

Tema	Podtema	Podtema	Literatura
Uvod i osnovni pojmovi			
APT			
	Detection		
			Ghafir, Ibrahim, and Vaclav Prenosil. "Advanced persistent threat attack detection: an overview." Int J Adv Comput Netw Secur 4.4 (2014): 5054.
Kibernetički kriminal			
	Općenito		
			Dehghanniri, Hashem, and Hervé Borrión. "Crime scripting: A systematic review." European Journal of Criminology 18.4 (2021): 504-525.
			Ho, Heemeng, Ryan Ko, and Lorraine Mazerolle. "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review." Computers & Security 115 (2022): 102611.
			Junger, Marianne, Victoria Wang, and Marleen Schlömer. "Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits." Crime science 9.1 (2020): 13.
			Ficara, Annamaria, et al. "Covert network construction, disruption, and resilience: A survey." Mathematics 10.16 (2022): 2929.
			Chainey, Spencer P., and Arantza Alonso Berbotto. "A structured methodical process for populating a crime script of organized crime activity using OSINT." Trends in Organized Crime 25.3 (2022): 272-300.
			Paquet-Clouston, Masarah, and Sebastián García. "On the motivations and challenges of affiliates involved in cybercrime." Trends in Organized Crime (2022): 1-30.
			Collier, Ben, and Alice Hutchings. "Cybercrime: a social ecology." The oxford handbook of criminology (2023): 456-478.
			Cárdenas, Alvaro, et al. "An economic map of cybercrime." TPRC, 2009.
			McGuire, Michael. "It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime." The human factor of cybercrime. Routledge, 2019. 3-28.
			Lusthaus, Jonathan, et al. "Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions." Trends in Organized Crime (2023): 1-24.

	History/Evolution		
			Grabosky, Peter. "The evolution of cybercrime, 2006–2016." Cybercrime through an interdisciplinary lens. Routledge, 2016. 29-50.
			Dupont, Benoît, Francis Fortin, and Rutger Leukfeldt. "Broadening our understanding of cybercrime and its evolution." Journal of Crime and Justice (2024): 1-5.
	Crime Scripts		
			Cornish, Derek B. "The procedural analysis of offending and its relevance for situational prevention." Crime prevention studies 3.1 (1994): 151-196.
	Kriptoalute		
			Deuber, Dominic, Viktoria Ronge, and Christian Rückert. "Sok: Assumptions underlying cryptocurrency deanonymizations." Proceedings on Privacy Enhancing Technologies 3 (2022): 670-691.
			Gomez, Gibran, Kevin van Liebergen, and Juan Caballero. "Cybercrime bitcoin revenue estimations: Quantifying the impact of methodology and coverage." Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023.
			Silfversten, Erik, et al. Exploring the use of Zcash cryptocurrency for illicit or criminal purposes. Santa Monica, CA, USA: RAND, 2020.
			Sanz-Bas, David, et al. "Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain." Laws 10.3 (2021): 57.
			Dawes Centre for Future Crime at UCL, Cryptocurrencies and future crime, Policy brief, February 2021.
			Butler, Simon. "Criminal use of cryptocurrencies: a great new threat or is cash still king?." Journal of Cyber Policy 4.3 (2019): 326-345.
			Guidara, Achraf. "Cryptocurrency and money laundering: A literature review." Corporate Law & Governance Review 4.2 (2022): 36-41.

