UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”

FAKULTETI I SHKENCAVE MATEMATIKO – NATYRORE

Departamenti: Matematikë – Programi: Shkenca Kompjuterike



**PUNIM SEMINARIK**

**Lënda:** Inteligjenca artificiale

**Tema:** Inteligjenca artificiale dhe siguria kibernetike

**Punuar nga:** Erona Gashi, Benita Mehmeti, Arben Syla

**Mars 2023**

# Abstrakti

Format e ndryshme të inteligjencës artificiale janë duke mundësuar cdo ditë e më shumë inovacione sa i përket sigurisë digjitale. Për nevojën e inteligjencës artificiale në këtë segment po ndikon mes të tjerash rritja e numrit të kërcënimeve nga keqdashësit e njëkohësisht vështirësia e përballimit të këtyre kërcënimeve nga ana e kompanive të targetuara nga këto sulme. Prezenca kaq e madhe e inteligjencës artificiale jo vetëm në fushën e sigurisë kibernetike mirëpo edhe në fusha të tjera, padyshim që sjellë nevojën për identifikimin e dobive dhe mangësive të saj në relacion me fushën ku zbatohet. Një gjë të tillë do të mundohemi të bëjmë në këtë punim, normalisht bazuar në punime shkencore paraprake të cilat kanë trajtuar pak a shumë të njëjtin problem. Origjinaliteti i këtij punimi bazohet në natyrën e tij hulumtuese si një sintezë e opinioneve tona të argumentuara përmes konkludimeve shkencore.

**Fjalët kyce:** artificial intelligence, cybersecurity, data security, threats, cybercrimes

# Hyrje

Kohëve të fundit ekziston një trend universal i investimit në teknologjitë e lidhura me inteligjencën artificiale për ballafaqimin me sfidat e jetës së përditshme, si përpunimit të të dhënave statistikore, aplikimit të saj në mjekësi apo transport, etj.. Hulumtuesit e ndryshëm, tashmë janë duke punuar në zbatimin e IA për zgjidhjen e shumë problemeve sa i përket sistemeve të sigurisë kibernetike në sektorë të ndryshëm [1]. Këto informata na shtyjnë neve drejt dëshirës për t’iu përgjigjur pyetjes se : Cili është impakti i IA në sigurinë kibernetike dhe anasjelltas?

Inteligjenca artificiale është bërë një mjet esencial në sigurinë kibernetike. Ajo mund të përdoret për detektimin dhe parandalimin e sulmeve kibernetike, identifikimin e dobësive, dhe analizimin e të dhënave për kërcënime potenciale.

Analizimi më i hollësishëm i këtyre informatave të mbledhura do të bëhet në vazhdimësi të punimit, me një përmbajtje si vijon. Në kapitullin e tretë flasim për metodologjinë e përdorur për gjetjen, grumbullimin, analizimin e punimeve shkencore dhe mënyrën e ngushtimit të kërkimit. Më pas, në kapitullin e katërt bëhet analiza e këtyre punimeve si nga ana e meta-data, ashtu edhe sa i përket përmbajtjes së tyre. Në kapitullin e gjashtë do të përmendim disa raste studimi të cilat mbështesin konkludimet e nxjerra nga analizimi i punimeve. Së fundi, e përfundojmë punimin duke shkruar konkluzionet e nxjerra nga analizimi i informacioneve të mbledhura si dhe duke sygjeruar implikime.

# Metodologjia

Në librarinë online IEEExplore, kërkojmë arikujt mbi temën duke shtypur së pari fjalët kyce të përmendura te abstrakti, të cilat kanë të bëjnë me inteligjencën artificiale dhe sigurinë e të dhënave në përgjithësi. Pasi rezultatet paraqesin një sasi tejet të madhe të artikujve, librave apo konferencave, e që është i pamundur leximi i të gjithave, na duhet të ngushtojmë kërkimin në dicka më specifike. Së pari caktojmë se artikujt e cilës periudhë dëshirojmë ti shfrytëzojmë, ku për ne ka qenë periudha 2019 – 2022. Pastaj filtrojmë kërkimin nga All Results në Open Access Only, për të pasur qasje vetëm tek artikujt që mund ti lexojmë tërësisht. Për të zvogëluar edhe më shumë numrin e artikujve në të cilët do bazohemi për krijimin e punimit tonë, filtrojmë Publication Topics duke selektuar vetëm temat e ngjashme me atë tonën, si p.sh.: security of data, data privacy, computer crime, artificial intelligence, cryptography, etj.. Një veprim i tillë e ngushton edhe më tepër diapazonin e hulumtimit, duke arritur në një numër artikujsh të mundur për tu lexuar dhe analizuar, për të cilin do flasim në analizën e meta – data në kapitullin e mëposhtëm. Në mënyrë të ngjashme bëhet seleksionimi i artikujve referencues edhe në libraritë e tjera të kërkimit që kemi përdorur, si Google Scholar, Science Direct dhe Springer.

