

Artificial Intelligence for CBRN threat detection: emerging opportunities and challenges for law enforcement and security practitioners

Maria Ustenko
Research Department
Zanasi & Partners
Modena, Italy

maria.ustenko@zanasi-alessandro.eu

Giulia Venturi
Research Department
Zanasi & Partners
Modena, Italy

giulia.venturi@zanasi-alessandro.eu

Abstract— This paper explores the emerging applications of Artificial Intelligence (AI) in addressing Chemical, Biological, Radiological, and Nuclear (CBRN) threats, from the perspective of law enforcement and intelligence practitioners, drawing on a curated literature review of recent scholar publications and patents (2024–2025). This work was supported by the project NOTIONES, that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853. The aim was to provide a horizon-scanning analysis of novel AI-driven capabilities relevant to real-world security operations. A range of AI-powered tools and systems—ranging from automated reconnaissance and threat prediction platforms to unmanned systems and advanced sensory interfaces—were identified as potentially transformative for public safety. While such developments promise to enhance situational awareness, response time, and risk mitigation, they also raise concerns related to operational complexity, reliability, ethical oversight, and human-machine interaction. This analysis confirms the critical need for security stakeholders to actively engage with the research and innovation landscape, ensuring the adoption of responsible and operationally fit technologies. The findings are based exclusively on open-source information and aim to support strategic technology foresight and practitioners' preparedness.

Keywords— *Artificial Intelligence, CBRN, Law enforcement, threat detection, horizon scanning, security technologies, NOTIONES, Public Safety*

I. INTRODUCTION

The evolving landscape of global security is marked by the increasing sophistication and accessibility of Chemical, Biological, Radiological, and Nuclear (CBRN) threats, alongside the persistent danger of Improvised Explosive Devices (IEDs).

For law enforcement agencies (LEAs) and intelligence practitioners, the early detection and effective neutralization of such threats is paramount to safeguarding urban and strategic environments. In this context, Artificial Intelligence (AI) is becoming a critical enabler for next-generation detection, assessment, and response capabilities.

This paper explores the role of AI technologies in supporting the mission of LEAs and security professionals by synthesizing key advancements identified through recent scientific literature and patent activity.

The analysis stems from the collaborative work carried out under Work Package 5 (WP5) of the NOTIONES project—an

EU-funded initiative dedicated to horizon scanning of novel technologies affecting the intelligence and security domain.

All data analyzed derives exclusively from open-source publications, with the aim of informing and enriching practitioner-led foresight efforts.

This proposed analysis draws on the literature review of recent scholar publications and patents.

II. LITERATURE REVIEW

The literature review included works published between January 2024 and September 2025, and focused on innovations relevant to CBRN threats detection.

The review was performed on two different online databases - Scopus [1] and The Lens [2] - through keyword search [*AI AND CBRN*] in the fields *title*, *abstract*, and *keywords*.

The initial search identified 21 records (4 from Scopus, 17 from Lens.org). After removing duplicates, all records were screened by title and abstract to assess eligibility according to predefined inclusion criteria:

- (i) the study must discuss AI methods relevant to detection, monitoring, response, or investigation of CBRN or related threats;
- (ii) relevance to operational use cases of LEAs, security practitioners, or forensic and investigative purposes;
- (iii) publication date between 2024 and 2025.

Exclusion criteria included:

- (i) articles limited to medical or purely laboratory biomedical applications without a clear link to CBRN security;
- (ii) studies with no mention of AI techniques.

Two articles [3] [4] were declared ineligible as both are high-level risk editorials not describing operational AI/CBRN tools. The screening process yielded 12 eligible studies, which were further examined through narrative synthesis.

Figure 1 depicts the PRISMA 2020 flow diagram for the literature review.