			Taleby Ahvanooy, Milad, et al. "Do dark web and cryptocurrencies empower cybercriminals?." International Conference on Digital Forensics and Cyber Crime. Cham: Springer International Publishing, 2021.
			Hendrickson, Joshua R., and William J. Luther. "Cash, crime, and cryptocurrencies." The Quarterly Review of Economics and Finance 85 (2022): 200-207.
			Kethineni, Sessa, and Ying Cao. "The rise in popularity of cryptocurrency and associated criminal activity." International Criminal Justice Review 30.3 (2020): 325-344.
			Trozze, Arianna, et al. "Cryptocurrencies and future financial crime." Crime Science 11 (2022): 1-35.
			Saiedi, Ed, Anders Broström, and Felipe Ruiz. "Global drivers of cryptocurrency infrastructure adoption." Small Business Economics 57.1 (2021): 353-406.
			Auer, Raphael, and David Tercero-Lucas. "Distrust or speculation? The socioeconomic drivers of US cryptocurrency investments." Journal of Financial Stability 62 (2022): 101066.
			Gomez, Gibran, Kevin van Liebergen, and Juan Caballero. "Cybercrime bitcoin revenue estimations: Quantifying the impact of methodology and coverage." Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023.
			Reddy, Eveshnie, and Anthony Minnaar. "Cryptocurrency: A tool and target for cybercrime." Acta Criminologica: African Journal of Criminology & Victimology 31.3 (2018): 71-92.
			Pritchett, Jordan. "Cryptocurrency: An Overview." Banking LJ 134 (2017): 547.
			Farell, Ryan. "An analysis of the cryptocurrency industry." Wharton Research Scholars 130 (2015): 1-23.
			Badawi, Emad, and Guy-Vincent Jourdan. "Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review." IEEE Access 8 (2020): 200021-200037.
			Barnes, Paul. "Crypto currency and its susceptibility to speculative bubbles, manipulation, scams and fraud." Journal of Advanced Studies in Finance (JASF) 9.2 (18) (2018): 60-77.
			Lisi, Andrea. "The involvement of cryptocurrency in online crimes." (2021).
			Bitcoin and Cryptocurrencies Law Enforcement Investigative Guide
			Pernice, Ingolf GA, and Brett Scott. "Cryptocurrency." Internet Policy Review 10.2 (2021): 1-10.
			Report of attorney general's cyber digital task force, Cryptocurrency enforcement framework , U.S. Department of Justice, October 2020.
			Chainalysis, The 2020 State of Crypto Crime , January 2020.
			Maese, Vivian A., et al. "Cryptocurrency: A primer." Banking LJ 133 (2016): 468.

		Pranje novca	
			Robert Hart, Tether Cryptocurrency Becoming 'Preferred Choice' Among Money Launderers And Scammers, UN Warns , Jan 15, 2024, Forbes. https://www.forbes.com/sites/roberthart/2024/01/15/tether-cryptocurrency-becoming-preferred-choice-among-money-launderers-and-scammers-un-warns/
			Kolachala, Kartick, et al. "SoK: money laundering in cryptocurrencies." Proceedings of the 16th International Conference on Availability, Reliability and Security. 2021.
			Möser, Malte, Rainer Böhme, and Dominic Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem." 2013 APWG eCrime researchers summit. Ieee, 2013.
			See, Kenneth. "The Satoshi laundromat: a review on the money laundering open door of Bitcoin mixers." Journal of Financial Crime 31.2 (2023): 416-426.
			Nazzari, Mirko. "From payday to payoff: Exploring the money laundering strategies of cybercriminals." Trends in Organized Crime (2023): 1-18.
			Custers, Bart, Jan-Jaap Oerlemans, and Ronald Pool. "Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies." European Journal of Crime, Criminal Law and Criminal Justice 28.2 (2020): 121-152.
		Cryptjacking	
			Bijmans, Hugo LJ, Tim M. Booij, and Christian Doerr. "Just the tip of the iceberg: Internet-scale exploitation of routers for cryptojacking." Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019.
			Varlioglu, Said, et al. "Is cryptojacking dead after coinhive shutdown?." 2020 3rd International Conference on Information and Computer Technologies (ICICT). IEEE, 2020.
			Tekiner, Ege, et al. "SoK: cryptojacking malware." 2021 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2021.
			Bijmans, Hugo LJ, Tim M. Booij, and Christian Doerr. "Inadvertently making cyber criminals rich: A comprehensive study of cryptojacking campaigns at internet scale." 28th USENIX Security Symposium (USENIX Security 19). 2019.

