



جامعة ناربغ العربية
للعلوم الأمنية
NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
١٩٧٨ عاصم



1st Artificial Intelligence Forum for Law Enforcement Uses

Forum Report
(Co-organized by NAUSS and UNICRI)

4 – 5 October 2023



Foreword by NAUSS

As the recognized scientific body of the Arab Interior Ministers Council and a distinguished regional institution, Naif Arab University for Security Sciences assumes a central role in the development of expertise and the progression of security-related decision-making across the Arab region. With its recently unveiled five-year strategic plan for 2023-2028, the university has taken a forward-thinking approach by prioritizing the integration of artificial intelligence within the law enforcement domain, cementing its position as a pioneer in acknowledging the paramount importance of this field.

In an era defined by the transformative power of technology, the Arab region is navigating the complex landscape of law enforcement with a growing concern about Artificial Intelligence (AI). Our mission at the Center of Excellence in Cybercrime and Digital Forensics (CoECDF) is to serve as a beacon of knowledge and expertise in the realm of AI applications for law enforcement. As we stand at the intersection of tradition and innovation, we recognize the imperative of embracing AI to address the evolving challenges and opportunities in law enforcement effectively. The adoption of AI in our region reflects our commitment to staying at the forefront of advancements in policing while acknowledging the need to adapt our strategies to the demands of the digital age.

This report represents a significant milestone in our continuous journey toward harnessing the potential of AI to enhance security, safety, and justice in our communities. It encapsulates our collective commitment to advancing the field of AI in law enforcement, emphasizing the importance of responsible and ethical use while maximizing its potential to safeguard our societies. It serves as a valuable resource for law enforcement agencies, policymakers, and all those engaged in the pursuit of a safer and more secure Arab region.

We extend our appreciation to our partners at UNICRI who have co-organized this forum, and we are dedicated to continued research and collaboration, adapting to the ever-changing landscape of technology and security. Together, we aim to shape a brighter, more resilient future for law enforcement in the Arab region.

Dr. Abdulrazaq Almorjan

Executive Director,

Center of Excellence in Cybercrimes & Digital Forensics (CoECDF),

Naif Arab University for Security Sciences (NAUSS).





Foreword by UNICRI

Artificial intelligence (AI) is undoubtedly one of the key technologies of our times. Signs of its transformative potential are already being seen in diverse fields, from agriculture to commerce, healthcare and entertainment - all across the globe. Indeed, although we continue to strive to bridge the digital divide between countries and regions, AI is truly a technology of global relevance. We are all on this journey together to understand, explore, and benefit from AI.

At the same time, certain parts of the world hold a specific and inseparable bond with AI. The Arab world is one that holds a uniquely prominent place in the story of AI. The rich historical and cultural heritage of this region have left an enduring imprint on mathematics and algorithmic principles, which constitute the very foundations for the field of AI. Indeed, Arab scholars like Muhammad al-Khwarizmi and Hasan Ibn al-Haytham are, in many ways, among the founding fathers of the field of AI. And the influence of this region continues to be seen today through words of Arabic origin, such as 'algorithm' itself.

For this reason, we are particularly proud to have partnered with the Naif Arab University for Security Sciences (NAUSS) and its Center of Excellence in Cybercrime and Digital Forensics (CoECDF) to convene the first AI Forum for Law Enforcement Uses for the Arab region. This forum brought together experts and practitioners from across the Arab world to collectively develop our knowledge and understanding of the application of AI in a law enforcement context and the ethical and human rights challenges. With this AI Forum, we went back to the very roots of AI as we carve out our path forward.

UNICRI has for many years now explored the promise and pitfalls of traditional information communications and technology and, more recently, emerging technologies in the context of justice, security, and the rule of law. In fact, our 2023-2026 Strategic Programme Framework identifies promoting the responsible use of new and emerging technologies to address crime and exploitation as one of the Institute's key priorities. In line with this, our Centre for Artificial Intelligence and Robotics in The Hague has been at the forefront of the discourse around the use of AI in the context of law enforcement, exploring how we define, institutionalize, and foster responsible AI innovation in policing. Our recently released Toolkit for Responsible AI Innovation in Law Enforcement is one of our key contributions to this field.

We hope that this report, which is the output of the inaugural AI Forum for the Arab region, will serve as another valuable resource for law enforcement agencies throughout the Middle East, North Africa and beyond. Yet it is just a stepping stone in our journey toward. We must continue to connect and work together to understand the potential of AI in the law enforcement community and, crucially, to understand and take affirmative action to ensure that its use reflects the principles for responsible and human rights compliant AI innovation in law enforcement.

Irakli Beridze

Head of the Centre for Artificial Intelligence and Robotics

United Nations Interregional Crime and Justice Research Institute (UNICRI)

Abbreviations & Acronyms

NAUSS	Naif Arab University for Security Sciences
CoECDF	Center of Excellence in Cybercrime & Digital Forensics
UNICRI	United Nations Interregional Crime and Justice Research Institute
INTERPOL	International Criminal Police Organization
UNCCT/UNOCT	United Nations Counter-Terrorism Centre / United Nations Office of Counter-Terrorism
KSA	Kingdom of Saudi Arabia
MOI	Ministry of Interior
LSE	London School of Economics
UCL	University College London
AI	Artificial Intelligence
LE	Law Enforcement
LEAs	Law Enforcement Agencies
NLP	Natural Language Processing
LLMs	Large Language Models
R&D	Research & Development
IoT	Internet of Things
OSINT	Open-Source Intelligence
ChatGBT	Chat Generative Pre-Trained Transformer



Acknowledgments

The inaugural Artificial Intelligence Forum for Law Enforcement Uses for the Arab region was a collaborative effort organized and co-hosted by the Centre of Excellence in Cybercrimes and Digital Forensics (CoECDF), Naif Arab University for Security Sciences (NAUSS), and the Centre for AI and Robotics at the United Nations Interregional Crime and Justice Research Institute (UNICRI). This report has been prepared by NAUSS with the support and input of UNICRI.

We express our sincere appreciation to His Highness Prince Dr. Bandar bin Abdullah bin Mishari Al Saud, Assistant Minister of Interior for Technology Affairs, for their patronage and support. Furthermore, we extend our heartfelt thanks to Dr. Abdulmajeed Al-Banyan, the President of NAUSS, for his steadfast support in hosting this international event. We would also like to express our gratitude to all speakers, and attendees who enriched the forum with their participation.

Disclaimer

The opinions, findings, conclusions and recommendations expressed herein are those of the experts and participants of the inaugural Artificial Intelligence Forum and do not necessarily reflect the views of the Naif Arab University for Security Sciences (NAUSS), United Nations Interregional Crime and Justice Research Institute (UNICRI) or the United Nations itself.

Copyright © 2023 Naif University Press

Naif University Press reserves all rights related to all or part of the content, and the rights to translate, return, transmit, store, retrieve or electronically modify information related to this content. The author acknowledges that the information contained in this content is true and accurate since its date and guarantees that any errors that may have occurred will be corrected, whether intentionally or unintentionally.