# Analiza

Google Scholar

Më së shumti publikime të artikujve të cilët përmbanin fjalët kyce të caktuara nga ne kishte në vitin 2021, me gjithsej 23 artikuj.

IEEExplore

Viti 2021 ishte viti me më së shumti publikime të artikujve lidhur me temën e këtij punimi, me gjithsej 60 artikuj të cilët përmbanin fjalët kyce të caktuara nga ne.

Një konferencë është mbajtur në vitin 2022 në lidhje me IA dhe sigurinë kibernetike.

Springer

Sa I përket libraris Springer, më së shumti publikime kishte në vitin 2022, ku shihet se të 5 – ta publikimet janë libra, ndryshe nga libraritë e tjera, të cilat fokusin kryesor e kishin në artikuj dhe konferenca.

Science Direct

Në librarinë online Science Direct, më së shumti publikime të lidhura me temën tonë janë bërë gjatë vitit 2020 me gjithsej 6 artikuj.

# Ndikimi I IA në sigurinë kibernetike

Mekanizmat mbrojtës tradicionalisht të bazuar në signatures dhe rules janë duke u ballafaquar me sfida me rritjen e sasisë së informatave të shpërndara në Internet. Në anën tjetër, hakerët kibernetik janë duke u përpjekur të qëndrojnë gjithnjë një hap përpara zbatuesve të ligjit me gjenerimin e teknikave sulmuese të reja, të zgjuara, dhe të ndërlikuara, si dhe me implementimin e teknologjive të avancuara duke përfshirë këtu edhe inteligjencën artificiale për ti bërë sjelljet e tyre kundërshtare edhe më të sofistikuara dhe efikase. Si pasojë, hulumtuesit në sigurinë kibernetike kanë filluar të investigojnë qasjet e bazuara në inteligjencën artificiale siq janë machine learning dhe deep learning, në vend të teknikave tradicionale të sigurisë kibernetike duke përfshirë këtu teorinë e lojrave, rate control, dhe sistemet autonome për të rritur performancën e sistemeve mbrojtëse kibernetike [2].

Për shkak të limitimeve të qasjeve të bazuara në IA, edhe aplikimet e IA në fushën e sigurisë kibernetike janë bërë më problematike. Një gjë tjetër që ndikon në këtë dukuri është edhe vet natyra e modeleve IA, që i përngjason kutisë së zezë, e që kësaj i duhet kushtuar vëmendje e vecantë gjatë integrimit të modeleve IA në domenën e sigurisë kibernetike [3].

Pasi që modelet IA kanë karakteristika black – box, vendimet e gjeneruara nga modelet e bazuara në IA lidhur me sigurinë kibernetike kanë mungesë të arsyeshmërisë (racionales) dhe justifikueshmërisë dhe si pasojë është e vështirë që njerëzit të kuptojnë se si janë prodhuar këto rezultate [4].

Në raste të tilla, mekanizmat kibernetik mbrojtës do të bëheshin tejet të ndjeshme ndaj shkeljeve të informacioneve dhe ndaj kërcënimeve kibernetike të bazuara në IA [5].

# Përdorimi i IA për ballafaqimin me krimet kibernetike

Një nga rreziqet më të mëdha kibernetike në Internetin e sotëm janë malwares, ku implementimi i masave efektive të mbrojtjes ka nevojë për analizën e shpejtë të një vëllimi gjithmonë në rritje të malwares. Teknikat ekzistuese për detektimin e malware mund të kategorizohen në dy tipe kryesore: detektimi statik dhe detektimi dinamik [6].

1. Detektimi statik i malware analizon binarin e malware pa e ekzekutuar kodin. Përkundrazi, mjeti për dekompilim shfrytëzohet për të marrë kodet e dekompiluara dhe për inspektimin e instruksioneve të përfshira në kod. Sidoqoftë, kjo strategji mund të kundërshtohet lehtësisht me përdorimin e metodave si errësimi apo inkorporimi i të metave sintaksore.
2. Detektimi dinamik i malware merret me ekzekutimin e kodit të malware në ndonjë sistem testues ku monitoron sjelljen e malware dhe vet sistemit [7].

