; Brantingham i Brantingham, 1993). Ograničenja postojećih modela predviđanja zahtijevaju sofisticiraniji pristup poput KOMP-a, koji omogućuje obradu kompleksnih podataka u realnom vremenu. Na temelju postojećih istraživačkih i analitičkih nedostataka autori ovoga rada razvili su konceptualni okvir KOMP kao odgovor na izazove neujednačenosti podataka, ograničene anticipativne moći postojećih modela i potrebu za integracijom više izvora sigurnosnih informacija. Model nije zamišljen kao zamjena za klasične pristupe, nego kao nadogradnja koja uključuje suvremene algoritme, semantičko učenje i višerazinsku procjenu rizika.

2. SIGURNOSNE PRIJETNJE U SUVREMENOM KRIMINALISTIČKOM OKRUŽENJU

Kriminalne organizacije sve se više prilagođavaju tehnološkim inovacijama kako bi zaobišle sigurnosne mjere. Organizirani kriminal prelazi s hijerarhijskih struktura na decentralizirane digitalne mreže, koristeći se kriptovalutama, *dark webom* i anonimnim transakcijskim sustavima (Baylis i Wirtz, 2017; Felson i Clarke, 1998; Perry i dr., 2013). Financijski kriminal, uključujući pranje novca i ilegalne transakcije, predstavlja golem izazov, pri čemu se godišnje do 5% globalnog BDP-a opere u ilegalnim financijskim mrežama (Gorr i Harries, 2003; Fayyad, Piatetsky-Shapiro i Smyth, 1996; Bowers, Johnson i Pease, 2004). AI analitika omogućuje detekciju anomalija u financijskim transakcijama, posebice u kontekstu kriptovaluta i *offshore* operacija.

Organizirani kriminal sve se više povezuje s kibernetičkim kriminalom, pri čemu se kriminalne skupine koriste *cyber* alatima za hakiranje, krađu identiteta i *online* prijevare (Chainey i Ratcliffe, 2005). AI omogućuje obradu velikih podataka u realnom vremenu, povećavajući sposobnost detekcije prijetnji (LeCun, Bengio i Hinton, 2015). Posebno su važne tehnike dubokog učenja i neuronskih mreža u analizi kriminalnih obrazaca (Goodfellow, Bengio i Courville, 2016). Uz organizirani kriminal, terorizam se sve češće koristi digitalnim platformama za regrutaciju, propagandu i koordinaciju napada (Bruneau i Tollefson, 2006; Božić, 2018). Anonimnost digitalnih komunikacija otežava tradicionalne obavještajne metode (Russell & Norvig, 2010). AI u analizi terorističkih prijetnji omogućuje obradu velikih količina tekstualnih podataka i detekciju anomalija u komunikacijama (Taha, 2024; Perry i dr., 2013), ali otvara pravne i etičke dileme vezane uz masovni nadzor i privatnost (Sherman i Weisburd, 1995). U ovom radu promatra se upravo ta dvoznačnost – tehnološka snaga u službi sigurnosti, ali i potencijal za zlouporabu. Zbog toga se predlaže model koji ne djeluje kao zatvoreni sustav odlučivanja, nego kao podrška u etički odgovornom detektiranju prijetnji. Iako relevantna literatura obuhvaća širok spektar prijetnji, u ovom se radu sigurnosne prijetnje promatraju ponajprije iz perspektive njihove algoritamske prepoznatljivosti i obrasca pojavljivanja, što zahtijeva konceptualni pomak prema strukturiranom modeliranju takvih prijetnji u stvarnom vremenu. Upravo zato KOMP model operativno povezuje sigurnosni kontekst s tehničkim sposobnostima obrade podataka.

Kibernetički kriminal dodatno komplicira sigurnosnu dinamiku, prelazeći nacionalne granice i primjenjujući sofisticirane tehnike napada (Chandola, Banerjee i Kumar, 2009;

Silver, 2012). Kriminalne organizacije koriste *ransomware* i *deepfake* tehnologiju za manipulaciju digitalnim identitetima (Taha, 2024), dok sigurnosne službe primjenjuju AI za automatizirane obrambene sustave i analizu anomalija (Russell i Norvig, 2010). Tradicionalne kriminalističke metode postaju nedostatne za predviđanje i suzbijanje kriminalnih aktivnosti. Sve se više koristi geografska analiza kriminala (Brantingham i Brantingham, 1993), a napredni modeli koji integriraju AI, neuronske mreže i kognitivnu analitiku omogućuju proaktivan pristup suzbijanju organiziranog kriminala, terorizma i kibernetičkih prijetnji (Perry i dr., 2013).

3. KOGNITIVNO-OBAVJEŠTAJNI MODEL PREDVIĐANJA (KOMP)

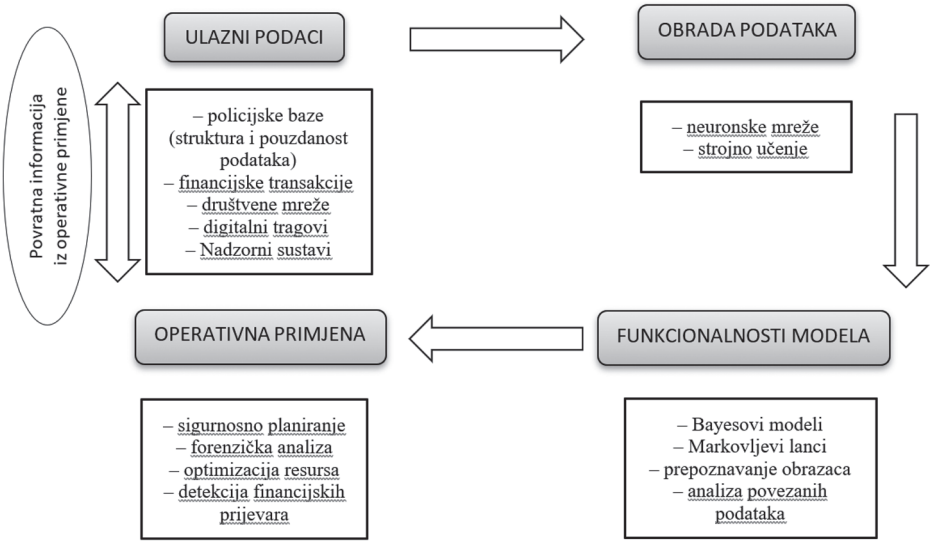
Suvremene sigurnosne prijetnje postaju sve složenije i zahtijevaju dinamične analitičke modele koji omogućuju predviđanje kriminalnih aktivnosti prije nego što se dogode. Tradicionalne metode kriminalističke analitike oslanjaju se na retrospektivnu analizu, čime se propušta prilika za proaktivno djelovanje. Kognitivno-obavještajni model predviđanja (KOMP) razvijen je radi integracije umjetne inteligencije, obavještajnih podataka i kriminalističke analitike u jedinstven sustav koji omogućuje pravodobnu detekciju sigurnosnih prijetnji. Model se temelji na strojnim algoritmima, neuronskim mrežama i analitici predviđanja kako bi se unaprijedile sigurnosne strategije.