<https://doi.org/10.26735/ZCPK3390>

Contact

For further details regarding this report, contact the Center of Excellence in Cybercrimes and Digital Forensics at coecdf@nauss.edu.sa



Table of Contents

Foreword (NAUSS).....	3
Foreword (UNICRI).....	5
Abbreviations & Acronyms	6
Acknowledgments	7
Executive Summary	10
Key Findings	12
1. Introduction.....	15
2. Problem Definition	15
3. NAUSS Work in the Area of Artificial Intelligence	16
4. 1st Artificial Intelligence Forum for Law Enforcement Uses	17
4(a). Objectives.....	18
4(b). Themes & Sub-themes.....	18
4(c). Format, Activities & Participants	19
5. Findings from the 1st AI Forum for Law Enforcement Uses	20
5(a). High-level Panel Discussion on “Harnessing AI in Law Enforcement”	20
5(a1). Key Findings of High-Level Panel Discussion	22
5(b). Theme 1: AI-based Capabilities in Law Enforcement	23
5(b1). Key Findings of Theme 1	31
5(c). Theme 2: AI Challenges for the Arab Region	32
5(c1). Key Findings of Theme 2.....	40
5(d). Theme 3: The Malicious Uses of AI	40
5(d1). Key Findings of Theme 3	49
5(e). Theme 4: Responsible AI Innovation and Building Capacities for Responsible Use.....	50
5(e1). Key Findings of Theme 4	53
6. Conclusion	54
7. Recommendations	56
References:.....	59
Appendix 1	60




Executive Summary

In response to the global proliferation of artificial intelligence (AI), the widespread discourse around the potential legal and ethical concerns surrounding its application in law enforcement, and the ever-looming potential for its malicious use by criminals and terrorists, NAUSS and UNICRI jointly launched the inaugural AI Forum for Law Enforcement Uses focusing on the Arab region. The forum convened law enforcement experts, academic scholars, and industry professionals from across the globe, intending to foster a comprehensive dialogue on AI in the context of the Arab region. Through this concerted effort, the forum sought to gain a deeper understanding of the prevailing AI landscape, foster responsible AI adoption, and confront challenges related to its implementation in the Arab region. This collaborative endeavour was organized around four central themes: (1) Exploring AI-Based Capabilities in Law Enforcement, (2) Addressing AI Challenges Specific to the Arab Region, (3) Examining the Potential for Malicious AI Applications, and (4) Promoting Responsible AI Innovation and Capacity Building for Ethical Use.

This report contains recommendations extracted from the Forum presentations, use cases, group discussions, and survey responses for the establishment a foundational framework for the utilization of AI within the realm of law enforcement, mainly focusing on its implications and applications within the Arab countries. This document seeks to provide a pioneering perspective on the role and significance of AI in law enforcement in Arab nations. By highlighting the findings and insights contained within, it aims to set the stage for a more informed and strategic approach to incorporating AI technologies into law enforcement practices. Ultimately, this report serves as a valuable resource for all stakeholders in the field, offering a blueprint for the responsible and innovative integration of AI solutions in the Arab law enforcement sector. A detailed list of all the forum's use cases is available in Appendix-1.

The report's key findings highlighted critical challenges in the adoption and integration of AI within law enforcement. These challenges encompass several key areas, including the lack of resources, technological infrastructure, data quality and availability, regulatory frameworks, skills, specialized training & education, regional and international collaboration, institutional openness, and established guidelines for responsible AI use to all be relevant in the context of Arab law enforcement agencies. Participants also underscored during the Forum the increasing diversity and application of malicious AI applications, sounding alarms around the growing accessibility of the technology and the rapidly evolving threat landscape. Lastly, the findings also highlighted the participant's awareness of the responsible uses of AI, yet emphasized the urgent requirement for enhanced training and education on ethical considerations, privacy issues, and bias concerns.



The recommendations derived from the insights and critical findings of AI experts in law enforcement, industry, and academia offer a comprehensive guide for Arab countries as they navigate the evolving landscape of AI applications within the law enforcement sector. They emphasize the proactive integration of AI technologies in law enforcement agencies, highlighting the need to bridge the gap between recognizing AI's potential and effectively implementing it in practice. The implementation, however, must be paired with a robust legal framework with clear guidelines and regulatory frameworks, which are essential to ensure the ethical and responsible deployment of AI within law enforcement. These guidelines serve not only to promote responsible use but also as safeguards against potential misuse, ultimately fostering public trust in AI technologies used in law enforcement.

Ensuring budget flexibility is crucial to expanding AI use in law enforcement, allowing broader adoption and getting its benefits. Investing in AI research and training resources keeps law enforcement up-to-date with technology, helping tackle new challenges and seize opportunities. Emphasizing training programs is key to filling knowledge gaps and enabling successful AI integration in law enforcement. Also, encouraging collaboration and knowledge sharing among law enforcement agencies is vital. Breaking down barriers to exchange knowledge fosters collaboration and sharing AI best practices. Addressing data availability challenges is crucial, as data is essential for AI applications. Promoting data collection and sharing initiatives within the law enforcement community is encouraged.


In summary, the recommendations present a comprehensive strategic framework for Arab nations, steering them toward the responsible, efficient, and ethical use of AI within the realm of law enforcement. They not only address the potential benefits of AI but also tackle the various challenges and considerations linked to its integration.




Key Findings

The key findings of AI Forum are:

- i. Training, Education & Skills:** AI literacy in the region is classified as rudimentary to intermediate, according to survey findings - inadequate skills and training within law enforcement agencies for AI adoption pose a significant issue. While 90% of participants believe AI will enhance the precision and efficiency of operations, less than 20% have received training in AI-based tools. With AI's growing importance in policing, law enforcement personnel need improved AI literacy. A survey found that 43% of participants believe improving "Technical Capabilities & Knowledge" is a top priority, with 70% focusing on AI tools, software, applications, data handling, and privacy protection. Other topics for future training included drones, robotics, and specific AI applications such as predictive policing.
- ii. Research Areas:** In implementing AI in law enforcement, rigorous research is vital, especially in critical areas with significant national and international security implications. Participants emphasized the importance of research in border security (30%), surveillance, counter-terrorism (20%), cybercrime detection and prevention (20%), and the development of drones, robotics, and autonomous systems (15%) and data sovereignty and localization (15%).
- iii. Resources:** Law enforcement agencies face significant hurdles when trying to incorporate AI into their operations due to budget limitations and resource constraints. Creating and maintaining AI systems, as well as ensuring their responsible use, necessitate substantial financial commitments for hardware, software, training, and upkeep, which can be impractical for agencies with tight budgets and other financial priorities.
- iv. Regulation & Guidelines:** The absence of agreed-upon AI regulations and guidelines in law enforcement creates gaps, hindering consistent and ethical integration across diverse jurisdictions. More than 75% of participants indicated the absence of any frameworks, impeding standardized approaches, data-sharing, and cross-border collaboration. A comprehensive approach involving policy, regulation, transparency, data security, and quality management is urgently needed.
- v. Job Roles:** There is a critical necessity for creating job roles and attract the relevant expertise within law enforcement centred on AI, its use as well as the related legal and ethical elements of its use. Survey results revealed that the most pressing functions, in order of priority, as identified by 90% of participants, are AI engineers, data analysts, machine learning engineers, data scientists, and data engineers. These roles are pivotal in unlocking the full potential of AI technology and facilitating its effective integration within law enforcement agencies.

- 
- vi. Collaborations:** The lack of collaboration among law enforcement agencies, both regionally and globally, in AI integration poses challenges. To fully benefit from AI for crime prevention and investigation, sharing knowledge and best practices is vital. However, the lack of seamless cooperation hampers the development of standardized methods, cross-border collaboration and data availability and sharing, highlighted by participants as one of the primary hurdles in AI adoption.
- vii. Malicious AI:** The evolving AI threat landscape and its malicious applications are a significant concern for law enforcement, academia, and industry experts. 98% of participants believe that criminals are likely to use AI for malicious purposes. 80% highlighted deepfakes as their primary concern, followed by LLMs and Generative AI for malicious purposes. Within the Arab world, regional law enforcement experts highlighted deepfakes, drones, terrorism, and fraud as the most common examples of AI-enabled threats they've encountered. Of the attending organizations, less than 40% have implemented tools for detecting or preventing malicious uses of AI, with over 75% requesting the expansion of research and training in cybersecurity expertise, 62.5% in data analysis, and 56% in threat intelligence and machine learning. Regional future concerns of malicious AI uses were underscored as deepfakes, AI-generated disinformation, and attacks on critical infrastructure. This growing threat emphasizes the need for collaboration and innovation to combat AI-related criminal activities effectively.
- viii. Responsible AI:** Law enforcement's use of AI requires balancing legal and ethical concerns. Lawfulness, the minimization of harm, human autonomy and good governance are key to responsible use of AI in law enforcement and, in line with this, agencies should strive to enhance transparency, accountability, and privacy safeguards. Over 66% of attendees reported an absence of institutional guidelines for responsible AI, and 66% of no academic or educational programs on responsible AI. Under responsible use, participants expressed their needs for
- Training: AI fundamentals, ethics, data privacy & security, bias detection & mitigation,
 - Research: algorithm transparency, AI-enhanced investigation protocols, incident response & accountability, data privacy & security, bias & mitigation, and detection & auditing,
 - Skills: data handling, risk assessment, AI tools, ethical awareness, legal & regulatory knowledge, transparency & accountability.