Në praktikë, përdorimi i këtyre teknikave tradicionale për detektimin e malware dhe analizimi manual i secilit fajll të malware në një aplikacion merr shumë kohë dhe resurse. Andaj, shumë sisteme për detektimin e malware të bazuara në IA, e sidomos algoritmet deep learning, shfrytëzohen për detektimin e malware me performancë shumë herë më të lartë dhe me shumë më pak resurse [8].

Një studim i rëndësishëm mbi keqpërdorimin e IA flet mbi adoptimin e “personave në rrjet” të quajtur socialbots, të cilët sillen si njerëz. Edhe pse objektivi fillestar I socialbots ishte përkrahja e ndërgjegjësimit dhe bashkëpunimit mes njerëzve, shpesh ata janë përdorur me motive keqdashëse si për shembull në phishing, mashtrime, si dhe infiltrime politike të kampanjave në rrjetet sociale [9].

Seymour dhe Tully treguan se machine learning dhe deep learning mund të përdoren për social engineering; me përdorimin e IA, mesazhe të prodhuara masivisht të cilat përmbanin phishing links mund të shpërndaheshin në rrjetin social Twitter pa ndonjë pengesë. Për shkak se socialbots keqdashës bazohen në sjelljet e mëparshme të përdoruesve të caktuar dhe në profilet publike, detektimi i tyre është bërë një ndër sfidat kryesore të sigurisë kompjuterike. Nga perspektiva e shkencave sociale, këto teknika mund të influencojnë ose ndezin opinionet publike kur socialbots keqdashëse dizajnohen për performimin e ndonjë sulmi politik [10].

Mund të themi se ekzistojne 3 kategori në fushën e kërcënimeve kibernetike: zgjerimi i kërcënimit ekzistues, shfaqja e kërcënimeve të reja, dhe ndryshimi në karakterin tipik të kërcënimeve. Me rritjen e përdorimit të sistemeve IA, kostoja e detyrave që kërkojnë duar punëtore mund të zvogëlohen (për shembull: mass phishing) – ky rast paraqet zgjerimin e kërcënimit ekzistues. Kërcënimet e reja gjithashtu mund të paraqiten për të kryer detyra të cilat janë të parealizueshme nga njerëzit (për shembull: imitimi i zërave të njerëzve të caktuar, kontrollimi i disa dronëve përnjëherë, etj.) [11].

Themi se ka dy tipe të krimeve kibernetike në raport me IA: 1) IA si vegël e krimit dhe 2) IA si target i krimit. Këto janë krime tradicionale në hapësirën kibernetike, mirëpo janë ende kërcënime serioze të sigurisë. Me përdorimin e teknikave IA, keqbërësit mund të kryejnë një krim të ri kibernetik i cili ndoshta deri me ndodhjen e tij konsiderohej si një sulm i parealizueshëm. Andaj, tani diskutojmë teknikat IA që mund të përdoren për kryerjen apo ballafaqimin me krimet kibernetike [12].

1. IA si vegël e krimit

Hulumtime të kaluara tregojnë se IA mund të përdoret për phishing dhe efektiviteti i një gjëje të tillë vecse është vërtetuar. Një nga metodat më të rëndomta të phishing është krijimi i emailave mashtrues duke përdorur profilizim. Profilizimi përmes IA është studiuar aktivisht në fushën e biznesit, ku shembull tipik i tij është reklamimi i targetuar. Sidoqoftë, teknika e përdorur në reklamimin e targetuar, e cila është e bazuar në historinë e mëparshme të blerjeve apo interesave të klientit, mund të jetë e dobishme për sulmuesin. Hulumtuesit e kësaj dukurie e emëruan programin e tillë IA si chatbot. Ata parashikuan që IA do të përmirësoj strategjitë e mashtrimit të klientëve me përdorimin e chatbots keqdashës. Përderisa disa studime sugjerojnë përdorimin e aftësisë komunikuese të IA për të mirën e përbashkët, si për shembull për terapi sociale, për edukim, për diagnoza mjekësore, etj.. Ka poashtu brengosje se një aftësi e tillë mund të ngris nivelin e vjedhjes dhe mashtrimeve. Për aq sa zëri është një nga biometrikët e pazëvendësueshëm në mekanizmat e sigurisë, mund të jetë edhe armë e fortë për sulmuesit.

Lajmet e rrejshme janë një tjetër shembull i krimeve të avancuara, edhe pse lajmet e tilla kanë një histori të gjatë në social engineering, kohëve te fundit ka filluar të vërehet më tepër rrezikshmëria e tyre me ardhjen e shërbimeve të rrjeteve sociale. Në vecanti, lajmet e rrejshme kanë impakt të jashtëzakonshëm në situata politike si propaganda, zgjedhjet, etj.. Me teknikën deepfake, lajmet e rrejshme bëhen edhe më të fuqishme [13].

