Jurnal
ILMU KEPOLISIAN
ISSN : 2620-5025

Volume 17 / Nomor 3 / Desember 2023

ARTIFICIAL INTELLIGENCE (AI) AND INTERNET OF THINGS (IOT): THREATS OR FUTURE FOR THE POLICE?

[1]Alfin Reza Syahputra*, [2]Bagus Aditya, [3]Zulaikha Sari Handayani
[1]Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia 12160
[2,3]Telkom University, Bandung Regency, Indonesia 40257
e-mail: alfinrezas@gmail.com, [2]goesaditya@telkomuniversity.ac.id, [3]zulaisarikha@gmail.com

Abstract

This study examined the impact of Artificial Intelligence (AI) and Internet of Things (IoT) technologies in policing from the perspective of challenges, threats, and readiness. This study adapted a systematic literature review with data obtained from journals and previous research articles in 2020 – 2023. Previous studies concluded that crime is the shadow of civilization; therefore, the police must be able to keep up with the times. The development of an increasingly modern civilization causes more complex crime, AI and IoT will cause unimaginable crime potential. Countries all over the world have invested in the development of AI and IoT technologies for crime prevention and detection. The idea behind this investment is to make the crime predictable and detectable, allowing the police to enforce the law exactly and properly. AI systems are expected to overcome several human deficiencies, such as consistency in analyzing situations from multiple data sources, especially millions of data points from IoT devices.

Keyword: AI, IoT, Crime, Smart Policing, Predictive Policing

Introduction

In recent years, Artificial Intelligence (AI) and Internet of Things (IoT) have become an exciting focus of research to address system security issues across sectors. AI is an interdisciplinary research area that offers technological breakthroughs related to security systems (Apsara *et al*., 2020). Many investments were conducted in AI technology development to deal with security challenges in daily life, such as statistical data management, medicines, and transportation. Available data from key sectors, such as e-commerce, business, and government, provides important contributions to the development of machine learning and algorithmic solutions related to system security (Ahmad *et al*., 2021).

IoT is also a technology that is vital for controlling user security and privacy. IoT technology enables machines to obtain relevant information and process it consistently (Green, 2019). IoT is crucial to maintaining customer security and privacy in a security context. Furthermore, the concept of intelligence integrated into IoT technology is also a relevant factor (Blythe et al., 2019). Effective and secure communication in the IoT network becomes crucial throughout implementation. In the IoT context, communication protocols such as ZigBee, Bluetooth, Sigfox, Wi-Fi, and Z-Wave have gained popularity (Yigitcanlar *et al*., 2020).

However, like other technologies, AI and IoT also have security and privacy related challenges. IoT network security involves issues such as availability, data integrity, confidentiality, and authentication, which can hinder operational efficiency, resilience, and throughput (Osoba & Welser,

2017). To ensure the sustainability and scope of IoT network, security and privacy issues need to be addressed seriously. In order to address upcoming security threats, it is necessary to carry out comprehensive research on improving existing communication protocols and integrating AI-based solutions into IoT technology (Correia & Matos, 2021).

In addition, crime remains a part of the future and civilization's development in the context of police and law enforcement. The advancement of civilization is frequently correlated with an increase in crime rates (Caldwell *et al*., 2020). Police have undergone significant changes over the years, and various policing models have been tested and implemented. Security has always been a multifaceted topic, and police scholars and practitioners have had extensive discussions regarding how the modern police should respond to crime (Haque & Tasmin, 2020). In the operation of institutions and police practices, AI has played an increasingly important role, such as in the utilization of risk assessment algorithms, facial recognition technology, and predictive analytics systems (Khan *et al*., 2022). Data-driven approaches to crime resolution are also trending in crime resolution, with the machine's ability to identify patterns and discover connections that may take longer for humans (Tundis *et al*., 2020).