This ensures that law enforcement agencies protect data, prevent misuse, and address biases while using AI for public safety.



ix. Use cases: Improving the understanding of the range and scope of AI use cases in law enforcement is vital to ensure that law enforcement can explore this technology to its maximum potential. In this regard, continued dialogue and exchange around uses cases is needed. During the Forum, several pertinent examples of AI **use cases** for law enforcement were discussed, including:

- a. The Integrated Fan Journey at the FIFA World Cup - Qatar, enabled by AI,
- b. AI for Large Event Management and Public Safety,
- c. AI-Enabled Social Network Analysis Capabilities for Counter-Terrorism,
- d. AI-Enabled Phishing Websites Detection Tool,
- e. AI-Drone Object Detection and Surveillance.



1. Introduction

Artificial Intelligence (AI) is at the forefront of a technological revolution that is reshaping industries across the globe. At its most fundamental basis, AI is centered around the development of computer systems capable of performing specific tasks that would normally require human intelligence, such as understanding natural language, recognizing patterns, and making predictions. AI is a broad field in the domain of computer science and contains a broad range of technologies, techniques and subfields such as machine learning and deep learning.


In today's interconnected world, industries of all kinds are leveraging the power of AI to gain a competitive edge, improve efficiency, and drive innovation. AI is being positioned as a driving force behind the Fourth Industrial Revolution, affecting sectors as diverse as healthcare, transportation, finance, retail, agriculture, and law enforcement (McKinsey & Company, 2022).

AI plays a pivotal role in modern law enforcement, offering a wide range of tools and capabilities indispensable for maintaining public safety and ensuring efficient, data-driven policing (Chiancone, 2023). AI-based systems can analyze huge amounts of data to identify patterns and anomalies, aid in identifying hot spots for criminality and facilitating law enforcement to allocate resource appropriately. Facial recognition technology can support in the process of the identification of suspects, while natural language processing can help process large volumes of text-based evidence and improve investigative efficiency. Moreover, AI-based solutions can assist in real-time monitoring of security cameras, responding to emergencies, and automating routine administrative tasks, allowing law enforcement agencies to focus their resources on critical tasks and ultimately enhancing their ability to protect communities while upholding the principles of accountability and fairness.

2. Problem Definition

Recent developments in AI have significantly expanded its application across various industries, including law enforcement. Studies undertaken by the United Nations Interregional Crime and Justice Research Institute (UNICRI) and other international research bodies have shown that, much like the other sectors, law enforcement agencies (LEAs) worldwide have taken note of the potential of AI and begun to take their first steps with AI within the recent decade.

A transformative technology with immense potential, AI is increasingly being utilized to support the work of LEAs by enhancing capabilities through facial recognition, natural language processing (NLP), crime pattern analysis, cyber-attack detection and response, and more. Its deployment for law enforcement purposes is, however, sensitive and controversial. Because of the swift and recent growth of AI technology, regulatory frameworks have struggled to keep pace with advancements, resulting in many LEAs mainly operating in a sensitive domain without frameworks or guidance from a regulatory perspective (UNICRI, 2019). Consequently, there is a heightened risk of unintended



consequences due to bias, inaccuracies and accountability gaps, as well as privacy infringements, all of which contributes to eroding community trust.

Coupled with these challenges is the increasing adoption of AI for malicious uses (UNOCT, 2021). The threat of AI-enhanced attacks and tactics, such as deepfake content, cyberattacks, malware, social engineering, surveillance, etc., has raised alarms on all fronts. Between January and February of 2023, researchers observed a 135% increase in “novel social engineering” attacks, corresponding to the weaponization of generative AI and the widespread adoption of ChatGPT (Darktrace, 2023) Understanding these new criminal capabilities and challenges is critical for LEAs to ensure their safety and security.

The NAUSS-UNICRI convened Forum intended to provide a platform for law enforcement professionals, industry experts, and academia from both the Arab region and globally to come together, exchange knowledge, and explore the applications of AI in law enforcement responsibly, and exchange use cases and best practices in addressing the rise of malicious uses of AI - spotlighting the leading role of the Arab Region in AI.

3. NAUSS Work in the Area of Artificial Intelligence

With a vision to become the leading center for AI in Law Enforcement, the NAUSS Artificial Intelligence Lab (NAIL) aims to position itself to support LEA in embracing AI technology and shape the future of policing in the region by providing relevant education, training consultancy, and conducting applied research & development. Areas of focus under the umbrella of AI include Financial Crime, Cybercrime, Cyber-enabled Crime, Terrorism, and Public Safety.

The NAIL's strategic objectives, as announced at the forum, are:

- i. Specialized Human Capacity in AI for Law Enforcement
 - Develop specialized human capacity through education, training & events,
 - Focus on critical areas for capacity building: Machine Learning, Computer Vision, Natural Language Processing, and responsible uses of AI,
 - Develop a new AI workforce framework for the future of policing.
- ii. R&D of innovative AI-based solutions for law enforcement:
 - Perform applied research and development of innovative AI-based solutions for law enforcement,
 - Develop a technology incubation facility to support innovation for AI-based security/future policing,
 - Identify & define areas of common interest through stakeholder collaboration.

iii. Support data-driven decision-making & provide consultancy to stakeholders:

- Support LEAs' decision-making through Technical Reports, Technological Roadmaps, Regulations and policy.
- Provide consultancy to LEAs.

International partnerships in the Lab include INTERPOL, UNICRI, and UNCCT. Under the INTERPOL & UNICRI collaboration is the development of the following training programs:

- AI Workforce Framework for Future Policing,
- AI for LEAs Professional Training Programs,
- Capacity-building in terms of Responsible AI Innovation in LE,
- Impact Assessment Tool for AI & Drones

In terms of expected outcomes, the NAIL seeks to:

- i. Produce subject matter experts in AI and robotics for LEAs.
- ii. Develop AI-based tools for specific policing.
- iii. Produce technical reports for decision-makers.
- iv. Provide advanced consultancy services to LEAs.
- v. Host state-of-the-art laboratories and HPC facilities for R&D purposes.
- vi. Become the reference point for Arab countries on matters of AI in LE.

4. 1st Artificial Intelligence Forum for Law Enforcement Uses

The main goal of this Forum in its first edition was to provide a platform for law enforcement professionals, industry experts, and academia from both the Arab region and globally to come together, exchange knowledge, and explore the applications of AI in law enforcement responsibly, and exchange use cases and best practices in addressing the rise of malicious uses of AI. The Forum aimed to foster discourse and collaboration around the opportunities and challenges of AI in law enforcement and facilitate the sharing of knowledge and expertise around emerging topics and trends. The Forum sought to support regional law enforcement professionals to effectively and responsibly use AI to enhance their operational capabilities, improve public safety, and combat malicious uses of AI.



4(a). Objectives


Recognizing the broad scope of the potential areas of interest, the Forum objectives were:

- To explore emerging trends and developments in AI technologies relevant to law enforcement.
- To identify policing use cases and best practices for crime detection and prevention.
- To understand emerging threats related to the malicious use or misuse of AI.
- To advance the responsible use of AI in law enforcement, addressing ethical and legal issues.
- To understand the need for law enforcement to integrate AI-based technologies.

4(b). Themes & Sub-themes

The main theme for the Forum was to highlight the roles of AI for law enforcement in Arab countries to enhance its policing operations in a responsible and effective manner. The Forum was organized into four sub-themes, which are as follows:

- **AI-based Capabilities in Law Enforcement:** Use of AI technology for law enforcement in video, audio, natural language processing, and resource optimization in policing. By leveraging AI algorithms, law enforcement organizations can make knowledge-driven decisions to improve crime detection and prevention. Specific topics included Visual Processing & Surveillance, Audio Processing & Voice Profiling, Resource Optimization for Hot-Spot Mapping, Allocation & Scheduling, and Natural Language Processing (NLP) for social media analysis. This theme aimed at better understanding the application of AI in law enforcement.
- **AI Challenges for the Arab Region:** Each agency, country, and region faces challenges in terms of the development and deployment of AI. The Arab region itself faces unique challenges, distinct from other areas. This theme focused on understanding the specific challenges the Arab regions face and the ways and means agencies seeking to deploy AI can overcome these challenges. This will include issues such as AI-based tools using Arabic languages, laws & regulations, public acceptance, and datasets. It also highlighted specific AI use cases being explored to address particular threats in the Arab region.
- **Malicious Use of AI:** Generative AI technologies, such as Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), have shown remarkable progress in synthesizing realistic images, videos, audio, and text. Although powerful tools for creative applications, they can also be exploited for malicious purposes, causing significant threats to society, such as deepfake videos and fake news. This theme explored how AI can and is used maliciously and what measures can be taken to address these threats.