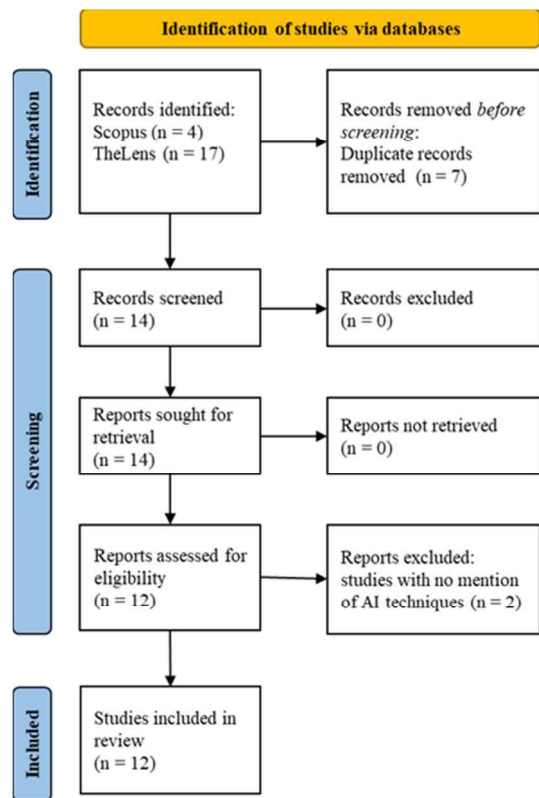


Fig.1 PRISMA 2020 flow diagram for the literature review

Findings were grouped thematically to identify potential applications of AI for CBRN threat detection, risk assessment, and operational support to LEAs.

These works fall into four three thematic clusters:

- 1) detection and sensing technologies [5] [6] [7],
- 2) preparedness and training [8] [9] [10],
- 3) governance and dual-use risk assessment [11] [12] [13] [14] [15].

In addition to these, two outlier was found about operational command-and-control architectures [16].

The first set of contributions demonstrates how AI can enhance real-time CBRN detection and environmental sensing. The EU-SENSE study explores the integration of sensor networks with AI-driven fusion algorithms to detect hazardous substances in airports, offering a concrete example of technology deployment in civil security settings [5]. Similarly, the review of unmanned aerial vehicles highlights how drones equipped with AI-based autonomy and CBRN sensors can extend reconnaissance capabilities while reducing responder exposure in contaminated areas [6]. Pálhalmi and Mező present an innovative AI-powered microscopy platform for airborne pathogen detection, demonstrating real-time classification of bioaerosols with direct relevance to LEA biodefense and environmental monitoring operations [7]. Together, these works underscore the potential of AI-enhanced sensor platforms to reduce time-to-detection, minimize personnel risk, and support rapid decision-making in field operations.

The second cluster highlights the role of AI in preparedness, training, and decision-support (simulation, analytic synthesis). Research by [8], the mixed-methods work

develops a CBRN preparedness assessment tool and operational response guidelines using NLP, sentiment analysis and unsupervised clustering to analyse expert interviews and literature. For LEAs, the work shows how AI content analysis can inform tabletop exercise design, consensus-building across agencies, and prioritisation of training and SOP updates. Complementary work [9] validates the use of text mining and dimensionality reduction techniques such as Principal Component Analysis (PCA) and t-distributed Stochastic Neighbor Embedding (t-SNE), to re-analyse disaster medicine experts' feedback, showing how AI can systematically identify consensus and capability gaps. A review on virtual reality training further argues that combining AI, human-computer interaction, and psychology can deliver adaptive, immersive simulations for CBRN exercises [10]. Collectively, these studies suggest that AI can help standardise after-action reviews, accelerate consensus-building across agencies, and provide scalable, immersive tools for enhancing readiness.

The third set of articles addresses the governance and dual-use risks of AI models in CBRN contexts, focusing on prevention of misuse. The work of Khlaaf et al. critiques current policy debates that overemphasise hypothetical risks while neglecting immediate military applications of foundation models for surveillance and targeting, raising concerns that are indirectly relevant to LEAs [11]. Barrett et al. propose the BRACE framework, which combines open benchmark testing and closed red-team evaluations to identify hazardous capabilities of foundation models, including those that could support toxic chemical design or cyber-biological attacks [12]. Barez et al. examine the limitations of machine unlearning in removing dangerous knowledge from AI systems, warning that recombination of benign knowledge could still regenerate harmful pathways [13]. Similarly, Uuk et al. report findings from an expert survey on mitigation strategies for systemic AI risks, recommending pre-deployment risk assessments, third-party audits, and incident reporting as the most effective safeguards [14]. The work on dual-use capabilities of concern of biological AI models [15] maps historic life-science dual-use thinking onto biological AI models and argues for pre-deployment evaluation that prioritises high-consequence capabilities (those enabling pathogen design or manipulation). For LEAs, the paper offers a practical risk taxonomy and recommends evaluation and access controls to reduce biosafety/biosecurity misuse risk.

These studies do not present field-ready tools but are directly relevant for LEA intelligence assessment units, procurement officers, and policymakers tasked with ensuring safe adoption of AI in sensitive domains.

The literature also provides insights into operational architectures for command and control (C2) that could inform LEA adoption of AI-enabled systems. A study on AI in military command and control illustrates how sensor webs, autonomous robotics, and algorithmic image analysis can be integrated into digitised C2 pipelines for improved situational awareness [16], lessons which can be adapted for civilian crisis management. Khlaaf et al. further caution against overlooking the near-term risks of foundation models repurposed for military surveillance or targeting, a concern that may equally apply to civil security operations [11]. These findings emphasise the importance of adapting tested military architectures for LEAs while ensuring strict human-in-the-loop oversight and legal compliance.