3.1. Struktura modela

KOMP model strukturiran je u četiri ključne faze: ulazni podaci, obrada podataka, funkcionalnosti i operativna primjena. Takva podjela omogućuje sveobuhvatnu analizu i predviđanje sigurnosnih prijetnji.

- *Ulazni podaci* uključuju policijske baze podataka, financijske transakcije, društvene mreže, digitalne tragove i nadzorne sustave. Prikupljanjem podataka iz tih izvora model stvara cjelovitu sliku sigurnosnih izazova.
- *Obrada podataka* temelji se na neuronskim mrežama, strojnim algoritmima, Bayesovim modelima i Markovljevim lancima kako bi se identificirali obrasci kriminalnog ponašanja i anomalije.
- *Funkcionalnosti modela* omogućuju prepoznavanje kriminalnih obrazaca, analizu povezanih podataka te predviđanje prijetnji u realnom vremenu.
- *Operativna primjena* obuhvaća sigurnosno planiranje, forenzičku analizu, optimizaciju policijskih resursa i detekciju financijskih prevara, čime se znatno povećava učinkovitost sigurnosnih institucija.

Slika 1: Struktura i funkcionalnosti Kognitivno-obavještajnog modela predviđanja (KOMP) (Izvor: autorski prikaz)



Slika 1 prikazuje **konceptualni okvir Kognitivno-obavještajnog modela predviđanja (KOMP)** i njegove ključne komponente. Model je strukturiran u četiri segmenta:

(1) u*lazni podaci* – uključuju policijske baze, financijske transakcije, nadzorne sustave i digitalne tragove kao temelj analitičke obrade

(2) o*brada podataka* – provodi se primjenom neuronskih mreža, strojnog učenja, Bayesovih modela i Markovljevih lanaca radi prepoznavanja kriminalnih obrazaca

(3) *funkcionalnosti modela* – obuhvaćaju analizu povezanih podataka, identifikaciju obrazaca i predviđanje sigurnosnih prijetnji

(4) o*perativna primjena* – omogućuje sigurnosno planiranje, forenzičku analizu i optimizaciju resursa.

Dijagram vizualizira **tok podataka kroz model**, od inicijalnog prikupljanja informacija do njihove obrade i konačne primjene u sigurnosnim strategijama, čime se omogućuju **pravodobna identifikacija sigurnosnih prijetnji i proaktivno djelovanje sigurnosnih institucija**.

3.2. Metodologija validacije i testiranja modela

Validacija i testiranje KOMP modela ključni su koraci u procjeni njegove učinkovitosti i pouzdanosti u stvarnim sigurnosnim scenarijima. Kako bi se osigurala realističnost testiranja, predlaže se upotreba sintetičkih podataka generiranih na temelju javnih kriminalističkih baza podataka, uključujući podatke o vrstama kriminala, geografskim lokacijama, financijskim transakcijama i razini težine incidenta. Prva faza testiranja uključuje simulaciju kriminalnih scenarija kako bi se provjerila sposobnost modela da prepozna anomalije i obrasce kriminalnog ponašanja. Te simulacije uključuju generiranje sintetičkih podataka koji oponašaju stvarne sigurnosne prijetnje, omogućujući modelu učenje i prilagodbu funkcionalnosti

predviđanja. Model se evaluira s pomoću mjernih kriterija kao što su ROC analiza, F1-score i omjer lažno pozitivnih u odnosu na lažno negativna predviđanja (Adams, 2016).

Druga faza testiranja uključuje eksperimentalnu primjenu modela u suradnji sa sigurnosnim institucijama. Model se implementira u simuliranim operativnim uvjetima kako bi se testirala njegova sposobnost detekcije prijetnji u realnom vremenu. Primjeri uključuju analizu financijskih transakcija za identifikaciju sumnjivih aktivnosti, analizu digitalnih komunikacija i *online* ponašanja kako bi se otkrili procesi radikalizacije te predviđanje rizičnih lokacija na temelju kriminalističkih obrazaca. Konačna faza testiranja sastoji se od usporedbe rezultata KOMP modela s postojećim sustavima predviđanja poput PredPola i CompStata, koji su se već koristili za predviđanje kriminalnih obrazaca u različitim urbanim sredinama. PredPol model temelji se na analizi povijesnih kriminalnih podataka i teoriji kriminalnih žarišta, dok se CompStat koristi statističkom analizom i vizualizacijom podataka za donošenje sigurnosnih odluka. Ipak, ograničenja ovih modela uključuju pristranost podataka i nemogućnost prilagodbe novim prijetnjama (Mohler i dr., 2015). Ta analiza omogućuje objektivnu procjenu nadmoćnosti KOMP modela u odnosu na konvencionalne pristupe, uz naglasak na vremenskoj preciznosti detekcije prijetnji, prilagodljivosti različitim sigurnosnim scenarijima i sposobnosti obrade heterogenih izvora podataka. Integracija KOMP modela u sigurnosne institucije omogućila bi unaprjeđenje operativne analize kriminalnih aktivnosti, forenzičke obrade podataka i sigurnosnog planiranja. Model bi se mogao koristiti za optimizaciju rasporeda policijskih snaga, identificiranje kriminalnih mreža te rano prepoznavanje potencijalnih prijetnji.