- 
- **Responsible AI Innovation & Building Capacities for Responsible Use:** Responsible AI innovation consists of integrating AI systems into law enforcement work in ways that align with policing principles and are ethically sound and compliant with human rights and other applicable laws. This theme explored what this entails and how LEAs can enhance their readiness to use AI responsibly and build capacities to implement responsible AI innovation.

4(c). Format, Activities & Participants

The event took place entirely in person over the course of two days, from October 4th to 5th, 2023, on the NAUSS Campus in Riyadh, the Kingdom of Saudi Arabia.

The forum hosted the following activities:

- i. A high-level panel discussion on “Harnessing AI in law enforcement for Arab Countries.”
- ii. E-poster Presentations on “AI use cases in Arab Countries.”
- iii. Group Discussion I: “AI Challenges & Opportunities for Law Enforcement in the Arab Countries”
- iv. Group Discussion II: “Dark Side of AI for Malicious Activities in the Arab Countries”
- v. Responsible AI Toolkit Workshop: “Putting Responsible AI Innovation into Practice - Scenario-based discussion.”

This event brought together a total of 130 participants, including law enforcement experts from 18 different countries, global academic and industry experts, and members of UNICRI, UNCCT, and INTERPOL.



5. Findings from the 1st AI Forum for Law Enforcement Uses

5(a). High-level Panel Discussion on “Harnessing AI in Law Enforcement”

To inaugurate the forum, a high-level panel discussion convened experts and stakeholders from various sectors to deliberate on the overarching theme: “The Future of AI in Law Enforcement.” Prominent figures from government bodies, law enforcement agencies, international organizations, the private sector and academia spearheaded the conversation, addressing the pivotal role of AI and its application in law enforcement.

From an international law enforcement perspective, a member from INTERPOL’s Responsible AI Laboratory spoke about the current state of AI use in law enforcement. They confirmed that AI has begun to be integrated into many components of law enforcement activity; however, they stressed that the broader global adoption has started to reflect some common challenges, namely a lack of resources and infrastructure. In the countries that have embraced this technology, a notable absence of universally agreed-upon regulatory and implementation frameworks for AI deployment has emerged. This void results in challenges related to information sharing and the isolated development of AI initiatives.

A representative from the private sector perspective delved into the prospective impact of AI in the region from an industry angle, extending its relevance to law enforcement and beyond. They highlighted the significance of regional collaboration, advocating for unity at both regional and international levels to harness the technology’s potential for economic growth across various sectors. They also emphasized the transformative power of AI in enhancing healthcare systems, law enforcement operations, and other industries. Still, they emphasized the necessity of substantial infrastructure investments to facilitate its effective integration and adoption.

Providing a regional outlook, a delegate from a government body outlined a ministerial AI strategy and the overall state of AI readiness. They reiterated the Ministry’s initial emphasis on traditional AI applications but noted their ongoing exploration and testing of novel, emerging applications to expand and establish enduring utilization models. They also underscored the significance of collaborative efforts across various sectors to foster sustainable innovation, thus guaranteeing its responsible and optimal application.

Bridging back to an international scale, a representative of UNICRI discussed the biggest risks/challenges in terms of the integration of AI into law enforcement. They began by stressing the paradigm-shifting and transformative nature of AI, emphasizing that its adoption will fundamentally reshape law enforcement procedures and systems. However, such a profound transformation necessitates preparedness in various aspects, including technological infrastructure, data quality, skills, and organizational adaptability. In the absence of these elements, law enforcement agencies must prioritize the acquisition of AI capabilities, encompassing essential skills, technologies, and resources for effective AI utilization in law enforcement. Finally, the speaker highlighted the delicate balance required between harnessing AI for safety and security and addressing the ethical and privacy concerns accompanying its adoption. During the high-level discussion, a question was presented to the audience as shown below. Fig. 1 illustrates the real-time poll responses from the participants.



What, in your view, are the biggest risks/challenges you see in terms of the integration of AI into law enforcement? ما هي الصعوبات التي تواجهكم في استخدامات تقنيات الذكاء الاصطناعي في المجالات الأمنية؟

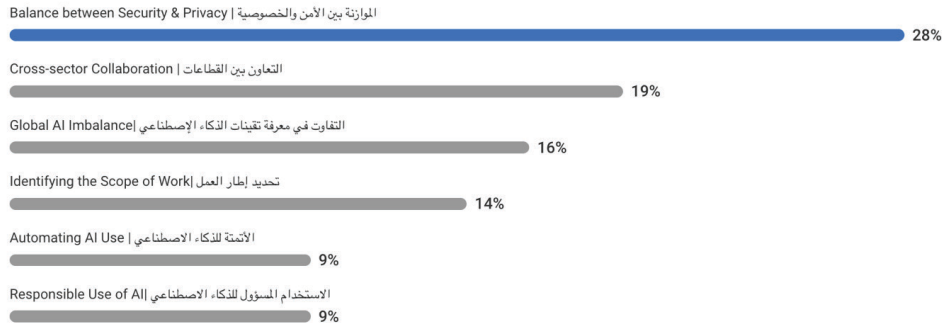


Figure. 1. High-level panel audience poll question one

Most participants, including various law enforcement experts, academia, and industry professionals, expressed their concern over striking the balance between Security & Privacy (28%) when integrating AI into law enforcement.

Next, a speaker from academia discussed the profound transformative impact of AI technology and underscored the tangible challenges and threats posed by the criminal use of AI. In addressing emerging and existing concerns, the speaker emphasized the necessity for collaboration among law enforcement and stakeholders to confront these rapidly developing threats collectively. He stressed that the security sector bears the responsibility of exploring, comprehending, and mitigating these threats, harnessing AI to combat malicious AI applications.

While discussing the question, “What should law enforcement agencies prioritize going forward?”, some panelists emphasized the importance of transparency, accountability, and safeguarding the security and privacy of both data and citizens. The government representative underlined the pressing need to prepare for, understand, and adapt to ongoing developments in the field. He highlighted the importance of focusing efforts and investing significantly in this domain. According to him, the primary challenge lies in being adequately prepared for the evolving landscape of AI, and he stressed the time-sensitive nature of the challenge and the necessity to make the most of the available time to prepare for what’s coming next. The academic speaker pointed to two specific challenging areas. First, the collaboration and coordination with the various stakeholders to achieve the best possible outcomes, and second, acquiring the necessary technical skills to manage the complexities of advanced systems.

During the audience interaction, an overwhelming majority (43%) echoed the academic speaker’s views, expressing their preference for LEAs to concentrate on “Technical Capabilities & Knowledge,” as evidenced by the live poll results shown in Fig. 2.