III. PATENTS REVIEW

Figure 2 depicts the PRISMA 2020 flow diagram for the patents review.

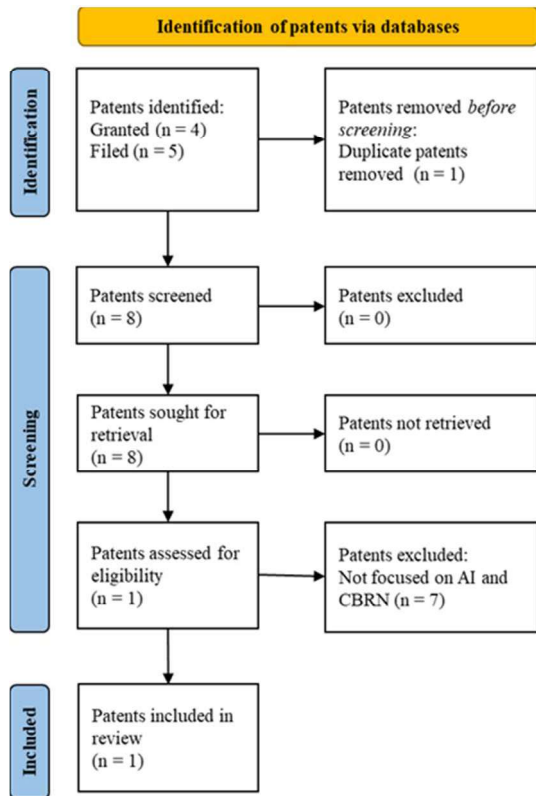


Fig.2 PRISMA 2020 flow diagram for the patents' review

The patents review included patents granted between January 2024 and September 2025 and was performed on the The Lens [2] patent database - through keyword search [*AI AND CBRN*] in *all fields*. The search resulted in 4 patents.

Three patents [17] [18] [19] were ineligible for analysis because they were not focused on AI nor on CBRN.

One patent [20] was focused on CBRN but not on AI. It regards the invention of a “*Maskless respiratory and eye protection device for aerosols and vapors*” including CBRN contaminants, but there is no mention of Artificial Intelligence, making it ineligible for analysis. Thus, the review of granted patents did not lead to useful results.

A second patents review was performed on patent applications (application filed, but not granted yet) between January 2024 and September 2025 on the The Lens [2] patent database - through keyword search [*AI AND CBRN*] in *all fields*. The search resulted in 4 patents.

Three patents [21] [22] [23] were ineligible for analysis because they were not focused on AI and/or CBRN.

The fourth patent “*Artificial Intelligence-based threat prediction system and method for CBRN*” [78] describes an AI-driven system for real-time incident threat analysis, particularly useful in crisis scenarios involving chemical, biological, radiological, or nuclear (CBRN) threats.

The system leverages machine learning models to process sensor data, geospatial intelligence, and historical incident

patterns, dynamically adapting recommendations for first responders and command centers. The platform integrates decision-support dashboards and AI-assisted triage tools to prioritize response actions. It is designed for use in multi-agency emergency environments, making it highly suitable for LEAs, civil protection units, and defense organizations.

The patent emphasizes interoperability and scalability across different data sources, which could improve situational awareness and coordination during CBRN emergencies.

IV. DISCUSSION

The literature review illustrated the breadth of AI applications in CBRN threat management, with clear implications for the operational needs of LEAs. From robotic systems that autonomously explore contaminated zones to software that simulates complex threat environments for training purposes, these innovations enhance both preparedness and response efficiency.

For LEAs, the relevance of such technologies lies not only in their technical sophistication but in their potential to address longstanding capability gaps. Traditional methods for detecting and assessing CBRN threats are often slow, hazardous, or dependent on scarce human expertise. AI, by contrast, offers scalable solutions capable of real-time analysis, pattern recognition, and autonomous decision support.

However, integrating AI into security workflows is not without challenges. Questions remain about the interoperability of new systems with existing infrastructure, the explainability of AI-driven decisions in high-stakes scenarios, and the ethical implications of automating elements of threat detection and response. Moreover, the deployment of such technologies requires training, institutional buy-in, and rigorous validation in operational environments—none of which can be overlooked.