		Scams	
			Bartoletti, Massimo, et al. " Cryptocurrency scams: analysis and perspectives. " Ieee Access 9 (2021): 148353-148373.
	Infrastruktura		
			Collier, Benjamin, et al. " Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. " (2020).
	Kriminalne skupine		
		Conti	
			Alzahrani, Saleh, Yang Xiao, and Sultan Asiri. "Conti Ransomware Development Evaluation." Proceedings of the 2023 ACM Southeast Conference. 2023.
			Alzahrani, Saleh, Yang Xiao, and Sultan Asiri. "Conti Ransomware Development Evaluation." Proceedings of the 2023 ACM Southeast Conference. 2023.
			Alzahrani, Saleh, Yang Xiao, and Wei Sun. "An analysis of conti ransomware leaked source codes." IEEE Access 10 (2022): 100178-100193.
			Cymru, Team. "Analyzing ransomware negotiations with CONTI: An in-depth analysis." (2022).
			Gray, Ian W., et al. "Money Over Morals: A Business Analysis of Conti Ransomware." 2022 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2022.
			Ruellan, Estelle, Masarah Paquet-Clouston, and Sebastian Garcia. "Conti Inc.: Understanding the Internal Discussions of a large Ransomware-as-a-Service Operator with Machine Learning." arXiv preprint arXiv:2308.16061 (2023).
			Stolk, Valentijn. "You Win Some You Ransom: Reconstructing the ransomware ecosystem using ground truth communication data of the Conti ransomware gang." (2022).
			Williams, Kameron A. Conti Ransomware Gang: An Analysis of the Group's Motives and Methods. Diss. Utica University, 2022.
		LockBit	
			Understanding ransomware threat actors: LockBit, CISA, June 14, 2023.
		Akira	
			#StopRansomware: Akira Ransomware, April 18, 2024

		Gozi	
			Lusthaus, Jonathan, Jaap Van Oss, and Philipp Amann. "The Gozi group: A criminal firm in cyberspace?." European Journal of Criminology 20.5 (2023): 1701-1718.
			Jackson, Don. "Gozi trojan." Retrieved August 13 (2007): 2013.
	Darknet		
			Fachkha, Claude, and Mourad Debbabi. "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization." IEEE Communications Surveys & Tutorials 18.2 (2015): 1197-1227.
			Ball, Matthew, and Roderic Broadhurst. "Data capture and analysis of darknet markets." Available at SSRN 3344936 (2021).
			Lacson, Wesley, and Beata Jones. "The 21st century darknet market: lessons from the fall of Silk Road." International Journal of Cyber Criminology 10.1 (2016): 40.
			Wang, Meiqi, et al. "Who are in the darknet? Measurement and analysis of darknet person attributes." 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, 2018.
			Rudesill, Dakota S., James Caverlee, and Daniel Sui. "The deep web and the darknet: A look inside the internet's massive black box." Woodrow Wilson International Center for Scholars, STIP 3 (2015).
			Drugs and the darknet: Perspectives for enforcement, research and policy , Europol, 2017
			Broadhurst, Roderic, et al. "Malware trends on 'darknet'crypto-markets: Research review." Available at SSRN 3226758 (2018).
			Bayoumy, Yara Fareed Fahmy, Per Håkon Meland, and Guttorm Sindre. "A netnographic study on the dark net ecosystem for ransomware." 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, 2018.
			Darknet markets ecosystem: Lifetimes and reasons for closure of over 100 global darknet markets offering drugs, sorted by date , Europol, 2018, poster
	Darkweb		
			Kumar, Aditi, and Eric Rosenbach. "The truth about the dark web." Finance and Development 56.3 (2019): 22-25.
			Schäfer, Matthias, et al. "BlackWidow: Monitoring the dark web for cyber security information." 2019 11th International Conference on Cyber Conflict (CyCon). Vol. 900. IEEE, 2019.