In this context, this study aims to explore the role and potential of AI and IoT in accomplishing system security challenges, with a focus on policing context implementation. By understanding the potential and risks of these technologies, we can develop an effective approach to dealing with future security challenges. As a result, the authors will conduct research on AI and IoT: A threats or a future for the police in this study.

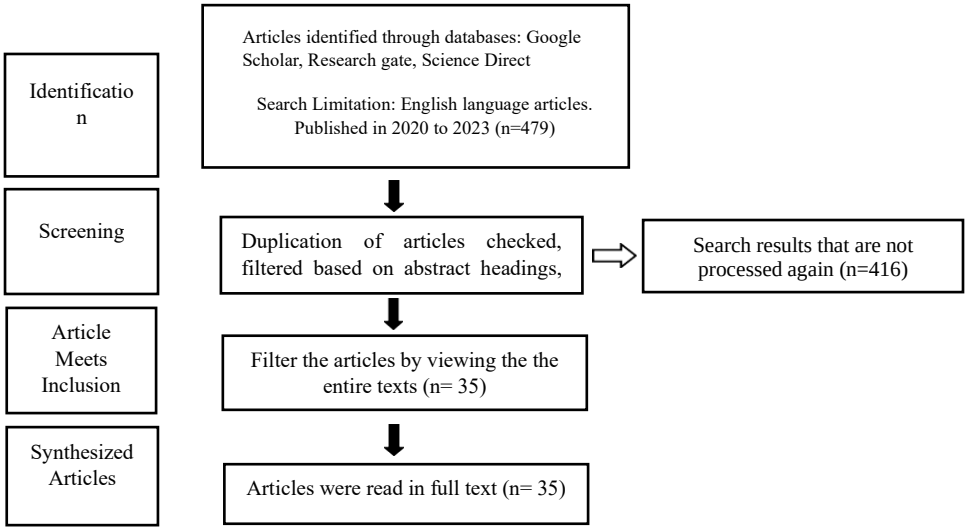
Research Methodology

The literature review in this study was conducted through a systematic search of international journals and proceedings databases. The literature search techniques use keywords that correspond to research questions. The list of keywords that will be used as the basis for literature searches is AI, IoT, predictive policing and smart policing. Search for articles in English with publication years limited to the last 3 years (2020-2023) and articles on the potential and threats of AI and IoT that impact the security sector and its development.

Results And Discussions

Research Result: Scheme or Diagram (PRISMA)

Figure 1. Describe the process of selecting articles using the Preferred Reporting Systematic Reviews and Meta-analysis (PRISMA) guidelines. The initial search revealed that the number of articles from 2020-2023 is 479 articles. The screening article comes next, a total of 37 papers have been advanced to the next level. The quality of the articles was evaluated so that as many as 37 articles were synthesized in the final report from the literature.



Source: Processed by Author

Figure 1. PRISMA Diagram

The researcher selected the obtained articles and extracted data on each article from each database. The results of the article are reviewed regarding AI and IoT: threat or future for the police.

Table 1. AI and IoT: Threat or Future for the Police

Researcher	Objectives	Result
(Akthar, 2022)	To create and discover the effectiveness of remote spy robot using the Internet of Things	A remote spy robot is a "detachable" robot that acts as an "insider" in a variety of military, police, security, and rescue operations. It can be applied in hazardous, hostile, or closed environments. These robots have critical visual intelligence that can save lives and reduce property damage.
(Frank *et al*., 2022)	To detail the new form of attack accurately and detect the temperature around DRAM carrier device.	Attacks can only be carried out by compromising IoT software without requiring hardware modification or physical access. This inspection can be performed at a temperature resolution of up to 0.5◦C in the range of 0◦C to 70◦C. It even works on devices that do not have a specific temperature sensor.
(Huang *et al*., 2022)	To describe and analyze the potential and challenges of convergence between Artificial Intelligence (AI) and Internet of	Convergence between Artificial Intelligence (AI) and Internet of Things (IoT) in the context of smart law enforcement or smart policing. The author focuses on how the integration of AI and