In addition to this, an emerging concern among practitioners is the dual-use nature of some AI innovations, especially those in open-access formats. Tools designed for cybersecurity or industrial use can potentially be repurposed by malicious actors to evade detection or amplify threats. This underscores the need for continuous technology monitoring and cross-sector collaboration among R&D entities, policymakers, and operational agencies.

Finally, it is paramount to highlight the importance of structured technology horizon scanning as a method. By proactively identifying and assessing AI tools in the early stages of their technological lifecycle, LEAs can better anticipate disruptive shifts, inform procurement decisions, and engage with developers to shape technology for public good.

V. IMPLICATIONS FOR LAW ENFORCEMENT AGENCIES AND PRACTITIONERS

The reviewed technologies and approaches demonstrate growing potential to reshape how law enforcement agencies (LEAs) and intelligence practitioners detect, prevent, and respond to emerging threats.

From an operational standpoint, the integration of AI-based systems into surveillance, reconnaissance, and threat assessment platforms holds immediate relevance. Technologies such as AI-powered biosensors, predictive

analytics for CBRN events, and unmanned systems with modular payloads offer not just theoretical advancements but tangible tools for use in the field.

Importantly, the deployment of AI in CBRN detection is not solely about speed or automation; it introduces new layers of adaptability and risk management. For instance, intelligent microscopy platforms and mobile detection kits enable LEAs to operate with greater autonomy in dispersed environments, reducing dependency on centralized labs and allowing faster decision-making in critical moments.

Practical integration still demands more than technological readiness. For these systems to be actionable, LEAs will need to address interoperability with existing platforms, standardize evaluation protocols, and train personnel in systems thinking and ethical risk assessment. Crucially, many of these technologies are dual-use in nature, making governance frameworks and cross-border regulatory cooperation essential.

The findings reinforce the need for specialized units within agencies tasked with technology scanning, AI deployment strategy, and continuous dialogue with developers and EU security research bodies. These structures would enable agencies to not only adopt but also adapt technologies to context-specific needs—bridging the gap between innovation and daily operational requirements.

VI. CONCLUSIONS AND RECOMMENDATIONS

Artificial Intelligence is poised to play a transformative role in enhancing the capabilities of LEAs in the detection, prediction, and response to CBRN threats.

The technologies reviewed—from AI-enabled unmanned systems to predictive platforms and bio-detection tools—reflect a robust innovation pipeline with clear relevance to real-world security challenges.

Taken together, the evidence base indicates that AI can strengthen LEA responses to CBRN incidents across the full cycle of detection, preparedness, governance, and operational coordination. However, the review also highlights a divide between research that offers tangible, field-ready technologies (e.g. EU-SENSE, UAV reconnaissance, AI microscopy) and research that provides strategic-level governance frameworks (e.g. BRACE, dual-use taxonomies, unlearning limitations).

Bridging this gap will require sustained pilot testing, cross-agency exercises, and procurement policies that integrate both technological innovation and governance safeguards.

Indeed, effective integration of AI into law enforcement operations requires more than technological adoption. It calls for strategic alignment between developers and end-users, comprehensive testing and validation in controlled environments, and robust training protocols. Furthermore, ethical and legal frameworks must evolve in tandem to address concerns related to autonomy, accountability, and data use.

The horizon scanning activities conducted within WP5 of the NOTIONES project, through collaborative Working Groups, have demonstrated the value of early and sustained engagement with technological trends. By leveraging open-source intelligence and expert analysis, these efforts help ensure that LEAs remain informed, adaptive, and proactive in

the face of emerging threats. Continued investment in such interdisciplinary initiatives will be essential to harness the full potential of AI for public safety.

ACKNOWLEDGMENT

This work was supported by the project NOTIONES, that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853.

The objective of the NOTIONES (*iNteracting netwOrk of iTelligence and securItY practitiOners with iNdustry and acadEmia actorS*) project is to build a pan-European network of practitioners from the security and intelligence services, from the Industry – including SMEs – and from the Academia, with the objective to enhance their interaction and identify specific technology and innovation requirements, needs, expectations and gaps.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