1. IA si target i krimit

IA mund të kryej detyra të cilat më përpara ishin të pazgjidhura, me shumë pak kosto dhe punë. Duke bërë kopje të sistemeve IA, efekti do mund të jetë i njëjtë sikurse punësimi i shumë analistëve njerëzor. Kjo karakteristikë u jep sulmuesve mundësine për të pasur akses të paautorizuar. Për shembull: autentifikimi përmes fjalëkalimit, teknika më fundamentale e autentifikimit të përdoruesve, do të ishte nën rrezik. Dictionary attack, e konsideruar si një nga mënyrat më efektive për gjetjen e fjalëkalimeve, përdorë fjalë apo fraza të njohura të cilat priten të jenë të përdorura si fjalëkalime. Kur krijohet fjalori, më së shumti përdoret teknika e social engineering e cila merr informacione të viktimës online, si p.sh. datëlindja, numri i telefonit, adresa, etj.. Mbledhja e informacioneve kërkon sasi të konsiderueshme të kohës dhe mundit, por sistemet IA të dizajnuara për të automatizuar social engineering mund të kryejnë detyrën pa mundim. Teknikat për detektimin e automatizuar të dobësive të sistemeve do të ishin instrumente të dobishme për kriminelët. Një potencial të tillë e kanë parashikuar edhe hulumtuesit. Ata demonstruan se përdorimi I CNN (convolutional neural network) dhe tree ensembles krijojnë disa avantazhe ndaj analizës tradicionale statike. Poashtu paraqitën një metodë për zbulimin e dobësive në large – scale. Duke përdorur metodën e propozuar, programet që kanë dobësi mund të identifikoheshin pa pasur nevojë të analizohej kodi i tyre burimor. Krahas këtyre studimeve, metoda të ndryshme për detektimin e dobësive janë hulumtuar aktivisht. Edhe pse ato janë dizajnuar për të mirën publike, keqbërësit mund ti përdorin këto teknika për gjetjen e sistemeve të dobëta. IA bëhet target i krimit varësisht nga niveli i cenueshmërisë së vet sistemit. Një numër i konsiderueshëm artikujsh janë marrë me taksonominë e kërcënimeve të sigurise; sulmet white – box dhe black – box janë modelet tipike të kërcënimeve. Sulmi me njohuri sa i përket bashkësisë së të dhënave, arkitekturës dhe parametrave të sistemeve të targetuara quhet sulm i tipit white – box. Ndërkaq, sulmet e tipit black – box përmbajnë pak për të mos thënë fare informacione rreth strukturës së sistemit të targetuar.

IA po përdoret jashtëzakonisht shumë në sisteme dhe aplikacione të ndryshme. Si pasojë e natyrës së saj duale, ekzistojnë gjithashtu shqetësime se IA mund të bëhet e dëmshme për njerëzit. Për të performuar aktivitete ilegale, keqbërësit mund të përdorin IA djallëzisht ose të sulmojnë sistemet IA duke shfrytëzuar dobësitë e qenësishme të sistemeve të viktimizuara [14].

# Rast studimi – DarkTrace for Cybersecurity

DarkTrace është një kompani e sigurisë kibernetike e cila përdorë algoritme të machine learning për detektimin dhe përgjigjen ndaj sulmeve kibernetike. Platforma është e dizajnuar për të mësuar modele të sjelljes normale të rrjeteve, pajisjeve, dhe përdoruesve të një organizate, dhe për të detektuar anomali të cilat mund të jenë indikatorë të një sulmi kibernetik.

Një nga vetitë e saj më të shquara është aftësia e saj për të detektuar dhe për të i’u përgjigjur kërcënimeve të panjohura – kërcënime këto që nuk janë identifikuar ende nga teknikat tradicionale të detektimit të sulmeve kibernetike. Kjo është vecanërisht e dobishme në detektimin e sulmeve zero – day, ku një sulmues shfrytëzon një dobësi jo të ditur më parë në një produkt softuerik apo harduerik [15].

Një tjetër benefit i DarkTrace që duhet cekur është aftësia e saj për të i’u përgjigjur sulmeve në kohë reale. Kjo mundësohet nga natyra e saj autonome – platforma mund të ndërmarri veprime të menjëhershme për të zbutur një kërcënim pa pasur nevojë për ndërhyrje nga njerëzit.