	Things (IoT) convergent in the context of smart law enforcement or smart policing.	IoT can improve operational effectiveness and law enforcement performance.
(Ahmad *et al*., 2021)	To evaluate and reduce the range of attacks on IoT devices	There are four main techniques to protect the IoT environment: Edge Computing, Fog Computing, Block Chain, and Machine Learning.
(King *et al*., 2020)	To discover predictable AI threats. Provide a synthesis of current and possible solutions for ethics, policymakers, and law enforcement organizations.	AI as an autonomous intelligent body. There is an interdisciplinary analysis of threats and anticipated solutions related to Artificial Intelligence (AI) crimes.
(Tundis *et al*., 2020)	To detect and track real-world criminals using IoT systems	A system based on social IoT devices will be developed to support real-world detection and tracking of criminals. The proposed model and algorithm specified above have been evaluated via a simulator to demonstrate the logic of the system's functioning, while the functionality of the application has been assessed through user studies conducted on a group of 30 users.
(Caldwell *et al*., 2020)	To identify possible applications of the Artificial Intelligence (AI) and related technologies in criminal acts	To create a catalog of potential criminal and terror threats arising from increased adoption and power of artificial intelligence, and to rank these threats in terms of expected victim loss, criminal advantage, criminal achievement, and difficulty of defeat. Eighteen threat categories were identified and evaluated. The top five out of six ratings have broad social impact, such as involving fake content generated by AI or can operate on a large scale through the use of AI automation; the sixth is the misuse of driverless vehicle technology for terrorist attacks.

(Afzal & Panagiotopoulos, 2020)	Smart policing can be an increasingly in-demand field in government research management and digital public.	Previous work has focused on social media communication or predictive policing. While this review identifies several new applications related to new forms of data and their appropriate role for policing. This research developed a framework for demonstrating the relationship between the smart data use with police approaches and strategies.
(Sandhu & Fussey, 2021)	Officers will rely on computer software and smartphone apps to instruct them about where and who to police, just like Uber drivers rely on similar technology to instruct them about passenger pick-up points.	Many police officers have detailed awareness of the limitations of predictive technology, those caused by errors and biases in data input. This awareness has caused many officers to develop a skeptical attitude toward predictive technology, in some cases, these officers have expressed a reluctance to use predictive technology.

Source: Processed by Author

AI and IoT Become Threats and Potential Crimes

AI can be involved in crime in various ways. Most obviously, AI can be used as a tool to facilitate criminal action against real-world targets: predicting the behavior of people or institutions to discover and exploit vulnerabilities; generating fake content to be used in blackmail or to defame reputation; committing acts that the criminal perpetrators cannot or do not want to do for reasons of danger, physical size, reaction speed, and so on. Despite its new methods, the crime itself may be the traditional types of theft, blackmail, intimidation, terror (Caldwell *et al*., 2020). Hacking and data theft can be used as remote criminal action modes. Making the data owner as a target, the victim even appears to be a criminal, while the actual perpetrator hides using a fake identity, using someone else's data to commit crimes. Even when tracking is done, the found data is fake and does not identify the actual perpetrator.

Amid the accelerated application of digital automation over the past five years, the risk of cyberattacks continues to rise. Examples of threats and potential crimes include audio or video impersonation, driverless vehicles as weapons, tailored phishing, disrupting AI-controlled systems, AI-authored fake news, large-scale blackmail, military robots, snake oil, learning based cyber-attacks, autonomous attack drones, data poisoning, online eviction, tricking face recognition, burglar bots, market bombing, evading AI detection, bias exploitation, AI-assisted stalking, and forgery. With the marks of the case, efforts are needed to increase awareness and knowledge to the public to stay alert (Caldwell *et al*., 2020).

