

Original Scientific Paper/Original naučni rad  
Paper Submitted/Rad primljen: 31.12.2025.  
Paper Accepted/Rad prihvaćen: 10.01.2026.  
DOI: 10.5937/SJEM2601011M

UDC/UDK: 004.8:355.45

## Значај вештачке интелигенције у заштити националне безбедности

Dejan Milenković<sup>1</sup>, Katarina Štrbac<sup>2</sup>, Jelena Mitić<sup>3</sup>

<sup>1</sup> Ministry of Interior, [dejanmilenkovic1979@yahoo.com](mailto:dejanmilenkovic1979@yahoo.com),

<sup>2</sup> School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia, [katarina.strbac@fim.rs](mailto:katarina.strbac@fim.rs),

<sup>3</sup> School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia, [jelena.mitic@fim.rs](mailto:jelena.mitic@fim.rs),

**Апстракт:** Вештачка интелигенција (ВИ) представља један од кључних технолошких иновативних алата у домену националне безбедности, омогућавајући значајна унапређења у обради података, анализи безбедносних претњи и подршци процесу доношења одлука. Њена примена у безбедносним структурама Републике Србије потенцијално доприноси већој ефикасности и прецизности у превенцији и откривању терористичких активности, организованог криминала, сајбер напада и других облика угрожавања безбедности. Посебан значај добија у контексту анализе великих података (big data), где омогућава идентификацију обрасца и индикатора потенцијалних претњи, чиме се омогућава проактиван и благовремен одговор. У оквиру специјалних истражних мера – попут електронског надзора, тајног праћења, видео-надзора, симулираних трансакција, контролисаних испорука и тајних истрага – примена ВИ може значајно повећати ефикасност и смањити оперативни ризик. Рад анализира кључне области примене ВИ у контексту националне безбедности, технолошке и институционалне изазове у њеној имплементацији, као и релевантне етичке и правне аспекте. Циљ рада је да се укаже на значај интеграције савремених ВИ решења у постојеће безбедносне системе и да се допринесе стратешком планирању развоја националне безбедности у дигиталном добу.

**Кључне речи:** национална безбедност, вештачка интелигенција, специјалне истражне мере, организовани криминал, тероризам, сајбер-безбедност.

## The Significance of Artificial Intelligence in National Security Protection

**Abstract:** Artificial Intelligence (AI) is a key technological tool in national security, enabling significant improvements in data processing, threat analysis, and decision support. Its application to the security structures of the Republic of Serbia potentially contributes to greater efficiency and precision in preventing and detecting terrorist activities, organised crime, cyber-attacks, and other security threats. It gains particular significance in big data analysis, where it enables the identification of patterns and indicators of potential threats, thereby facilitating a proactive, timely response. Within special investigative measures – such as electronic surveillance, covert tracking, video surveillance, simulated transactions, controlled deliveries, and clandestine investigations – the application of AI can significantly increase efficiency and reduce operational risk. The paper analyses key areas of AI application in the context of national security, the technological and institutional challenges in its implementation, and the relevant ethical and legal aspects. The work aims to highlight the importance of integrating contemporary AI solutions into existing security systems and to contribute to the strategic planning of national security development in the digital age.

**Keywords:** national security, artificial intelligence, special investigative measures, organised crime, terrorism, cybersecurity.

### 1. Introduction

The national security of the Republic of Serbia faces a growing number of complex, multidimensional threats, including terrorism, organised crime, cyberattacks, and hybrid security challenges. In the contemporary security environment, the rapid development of advanced technologies creates the preconditions for applying new tools

and methods to counter these challenges, with artificial intelligence (AI) increasingly emerging as a key national security resource.

Protecting national security is the primary responsibility of the national security system, defined as a subsystem of the state and society composed of state and non-state actors, civilian and military sectors, tasked with preserving national interests and values from military and non-military security challenges, risks, and threats (Mijalkovic, 2007).