			Nazah, Saiba, et al. " Evolution of dark web threat analysis and detection: A systematic approach. " Ieee Access 8 (2020): 171796-171819.
			Finklea, K. " Dark Web ", Congressional Research Service, March 10, 2017.
			Saleem, Javeriah, Rafiqul Islam, and Muhammad Ashad Kabir. "The anonymity of the dark web: A survey." IEEE Access 10 (2022): 33628-33660.
			Gupta, Abhineet, Sean B. Maynard, and Atif Ahmad. " The dark web phenomenon: A review and research agenda. " arXiv preprint arXiv:2104.07138 (2021).
			Liggett, Roberta, et al. "The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets." The Palgrave handbook of international cybercrime and cyberdeviance (2020): 91-116.
			Haslebach, Andreas, Jeremiah Onalapo, and Gianluca Stringhini. "All your cards are belong to us: Understanding online carding forums." 2017 APWG symposium on electronic crime research (eCrime). IEEE, 2017.
			Zhao, Ziming, et al. "Mules, seals, and attacking tools: Analyzing 12 online marketplaces." IEEE Security & Privacy 14.3 (2016): 32-43.
	Ad Networks		
			Richet, Jean-Loup. "How cybercriminal communities grow and change: An investigation of ad-fraud communities." Technological Forecasting and Social Change 174 (2022): 121282.
			Stone-Gross, Brett, et al. "Understanding fraudulent activities in online ad exchanges." Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. 2011.
			Zarras, Apostolis, et al. "The dark alleys of madison avenue: Understanding malicious advertisements." Proceedings of the 2014 conference on internet measurement conference. 2014.
			Chen, Gong, et al. "In-depth survey of digital advertising technologies." IEEE Communications Surveys & Tutorials 18.3 (2016): 2124-2148.
			Pooranian, Zahra, et al. "Online advertising security: Issues, taxonomy, and future directions." IEEE Communications Surveys & Tutorials 23.4 (2021): 2494-2524.
	Blackhat SEO		

			Leontiadis, Nektarios, Tyler Moore, and Nicolas Christin. "A nearly four-year longitudinal study of search-engine poisoning." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.
			Liao, Xiaojing, et al. "Characterizing long-tail SEO spam on cloud web hosting services." Proceedings of the 25th International Conference on World Wide Web. 2016.
			Huang, Danny Yuxing, et al. "Pinning down abuse on google maps." Proceedings of the 26th International Conference on World Wide Web. 2017.
			Yang, Ronghai, et al. "Scalable detection of promotional website defacements in black hat {SEO} campaigns." 30th USENIX Security Symposium (USENIX Security 21). 2021.
			Gudivada, Venkat N., Dhana Rao, and Jordan Paris. "Understanding search-engine optimization." Computer 48.10 (2015): 43-52.
			Wang, David Y., Stefan Savage, and Geoffrey M. Voelker. "Juice: A Longitudinal Study of an SEO Botnet." NDSS. 2013.
			Wang, Yi-Min, and Ming Ma. "Detecting stealth web pages that use click-through cloaking." Microsoft Research Technical Report, MSR-TR (2006).
			Howard, Fraser, and Onur Komili. "Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware." Sophos Technical Papers (2010): 1-15.
			Yang, Ronghai, et al. "Scalable detection of promotional website defacements in black hat {SEO} campaigns." 30th USENIX Security Symposium (USENIX Security 21). 2021.
			Du, Kun, et al. "The {Ever-Changing} labyrinth: A {Large-Scale} analysis of wildcard {DNS} powered blackhat {SEO}." 25th USENIX Security Symposium (USENIX Security 16). 2016.
	Crime-as-a-service		
			Šembera, Vít, et al. "Cybercrime specialization: An exposé of a malicious Android Obfuscation-as-a-Service." 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2021.
			Manky, Derek. "Cybercrime as a service: a very modern business." Computer Fraud & Security 2013.6 (2013): 9-13.
			Samani, Raj, and Francois Paget. "Cybercrime exposed: Cybercrime-as-a-service." McAfee, Inc (2013).