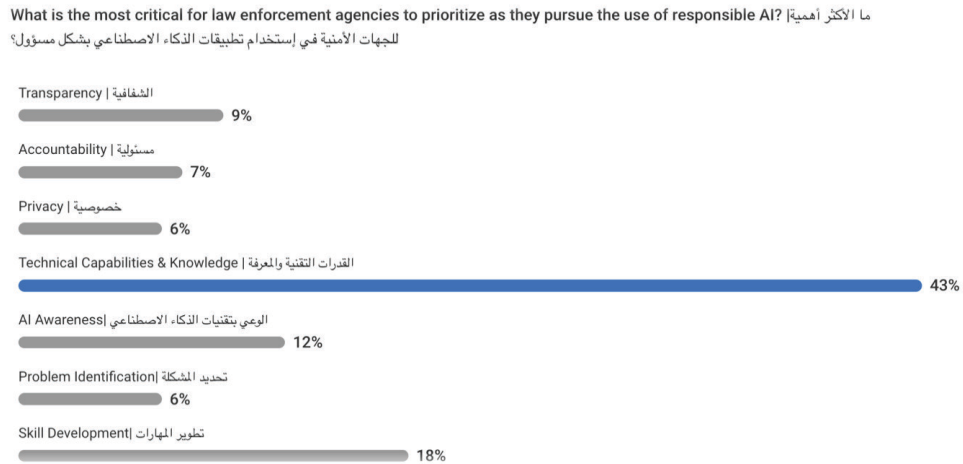



Figure. 2. High-level panel audience poll question one

5(a1). Key Findings of High-Level Panel Discussion

- 1. Challenges in Global Adoption of AI in Law Enforcement:** INTERPOL highlighted that AI is being integrated into various aspects of law enforcement globally, but common challenges have emerged. These include a lack of resources and infrastructure, as well as a lack of universally agreed-upon regulatory and implementation frameworks for AI deployment. This absence of a framework leads to difficulties in sharing information and isolated AI development initiatives.
- 2. Need for Regional Collaboration:** The private sector emphasized the importance of regional collaboration in harnessing the potential of AI for economic growth across various sectors, including law enforcement. They underlined the transformative power of AI but stressed the necessity for substantial infrastructure investments to facilitate effective integration and adoption.
- 3. AI Strategy and Readiness:** Government entities highlighted the AI strategy and the state of AI readiness. While the initially focus was on traditional AI applications, they are exploring novel emerging applications to expand and establish enduring utilization models. They also highlighted the significance of collaborative efforts across various sectors for sustainable innovation.
- 4. Risks and Challenges of AI Integration:** UNICRI highlighted that integrating AI into law enforcement is a paradigm shift that will fundamentally reshape procedures and systems. They stressed the need for preparedness regarding technological infrastructure, data quality, skills, and organizational adaptability. Finding a balance between harnessing AI for safety and addressing ethical and privacy concerns is a significant challenge.

- 
5. **Prioritizing Transparency, Accountability, and Technical Skills:** All panelists emphasized the importance of transparency, accountability, and safeguarding data and citizens' privacy. The government representative underscored the pressing need to prepare for ongoing developments in the field and the challenge of being adequately prepared for the evolving landscape of AI. The academic speaker pointed to two specific challenging areas: collaboration with various stakeholders to achieve the best outcomes and acquiring the necessary technical skills to manage advanced systems.

5(b). Theme 1: AI-based Capabilities in Law Enforcement

Under Theme 1, speakers and participants explored how AI systems can play a role in law enforcement. They highlighted the various operational advantages they can present, the importance of responsible AI, and specific AI use cases from the Arab Region as practical examples of implementing this technology.

To gain an initial insight into the regional familiarity with AI implementation in law enforcement, we examine the survey findings conducted as part of Theme 1. When inquired about their general awareness of AI utilization in law enforcement, **80%** of the participants answered affirmatively, whereas 20% responded adversely. In the same line of questioning, slightly over 50% have encountered or utilized AI-based tools or systems in law enforcement. This suggests that awareness of these new technological capabilities is expanding, but their adoption and implementation are progressing at a considerably slower pace.

i. Presentation: AI-based Capabilities in Law Enforcement - by an Innovation and Technology Crime Officer from INTERPOL.

During their presentation, the representative from INTERPOL commenced by emphasizing that AI has already surpassed humans in several tasks. They then detailed the challenges associated with AI-based capabilities in law enforcement, which encompassed:

- i. **Lack of regulatory framework and established case law:** referring to the absence of clear and comprehensive legal guidelines and precedents in the context of AI in law enforcement.
- ii. **Rapid developments in AI:** can pose challenges for law enforcement agencies, struggling to keep pace with advancements and ensure tools remain practical and ethical.
- iii. **Disparities in AI literacy and infrastructure:** create inequalities in the implementation and effectiveness of AI solutions in LEAs and nations worldwide.
- iv. **Limited knowledge exchange:** barriers to knowledge exchange, such as competition, security concerns, or reluctance to share insights, hinder progress in the field.

- v. **Public trust:** building and maintaining public trust is paramount in law enforcement. Using AI for tasks like predictive policing or surveillance can raise concerns about privacy and bias.
- vi. **Budget constraints:** can limit the extent to which AI can be effectively employed, as AI solutions and infrastructure tend to be expensive.
- vii. **Resistance to change:** officers and staff may resist adopting new technologies, fearing disruption and replacement.


The speaker expanded upon the prevalent AI applications encountered in law enforcement:

Table 1. AI applications in Law Enforcement

Image Analysis	Text & Speech Analysis	Risk Evaluation & Predictive Policing	Content Generation	Process Optimization & Workflow Automation
Biometric Facial Recognition	Social media and online forum monitoring to detect suspicious or criminal behaviour	Predict geographical crime hotspots in cities	Create fake identities, e.g., on social media, for investigations & operations	Improve the speed and accuracy of cyber-related incident detection and response
Support for officers in crimes against children's investigations	Match audio samples from crime scenes or phone calls to individuals	Evaluate the risk of accidents or crowd crushing in crowd gatherings/big events	Chatbots in smart police stations	Support for law enforcement emergency call centers
License plate recognition		Support city traffic management	Generate synthetic data	Improve traffic management
Anomaly detection in smart city cameras	Support to shift through police reports and interview tales	Predict likelihood of someone committing a crime based on mined social media data	Language support	Support for criminal analysis units
Tattoo image analysis				

ii. Use-Case: The Integrated Fan Journey at the FIFA World Cup, Qatar - by a representative from the Ministry of Interior, Qatar.

In this presentation, the speaker explained how Qatari MOI deployed the 'Hayya' platform, a connected and integrated IT platform aimed at centralizing the entire fan experience during the FIFA World Cup in Qatar in one place. The platform integrated 20+ systems for fan convenience and safety, including their information, security check, border control, transport system, hotels/residences, mobile cards, FIFA ticketing system, stadium access, FAN zone access, health services, and security




profiling information and data. MOI, Qatar representative went on to explain the use of AI (data science & analytics) in various components of the World Cup Organization, such as:

- i. **Queue Management at the airport & stadiums**, reducing queues, screenings, and managing the 40,000-80,000 daily fans visiting stadiums.
- ii. **Video Analytics (Computer Vision)**, supporting significantly in improving crime prevention (by 60%), detection, management of security operations, and increasing efficiency in incident response x10. The same systems were used for (1) Offender Search & Identification (80% accuracy), (2) Enhanced Security, (3) Prevent Terrorism & Violence, and (4) Monitor Access to Restricted Areas. Using AI, it took, on average, 0.3 seconds to search in a database of 1,500,000,000 faces.
- iii. **Intelligent Radar System (URS)**, technology was used for wanted vehicle identification (stolen vehicles, offender vehicle), to detect drivers using phones or not wearing seatbelts and alerting relevant authorities, and to identify vehicles parked in prohibited spots.
- iv. **Health Care Capacity Planning & Operation**, used AI tools for demand and capacity forecasting, connecting all healthcare organizations, clinics, mobile medical units, ambulances, and staff across Qatar.
- v. **Using AI for Health Care**, using *Avey* this innovative healthcare solution (1) self-diagnosed instantly with the most accurate AI diagnostic algorithm in the world, (2) connected with the right doctors physically or virtually, (3) order medicines and more follow-up procedures effectively.

iii. Use-Case: AI for Large Event Management & Public Safety - by a Professor from the Nanyang Technological University, Singapore.

Within the Digital Trust Centre framework, the speaker showcased AI research in the realm of large event management and public safety. The presentation delved into typical machine learning applications, such as object detection, face recognition, and machine translation, emphasizing the effectiveness of deep neural networks in these tasks. The discussion expanded to video analytics and deep learning, covering areas like object classification, pedestrian detection, cross-camera person re-ID, visual anomaly detection, action recognition, and person tracking. The speaker introduced topics like 'Deep Learning for Multi-Object Tracking,' 'Multi-media in Analytics in LE Operations,' and 'Intelligence Analytics & Decision Support,' leading into AI for next-generation law enforcement operations.