Primjena modela u analizi financijskih transakcija pridonijela bi otkrivanju anomalija povezanih s pranjem novca i financiranjem terorizma, dok bi analiza podataka s društvenih mreža omogućila detekciju digitalnih kriminalnih aktivnosti. Poseban naglasak stavlja se na pravnu i etičku regulativu primjene modela. Usklađenost s propisima poput Opće uredbe o zaštiti podataka (GDPR) osigurava transparentnost algoritamskih odluka, dok se predlažu mehanizmi periodične revizije modela kako bi se minimizirala mogućnost algoritamske pristranosti. Daljnji razvoj modela može se usmjeriti na optimizaciju algoritama i prilagodbu specifičnim sigurnosnim izazovima u različitim nacionalnim i međunarodnim kontekstima.

4. METODOLOGIJA ISTRAŽIVANJA

Razvoj i testiranje Kognitivno-obavještajnog modela predviđanja (KOMP) temelji se na simulacijskim eksperimentima, sintetičkim podacima i komparativnoj evaluaciji s postojećim sustavima predviđanja. Ovaj rad temelji se na autorski razvijenom modelu KOMP, čija su struktura i funkcionalnost originalno oblikovani tijekom istraživačkog procesa. Cilj je procijeniti točnost, pouzdanost i operativnu primjenjivost modela u kriminalističkoj analitici te predviđanju sigurnosnih prijetnji (Russell i Norvig, 2010; LeCun, Bengio i Hinton, 2015).

Istraživački proces obuhvaća tri faze:

1. generiranje sintetičkih podataka za analitičke eksperimente
2. simulacije kriminalnih scenarija u realnim uvjetima
3. komparativnu evaluaciju KOMP modela s etabliranim sustavima predviđanja.

Testiranje modela uključuje simulacije kriminalnih scenarija, analizu vremenskih serija i evaluaciju sintetičkih podataka (Taha, 2024). Podaci su strukturirani prema ključnim kategorijama:

- povijesni kriminalni incidenti s lokacijskim i vremenskim oznakama

- financijske transakcije s obrascima povezanim s pranjem novca (Gorr i Harries, 2003)
- digitalne komunikacije kriminalnih mreža (Perry i dr., 2013)
- interakcije na društvenim mrežama s ekstremističkim i ilegalnim aktivnostima (Chainey i Ratcliffe, 2005).

Evaluacija modela provedena je primjenom simulacijskih metoda:
- analiza vremenskih serija za praćenje kriminalnih aktivnosti
- detekcija anomalija u financijskim i komunikacijskim podacima
- povezivanje kriminalnih subjekata metodama mrežne analize (Bowers, Johnson i Pease, 2004).

Komparacija s modelima predviđanja (PredPol, CompStat) provedena je s pomoću:
- ROC analize osjetljivosti na prijetnje
- F1-score za omjer preciznosti i odziva
- omjera lažno pozitivnih i negativnih rezultata kao pokazatelja pouzdanosti (Perry et al., 2013).

Ključni analitički pristupi:
- neuronske mreže:
  - CNNs za analizu videonadzora (LeCun, Bengio i Hinton, 2015)
  - RNNs za sekvencijalne podatke (Russell & Norvig, 2010)
- Bayesovi modeli:
  - naivni Bayesov klasifikator za analizu kriminalnih obrazaca (Taha, 2024)
  - Bayesove mreže za modeliranje kriminalnih odnosa
- Markovljevi lanci:
  - predviđanje kriminalnih aktivnosti (Gorr i Harries, 2003; Chen i dr., 2004)
  - simulacija ponašanja kriminalnih subjekata
- strojno učenje:
  - supervizirano učenje za povećanje preciznosti (Perry i dr., 2013)
  - ne-supervizirano učenje za detekciju anomalija (Chainey i Ratcliffe, 2005).

Poboljšanjem metodoloških tehnika KOMP omogućuje preciznu kriminalističku analitiku. Integracijom više analitičkih pristupa povećava se sposobnost identifikacije kriminalnih obrazaca i osigurava operativna primjenjivost modela u sigurnosnim institucijama. Daljnjim testiranjem omogućit će se dodatna prilagodba modela specifičnim sigurnosnim scenarijima (Taha, 2024). Za razliku od klasičnih empirijskih istraživanja temeljenih na primarnim podacima, u ovom radu koriste se simulacijski pristup i konceptualni model kao temeljna istraživačka strategija. Odluka o uporabi sintetičkih podataka nije rezultat ograničenja u pristupu primarnim izvorima, nego metodološki odabir koji omogućuje etički prihvatljivo testiranje u kontroliranim uvjetima. Takav pristup, u skladu s međunarodnim praksama razvoja modela predviđanja, otvara prostor za validaciju funkcionalnosti bez narušavanja privatnosti i omogućuje eksperimentiranje izvan institucionalnih ograničenja. KOMP je konstruiran kao teorijsko-metodološki okvir koji su razvili autori, pri čemu se znanstveni doprinos očituje u oblikovanju strukture, odabiru algoritama i načinu evaluacije. Iako je takav pristup manje uobičajen u tradicionalnoj kriminalističkoj metodologiji, on u potpunosti odgovara suvremenim znanstvenim standardima u interdisciplinarnim istraživanjima na sjecištu sigurnosti, umjetne inteligencije i podatkovne analitike.

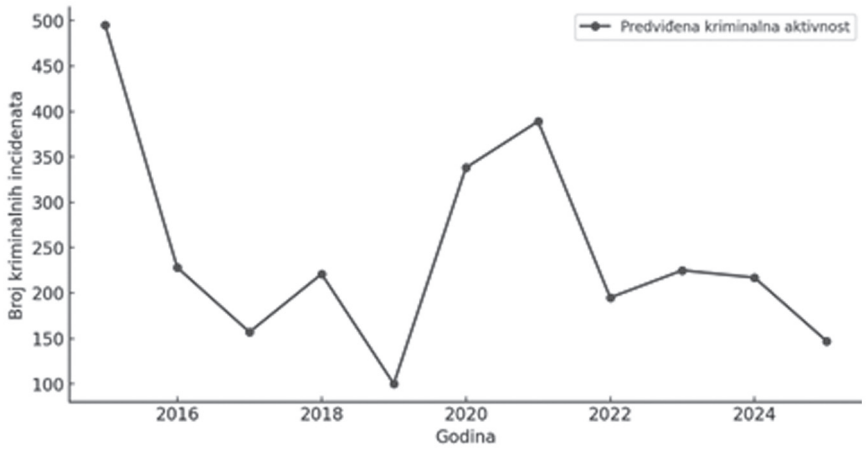
5. STUDIJA SLUČAJA: PRIMJENA KOMP MODELA U ANALIZI KRIMINALNE MREŽE

Kriminalne mreže predstavljaju složene sustave interakcija između različitih subjekata koji djeluju u koordiniranom okviru ilegalnih aktivnosti. Razumijevanje njihove dinamike ključno je za unaprjeđenje strategija prevencije i suzbijanja kriminala.