			Sood, Aditya K., and Richard J. Enbody. "Crimeware-as-a-service—a survey of commoditized crimeware in the underground market." International journal of critical infrastructure protection 6.1 (2013): 28-38.
		Ransomware-as-a-service	
			https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas
			Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. "The Ransomware-as-a-Service economy within the darknet." Computers & Security 92 (2020): 101762.
		Access-as-a-service	
			https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/
	Botnets		
			Bailey, Michael, et al. "A survey of botnet technology and defenses." 2009 Cybersecurity Applications & Technology Conference for Homeland Security. IEEE, 2009.
			Bottazzi, Giovanni, and Gianluigi Me. "The botnet revenue model." Proceedings of the 7th International Conference on Security of Information and Networks. 2014.
			Georgoulas, Dimitrios, et al. "Botnet business models, takedown attempts, and the darkweb market: A survey." ACM Computing Surveys 55.11 (2023): 1-39.
			Mahmoud, Muhammad, Manjinder Nir, and Ashraf Matrawy. "A survey on botnet architectures, detection and defences." Int. J. Netw. Secur. 17.3 (2015): 264-281.
			Putman, C. G. J., and Lambert JM Nieuwenhuis. "Business model of a botnet." 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). IEEE, 2018.
			Rodríguez-Gómez, Rafael A., Gabriel Maciá-Fernández, and Pedro García-Teodoro. "Survey and taxonomy of botnet research through life-cycle." ACM Computing Surveys (CSUR) 45.4 (2013): 1-33.
			Stone-Gross, Brett, et al. "Analysis of a botnet takeover." IEEE Security & Privacy 9.1 (2010): 64-72.

			Stone-Gross, Brett, et al. " Your botnet is my botnet: analysis of a botnet takeover. " Proceedings of the 16th ACM conference on Computer and communications security. 2009.
			Zeidanloo, Hossein Rouhani, and Azizah Abdul Manaf. " Botnet command and control mechanisms. " 2009 second international conference on computer and electrical engineering. Vol. 1. IEEE, 2009.
			Musotto, Roberto, and David S. Wall. " More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. " Trends in Organized Crime (2020): 1-19.
			Stringhini, Gianluca, et al. "The harvester, the botmaster, and the spammer: On the relations between the different actors in the spam landscape." Proceedings of the 9th ACM symposium on Information, computer and communications security. 2014.
			Bleaken, Dan. "Botwars: the fight against criminal cyber networks." Computer Fraud & Security 2010.5 (2010): 17-19.
		Mirai	
			Antonakakis, Manos, et al. " Understanding the mirai botnet. " 26th USENIX security symposium (USENIX Security 17). 2017.
		Zeus	
			Binsalleeh, Hamad, et al. " On the analysis of the zeus botnet crimeware toolkit. " 2010 eighth international conference on privacy, security and trust. IEEE, 2010.
		Hajime	
			Herwig, Stephen, et al. " Measurement and analysis of Hajime, a peer-to-peer IoT botnet. " Network and Distributed Systems Security (NDSS) Symposium. 2019.
	Ransomware		
			Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. " Your files have been encrypted: A crime script analysis of ransomware attacks. " Trends in Organized Crime (2023): 1-27.
			Cable, Jack, Ian W. Gray, and Damon McCoy. " Showing the Receipts: Understanding the Modern Ransomware Ecosystem. " arXiv preprint arXiv:2408.15420 (2024).
			Kshetri, Nir, and Jeffrey Voas. " Do crypto-currencies fuel ransomware?. " IT professional 19.5 (2017): 11-15.

Špijunaža			
	Industrijska špijunaža		
			Hou, Tie, and Victoria Wang. "Industrial espionage—A systematic literature review (SLR)." computers & security 98 (2020): 102019.
	Špijunski software		
		Pegasus	
			Rudie, J. D., et al. "Technical analysis of the nso group's pegasus spyware." 2021 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2021.
			Chourasiya, Sidhant, et al. "Pegasus spyware: A vulnerable behaviour-based attack system." 2023 2nd international conference on edge computing and applications (ICECAA). IEEE, 2023.
			Scott-Railton, John, et al. Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware. 2017.
			Chawla, Ajay. "Pegasus Spyware—'A Privacy Killer'." Available at SSRN 3890657 (2021).
			Marczak, Bill, et al. Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries. 2018.
Cenzura			
			A Survey of Worldwide Censorship Techniques J. L. Hall, M. D. Aaron, A. Andersdotter, B. Jones, N. Feamster, M. Knodel (DOI: 10.17487/RFC9505)
Privatnost			
			Report from the Internet Privacy Workshop A. Cooper [January 2012] (DOI: 10.17487/RFC6462)
	Web		
			Lerner, Ada, et al. "Internet jones and the raiders of the lost trackers: An archaeological study of web tracking from 1996 to 2016." 25th USENIX Security Symposium (USENIX Security 16). 2016.
Društvene mreže			
	Scamming		
			Li, Xigao, Amir Rahmati, and Nick Nikiforakis. "Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms." Proceedings 2024 Network and Distributed System Security Symposium. 2024.
			Liu, Enze, et al. "Give and Take: An End-To-End Investigation of Giveaway Scam Conversion Rates." arXiv preprint arXiv:2405.09757 (2024).