The speaker also highlighted AI's potential in the legal industry, pointing out the key benefits of Generalized Boosted Trees (GBT), including automating routine tasks, swiftly and accurately analyzing



large unstructured text data, uncovering hidden insights, and ensuring contract quality consistency among different parties.

The presentation also featured a segment on ‘AI for Cyber Threat Intelligence,’ exploring AI-enabled tools like document analytics, auto-summarization, NLP, and text-mining in the context of cybersecurity operations. The speaker shared lessons from translational research, including the importance of developing AI through systems engineering, leveraging domain-specific AI with machine learning and domain knowledge, and prioritizing human intelligence in designing complex intelligence systems to mirror user work processes.

iv. E-poster Presentations

- **Abusive Content Detection on X Using Machine Learning**

A law enforcement expert emphasized a crucial problem during their presentation: the vast amount of big data produced on social media, which cannot be effectively managed using manual methods. They pointed out that criminals using social media to display illegal activities can harm law enforcement’s image and public trust. Additionally, this criminal content on social media can have a significant impact on a large part of the population, necessitating automated investigation by authorities.

The project developed by law enforcement expert aimed to develop a machine learning model to detect abusive or hate speech content in social media accounts, specifically on a platform like Twitter. This detection would help identify users potentially engaged in criminal activities.

To achieve this goal, the expert employed three distinct machine learning algorithms: Logistic Regression (LR), Random Forest (RF), and Support Vector Machine (SVM). The approach involved converting raw data into meaningful features using the Bag of Words (BOW) technique, which focused on the presence and frequency of words to create a vector representation. Additionally, Term Frequency-Inverse Document Frequency (TF-IDF) was used to assess the significance of each word, considering its prevalence within a specific document and its rarity across a broader collection of documents. The model development process was carried out using Python, and two datasets, one containing hate speech and the other abusive content, were used to train and test the machine learning models.

The achieved results were promising for all three machine learning algorithms, but Logistic Regression emerged as the most effective choice, showing superior performance in identifying abusive Twitter accounts.



- **Gait Recognition for Security Purposes to Improve Investigations based on Deep Learning**

In this poster presentation, the law enforcement expert discussed his research results regarding the use of deep learning in analyzing human gait patterns.

Gait recognition can identify individuals by their walking patterns, unaffected by appearance changes or low-light conditions. Traditional methods include Appearance-based and Skeleton-based approaches, but the expert's research introduced a sensor-based approach using smartphone signals for rapid identification in security applications.

The research shows that using sensors notably improves gait recognition, addressing issues in other methods. This approach, utilizing smartphones, offers potential benefits for law enforcement, enabling the collection of time-series gait data for security purposes.

- **Traffic Management Systems using AI**

During the presentation, the law enforcement specialist discussed the development of an intelligent traffic management system. They utilized artificial intelligence to collect road condition data, implemented Python and Java for database creation, and focused on relevant traffic information. Machine learning and deep learning techniques were employed to predict traffic conditions. The system integrated data from multiple sources, including weather and traffic factors, aiding in congestion management and finding alternate routes.

This project aims to offer traffic organizers important statistics using surveillance camera data instead of GPS data from vehicles. It can also connect with the licensing department to detect expired or unlicensed vehicles.

The presentation highlights AI benefits in traffic analysis, focusing on accuracy, feedback, security, minimal human involvement, and ethical alignment with national AI strategy. It's the first project from the Public Security AI Team, in line with the National AI Strategy for digital transformation.

- **On Prediction Models Part I** - by Director of Policing and Crime, Centre for Economic Performance, London School of Economics.

This poster presentation focuses on data-driven methods for understanding and predicting crime and incidents, using both bottom-up and top-down approaches. It emphasizes machine learning techniques, challenges in assessing police service demand, determinants of demand, and the use of data from 18 police forces. Additionally, it introduces a new approach for understanding road traffic accidents and explores top-down data applications for crowd counting and organized crime prediction.



Part II: Balanced Policing

The presentation introduces the concept of “Balanced Policing,” a strategic approach that seeks to optimize the allocation of police resources by striking a balance between fairness and deterrence. This framework acknowledges the inherent challenge of equitably distributing resources while simultaneously upholding public safety standards. The crucial aspects covered encompass pinpointing regions characterized by either excessive or insufficient policing, employing data analysis techniques for strategic resource allocation. Additionally, the presentation outlines prospective measures for enhancement, such as forecasting demand, experimenting with dynamic deployment strategies, expanding initiatives, exploring automation possibilities, and refining comprehension of the deterrence effects.

In summary, this poster presentation emphasizes the refinement of police resource allocation by seamlessly blending fairness and deterrence through sophisticated data-driven methodologies. The objective is strategically deploying officers to areas where their presence is paramount. Additionally, the presentation underscores the significance of ongoing improvement and evaluation in shaping an effective and adaptive policing strategy.

- **Smart Hotlines Processing, using Arabic NLP** - by Expert from Lebanon Internal Security Forces

This presentation discusses the implementation of Arabic Natural Language Processing (NLP) by the Lebanon Internal Security Forces to address misclassification issues in reports related to incidents, crimes, and investigations received through hotlines. Key points include the purpose of Arabic NLP to rectify misclassified reports, a schema illustrating the NLP process, challenges in implementation, categorization of crime reports into eleven labels, and the outstanding performance of the AraBERT model with a testing accuracy of 85.82% in understanding Arabic sentences and semantic relationships between words.

In summary, this poster presentation highlights the effective application of Arabic NLP within law enforcement to enhance the classification of reports related to incidents and crimes. It emphasizes the complexity of the Arabic language and the obstacles encountered during the implementation process, while highlighting the effectiveness of AraBERT in understanding Arabic text.

v. Regional Perspective

Among the individuals surveyed, a minority, comprising less than 20%, had undergone training related to AI-based tools. These individuals identified the following as the most prevalent subjects covered in their training:

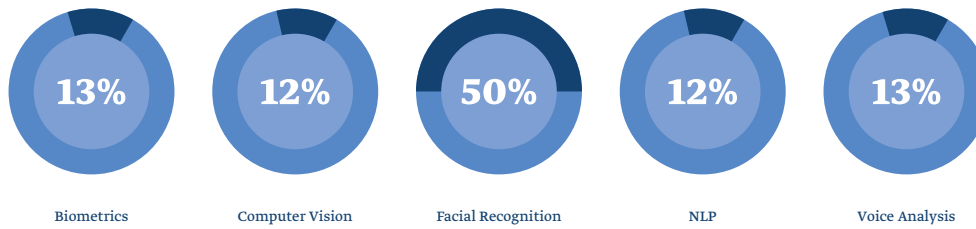


Figure 3. AI-based tools Training Subjects

In response to inquiries about AI’s potential to enhance the precision and efficiency of criminal investigations, an overwhelming majority of participants from law enforcement agencies responded positively (90%). However, when asked about the accuracy and reliability of AI algorithms and systems, the average trust rating was 2.91 out of 5. Participants rated their overall trust in AI technology 3 out of 5. These statistics reveal a widespread recognition of the technology’s advantages and some reservations concerning its trustworthiness and effectiveness.