Alternatively, AI system itself can become targets of criminal activity by avoiding protection systems that present obstacles to crime, avoiding detection or prosecution of crimes that have been

committed, or causing trusted or critical systems to fail or behave inappropriately to cause damage or undermine public trust. AI can also easily provide context for crime. Fraudulent activity may rely on the victim's belief that some AI functions are possible, even if they are not or are possible but not actually used in fraud (Jones, 2022).

The extent to which the diversity of these crimes can be enhanced by AI applications depends heavily on how much this technology has an impact on the computing environment. While robotics is growing rapidly, AI is more involved in digital crimes such as banking fraud than battles in pubs. Preference for the digital world over the physical world is a weak defense, even though contemporary societies rely heavily on complex computing networks, not only for finance and commerce but also all forms of communications, politics, news, employment, and social relations (Rigano, 2019). People now spend most of their lives online, getting most of their information there, and their online activities can build and destroy their reputation. This trend is likely to continue in the future. Such an online environment, where data is property and information power, is perfectly suited for exploitation by AI-based criminal activities that can lead to substantial real-world consequences (Madia, 2023).

In addition, unlike many traditional crimes, crimes in the digital realm are often highly replicable: once developed, techniques can be shared, replicated, or even sold, enabling potential marketing of criminal techniques or the provision of "crime as a service". This can lead to a decrease in technological barriers as criminals can redirect more challenging aspects of their AI-based crimes (McDaniel & Pease, 2021).

Security issues can develop in the IoT, which can be used to sabotage smart homes or internet-connected applications. Then for espionage or spying, internet-connected devices (IoT) can be remotely controlled, can harm, injure, kill, or burn. Smart cars can be controlled and then engineered like a broken machine or suicide. Doctrinarians use music and stories used by the perpetrator to influence the victim, commonly referred to as manipulation. IoT and AI in the future will be adapted across the lines and aspects of human civilization’s life. Of course, crimes through IoT and AI can have high levels of danger like biological and chemical weapons are even more dangerous.

Today's AI with deep blue and deep learning can beat the world's grandmaster chess players. Win other games with exponential learning. There is no doubt that AI can be smarter than humans. Intelligent AI (Super AI) in the future can even commit its own crimes with the help of IoT as legs, hands, and bodies. From crime with minimal impact to disruption of national security (as in the “Eagle Eye” movie).

AI and IoT are the Future for the Police in Smart Policing and Predictive Policing

As with the adoption of Artificial Intelligence and Internet of Things, there are questions to be asked and answered and issues to be addressed. Law enforcement agencies around the world are grappling with this and trying to find the right balance to leverage the benefits of this technology to combat and resolve crimes while maintaining privacy and security (Huang et al., 2022). Not only that, but also the emergence of various other types of attacks to steal user information and personal data from IoT devices. Security and emergency management are other applications of personal data from IoT systems (Gabriel, 2022). Most current military operations, mainly in the field of mining, use most machines for such tasks or even install wireless sensors to prevent unauthorized access to prohibited

areas. In most buildings, wireless sensors are installed to handle theft activity, control lighting systems, water systems, and more (Byun et al., 2014).

As with edge computing, data transmission is carried out via a network or device. Data movements are less than cloud computing and this will reduce security issues. Another issue is data compliance in some countries, so they do not want to share data with other countries and have some restrictions (Gkougkoudis *et al*., 2022). Therefore, with the use of edge computing, data compliance problems will be solved. As a result, if the user does not have a fast internet connection and everything needs to be sent to the cloud server, then the waiting time for the cloud server's response will be long enough to affect the security of a person or group (Blythe & Johnson, 2021).

The infrastructure of each city is becoming more and more smart as governments try to make their country grow very rapidly. More intelligent and connected infrastructure in countries provides real-time information to government officials (Frank *et al*., 2022). With the help of AI, real-time information can help detect crimes as soon as they occur. In the realm of police investigation, for example, solving complicated murder cases requires persistent investigation (Joh, 2019). When police officers visited the court, they took photos of where the crime occurred. The photos are used to find clues and evidence that can help unlock new links to the crime (King *et al*., 2020). An AI-enabled system can help detect clues from police photos. For example, a toy or gun from the crime scene, captured in photo, can be searched in police databases to find out if the same toy or gun was used in previous murders. This may not definitively link the previous offenders to current crimes, but it will open up a path of investigation worth trying (Ghosh *et al*., 2018).