In the global context, artificial intelligence already plays a significant role in various aspects of national security. Its application encompasses cybersecurity, intelligence and counterintelligence activities, big-data analysis, and operational support in combating organised crime and terrorism, particularly through specialised investigative methods.

Here's an overview of the key ways artificial intelligence contributes to protecting national security:

1. **Detection and prevention of cyber-attacks:** Modern algorithms enable automated analysis of network traffic and identification of anomalies indicating potential cyber threats. Applying AI in this domain enables early detection and rapid response, which is critically important for protecting critical infrastructure (Chen et al., 2021).
2. **Processing and analysis of data from intelligence sources:** AI facilitates the systematic organisation and analytical processing of intelligence data across multiple domains, including human intelligence (HUMINT), open-source intelligence (OSINT), technical intelligence (TECHINT), and signals intelligence (SIGINT), alongside diplomatic communications, media content, scientific publications, and other information streams. Automated processes accelerate the production of intelligence assessments and recommendations for decision-makers.
3. **Security-intelligence analysis and trend identification:** Through applying machine learning and statistical models, AI can identify behavioural patterns indicating the emergence of new security risks. This enables proactive action and incident prevention (Gonzalez et al., 2020).
4. **Management of unmanned aerial vehicles and drones:** Using AI in navigation and operational engagement of unmanned aerial vehicles enables the collection of precise intelligence data in real-time, reducing the need for direct engagement of human resources in high-risk zones (Walsh, 2019).
5. **Combating organised crime:** AI algorithms enable analysis of financial flows, video and audio surveillance, communication patterns, and movements of suspected individuals, thereby improving identification of crime networks and their activities. AI is used for risk modelling and predicting criminal phenomena (UNODC, 2021).
6. **Fighting terrorism and radicalisation: Tools for analysing** internet content (textual, visual, and audio material) enable identification of narratives and activities connected to extremist ideologies. AI can recognise communication patterns indicating the radicalisation process (Sandler, 2022).
7. **Predicting security events:** Applying historical data and trends enables building analytical models for forecasting future security challenges, contributing to long-term planning and preventive strategies.
8. **Biometric identification and border security:** AI is integrated into systems for facial recognition, voice recognition, fingerprints, and other biometric characteristics. These technologies are applied at checkpoints, airports, and border crossings to prevent illegal activities and identify individuals of security interest.

With further technological development and increasing algorithmic sophistication, AI's significance in protecting national security is expected to continue to grow. However, alongside technological progress, it's necessary to establish robust ethical and legal frameworks to regulate its application, aiming to prevent potential abuses and preserve citizens' fundamental rights and freedoms. While AI represents revolutionary progress across various social and technological sectors, including the security domain, it also raises numerous questions about privacy protection, freedom of movement, communication, and non-discrimination. Applying AI in security mechanisms—particularly in surveillance, predictive policing, and biometric data processing—must align with existing legal and ethical standards (Jobin, Ienca, & Vayena, 2019; Taddeo & Floridi, 2018). In this context, education and raising awareness of the ethical aspects of AI applications represent key prerequisites for its responsible and legitimate use in the security sector. Educational programs and training within security agencies that incorporate analysis of ethical dilemmas, legal regulations, and international standards can significantly contribute to building a system in which AI applications are transparent, proportional, and subject to democratic oversight (Cath et al., 2018). Only through an interdisciplinary approach—involving experts from law, ethics,

security, technological sciences, and public policy—is it possible to develop an applicable and effective model for responsible use of artificial intelligence in the context of protecting national security.