Confronting challenges and concerns in the implementation of AI-based capabilities in law enforcement, participants identified the following categories as their top concerns:

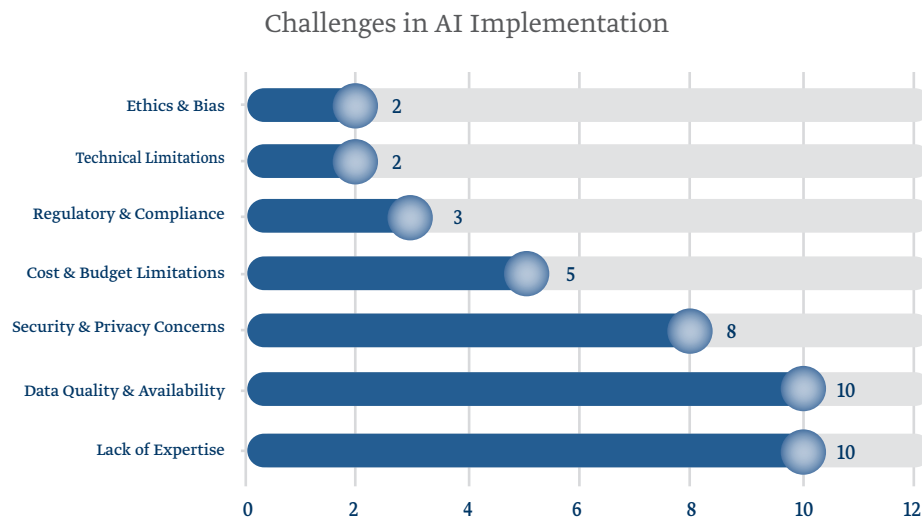


Figure 4. Challenges of AI Implementation

(Scale 0-10, 0 being least concerning, 10 being most)

Despite the challenges, when asked about the necessity for enhanced training, all participants (100%) responded affirmatively, underscoring a significant gap in the current lack of training opportunities and academic programs related to AI in law enforcement. When asked about the potential benefits of AI in law enforcement, participants demonstrated a knowledgeable understanding of the potential uses by mentioning the following:

- Traffic Management - 100%
- Facial Recognition - 90%
- Data Management - 72%
- Investigative Support - 81%
- Crime Prediction & Prevention - 72%
- Cybersecurity - 72%
- Predictive Policing - 63%
- Natural Language Process - 90%
- Crisis Intervention - 63%
- Evidence Analysis - 90%

However, regardless of their complexity and advanced perception of AI’s potential applications, participants identified the specific areas of training they consider requiring the most focus or improvement. This underscores a prevalent foundational understanding or proficiency in AI, as illustrated below:

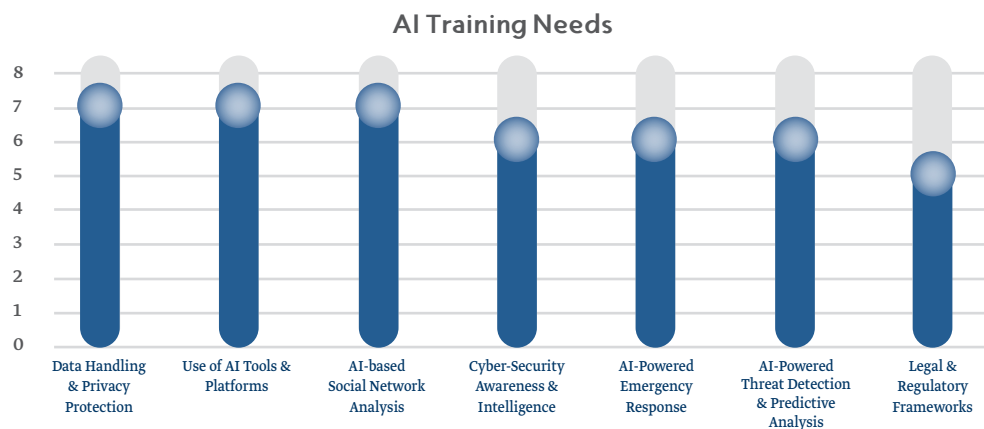


Figure. 5. AI Training needs

(Scale 0-8, 0 requiring least focus, 8 requiring most)

The survey results revealed a widespread need for training across various domains, emphasizing the existing shortcomings in the training environment. Linking to the required training areas, participants have highlighted the following topics as research areas that demand more attention in the future: Generative AI, Machine Learning, Robotics, Predictive Policing, Image & Video Analysis, Forensics Science, Data Science, and Biometrics.



5(b1). Key Findings of Theme 1

- i. Awareness and Adoption Disparity:** The survey during the AI Forum revealed that 80% of participants were aware of AI utilization in law enforcement, but only slightly over 50% had encountered or utilized AI-based tools or systems in law enforcement. This suggests that while awareness of and interest in AI in law enforcement is high, the adoption and implementation of AI technologies are progressing at a slower pace.
- ii. Challenges in AI-based Law Enforcement:**
 - a. Lack of Regulatory Framework:** There is a lack of clear and comprehensive legal guidelines and precedents in the context of AI in law enforcement.
 - b. Rapid AI Developments:** The rapid pace of AI advancements can pose challenges for law enforcement agencies in keeping up and ensuring the effective, and responsible, use of AI tools.
 - c. Disparities in AI Literacy and Infrastructure:** Inequalities in the understanding of AI as well significant divides in terms of the technical infrastructure to implement AI effectively exist across law enforcement agencies and nations.
 - d. Limited Knowledge Exchange:** Barriers to knowledge sharing, such as competition and security concerns, hinder progress in the field. Equally, the absence of platforms and communities for law enforcement to share experience amongst agencies constitutes an additional hurdle for this.
 - e. Building Public Trust:** The use of AI in law enforcement raises concerns from an ethical perspective, this is considerably more acute when looking at sensitive use cases such as predictive policing and surveillance. This can jeopardize public trust, which becomes a significant challenge for law enforcement.
 - f. Budget Constraints:** The expense of AI solutions and infrastructure can limit their effective use in law enforcement, as does putting in place the people and processes required to ensure its responsible use.
- iii. Practical AI Use Cases in Law Enforcement:** The use case presented by the Ministry of Interior in Qatar demonstrated the successful implementation of AI in law enforcement during the FIFA World Cup. AI was used for queue management, video analytics, intelligent radar systems, healthcare capacity planning, and AI-based healthcare solutions.



- iv. **AI’s Potential Benefits in Law Enforcement:** Participants recognized various potential uses of AI in law enforcement, including traffic management, facial recognition, investigative support, crime prediction and prevention, cybersecurity, predictive policing, natural language processing, crisis intervention, and evidence analysis.
- v. **Training Gap in AI for Law Enforcement:** Less than 20% of surveyed participants had received training on AI-based tools. However, all participants expressed the necessity for enhanced training, highlighting a significant gap in the current lack of training opportunities and academic programs related to AI in law enforcement.
- vi. **Specific Research Areas in Demand for Training:** Participants identified specific research areas that they believe require more attention and training in the future. These areas include Generative AI, Machine Learning, Robotics, Predictive Policing, Image & Video Analysis, Forensics Science, Data Science, and Biometrics.

5(c). Theme 2: AI Challenges for the Arab Region

Speakers under this theme presented some regional challenges that law enforcement agencies in the Arab region face or are likely to face in developing and deploying AI technology and possible ways to overcome these challenges.

i. Presentation: Overview of Regional Challenges - by the Technology Services Deliver Leader, IBM Technology - Expert Labs.

The IBM speaker presented the region’s challenges in the adoption of AI in various categories as shown in Table 2:

Table 2. Regional challenges in AI adoption

Planning & Expectations	Teamwork & Collaboration	Skillset	Models	Data
Look for areas where AI can be applied	AI requires strong teamwork and coordination from all business units	Invest in Education	Focus on core capabilities of MVP (Not AI)	Data is critical to training AI
AI is not a solution, understand the problem	Executive sponsorship is key	Senior members to support rest of the team	Look for opportunities to apply AI after MVP	Understand and obtain data early
Invest in design & user research upfront	Realistic data is important to train the models	Have a research mentality	Adopt agile methodologies	Data must be annotated for good quality
Do not force fit AI			Except failures	
	Ensure models are transparent			

ii. Use-Case: Smart Hotlines Processing, Using Arabic NLP - by a law enforcement official from Lebanon Internal Security Forces.

In this use-case presentation, a law enforcement specialist detailed their use of Arabic Natural Language Processing (NLP) to process heterogeneous multisource information in the context of hotlines.

The purpose behind implementing such technology was to address the issue of misclassified reports in cases of incidents, crimes, and investigations. The classification deficiencies had resulted in incorrect actions, incomplete analysis, and defective decision-making. The following NLP process schema illustrates the steps involved in utilizing this technology:

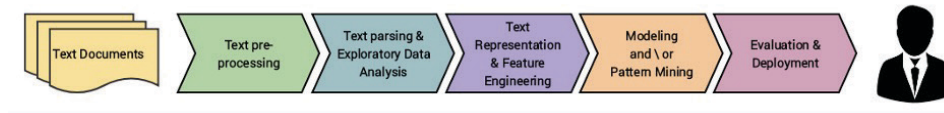


Figure. 6. Step-by-step NLP process


Some of the key findings from this use case concerning the execution methodology were:

- i. The Arabic language is intricate and challenging,
- ii. There is a lack of official free annotation tools,
- iii. There is a shortage of training data.