Disruption in addition to being rapid, also affects various productivity in life as well as social order. When the control or management of disruption is unable to balance or leave behind various counter-productive things that disrupt social order will emerge. In this situation, it is necessary to think about how the police and policing are able to deal with disruption proactively and solve problems. According to Moon *et al*. (2017) in the digital era or industrial revolution 4.0 which also leads to society 5.0, the policing model, in addition to morals and modern smart professionals is able to run smartly. In line with this, the smart policing model is implemented using regional approach models, the functional model, and the impact model on bureaucratic problems and society. Implemented for routine, special, and contingency police services. Smart policing in the implementation of conventional policing, e-policing and forensic policing.

In smart policing, support for research and development as well as laboratory development is critical and fundamental. Research is a crucial aspect of conceptualizing and reasoning logically in numerous ways. The smart policing model can be conceptualized, physically developed, technically, scientifically, and in terms of infrastructure and systems, as well as curriculum and education (Mukherjee & Halder, 2020).

Crime is an accumulation of patterns; it is not random. AI and IoT can support precise pattern reading. Utilizing AI technology can help with content monitoring. Monitoring content can help with prediction. In the end, crime prediction will ultimately help crime prevention (Banerjee *et al*., 2015). AI can help police monitor a person's digital footprint and detect unusual activity. The purpose of the police is not to enforce the law but rather to establish a sense of security, achieving security by preventing things that interfere with security, one of which is the prevention of crime and potential crimes. The police can accurately reduce crime with the application of AI and IoT in crime prevention

and detection (Michael Flynn, 2020). The use of AI in crime prevention and detection carries some inherent risks in addition to the advantages of IoT and AI. For example, a person may be identified as a criminal or suspect of criminal activity based on racial biases that may be inadvertently fed into AI and IoT systems (Comiter, 2019). To establish whether or not integrating AI and IoT to prevent crime is strategically appropriate, such risks must be evaluated in an open and transparent manner (Akthar, 2022).

In addition, AI and IOT are beneficial for predictive policing, which has the potential to involve areas beyond the criminal problem. Traffic management, for example, is well suited for predictive policing. High-frequency traffic data with consistent regularity patterns is an essential resource for policing activities in traffic flow regulation, including the mitigation or even avoidance of traffic accidents. Predictive policing includes mass demonstrations and forest and land fires that follow cyclical patterns all over time (Seldadyo *et al*., 2021). Data on the movement of bank account financial transactions that are possible or potentially profiled by some criminal acts, such as radicalism and terrorism, also contains certain patterns that can be explored through predictive policing. In fact, digital data on community mobility recorded, for example, by Google Mobility Index or telecommunication networks, plays an important role in predictive policing (Madia, 2023). Such data is useful not only in normal situations but also in pandemic situations when mobility and crowd restriction policies are implemented, a violation of which would be considered illegal. Predictive policing is technological on the microscale. Data from various sources, including in various forms, including various forms, such as searching, producing, recording, and sensing activities. This data is used in predictive policing to develop forecast about outcomes, followed by policing actions (McDaniel & Pease, 2021).

Cyberspace, like the universe, is a wider network. Crimes committed on the deep web have not been widely tracked or exposed (Riadi & Rusydi Umar, 2017). To avoid crimes caused by AI intelligence (Super AI), the police must develop Super AI as a virtual police force. The police must develop Super AI as a virtual police force. The development of Super AI as a virtual police force that is capable of investigating, analyzing, and anticipating crimes in cyberspace (surface web, deep web, dark web). Furthermore, Super AI Police has control over Super AI, which can conduct crimes on its own. Police personnel monitor the system and take preventive and enforcement actions, which are carried out by humans utilizing traditional means or technology. No crime is perfect, nor is technology, and no crime utilizing technology is perfect. To eradicate crime, the police must prepare methods, steps, technology, human resources, experts.