Anonimnost			
	Tor		
			Miller, Matthew, Joshua Stroschein, and Ashley Podhradsky. "Reverse Engineering a Nit That Unmasks Tor Users." (2016).
	Kinesko djelovanje		
			China's Hacker Network: What to Know https://www.nytimes.com/2024/02/22/business/china-hack-leak-isoon.html
			Massive leak shows Chinese firm hacked foreign govts, activists: analysts https://www.france24.com/en/live-news/20240222-massive-leak-shows-chinese-firm-hacked-foreign-govts-activists-analysts
			Giant leak reveals Chinese infosec vendor I-Soon is one of Beijing's cyber-attackers for hire https://www.theregister.com/2024/02/22/i_soon_china_infosec_leak/
			Leaked Files Show the Secret World of China's Hackers for Hire https://www.nytimes.com/2024/02/22/business/china-leaked-files.html
			A first analysis of the i-Soon data leak https://www.malwarebytes.com/blog/news/2024/02/a-first-analysis-of-the-i-soon-data-leak

			Massive Data Leak Exposes Sensitive Conversation Logs from Chinese Ministry of Public Security https://thecyberexpress.com/chinese-ministry-of-public-security-breach/
	Rusko djelovanje		https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia
			https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia
			https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
			https://cyberpeaceinstitute.org/news/story-of-the-escalation-of-threat-actors/
			Why the Russian Government Turns a Blind Eye to Cybercriminals https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499
		Internet Research Agency	
			DiResta, Renée, et al. "The Tactics and Tropes of the Internet Research Agency, New Knowledge Report prepared for the United States Senate Select Committee on Russian Interference in the 2016 Election." (2018).
Obavještajni rad u kibernetičkom prostoru			
			Gordon, Lawrence A., et al. "Empirical evidence on disclosing cyber breaches in an 8-K report: Initial exploratory evidence." Journal of Accounting and Public Policy 46 (2024): 107226.
			Dykstra, Josiah, et al. "Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments." Journal of Cybersecurity 9.1 (2023): tyad003.
			Borg, Lars C. "Improving intelligence analysis: Harnessing intuition and reducing biases by means of structured methodology." The International Journal of Intelligence, Security, and Public Affairs 19.1 (2017): 2-22.
			Shin, Bongsik, and Paul Benjamin Lowry. "A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished." Computers & Security 92 (2020): 101761.