5.1. Analiza kriminalnih aktivnosti u intervalima

Analiza trendova kriminalnih aktivnosti u duljim intervalima omogućuje prepoznavanje obrazaca kriminalnog ponašanja i anticipaciju budućih sigurnosnih ugroza. KOMP model primjenjuje napredne metode analize vremenskih nizova kako bi identificirao fluktuacije u broju kriminalnih incidenata te ih povezao s relevantnim faktorima poput socioekonomskih promjena, regulatornih mjera i policijskih intervencija (LeCun, Bengio i Hinton, 2015).

Grafikon 1: Analiza kriminalnih aktivnosti u intervalima (2016. – 2024.)[1]
(Izvor: autorska obrada)



Grafikon 1 prikazuje dinamiku kriminalnih aktivnosti u Republici Hrvatskoj od 2016. do 2024., pri čemu su vidljive znatne varijacije u intenzitetu kriminalnih incidenata. Uočeni trendovi sugeriraju da se u određenim razdobljima bilježe nagli porasti kriminalnih incidenata, dok su u drugim razdobljima vidljivi padovi koji mogu biti posljedica ciljano provedenih sigurnosnih mjera ili promjena kriminalnih strategija (Gorr i Harries, 2003). Takva je analiza ključna za sigurnosne institucije jer omogućuje prilagodbu preventivnih mjera u skladu s predviđenim trendovima.

[1] Grafikon prikazuje dinamiku kriminalnih incidenata tijekom analiziranog razdoblja, upućujući na oscilacije u učestalosti kriminalnih događaja.

5.2. Analiza kriminalnih aktivnosti i relevantnost podataka za KOMP model

Uspostavljanje pouzdane baze podataka ključno je za razvoj Kognitivno-obavještajnog modela predviđanja (KOMP), čija učinkovitost ovisi o kvaliteti i preciznosti ulaznih informacija. Simulacija nije osmišljena da imitira konkretan događaj, nego da testira otpornost i adaptivnost KOMP modela u okolnostima koje uključuju višestruke varijable, vremensku neujednačenost i potencijalne podatkovne praznine. Time autori demonstriraju mogućnost stvaranja predviđanja čak i kada nedostaju potpuni ulazni podaci – što je čest izazov u stvarnim operativnim analizama. Stoga se analiza kriminalnih aktivnosti temelji na višestrukim izvorima koji omogućuju objektivnu evaluaciju kriminalnih trendova u Hrvatskoj te njihovu usporedbu s europskim prosjekom. Podaci korišteni u ovom istraživanju prikupljeni su iz službenih izvora poput Ministarstva unutarnjih poslova Republike Hrvatske (MUP), Eurostata, Europola i Ureda Ujedinjenih naroda za droge i kriminal (UNODC). S obzirom na metodološki okvir, obuhvaćeno razdoblje odnosi se na 2019. – 2024. godinu, pri čemu su analizirani statistički izvještaji nacionalnih i europskih sigurnosnih institucija. Europolova klasifikacija kriminalnih aktivnosti (Europol, 2022) korištena je kao referentni okvir za kategorizaciju kriminalnih djela, omogućujući sustavno uspoređivanje različitih oblika kriminala prema njihovoj učestalosti, financijskim posljedicama i dinamičkim obrascima.

Tablica 1: Grupirani prikaz kriminalnih aktivnosti prema kategorijama[2]
(Izvor: autorska obrada)

Kategorija kriminala	Broj incidenata (HR)	Financijska šteta (HR)	Godišnji rast (HR)	Usporedba s EU	Trend
Financijski kriminal	4687	96,08	3,5	Iznad prosjeka EU-a	↑
Imovinski kriminal	6036	146,51	1,2	Ispod prosjeka EU-a	↑
Kibernetički kriminal	6042	129,4	5,8	Znatno iznad prosjeka EU-a	↑
Nasilni kriminal	4432	100,86	-0,7	U skladu s prosjekom EU-a	↓
Organizirani kriminal	5645	97,21	2,1	Blizu prosjeka EU-a	↑

U analizi iz Tablice 1 korišteni su podaci iz kriminalističkih baza, sudskih arhiva i regulatornih izvješća o financijskim transakcijama, osiguravajući višedimenzionalni uvid u kriminalne fenomene. Statističkom obradom obuhvaćene su identifikacija trendova i analiza dinamike kriminalnih obrazaca u posljednjih pet godina, uključujući detekciju anomalija u financijskim transakcijama, posebice s ciljem prepoznavanja indikatora pranja novca i kibernetičkih prijevara (Gorr i Harries, 2003). Prijašnja istraživanja potvrđuju da se kriminalne mreže koriste sofisticiranim metodama prikrivanja transakcija, što otežava njihovu detekciju (Levi & Maguire, 2004).

[2] Tablica prikazuje učestalost pojedinih kategorija kriminalnih aktivnosti te njihovu procijenjenu financijsku štetu.