The police are behind the crime?

Today's police force must be able to see how this civilization is going and what the future holds. As described by Bratton, *et al*. (2009: 3) suggest that we understand predictive policing as "forward-thinking crime prevention" that "links technology, management practices, real-time data analysis, problem solving, and informed policing to produce good outcomes - reduced crime, efficient agencies, and modern, innovative policing". Bratton, *et al*. Also detailing the elements of predictive policing include integrated information and operations, seeing the big picture, and advanced analytics and technology.

The actualization of the use of AI-based technology (super-AI) will help the police to adapt to civilization and implement predictive policing in an effort to prevent crime and reduce all possibilities that cause security and order instability.

In realizing social order characterized by the maintenance of security and public order as well as domestic security. The police are often in a race with crime. Police often lag behind crime. Especially in the current era of industrial revolution which makes shifts and changes faster. Since the era of the industrial revolution 4.0, technological development has reached a stage that human civilization may not have imagined before, very fast. Industry 4.0 applies IoT in the manufacturing workspace and then analyses the big data collected in cloud storage to efficiently improve autonomy and cybersecurity levels (Nahavandi, 2019). Even now, we are really looking at the transition to the industrial revolution 5.0 era. Nahavandi (2019) states that industry 5.0 will be a synergy between humans and autonomous machines. Autonomous labor will be responsive and aware of human intentions and desires. Humanity will work together with robots, not only without fear but also with peace of mind, knowing that their robotic co-workers understand them adequately and have the ability to collaborate effectively with humans.

Industry 5.0 will revolutionize manufacturing systems worldwide by removing tedious, dirty and repetitive tasks from human workers wherever possible. Robots and intelligent systems will permeate manufacturing supply chains and factory floors to an unprecedented degree Nahavandi (2019). What about the police? Police agencies, police education centers, police, and any agency, organization, or private sector that performs police functions must be prepared from now on to face this change. Of course, it will also be followed by changes/shifts in civilization and crime.

AI and IoT as one that provides a fundamental change in the phenomenon of crime in the future as well as the potential for the police to take a step ahead of crime, if it is indeed a concern for policy makers and executive managers in the police.

From now on, police forces should initiate and collaborate on research, academic studies with interdisciplinary and transdisciplinary approaches, and even evaluate policing models and policies. Police agencies around the world, academics, the private sector, and other police functionaries, must think about it and take steps from now on to dismiss the assertion that the police are always lagging behind crime, because in the future they will face the same context of challenges.

In the future, the police will be faced with crimes in the real world, crimes in cyberspace, or both. Thus, the public will demand the police to provide security and services in the real and virtual worlds, while maintaining human rights and privacy. Meanwhile, crime has evolved. In the real world with conventional crime, fiscal crime, white-collar crime, water crime, environmental crime, cross-border crime, extraordinary crime, and others. In the virtual world, it has utilized AI, IoT, digital financial technology (cryptocurrency or others), data theft, privacy violations, and cybercrime that results in real-world crimes.

If grouped together, the police in the future will be faced with conventional crimes, crimes using technology, crimes resulting from technological failures, crimes by technology itself at its will, and maintaining security and order in the real and virtual worlds. The boundaries of the real world are very clear, the police jurisdiction is based on the country or state or city. Cyberspace, on the other hand, has no boundaries. So police agencies must collaborate, not shift responsibility, co-opt jurisdiction or be indifferent to cyberspace.