			Ainslie, Scott, et al. "Cyber-threat intelligence for security decision-making: A review and research agenda for practice." Computers & Security 132 (2023): 103352.
			Peter C. Oleson (Ed), AFIO's Guide to the Study of Intelligence , Association of Former Intelligence Officers, 2016.
			Samtani, Sagar, et al. "Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence." Journal of Management Information Systems 34.4 (2017): 1023-1053.
			Kayode-Ajala, Olaolu. "Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption." Applied Research in Artificial Intelligence and Cloud Computing 6.8 (2023): 1-21.
			Major Mark J. Kneis II, The Surprise Hypothesis
			McCall Jr, Grover C. Exploring a Cyber Threat Intelligence (CTI) Approach in the Thwarting of Adversary Attacks: An Exploratory Case Study. Diss. Northcentral University, 2022.
			Shin, Bongsik, and Paul Benjamin Lowry. "A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished." Computers & Security 92 (2020): 101761.
		STIX	
		TAAXI	
		DISARM	
		The Vocabulary for Event Recording and Incident Sharing (VERIS)	https://verisframework.org/
	Analitičke metode		
			Chang, Welton, et al. "Restructuring structured analytic techniques in intelligence." Intelligence and National Security 33.3 (2018): 337-356.
			Beebe, Sarah Miller, and Randolph H. Pherson. Cases in intelligence analysis: Structured analytic techniques in action. CQ Press, 2014.
			Primer, A. Tradecraft. "Structured analytic techniques for improving intelligence analysis." CIA Center for the study of intelligence (2009).
			Coulthart, Stephen. "Why do analysts use structured analytic techniques? An in depth study of an American intelligence agency." Intelligence and National Security 31.7 (2016): 933-948.
			Coulthart, Stephen J. "An evidence-based evaluation of 12 core structured analytic techniques." International Journal of Intelligence and CounterIntelligence 30.2 (2017): 368-391.
			Marchand, Jérôme. "STRUCTURED ANALYTIC TECHNIQUES FOR INTELLIGENCE ANALYSIS." (2012): 684-686.

			Miksa, Rad. "Assessment tabling: an integrated structured analytic technique for improved intelligence analysis and reasoning visualisation." <i>Intelligence and National Security</i> (2024): 1-15.
			Ard, Michael J. "Structured Analytic Techniques: A Pragmatic Approach." <i>International Journal of Intelligence and CounterIntelligence</i> 37.2 (2024): 617-633.
			Latus, Matthew. <i>An Examination of Structured Analytic Techniques for the Improvement of Cybersecurity Intelligence Analysis</i> . MS thesis. Utica College, 2017.
			Pherson, Randolph H., and Richards J. Heuer Jr. Structured analytic techniques for intelligence analysis . Cq Press, 2020.
			Oosthoek, Kris, and Christian Doerr. "Cyber threat intelligence: A product without a process?." <i>International Journal of Intelligence and CounterIntelligence</i> 34.2 (2021): 300-315.
			Friedman, Jeffrey A., and Richard Zeckhauser. "Assessing uncertainty in intelligence." <i>Intelligence and National Security</i> 27.6 (2012): 824-847.
			Seker, Sadi Evren. "Computerized argument Delphi technique." <i>IEEE Access</i> 3 (2015): 368-380.
		Analysis of Competing Hypotheses	
			RaliaQuest, WannaCry: An Analysis of Competing Hypotheses, 18 May 2017. https://www.reliaquest.com/blog/wannacry-an-analysis-of-competing...
			Pope, Simon, and Audun Jøsang. " Analysis of competing hypotheses using subjective logic ." <i>Proceedings of the 10th International Command and Control Research and Technology Symposium (ICCRTS)</i> . 2005.
			RaliaQuest, REvil: Analysis of Competing Hypotheses, 28 July 2021. https://www.reliaquest.com/blog/revil-analysis-of-competing-hypotheses/
			Wilcox, John, and David R. Mandel. " Critical review of the analysis of competing hypotheses technique: lessons for the intelligence community ." <i>Intelligence and National Security</i> (2024): 1-22.
			RaliaQuest, The Devil, the Details, and the Analysis of Competing Hypothesis, 13. February 2020. https://www.reliaquest.com/blog/the-devil-the-details-and-the-analysis-of-competing-hypothesis/

			Heuer, J. R., et al. "ACH0: A Tool for Analyzing Competing Hypotheses." PARC, Palo Alto, CA (2004).
			Murukannaiah, Pradeep K., et al. "Resolving goal conflicts via argumentation-based analysis of competing hypotheses." 2015 IEEE 23rd International Requirements Engineering Conference (RE). IEEE, 2015.
	Izgradnja tima za CTI		
	Kritičko razmišljanje		
	Industrijski standardi		
	Obavještajni ciklus		
	Policija i obavještani rad		
	Vjerojatnost		
	Izvješća		
	Istraživanje		
Zloćudni kod (Malware)			Song, Linhai, et al. "Learning from big malwares." Proceedings of the 7th ACM SIGOPS Asia-Pacific Workshop on Systems. 2016.
			Rokon, Md Omar Faruk, et al. "{SourceFinder}: Finding malware {Source-Code} from publicly available repositories in {GitHub}." 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020). 2020.