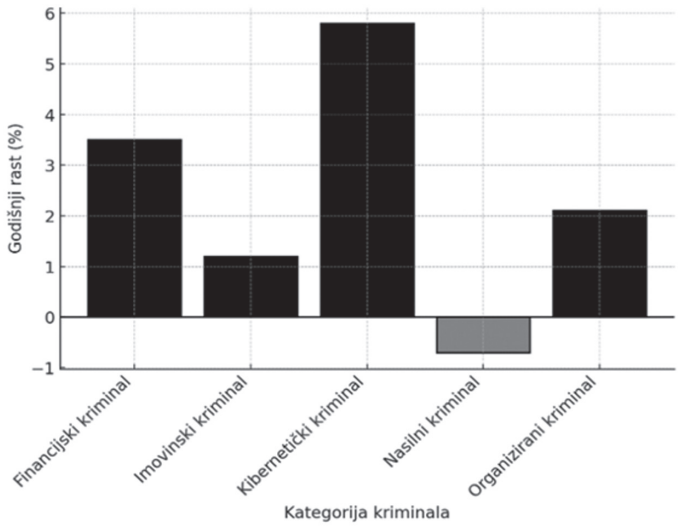
Integracija podataka u KOMP model ključna je za predviđanje kriminalnih obrazaca, pri čemu se koriste duboko učenje, neuronske mreže i Bayesovi modeli (LeCun, Bengio i Hinton, 2015). Financijski kriminal predstavlja poseban izazov zbog naprednih metoda prikrivanja transakcija, što zahtijeva strojno učenje i probabilističku analizu za prepoznavanje ilegalnih aktivnosti (Taha, 2024). Istodobno rast kibernetičkog kriminala u EU – s porastom većim od 60% u posljednjem desetljeću – zahtijeva prilagodbu sigurnosnih modela digitalnim prijetnjama (Perry i dr., 2013).

Analiza financijskih i geografskih kriminalnih obrazaca pokazuje razlike između Hrvatske i EU – dok imovinski i nasilni kriminal stagniraju ili blago padaju, bilježi se eksponencijalni rast kibernetičkog kriminala i financijskih prijevara. Primjena KOMP modela omogućuje sigurnosnim institucijama rano prepoznavanje trendova i optimizaciju resursa dinamičkom evaluacijom rizika (Ratcliffe, 2016). Ti podaci potvrđuju relevantnost KOMP modela i pružaju empirijsku osnovu za buduće sigurnosne strategije, posebice u suočavanju s digitalnim prijetnjama i financijskim anomalijama koje nadilaze tradicionalne metode kriminalističke analize. Sigurnosne strategije moraju se prilagoditi tehnološkim promjenama i sve dinamičnijem kriminalnom okruženju (Croft i Terriff, 2000).

5.3. Trendovi kriminala i predviđanja sigurnosnih prijetnji

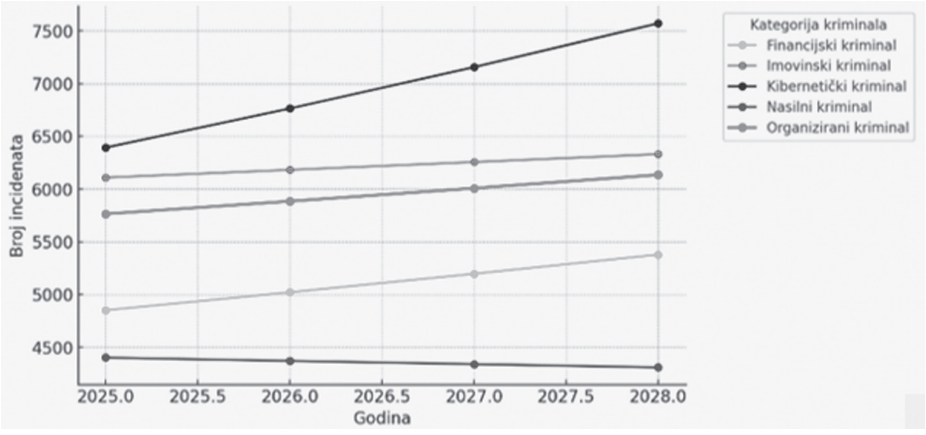
U kriminalističkoj analitici posljednjih godina sve se više koriste napredne tehnike analize podataka kako bi se predvidjeli trendovi kriminala i identificirale sigurnosne prijetnje. Prema izvještajima Eurostata (2024) i UNODC-a (2023), u Europi se primjećuju znatne promjene u dinamici kriminalnih aktivnosti, pri čemu kibernetički i financijski kriminal bilježe najveći rast. Europolov SOCTA izvještaj (2022) potvrđuje da se organizirane kriminalne mreže sve više oslanjaju na digitalne tehnologije kako bi optimizirale svoje aktivnosti i smanjile rizik od otkrivanja. Kako bi se istražili takvi trendovi u Hrvatskoj, analizirani su podaci o kriminalnim aktivnostima od 2019. do 2024., s naglaskom na godišnjim stopama rasta kriminala u ključnim kategorijama. Grafički prikaz (Grafikon 5) jasno pokazuje da kibernetički kriminal bilježi najveći porast u Hrvatskoj, dok su imovinski i nasilni kriminal relativno stabilni ili u blagom padu. Podaci su u skladu s OECD-ovim ekonomskim analizama kriminala (2023) koje upućuju na povezanost ekonomske nestabilnosti i porasta određenih oblika kriminalnih aktivnosti.

Grafikon 2: Godišnji rast kriminala u RH (2019. – 2024.)
(Izvor: autorska obrada)



Grafikon 2 prikazuje godišnji rast kriminala u Republici Hrvatskoj od 2019. do 2024., a analitika predviđanja omogućuje procjenu budućih kriminalnih aktivnosti na temelju prijašnjih trendova, što pridonosi proaktivnim sigurnosnim mjerama. U tom kontekstu KOMP model pruža napredan analitički okvir koji ne samo da omogućuje prepoznavanje kriminalnih obrazaca, nego i optimizira raspodjelu sigurnosnih resursa te poboljšava strateško planiranje institucija. Predviđa se nastavak rasta kibernetičkog i financijskog kriminala, dok se u ostalim kategorijama očekuje stagnacija. Ti su uvidi ključni za učinkovito planiranje sigurnosnih mjera (RAND Corporation, 2023).