Conclusions and Recommendations

The higher the crime rate, the more advanced a civilization. In the future, crime will make use of advanced technologies like as AI and IoT, which can be used to discover and analyze victims (victim behavior), as a tool for crime, to make criminals anonymous, and even to construct criminal profiles that appear like other people. This potential crime is not limited to criminal actions; it can potentially affect public order and national security, even have a connection with other countries. This is a threat and challenge for the police, and if they do not act from now on, it will be too late to overcome it. The police must take one step ahead of crime by investing in AI and IoT for crime prevention and detection, case disclosure, public order, and national security concerns. The idea behind this investment is that crimes can be easily predicted and detected using AI systems, and criminals can be tracked using a mix of AI and IoT systems. The convergence of criminal intelligence and national security needs based on AI and IoT is now required.

Reference

Abed, A. K., & Anupam, A. (2022). Review ofsecurity issues in Internet ofThings and artificial intelligence-driven solutions. *Wiley*, 1–18. https://doi.org/10.1002/spy2.285

Afzal, M., & Panagiotopoulos, P. (2020). Smart Policing: A Critical Review of the Literature. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12219 LNCS*. https://doi.org/10.1007/978-3-030-57599-1_5

Ahmad, I., Niazy, M. S., Ziar, R. A., & Khan, S. (2021). Survey on IoT: Security threats and applications. *Journal of Robotics and Control (JRC)*, *2*(1), 42–46. https://doi.org/10.18196/jrc.2150

Akthar, M. S. (2022). Long Range Spy Robot Using Internet of Things. *International Journal for Research in Applied Science and Engineering Technology*, *10*(6), 2954–2962. https://doi.org/10.22214/ijraset.2022.44489

Apsara, G., Amrithha, D., Ramya, R., & Chitra, R. (2020). Spy Robot Surveillance System using IoT. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, *8*(6), 128–133. https://doi.org/10.17148/IJIREEICE.2020.8627

Ashby, M. (2023). Forecasting crime trends to support police strategic decision making. *CrimRxiv*.

Banerjee, S., Van Hentenryck, P., & Cebrian, M. (2015). Competitive dynamics between criminals and law enforcement explains the super-linear scaling of crime in cities. *Palgrave Communications*, *1*. https://doi.org/10.1057/palcomms.2015.22

Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, *34*(1), 97–125. https://doi.org/10.1057/s41284-019-00211-8

Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity*, *5*(1), 1–10. https://doi.org/10.1093/cybsec/tyz005

Bratton W., Morgan J., & Malinowski S. (2009). *Fighting Crime in the Information Age: The Promise of Predictive Policing*. Available at https://publicintelligence.net/lapd-research-paper-fighting-crime-in-the-information-age-the-promise-of-predictive-policing/ (accessed 11 November 2023)

Byun, J. Y., Nasridinov, A., & Park, Y. H. (2014). Internet of things for smart crime detection. *Contemporary Engineering Sciences*, *7*(13–16), 749–754.

https://doi.org/10.12988/ces.2014.4685

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Comiter, M. (2019). Attacking artificial intelligence: AI's security vulnerability and what policymakers can do about it. *Belfer Center for Science and International Affairs | Harvard Kennedy Schhool*, *August*.

College of Policing. 2020. *Preparing policing for future challenges and demands*. Retrieved from https://www.college.police.uk/article/preparing-policing-future-challenges-and-demands

Correia, M. J., & Matos, F. (2021). The impact of artificial intelligence on innovation management: A literature review. *Proceedings of the European Conference on Innovation and Entrepreneurship, ECIE*, 222–230. https://doi.org/10.34190/EIE.21.225

Frank, F., Xiong, W., Anagnostopoulos, N. A., Schaller, A., Arul, T., Koushanfar, F., Katzenbeisser, S., Ruhrmair, U., & Szefer, J. (2022). *Abusing Commodity DRAMs in IoT Devices to Remotely Spy on Temperature*. 1–14.

Gabriel, I. (2022). Toward a Theory of Justice for Artificial Intelligence. *Daedalus*, *151*(2), 218–231. https://doi.org/10.1162/DAED_a_01911

Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial Intelligence in Internet of Things. *The Institution of Engineering and Technology*, 1–11.

Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. *Digital*, *2*(2), 143–163. https://doi.org/10.3390/digital2020009

Green, B. (2019). The Smart Enough City. In *The Smart Enough City* (Issue May). https://doi.org/10.7551/mitpress/11555.001.0001

Haque, A. K. M. B., & Tasmin, S. (2020). Security Threats and Research Challenges of IoT - A Review. *Journal of Engineering Advancements*, *01*(04), 170–182. https://doi.org/10.38032/jea.2020.04.008

Huang, C.-H., Chou, T.-C., & Wu, S.-H. (2022). Towards Convergence of AI and IoT for Smart Policing. *Journal of Global Information Management*, *29*(6), 1–21. https://doi.org/10.4018/jgim.296260

Joh, E. E. (2019). Policing the smart city. *International Journal of Law in Context*, *15*(2), 177–182. https://doi.org/10.1017/S1744552319000107

Jones, N. (2022). A Mixed Methods Social Network Analysis of San Diego Law Enforcement Task Forces and Agencies. *International Journal of Police Science*, *1*(2), 70–97. https://doi.org/10.56331/487529/ijps6

Khan, J. I., Khan, J., Ali, F., Ullah, F., Bacha, J., & Lee, S. (2022). Artificial Intelligence and Internet of Things (AI-IoT) Technologies in Response to COVID-19 Pandemic: A Systematic Review. *IEEE Access*, *10*, 62613–62660. https://doi.org/10.1109/ACCESS.2022.3181605

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In *Science and Engineering Ethics* (Vol. 26, Issue 1). Springer Netherlands. https://doi.org/10.1007/s11948-018-00081-0

Madia, J. D. (2023). Review of Predictive Policing and Artificial I ntelligence. *International Journal of Police Science*, *1*(1), 1–3.

McDaniel, J. L. M., & Pease, K. G. (2021). Policing, AI and choice architecture. In *Predictive Policing and Artificial Intelligence*. https://doi.org/10.4324/9780429265365-5

Michael Flynn. (2020). Urban Future with a Purpose. *Green Planning of Public Spaces*, 22–25.

Moon, H. Bin, Choi, H., Lee, J., & Lee, K. S. (2017). Attitudes in Korea toward introducing smart policing technologies: Differences between the general public and police officers. *Sustainability (Switzerland)*, *9*(10). https://doi.org/10.3390/su9101921

Mukherjee, A., & Halder, R. (2020). PoliceChain: Blockchain-Based Smart Policing System for Smart Cities. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3433174.3433618

Nahavandi, S. (2019). Industry 5.0—A human-centric solution. *Sustainability*, *11*(16), 4371.

Osoba, O., & Welser, W. (2017). The Risks of Artificial Intelligence to Security and the Future of Work. *The Risks of Artificial Intelligence to Security and the Future of Work*. https://doi.org/10.7249/pe237

Riadi, I., & Rusydi Umar, I. M. N. (2017). Forensic Analysis of Digital Evidence on Frozen Solid State Drives Using the National Institute of Standards and Technology (NIST) Method. *Jurnal Insand Comtech*, *2*(2).

Rigano, C. (2019). Intelligence To Address Criminal " I. *National Institute of Justice*, *Vol. 3*(No. 280), 1–10.

Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society*, *31*(1). https://doi.org/10.1080/10439463.2020.1803315

Seldadyo, H., Sudarto, E. R., & Sonta, A. (2021). Predictive Policing: Current and Future Policing. *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences*, 3906–3913.

Tundis, A., Kaleem, H., & Mühlhäuser, M. (2020). Detecting and tracking criminals in the real world through an IoT-based system. *Sensors (Switzerland)*, *20*(13), 1–27. https://doi.org/10.3390/s20133795

Yigitcanlar, T., Desouza, K. C., Butler, L., & Roozkhosh, F. (2020). Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. *Energies*, *13*(6). https://doi.org/10.3390/en13061473