## 2. Artificial Intelligence and National Security

Artificial intelligence encompasses the capacity of computational systems to perform tasks that conventionally require human cognitive abilities, such as experiential learning, speech recognition, decision-making, and natural language comprehension. Contemporary national security extends beyond the traditional preservation of state sovereignty and territorial integrity to encompass comprehensive societal protection, incorporating public health, economic stability, environmental sustainability, and social welfare. Modern national security frameworks additionally presuppose active state engagement in international and global security architectures. In this context, numerous international conventions and national strategies constitute the normative framework shaping the application of artificial intelligence to strengthen security. The Budapest Convention on Cybercrime (2001) establishes foundations for harmonising national legislation, improving investigations, and strengthening international cooperation in combating cybercrime (Council of Europe, 2001). Its implementation enables the application of AI to prevent, detect, and prosecute cyber offences. Similarly, the UN Convention against Transnational Organised Crime (2000) encourages the use of modern technologies, including AI, to discover and dismantle crime networks (United Nations, 2000). The Convention on the Rights of the Child and the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (2000) directly encourage applying AI tools in protecting children in digital space (United Nations, 2000a). At the strategic document level, the U.S. National Security Strategy (2017) incorporates AI applications to maintain technological superiority, protect intellectual property, and strengthen cyber defence (The White House, 2017). The European Union's Artificial Intelligence Strategy (2018) emphasises an ethical approach and promotes the application of AI to improve cybersecurity and combat terrorism (European Commission, 2022). The National Strategy for Artificial Intelligence of the Republic of Serbia (2019) aims to position the country as a regional leader in this field. The document encourages the development of sophisticated technological solutions for security, including surveillance, data analysis, and the prevention of terrorist and criminal activities (Ministry of Education, 2019). Additionally, the EU Artificial Intelligence Act (2024) supports global cooperation in research and development, emphasising the responsible use of AI in line with the UN Sustainable Development Goals.

Examples of artificial intelligence applications in security include:

- **Crime forecasting systems**, which predict locations and timeframes of potential criminal activities based on analysing large quantities of data, enabling more efficient use of police resources.
- **Border control systems**, employing facial recognition tools and behaviour analysis to prevent illegal crossings and terrorist activities.
- **Cybersecurity systems**, where AI is used for real-time detection and neutralisation of cyber threats, particularly in protecting critical infrastructure.
- **Crisis management**, where AI enables rapid data processing and analysis to support decision-makers during terrorist attacks or natural disasters.

These international conventions, strategies, and examples of good practice underscore the importance of a coordinated, ethically responsible, and technologically advanced approach to the application of AI in national and international security contexts.

At the institutional level, establishing inter-agency coordination among relevant bodies, such as the Ministry of Interior, the Security Information Agency, the Ministry of Defence, the Office for Information Technologies and e-Government, and the academic and research sector, is necessary. Establishing strategic working groups to assess the ethical and technological risks of projects involving AI in security represents an important step toward responsible implementation. From a technological perspective, developing sophisticated ICT infrastructure and big-data processing capabilities (data lakes, cloud-based analysis, real-time monitoring) is a prerequisite for effective AI applications. Also, strengthening domestic scientific research institutions and the security technology start-up ecosystem is essential to ensure technological independence and resilience against external risks.

## 3. Artificial Intelligence and Anti-Crime Intelligence Work

The application of artificial intelligence (AI) in anti-crime intelligence operations constitutes a substantial advancement in enhancing investigative efficiency, accuracy, and responsiveness, while simultaneously strengthening preventive capabilities. These technologically advanced systems enable real-time analysis of intelligence data, improving decision-making in combating crime and terrorism.

AI is used in the context of fighting crime through several complementary approaches:

- Crime intelligence analysis. AI is used to analyse data on behavioural patterns, demographic characteristics, and members of organised crime and terrorist groups, as well as the spatial and temporal patterns of criminal activity. This enables the identification of hotspots of future crime activity, allowing the proactive deployment of police forces and other resources.
- Crime network analysis. Using advanced tools for visualisation and data processing, AI enables the discovery of hidden connections within complex criminal structures. This is particularly significant in organised crime and terrorism cases, where mapping the structure and roles of individuals is crucial for dismantling the network.
- Surveillance and border security. Applying AI to border control systems involves using facial recognition, behavioural analysis, and automated identification of suspicious individuals. This significantly improves border services' capabilities in preventing illegal activities such as human trafficking and smuggling.
- Cybersecurity. In combating cybercrime, AI systems are used to identify and respond to attacks in real time. Applying machine learning algorithms enables the detection of anomalies in network activity, the identification of malicious activity, and the prevention of compromise of critical infrastructure.
- Forensics and digital evidence analysis. AI is applied in analysing digital traces, including video and audio recordings, electronic communications, metadata, and textual documents. AI-based tools can identify relevant evidence faster and more precisely, thereby accelerating investigations and improving prospects for successful judicial outcomes.
- Psychological profiling. By analysing digital communications and behaviour, AI can help create psychological profiles of potential perpetrators. These profiles can be crucially helpful in recognising motives and action patterns.
- Geospatial analysis. Using GIS systems combined with machine learning algorithms, AI enables the analysis of spatial and temporal patterns of criminal activities. Such analyses serve both operational and strategic planning of police and intelligence agency activities.
- Methodology, tactics, and techniques in criminalistics. Methodologically, AI enables the development of advanced investigative methods, particularly in combating organised crime, terrorism, and high-tech crime. In tactics, it enables more precise planning of covert operations and evidence processing. In the technical sphere, applying AI in analysing digital devices enables automated searching, filtering, and classification of large volumes of data.

Despite numerous advantages, applying AI in fighting crime carries significant challenges. Key among them are privacy concerns, the risk of algorithmic bias, and the potential for technology abuse for mass surveillance. Therefore, an AI application must align with existing legal and ethical standards and ensure clear democratic oversight and transparency in institutional operations.

#### **4. Artificial Intelligence and Special Investigative Methods**

Applying artificial intelligence (AI) to special investigative methods represents significant progress in combating organised crime, terrorism, and high-tech crime, enabling faster, more precise, and more systematic data collection and analysis. AI encompasses a range of tools and techniques that enable the processing of large volumes of data, the identification of behavioural patterns, the prediction of criminal activity, and the support of operational actions.

- Electronic surveillance and covert tracking. AI systems enable the integration and processing of data from various sources—including telephone communications, financial transactions, and video surveillance—in real-time. Applying machine learning algorithms enables the identification of suspicious activities and behavioural patterns, significantly improving surveillance efficiency for suspected individuals (Strohmeier, 2020).
- Covert tracking, recording, and communications surveillance leverage advanced biometric recognition technologies and intelligent data extraction algorithms to analyse substantial volumes of audio-visual evidence. These capabilities enable accelerated identification of relevant subjects and their interaction patterns while materially reducing the analytical demands placed on investigative personnel.
- Simulated operations and operational-technical means. Applying AI to simulated actions and GPS device installation enables tracking suspects' movements and predicting routes and contact points. Systems can analyse data in real-time and signal operationally significant patterns (Bachner, 2017).

- Controlled delivery. AI-based analytical modules can optimise controlled delivery plans, assess risk across scenarios, and suggest optimal tactical options, thereby increasing the effectiveness of such measures (Perols, 2011).
- Electronic data processing. AI tools enable processing textual content—messages, emails, social networks—using natural language processing (NLP) to discover threats and communication patterns (Chowdhury, 2010).

AI systems that enable continuous monitoring of public spaces and real-time recognition of suspicious activities are increasingly being utilised in urban environments. These systems can automatically alert relevant authorities, thereby enhancing preventive action (Buil-Gil, 2021). The use of AI in special investigative techniques must be fully aligned with legal and ethical frameworks. In the Republic of Serbia, these methods are regulated by the Criminal Procedure Code, the Law on Personal Data Protection, the Law on the BIA, and other regulations. Special attention must be paid to privacy protection, limitations on the application of technical means, and the right to due process. In addition to legal regulation, it is crucial to ensure systematic, continuous education of investigators to guarantee the professional, legally valid, and ethically acceptable application of AI in special investigative techniques. In this regard, cooperation between state authorities and scientific institutions is important, as well as monitoring best practices and comparative models from other countries.

The application of artificial intelligence (AI) in combating organised crime, terrorism, high-tech and economic crime represents a key turning point in the evolution of the state's security capabilities. This involves transforming traditional investigative approaches into more sophisticated, data-driven models that enable deeper, faster, and more precise analysis of crime phenomena. AI systems provide support through advanced crime-intelligence analysis, the identification of latent behavioural patterns, predictive analytics, and the rapid processing of large datasets, thereby significantly enhancing the operational and strategic capabilities of security structures.