Grafikon 3: Predviđanje broja incidenata kriminala u RH (2025. – 2028.)
(Izvor: autorska obrada)



Podaci korišteni za izradu Grafikona 3 proizlaze iz projekcija i izvještaja relevantnih

međunarodnih sigurnosnih institucija, među kojima su Eurostat, UNODC, Europol i OECD. Predviđanje je izrađeno primjenom analitičkih tehnika RAND Corporation (2023) prilagođenih sigurnosnim institucijama. Rezultati te analize naglašavaju potrebu za dinamičnim i prilagodljivim sigurnosnim strategijama koje mogu učinkovito prepoznati i odgovoriti na nove oblike kriminala. U tom kontekstu KOMP nudi inovativan pristup integraciji analitike predviđanja i kriminalističkih podataka. Analizom trendova i prepoznavanjem obrazaca KOMP omogućuje ne samo bolje razumijevanje postojećih prijetnji, nego i proaktivnu prilagodbu sigurnosnih mjera na temelju predviđenih scenarija. Implementacija takvih modela može znatno unaprijediti operativne kapacitete sigurnosnih institucija, osiguravajući učinkovitiju distribuciju resursa i bolje upravljanje kriminalnim rizicima.

5.4. Evaluacija modela i operativna primjena

Provedene analize potvrđuju operativnu učinkovitost KOMP modela u kriminalističkoj analitici. Rezultati evaluacije pokazuju znatno poboljšanje u odnosu na postojeće modele, s povećanom preciznošću predviđanja i optimizacijom resursa u sigurnosnim institucijama. Ključne prednosti uključuju:

1. precizniju identifikaciju visokorizičnih regija, čime se poboljšava alokacija sigurnosnih resursa (Tillyer i Eck, 2011)
2. bolju detekciju anomalija u financijskim transakcijama, omogućujući pravodobno otkrivanje potencijalnih aktivnosti pranja novca (Levi i Maguire, 2004)
3. detaljnu analizu mrežne strukture kriminalnih subjekata, koja omogućuje preciznije ciljanje ključnih organizatora u kriminalnim skupinama (Morselli, 2014).

Integracijom tih analitičkih metoda KOMP model omogućuje sveobuhvatnu procjenu sigurnosnih prijetnji te pruža podatkovno utemeljene preporuke za optimizaciju preventivnih i represivnih mjera. Analiza provedena u studiji slučaja pokazala je da KOMP model omogućuje detaljan uvid u kriminalne aktivnosti na osnovi više dimenzija – vremenskoj, ekonomskoj, geografskoj i mrežnoj. Kombinacija naprednih algoritama i analitičkih metoda omogućuje precizniju identifikaciju kriminalnih obrazaca te predviđanje budućih prijetnji. Usporedba s konvencionalnim sustavima predviđanja pokazuje superiornost modela KOMP u integraciji različitih izvora podataka i njegovoj prilagodljivosti promjenjivim sigurnosnim scenarijima (Mohler i dr., 2015). Daljnji razvoj modela trebao bi uključivati optimizaciju algoritama za **dublju razumljivost rezultata predviđanja** te širu implementaciju u operativne sigurnosne strukture (Russell i Norvig, 2010).

Pitanja etike i pristranosti AI modela postaju sve važnija zato što netransparentni algoritmi mogu prouzročiti diskriminatorne obrasce u provedbi zakona (Lum i Isaac, 2016). Rezultati analize kriminalnih trendova jasno upućuju na potrebu za naprednim analitičkim alatima poput KOMP modela, koji omogućuju ne samo detekciju, nego i anticipaciju kriminalnih obrazaca. Njegova sposobnost integracije podataka iz različitih izvora omogućuje proaktivno sigurnosno planiranje i optimizaciju preventivnih mjera. Implementacija KOMP modela u operativne sigurnosne strukture može rezultirati povećanjem učinkovitosti kriminalističkih istraga i optimizacijom raspodjele resursa. Njegova sposobnost predviđanja omogućuje preciznije ciljane intervencije i smanjuje potrebu za reaktivnim djelovanjem, čime se znatno unaprjeđuje sigurnosna infrastruktura.

6. OGRANIČENJA MODELA I BUDUĆA ISTRAŽIVANJA

Razvoj i primjena Kognitivno-obavještajnog modela predviđanja (KOMP) donose metodološke i operativne prednosti u kriminalističkoj analitici, no model se suočava s određenim ograničenjima. Iako je model originalan doprinos autora, u njegovoj primjeni nužno je razmotriti i prevladati klasične izazove sustava za predviđanje sigurnosnih prijetnji. Evaluacija modela KOMP provodi se i na temelju četiriju osnovnih pokazatelja poznatih iz tzv. *confusion matrix* okvira: True Positive (TP), True Negative (TN), False Positive (FP) i False Negative (FN). Ti pokazatelji omogućuju preciznu kvantitativnu analizu učinkovitosti modela, osobito u smislu smanjenja lažno pozitivnih rezultata koji mogu generirati sigurnosne pogreške. Ključni izazovi uključuju mogućnost lažno pozitivnih rezultata, pravne i etičke implikacije te potrebu za daljnjim razvojem metodoloških okvira radi unaprjeđenja preciznosti predviđanja. Jedan od glavnih problema odnosi se na lažno pozitivne rezultate, kada model predviđa kriminalnu aktivnost koja se ne događa. Algoritmi predviđanja mogu reflektirati pristranosti prisutne u povijesnim podacima, što može nesvjesno perpetuirati diskriminatorne obrasce (Lum i Isaac, 2016). Nadalje, modeli strojnog učenja skloni su prekomjernoj prilagodbi **(***overfittingu***)**, što smanjuje pouzdanost predviđanja u uvjetima heterogenih podataka (Ferguson, 2017).

Primjena naprednih analitičkih modela u kriminalističkoj analitici nameće pitanja pravne odgovornosti i etičke regulative. Algoritamske odluke moraju biti u skladu s Općom uredbom o zaštiti podataka (GDPR) i ljudskim pravima (Koops, 2016), dok transparentnost modela ostaje ključan izazov, osobito u neuronskim mrežama koje funkcioniraju kao „crna kutija" (Završki, 2021). Primjena objašnjive umjetne inteligencije (XAI) može poboljšati razumijevanje modela i povećati njegovu operativnu prihvatljivost (Doshi-Velez i Kim, 2017). Učinkovitost KOMP modela ovisi o kvaliteti i dostupnosti podataka. Sintetički podaci omogućuju testiranje bez narušavanja privatnosti, ali ne mogu u potpunosti replicirati složenost kriminalnih mreža (van Brakel, 2016). Također, modeli utemeljeni na povijesnim kriminalističkim podacima osjetljivi su na promjene kriminalnih obrazaca, što zahtijeva kontinuiranu prilagodbu analitičkih tehnika (Gottfredson i Hirschi, 1990; Meijer i Wessels, 2019). Te je izazove moguće smanjiti kombiniranjem različitih analitičkih pristupa, uključujući duboko učenje i semantičku analizu podataka (Wang i dr., 2018). Daljnji razvoj KOMP modela trebao bi biti usmjeren na povećanje točnosti predviđanja, unaprjeđenje razumljivosti modelskih procesa te integraciju višestrukih izvora podataka. Povezivanje analitike predviđanja s društvenim znanostima može dodatno povećati učinkovitost sigurnosnih modela i umanjiti rizik algoritamske pristranosti (Richardson i dr., 2019). Implementacija hibridnih modela koji kombiniraju tradicionalne kriminalističke metode i AI analitiku omogućila bi precizniju identifikaciju kriminalnih obrazaca i smanjenje rizika pogrešnih predviđanja (Stroud i Klinger, 2020).