	Kompleksnost		
			Calleja, Alejandro, Juan Tapiador, and Juan Caballero. "A look into 30 years of malware development from a software metrics perspective." Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19. Springer International Publishing, 2016.
			Lindorfer, Martina, et al. "Lines of malicious code: Insights into the malicious software industry." Proceedings of the 28th annual computer security applications conference. 2012.
	Povijest		
			Milošević, Nikola. "History of malware." arXiv preprint arXiv:1302.5392 (2013).
	Reverziranje		
			Muralidharan, Trivikram, et al. "File Packing from the Malware Perspective: Techniques, Analysis Approaches, and Directions for Enhancements." ACM Computing Surveys 55.5 (2022): 1-45.
			Banescu, Sebastian, and Alexander Pretschner. "A tutorial on software obfuscation." Advances in Computers 108 (2018): 283-353.
			Beaman, Craig, et al. "Ransomware: Recent advances, analysis, challenges and future research directions." Computers & security 111 (2021): 102490.
		Android	
			https://github.com/strazzere/android-unpacker
	Antivirusna podrška		
Threat Hunting			
			Nour, Boubakr, Makan Pourzandi, and Mourad Debbabi. "A survey on threat hunting in enterprise networks." IEEE Communications Surveys & Tutorials (2023).

			Mahboubi, Arash, et al. "Evolving techniques in cyber threat hunting: A systematic review." Journal of Network and Computer Applications (2024): 104004.
			Strom, Blake E., et al. "Finding cyber threats with ATT&CK-based analytics." The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202 (2017).
			Jadidi, Zahra, and Yi Lu. "A threat hunting framework for industrial control systems." IEEE Access 9 (2021): 164118-164130.
			Ajmal, Abdul Basit, et al. "Offensive security: Towards proactive threat hunting via adversary emulation." IEEE Access 9 (2021): 126023-126033.
Nesortirano			
			Yamagishi, Rei, Shota Fujii, and Tatsuya Mori. "Users Feel Guilty: Measurement of Illegal Software Installation Guide Videos on YouTube for Malware Distribution." arXiv preprint arXiv:2407.16132 (2024).
			Acharya, Bhupendra, et al. "Conning the crypto conman: End-to-end analysis of cryptocurrency-based technical support scams." 2024 IEEE Symposium on Security and Privacy (SP). IEEE, 2024.
			Miramirkhani, Najmeh, Oleksii Starov, and Nick Nikiforakis. "Dial one for scam: Analyzing and detecting technical support scams." 22nd Annual Network and Distributed System Security Symposium (NDSS). Vol. 16. 2016.
			Alzghoul, Jamil R., Emad E. Abdallah, and Abdel-hafiz S. Al-khawaldeh. "Fraud in Online Classified Ads: Strategies, Risks, and Detection Methods: A Survey." Journal of Applied Security Research 19.1 (2024): 45-69.
			Franco, Javier, et al. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." IEEE Communications Surveys & Tutorials 23.4 (2021): 2351-2383.
			Jung, Bo Ra, Kyung-Shick Choi, and Claire Seungeun Lee. "Dynamics of dark web financial marketplaces: An exploratory study of underground fraud and scam business." International Journal of Cybersecurity Intelligence & Cybercrime 5.2 (2022): 4-24.
			Dudani, Sahil, et al. "The current state of cryptocurrency forensics." Forensic Science International: Digital Investigation 46 (2023): 301576.
			Raikwar, Mayank, Danilo Gligoroski, and Katina Kravevska. "SoK of used cryptography in blockchain." IEEE Access 7 (2019): 148550-148575.

			Vandepeer, Charles. Rethinking threat: intelligence analysis, intentions, capabilities, and the challenge of non-state actors. Diss. 2011.
--	--	--	--