In the field of organised crime, the application of specialised investigative techniques, combined with AI, enables the analysis of social networks and structures within criminal organisations. Through sophisticated network analysis tools, it is possible to identify key actors, intermediaries, and the operational mechanisms of criminal networks (Xu & Chen, 2005). By combining these methods with predictive algorithms, tools are obtained to anticipate the activities and movements of organised groups (Chen et al., 2004).

In the field of counterterrorism, AI contributes to the analysis of digital traces, particularly on social networks, where radicalisation processes and the dissemination of extremist content can be detected. The application of special methods, such as covert surveillance, undercover operations, and open-source intelligence analysis (OSINT), supported by AI, enables timely detection of communication patterns and early warning of potential terrorist threats (Agarwal & Sureka, 2015).

When it comes to high-tech crime, AI enables advanced network traffic analysis, anomaly identification, and automated response to cyber threats in real time (Nguyen et al., 2020). Additionally, machine learning algorithms serve for the classification and identification of malicious software, thereby enabling faster and more precise protection of critical infrastructure (Buczak & Guven, 2016). In the domain of economic crime, special investigative techniques, such as financial monitoring, forensic auditing, and money flow tracking, gain a new dimension through AI integration. By analysing large datasets of transactional data, it is possible to detect irregularities indicative of money laundering, tax evasion, or financial manipulation (Perols, 2011; Jans et al., 2010). AI thereby accelerates the detection and prosecution of complex economic criminal offences. Overall, the synergy between artificial intelligence and special investigative techniques represents an essential instrument in the modern response to increasingly dynamic, technologically advanced, and transnational forms of crime. Its application contributes not only to more efficient crime suppression but also to enhancing the preventive and strategic capabilities of the security system.

## 5. Conclusion

In conditions of accelerated technological development and an increasingly complex security environment, the application of artificial intelligence to national security functions represents a necessary step toward modernising and enhancing the state's capacity to respond to contemporary threats. Artificial intelligence is becoming a key component of the security-intelligence system, which is based on institutional coordination, legal regulation, and technological infrastructure.

Institutions responsible for national security, as implementers of AI technologies, represent integral parts of the broader security-intelligence system. Their role encompasses the systematic collection, processing, and interpretation of data, using advanced machine learning algorithms and analysis of large volumes of information.

The use of AI in this context enables deeper situational awareness, faster response, and more efficient protection of the vital interests of the state and its citizens.

The key areas in which AI enhances the security system include:

- **Data collection** – from multiple sources, including open-source (OSINT), closed (HUMINT, SIGINT), and technical methods;
- **Processing and analysis** – through the application of machine learning algorithms for threat identification, pattern recognition, and anomaly detection;
- **Interpretation and presentation of results** – through the generation of analytical reports and support for decision-makers;
- **Multi-agency cooperation** – with AI support in connecting and exchanging information between institutions for improved coordination.

The use of artificial intelligence significantly contributes not only to operational efficiency but also to the strategic planning of national security. Its integration enables a more flexible, predictive, and evidence-based approach to security challenges.

However, alongside all the advantages, it is necessary to consistently emphasise the need for the balanced application of AI in accordance with the principles of the rule of law, the protection of human rights, transparency, and democratic oversight. Challenges such as privacy protection, algorithmic bias, and legal uncertainty must be at the centre of future normative and institutional development. Overall, the application of artificial intelligence to protect national security represents not only technological progress but also a new paradigm for shaping contemporary security policies. Its effective and responsible application can significantly enhance the state's capacity to protect its interests and respond to the complex challenges of the 21st century.