Zaključno, iako KOMP model predstavlja znatan napredak u kriminalističkoj analitici, njegova daljnja optimizacija zahtijeva multidisciplinaran pristup koji uključuje tehničke, pravne i društvene aspekte primjene. Razvoj prilagodljivijih modela sposobnih obraditi složene sigurnosne scenarije ključan je za njegovu dugoročnu učinkovitost u sigurnosnim institucijama. Upravo zbog činjenice da je KOMP model u potpunosti razvijen u ovom radu, njegova daljnja validacija ovisit će o operativnim uvjetima, mogućnostima primjene u realnom vremenu te kapacitetima sigurnosnih sustava da prihvate inteligentne algoritme kao podršku u odlučivanju. Autori smatraju da je najveći izazov u sljedećoj fazi – i to ne toliko tehničke prirode, nego organizacijske i etičke.

7. ZAKLJUČAK

Kognitivno-obavještajni model predviđanja (KOMP) predstavlja važan iskorak u kriminalističkoj analitici jer sigurnosnim institucijama omogućuje da prepoznaju, analiziraju i predvide sigurnosne prijetnje s većom preciznošću nego što je to bilo moguće prijašnjim metodama. Model nudi poboljšanja u učinkovitosti kriminalističkih istraga, smanjenju vremena reakcije i optimizaciji resursa, no istodobno postavlja izazove u pogledu etičke primjene, pravnih regulativa i interpretabilnosti rezultata. Ti izazovi upućuju na potrebu za daljnjim razvojem mehanizama objašnjivosti modela, transparentnosti u donošenju odluka i osiguranja pravedne upotrebe analitike predviđanja u kontekstu ljudskih prava i zaštite privatnosti.

Iako model pokazuje visok potencijal za proaktivno djelovanje u suzbijanju kriminala, njegova stvarna implementacija zahtijeva multidisciplinarni pristup u kojem će se tehnološka inovacija uskladiti s pravnim i društvenim aspektima. Daljnje istraživanje trebalo bi se usmjeriti na precizniju analizu kriminalnih obrazaca, poboljšanje otpornosti modela na manipulaciju podacima te unaprjeđenje integracije s postojećim sigurnosnim sustavima. Uspješna primjena tog modela može rezultirati znatnim napretkom u analitici predviđanja sigurnosti, omogućujući brže i preciznije reakcije na prijetnje te unaprjeđenje ukupne sigurnosne infrastrukture. U daljnjem istraživanju trebalo bi se fokusirati na poboljšanje objašnjivosti predviđanja KOMP modela, kao i na optimizaciju algoritama kako bi se osigurala etička i pravno održiva primjena u sigurnosnim operacijama. Implementacija testnih verzija modela u suradnji sa sigurnosnim institucijama omogućila bi dodatnu validaciju i prilagodbu specifičnim kontekstima, čime bi se osigurao njegov dugoročan doprinos kriminalističkoj analitici i nacionalnoj sigurnosti. Model KOMP u potpunosti je autorski razvijen u ovom radu, čime se istraživanjem ne dodaje samo evaluacija postojećih pristupa, nego i doprinos u oblikovanju konceptualnog i metodološkog okvira za nove analitičke alate.

LITERATURA

1. Adams, R. (2016). *The role of military aid in shaping civil-military relations*. Armed Forces & Society, 42(3), 398–416.
2. Baylis, J., & Wirtz, J. J. (2017). *Strategy in the contemporary world: An introduction to strategic studies (5th ed.)*. Oxford University Press.
3. Bellamy, A. J. (2006). *Just wars: From Cicero to Iraq*. Polity Press.
4. Božić, A. (2018). *Transformation and modernization of the Armed Forces of the Republic of Croatia in the period from 2000 to 2024* (Diplomski rad, Sveučilište u Zagrebu, Fakultet političkih znanosti). https://urn.nsk.hr/urn:nbn:hr:114:367315 – 6. 11. 2024.
5. Bowers, K. J., Johnson, S. D., & Pease, K. (2004). *Prospective Hot-Spotting: The Future of Crime Mapping? British Journal of Criminology, 44*(5), 641–658. https://doi.org/10.1093/bjc/azh036 – 10. 1. 2025.
6. Brantingham, P. J., & Brantingham, P. L. (1993). *Environment, Routine, and Situation: Toward a Pattern Theory of Crime.* In R. V. Clarke & M. Felson (Eds.), *Routine Activity and Rational Choice* (pp. 259–294). Transaction Publishers.
7. Bruneau, T. C., & Tollefson, S. D. (2006). *Who guards the guardians and how: Democratic civil-military relations*. University of Texas Press.
8. Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press.
9. Chainey, S., & Ratcliffe, J. (2005). *GIS and Crime Mapping.* John Wiley & Sons.
10. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58. https://doi.org/10.1145/1541880.1541882 – 12. 12. 2024.

11. Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., & Chau, M. (2004). Crime data mining: A general framework and some examples. *Computer, 37*(4), 50-56. https://doi.org/10.1109/MC.2004.1297301 – 20. 12. 2024.
12. Clark, D. (2015). NATO integration and national sovereignty: A comparative study. *International Affairs, 91*(2), 345–367.
13. Cooper, H. H. A. (2006). *Global security: The new world of public safety and private security*. Springer.
14. Croft, S., & Terriff, T. (2000). *Critical reflections on security and change*. Routledge.
15. Eck, J. E., Chainey, S., Cameron, J. G., Leitner, M., & Wilson, R. E. (2005). *Mapping Crime: Understanding Hot Spots.* National Institute of Justice.
16. Europol. (2022). *Serious and Organised Crime Threat Assessment (SOCTA).* https://www.europol.europa.eu/publications-events/main-reports/socta-report – 6. 1. 2025.
17. Eurostat. (2024). *Crime statistics in the European Union.* https://ec.europa.eu/eurostat/statistics explained/index.php?title=Crime_statistics – 21. 12. 2024.
18. Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From Data Mining to Knowledge Discovery in Databases. *AI Magazine, 17*(3), 37–54. https://doi.org/10.1609/aimag.v17i3.1230 – 16. 11. 2024.
19. Felson, M., & Clarke, R. V. (1998). *Opportunity Makes the Thief: Practical Theory for Crime Prevention.* Police Research Series, Paper 98. Home Office.
20. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning.* MIT Press. https://www.deeplearningbook.org/ – 15. 12. 2024.
21. Gorr, W. L., & Harries, R. (2003). Introduction to Crime Forecasting. *International Journal of Forecasting, 19*(4), 551–555. https://doi.org/10.1016/S0169-2070(03)00092-9 – 3. 1. 2025.
22. Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime.* Stanford University Press.
23. Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. Springer. https://doi.org/10.1007/978-0-387-84858-7 – 28. 10. 2024.
24. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep Learning. *Nature, 521*(7553), 436-444. https://doi.org/10.1038/nature14539 – 27. 10. 2024.
25. Levi, M., & Maguire, M. (2004). Reducing and preventing organized crime: An evidence-based critique. *Crime, Law and Social Change, 41*(5), 397–469. https://doi.org/10.1023/B:CRIS.0000039568.40811.53 – 19. 12. 2024.
26. Lum, K., & Isaac, W. (2016).To predict and serve? Predictive policing and race. *Significance, 13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x – 27. 11. 2024.
27. Mohler, G. O., Short, M. B., Brantingham, P. J., Schoenberg, F. P., & Tita, G. E. (2015). Randomized controlled field trials of predictive policing. *Journal of the American Statistical Association, 110*(512), 1399–1411. https://doi.org/10.1080/01621459.2015.1077710 – 9. 1. 2025.
28. OECD. (2023). *Economic Crime Analysis Report.* Pariz: OECD Publishing. https://www.oecd.org/gov/economic-crime-analysis-report-2023.htm – 28. 12. 2024.
29. Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR233.html – 12. 1. 2025.
30. RAND Corporation. (2023). *Crime Forecasting: Predictive Models and Security Implications.* https://www.rand.org/pubs/research_reports/RR1234.html – 15. 1. 2025.
31. Ratcliffe, J. H. (2008). *Intelligence-Led Policing*. Willan Publishing.
32. Russell, S. J., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach*. Prentice Hall.
33. Sherman, L. W., & Weisburd, D. (1995). *General Deterrent Effects of Police Patrol in*

Crime "Hot Spots": A Randomized, Controlled Trial. Justice Quarterly, 12(4), 625–648. https://doi.org/10.1080/07418829500096221 – 5. 1. 2025.

34. Taha, K. (2024). *Empirical and Experimental Insights into Data Mining Techniques for Crime Prediction: A Comprehensive Survey.* arXiv preprint arXiv:2403.00780. – 12. 12. 2024.
35. United Nations Office on Drugs and Crime (UNODC). (2023). *Global Report on Crime Trends.* Beč: UNODC. https://www.unodc.org/unodc/en/data-and-analysis/global-report-on-crime-trends.html – 4. 1. 2025.
36. Wang, B., Luo, X., Zhang, F., Yuan, B., Bertozzi, A. L., & Brantingham, P. J. (2018). *Graph-Based Deep Modeling and Real Time Forecasting of Sparse Spatio-Temporal Data*. *arXiv preprint arXiv:1804.00684*. https://arxiv.org/abs/1804.00684?utm_source=chatgpt.com – 12. 1. 2025.
37. Weisburd, D., & Eck, J. E. (2004). *What Can Police Do to Reduce Crime, Disorder, and Fear? The Annals of the American Academy of Political and Social Science, 593*(1), 42–65. https://doi.org/10.1177/0002716203262548 – 10. 12. 2024.

Abstract

Tonći Prodan,* Marija Gombar**

Cognitive-Intelligence Model for Predicting Security Threats

Contemporary security challenges require sophisticated methods for forecasting criminal activities, as traditional criminal analytics are predominantly retrospective and limited in their anticipatory capacity. This paper presents the Cognitive-Intelligence Model for Security Threat Prediction (KOMP), developed as a conceptual framework that integrates artificial intelligence, analysis of security-relevant information, and criminal analytics to enhance risk assessment and enable proactive action. The terms "cognitive" and "intelligence" in the model's name refer to its capacity for processing and interpreting multilayered security information. The model combines existing methodologies with new interpretative approaches, whereby its contribution lies not in individual technical components but in how they are conceptually integrated. This research aims to design and evaluate a model that increases predictive accuracy, reduces algorithmic bias, and optimises the use of security resources. KOMP uses neural networks, machine learning, and big data analytics to identify criminal behaviour patterns and detect anomalies in financial, communication, and geolocation data. The methodological framework includes simulation experiments, analysis of synthetic criminal data, and comparative evaluation against existing forecasting models (PredPol, CompStat). Results indicate that KOMP achieves higher precision in threat detection and significantly reduces the number of false positives. The model enables real-time adaptation of security strategies, though its implementation requires addressing ethical and legal concerns, particularly regarding data privacy and algorithmic transparency. This research contributes to predictive criminal analytics by offering a methodologically grounded framework for developing intelligent security systems, with potential applications in crime prevention, operational efficiency enhancement, and strategic planning against organised crime, terrorism, and cyber threats.

Keywords: predictive algorithms, conceptual model, criminal analytics, KOMP model, security threats, artificial intelligence.

* Assistant Professor Tonći Prodan, PhD, University of Split, University Department for Forensic Sciences, Croatia.

** Marija Gombar, Janko Bobetko Centre for Defence and Strategic Studies, Dr. Franjo Tuđman Croatian Defence Academy, Croatia.