DarkTrace është implementuar në organizata të ndryshme, duke përfshirë këtu edhe kompaninë multinacionale farmaceutike, AstraZeneca. Platforma ka qenë e dobishme në detektimin e një numri të caktuar të sulmeve të avancuara kundrejt kompanisë, duke përfshirë këtu një sulm ransomware i cili do të mund të shkaktonte dëme të konsiderueshme ndaj veprimtarisë së kompanisë [16].

1. Përfundimi

Nuk është fare i vështirë kuptimi i faktit, pas gjithë informatave të renditura më larte, se teknikat dhe metodat tradicionale të ballafaqimit me krimet kibernetike nuk janë të mjaftueshme për evitimin apo luftimin e tyre. Këtu hyn në punë IA dhe në përgjithësi sistemet IA të cilat po mundësojnë mbrojtjen nga to dhe detektimin më me lehtësi dhe në mënyrë më efektive të sulmeve të sofistikuara kibernetike. Konkluzioni ynë është që IA sa i përket fushës së sigurisë kibernetike ka arritur ndikim të dukshëm në: detektimin dhe parandalimin e kërcënimeve, në monitorimin dhe përgjigjen real – time ndaj sulmeve të mundshme, analizimin parashikues për identifikimin e modeleve të njëjta të sulmeve, etj..

Përmendja e gjithë këtyre avantazheve të përdorimit të IA në këtë fushë, nuk e bën IA “bulletproof”, pasi edhe ajo has në calime dhe ngecje. Një gjë të tillë e mundësojnë të dhënat me të cilat “ushqehen” këto sisteme. Pikërisht, këto të dhëna, sulmuesit mundohen ti ndryshojnë, dhe në njëfar forme mashtrojnë algoritmet IA.

Edhe frika e njerëzve nga zëvendësimi i tyre me sistemet IA përbën një shqetësim madhor, po aq sa është shqetësues fakti se vet sistemet IA janë të dëmshme për ta dhe të mirën publike. Mirëpo, nuk duhet anashkaluar faktin se, sistemet IA janë aq inteligjente sa ne i bëjmë ato, andaj përdorimi i tyre si për të mirë si për të keq varet plotesisht nga qëllimet e krijuesve dhe përdoruesve të tyre.

# Referenca

[1] The impact of Artificial Intelligence on data system security: a literature review [Albérico Rosário and Ricardo Raimundo] [Published: 2 August 2021]

[2] The impact of Artificial Intelligence on data system security: a literature review [Albérico Rosário and Ricardo Raimundo] [Published: 2 August 2021]

[3] The impact of Artificial Intelligence on data system security: a literature review [Albérico Rosário and Ricardo Raimundo] [Published: 2 August 2021]

[4] The impact of Artificial Intelligence on data system security: a literature review [Albérico Rosário and Ricardo Raimundo] [Published: 2 August 2021]

[5] The impact of Artificial Intelligence on data system security: a literature review [Albérico Rosário and Ricardo Raimundo] [Published: 2 August 2021]

[6] A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges [Published: 12 July 2021] [Authors: Duan Dai & Sahar Boroomand]

[7] Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues [Authors: Doowon Jeong] [Published:7 October 2020]

[8] Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues [Authors: Doowon Jeong] [Published:7 October 2020]

[9] Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues [Authors: Doowon Jeong] [Published:7 October 2020]

[10] Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues [Authors: Doowon Jeong] [Published:7 October 2020]

[11] The impact of Artificial Intelligence on data system security: a literature review [Albérico Rosário and Ricardo Raimundo] [Published: 2 August 2021]

[12] Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues [Authors: Doowon Jeong] [Published:7 October 2020]

[13] Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues [Authors: Doowon Jeong] [Published:7 October 2020]

[14] Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues [Authors: Doowon Jeong] [Published:7 October 2020]

[15] <https://darktrace.com/blog>

[16] <https://darktrace.com/blog>

# Përmbajtja

[1. Abstrakti 2](#_Toc130515633)

[2. Hyrje 2](#_Toc130515634)

[3. Metodologjia 3](#_Toc130515635)

[4. Analiza 3](#_Toc130515636)

[5. Ndikimi I IA në sigurinë kibernetike 4](#_Toc130515637)

[6. Përdorimi i IA për ballafaqimin me krimet kibernetike 5](#_Toc130515638)

[7. Rast studimi – DarkTrace for Cybersecurity 7](#_Toc130515639)

[8. Referenca 8](#_Toc130515640)

[9. Përmbajtja 10](#_Toc130515641)