## Literature

1. Agarwal, S., & Sureka, A. (2015). Using K-means clustering for detecting coordinated cyber-attack activities in a highly interactive online social network. *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 777–782.
2. Artificial Intelligence Act (Regulation (EU) 2024/1689). (2024, June 13). Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
3. Bachner, J. (2017). Predictive policing: Forecasting crime for law enforcement. *IEEE Technology and Society Magazine*, 36(4), 34–42.
4. Bandyopadhyay, S., & Sandler, T. (2022). Effects of defensive and proactive measures on competition between terrorist groups. *Journal of Conflict Resolution*, 66(10), 1797–1825. <https://doi.org/10.1177/00220027221108432>
5. Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). Does predictive policing lead to biased arrests? *Statistics and Public Policy*, 5(1), 1–6.
6. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
7. Buil-Gil, D. (2021). Automated surveillance systems: Ethical and legal issues. *Surveillance & Society*, 19(1), 56–71.
8. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the “good society”: The US, EU, and UK approach. *Science and Engineering Ethics*, 24(2), 505–528.
9. 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.
10. Chowdhury, G. (2010). Natural language processing. *Annual Review of Information Science and Technology*, 45(1), 101–134.
11. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). <https://rm.coe.int/1680081561>
12. European Commission. (2018). Artificial Intelligence for Europe (COM(2018) 237 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>
13. Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.
14. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), 137–144.

15. González Fuster, G. (2020). Artificial intelligence and law enforcement: Impact on fundamental rights. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL\\_STU\(2020\)656295\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf)
16. Government of the Republic of Serbia. (2019). Strategy for the development of artificial intelligence in the Republic of Serbia. <https://www.srbija.gov.rs/tekst/en/149169/strategy-for-the-development-of-artificial-intelligence-in-the-republic-of-serbia.php>
17. Jans, M., Lybaert, N., & Vanhoof, K. (2010). A framework for internal fraud risk reduction at IT integrating business processes: The IFR2 framework. *Information Management & Computer Security*, 18(2), 111–127.
18. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399.
19. Li, Z. (2019). Facial recognition technology in criminal investigations. *Criminal Justice Review*, 44(2), 205–221.
20. Мијалковић, С. (2007). О кризи националног система безбедности Републике Србије [On the crisis of the national security system of the Republic of Serbia]. *Ревија за безбедност*, 5, 41–45.
21. Министарство просвете, науке и технолошког развоја Републике Србије. (2019). Национална стратегија за вештачку интелигенцију за период 2020–2025 [National strategy for artificial intelligence for the period 2020–2025]. <https://www.mpn.gov.rs>
22. Ng, K. C., So, M. K. P., & Tam, K. Y. (2021). A latent space modeling approach to interfirm relationship analysis. *ACM Transactions on Management Information Systems*, 12(2), Article 10. <https://doi.org/10.1145/3424240>
23. Nguyen, T. T., Reddi, V. J., Yosinski, J., & Hooker, S. (2020). Machine learning for cybersecurity: A comprehensive survey. *Journal of Information Security and Applications*, 53, 102–124.
24. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
25. Perols, J. L. (2011). Financial statement fraud detection using a cross-sectional approach. *Journal of Forensic Accounting Research*, 12(1), 15–31.
26. Strohmeier, M. (2020). Big data analytics for crime prevention: Applications and challenges. *Journal of Data Intelligence*, 2(3), 123–136.
27. Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751–752.
28. United Nations. (2000a). United Nations Convention against Transnational Organized Crime and the Protocols Thereto. <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>
29. United Nations. (2000b). Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. <https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child>
30. United Nations Office on Drugs and Crime. (2021). Darknet cybercrime threats to Southeast Asia. [https://www.unodc.org/roseap/uploads/documents/Publications/2021/Darknet\\_Cybercrime\\_Threats\\_to\\_Southeast\\_Asia\\_report.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf)
31. Walsh, T. (2019). 2062: The world that AI made. Black Inc.
32. White House. (2017). National security strategy of the United States of America. <https://www.whitehouse.gov>
33. Xu, J., & Chen, H. (2005). Criminal network analysis and visualization. *Communications of the ACM*, 48(6), 100–107. <https://doi.org/10.1145/1064830.1064834>