REFERENCES

- [1] Elsevier, «Scopus,» 30 September 2025. [Online]. Available: <https://www.scopus.com>.
- [2] Cambia, «The Lens,» 30 September 2025. [Online]. Available: <https://www.lens.org/>.
- [3] R. C. Armitage, «Artificial General Intelligence and Its Threat to Public Health,» *Journal of Evaluation in Clinical Practice*, vol. 31, n. 6, 2025.
- [4] K. Carlson, «Highlights of the Issue,» *SuperIntelligence - Robotics - Safety & Alignment*, vol. 1, n. 1, 2024.
- [5] M. Gawlik-Kobylińska, M. Urban e G. Gudzbeler, «The EU-SENSE System as a Tool to Support Airport Security,» *Lecture Notes in Networks and Systems*, 2025.
- [6] P. Gaurav, P. Manimaran, M. Ashutosh e S. Aditya, «Unmanned aerial vehicles: An inevitable armamentarium in Armed Forces Medical Services,» *Medical Journal Armed Forces India*, 2025.
- [7] J. Pálhalmi e A. Mező, «AI-Powered Microscopy Platform for Airborne Biothreat Detection,» in *Paradigms on Technology Development for Security Practitioners*, Springer Nature Switzerland, 2024, p. 117–127.
- [8] H. Farhat, , G. Ciottonne, G. Alinier, A. M. Batt, J. Laughton , M. Helou, N. Bajow e M. B. Dhiab, «Empowered Analysis Using Artificial Intelligence Algorithms for a New Era of Health Sector Preparedness and Response Strategies to Chemical, Biological, Radiological, and Nuclear Major Incidents in the Middle East and North Africa,» *Prehospital and Disaster Medicine*, vol. 40, n. S1, 2025.
- [9] H. Farhat, M. Helou, N. Bajow, W. Abougallala, L. AL-Shaikh, J. Laughton, M. B. Dhiab e G. Alinier, «Validating Disaster Medicine Experts' Feedback Outcome Using Artificial Intelligence Computing Techniques,» *Disaster Medicine and Public Health Preparedness*, vol. 18, 2024.
- [10] R. Kumar Rai , D. Kumar, S. Shekhar Jha, R. Singh Kanwar e R. Bansal, «Reviewing Virtual Reality's Potential in CBRN Training: Synergizing AI, HCI, and Psychology for Immersive Preparedness,» *Lecture Notes in Computer Science*, pp. 440–453, 2025.

- [11] H. Khlaaf, S. M. West e M. Whittak, «Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting», arXiv (Cornell University), 2024.
- [12] A. M. Barrett, K. Jackson, E. R. Murphy, N. Madkour e J. Newman, «Benchmark Early and Early and red team often», UC Berkeley CLTC White Paper, 2024.
- [13] F. Barez, T. Fu, A. Prabhu, S. Casper, A. Sanyal, A. Bibi, A. O'Gara, R. Kirk, B. Bucknall, T. Fist, L. Ong, P. Torr, K.-Y. Lam, R. Trager, D. Krueger, S. Mindermann, J. Hernandez-Orallo, M. Geva e Y. Gal, «Open Problems in Machine Unlearning for AI Safety», Preprint; arXiv (Cornell University), 2025.
- [14] R. Uuk, A. Brouwer, T. Schreier, N. Dreksler, V. Pulignano e R. Bommasani, «Effective Mitigations for Systemic Risks from General-Purpose AI», Preprint Open Access Open Access arXiv (Cornell University), 2025.
- [15] J. Pannu, D. Bloomfield, R. MacKnight, M. S. Hanke, A. Zhu, G. Gomes, A. Cicero e T. V. Inglesby, «Dual-use capabilities of concern of biological AI models», PLoS computational biology, vol. 21, n. 5, 2025.
- [16] Հայկական բանակ / Armenian Army, «Artificial intelligence: new uses and impacts on military command and control», 2024.
- [17] K. Inc, «Unmanned system maneuver controller systems and methods». Brevetto US 12242284 B2, March 2025.
- [18] P. K. Inc, «Maskless respiratory and eye protection device for aerosols and vapors including chemical, biological, radiological, and nuclear (CBRN) contaminants». Brevetto US 12343573 B1, July 2025.
- [19] P. L. Llc, «Smart military communication system and method». Brevetto US 12261953 B2, March 2025.
- [20] T. U. S. o. A. a. R. b. t. S. o. t. Army, «Dynamic graphical user interface generation and update based on intelligent network communications». Brevetto US 11960710 B1, April 2024.
- [21] L. I. Inc, «Systems And Methods For Temperature Controlled Biologics Storage, Delivery, Integrity, And Security». Brevetto US 2025/0170021 A1, May 2025.
- [22] X. R. E. Ltd, «Systems And Methods For Managing Unmanned Vehicle Interactions With Various Payloads». Brevetto US 2025/0028335 A1, January 2025.
- [23] U. Arizona, «Plant-Based Extracellular-Like Vesicles For Biotherapeutic Applications». Brevetto WO 2024/155941 A1, July 2024.
- [24] N. Hyunwoo, K. Minjae, S. Jungjae e L. Byuncheon, «Artificial Intelligence-based threat prediction system and method for CBRN». US Brevetto US 2025/0028932 A1, 23 January 2025.