The Arabic crime tests fell into classification under eleven different labels as shown in Table 3:

Table 3. Classification of crimes

أفعال ضد الملكية	Acts against poverty
أعمال ضد السلامة العامة وأمن الدولة	Acts against public safety & state security
اعمال تسبب الضرر للشخص	Acts that cause harm to the person
أعمال التي تنطوي على المؤثرات العقلية أو المخدرات	Works involving psychotropic substances or drugs
أعمال ضد النظام العام والسلطة وأحكام الدولة	Acts against public order, authority and state provisions
افعال تسبب الوفاة	Acts causing death
أعمال التي تنطوي على احتيال أو الخداع أو الفساد	Acts involving fraud, deception or corruption
أفعال الضارة ذات الطابع الجنسي	Harmful acts of a sexual nature
اشتباه بجرم	Suspicion of a crime
مخالفات و حوادث اخرى	Other violations & different accidents
مختلف	Different



Among all the classification models employed, AraBERT demonstrated a testing accuracy of 85.82%. It excelled in comprehending the meaning and context of Arabic sentences, as well as in understanding the semantic relationships between Arabic words.

iii. Use-Case: AI-Enabled Social Network Analysis Capabilities for Counter-Terrorism - by a speaker from Kulindalytics.

In the use case presented by Kulindalytics, an expert explained the application of AI in social media network analysis, surpassing the limitations of human experts conducting manual analysis. The expert described the utilization of AI techniques, including:

- Algorithms for identifying abnormal activity within networks,
- Automated data collection and alerts at scale,
- Machine Learning for languages, sentiment analysis, and keyword trends,

These AI techniques enabled the execution of methods and approaches such as network and pattern analysis, direct engagement, network infiltration, and the analysis of themes, narratives, and content. These tasks, traditionally performed manually by human experts, were now automated.

However, while integrating AI into these previously manual domains, automating processes for real-time insights, new outputs, and data streams, the expert also identified certain AI limitations or “blind spots,” which include:




Table 4. AI limitations in Social Network Analysis

Area of understanding	Example weaknesses of AI	How AI sees the world	How humans see the world
Context and nuance	Understanding languages, slang, humor, satire, history, tribalism, and intertwined emotions such as anger, fear, and resentment	Seeks to understand how facts fit into history	Harbors emotions that cause the past to affect the present and the future
Human connections and communication	Understanding the human desire for purpose and the need to feel understood	Interprets communication at face value	Seeks deeper meaning and subtle messages in words, tone, phrases, and body language
Intentions	Differentiating between threats vs. the exploration of ideas, organic interactions vs. motives	Does not assume ulterior motives, interprets information at face value, and is not suspicious	Almost always suspicious and expects ulterior motives
The human experience	Viewing information through a lens that reflects a human perspective	Does not make real-life / on-the-ground connections and is objective without empathy	Constantly aware of real-life connections, self-centered but also empathetic

The expert characterized AI as perceiving the world through facts and statistics, in contrast to humans, who see it through stories and emotions. When AI lacks a complete understanding of the contextual aspects of a narrative, it can make incorrect recommendations and decisions and occasionally miss potential threats. Nonetheless, AI proves highly valuable when employed within specific bounds of social network analysis. The expert described the current state of AI as “just smart enough to be dangerous unless implemented with great care. Incredibly powerful when correctly placed.”

In terms of crafting an AI implementation strategy, the expert outlined the following key applications of AI that offer low risk and high benefits:

- Collect information: scrape social media and crawl websites, combine geospatial data,

- 
- Process information: generate social networks, categorize media content, and combine with OSINT,
 - Identify anomalies: flag accounts that consistently interact with or post content in VE networks.

To ensure that AI remains within its designated scope, the expert advised establishing safeguards such as “no-go zones” and rules of engagement for AI usage in social network analysis. These safeguards include:

- Setting specific goals and desired outcomes
- Setting human context boundaries to create “givens”
- Identifying areas where AI and other technologies are best placed
- Assess the four category blind spots.

iv. Use-case: AI-Enabled Phishing Websites Detection Tool – by an AI Expert from the Naif Arab University for Security Sciences (NAUSS).

An AI Expert from NAUSS delivered a use-case presentation on AI-Enabled Phishing Websites Detection Tool. Phishing is the malicious act of stealing personal information online with the intent to commit financial fraud. It typically involves unsolicited communications via email, SMS, or websites, where the attacker poses as a trustworthy third party to trick victims into revealing sensitive data, like login credentials and payment information. In the fourth quarter of 2022, APWG observed a record-breaking 1,350,037 phishing attacks, marking a concerning trend. A project at NAUSS is underway to combat this issue by developing a robust phishing website detection system utilizing machine learning and deep learning techniques. This system aims to create its dataset focused on phishing websites in the Arab region and analyze existing benchmark data. The goal is to empower law enforcement agencies and cybercrime investigators with a tool to detect phishing websites effectively. Currently in the conceptual phase, the project’s completion is expected to benefit law enforcement agencies, cybercrime investigators, and financial institutions and enhance community awareness through sharing its findings with local and international law enforcement agencies.

v. Use-case: AI-Drone Object Detection and Surveillance – By a Drone Expert from the Naif Arab University for Security Sciences (NAUSS).

A professor from NAUSS gave an informative presentation on their advanced drone technology work, primarily focused on R&D for law enforcement. They emphasized AI and drone training, showcasing the NAUSS Drone Laboratory, which integrates AI with drones to detect dangerous objects at crime scenes, even in low-light conditions. They discussed their use of Large Language Models and Transformer architecture for object detection, outperforming the popular machine learning model, i.e., YOLO version 5. They also highlighted the development of a fully automated Dangerous Object Detection Recognition (DFR) command center system that works with drones, offering promising security solutions. Ongoing research aims to enhance this technology’s performance.

vi. Regional perspective


As per the surveys, when inquired about the primary hurdles in adopting AI technologies for crime prevention and investigation, the majority of participants cited **“Data Availability”** as the central challenge. Regarding institutional obstacles in AI implementation, participants identified the following as the foremost challenges: a lack of legislative frameworks, concerns about citizen privacy, limited legal and technical knowledge, institutional resistance, inadequate funding and resources, insufficient AI skills and awareness, a scarcity of available data, and limited work experience.

Efforts to gain a deeper understanding of these challenges led to examining specific country and organization use cases. Table 5 highlights the most notable challenges identified in implementing AI solutions, drawing from reports by law enforcement experts from the Arab countries.

Table 5. Regional challenges in implementing AI solutions

Arab Countries Challenges	
Lack of High-Quality Data	Lack of Technological Infrastructure
Lack of Training	Discrepancies in AI Knowledge
Data Privacy	Lack of Knowledge
Technical Difficulties	Funding & Budget Limitations
Security	Lack of Expertise
Unclear Goals	Lack of Technical Staff

Along with the apparent lack of data, over **75%** of regional participants reported the absence of regional or international frameworks or guidelines related to law enforcement’s use of AI - indicating a clear gap in regulatory and legislative frameworks.



Regarding the AI literacy of law enforcement experts in the region, participants at the forum generally rated their experience and knowledge as falling within the **beginner** to **intermediate range**. When asked about strategies to cultivate a highly skilled regional workforce in AI and data analytics, participants offered the following recommendations:

- i. Integrating AI training into LEAs training programs from an early stage.
- ii. Enhancing education in mathematics, statistics, data analytics, data science, and programming.
- iii. Establishing regionally standardized AI academic and training programs.
- iv. Offering training and professional courses suitable for all levels and ranks within law enforcement.
- v. Maintaining up-to-date course materials to reflect the evolving AI landscape.
- vi. Providing training on both the malicious and responsible uses of AI.

As for future topics of training, participants voted on their preferences as indicated below:

- AI Tools & Software - 50%
- AI in Drones & Robotics - 15%
- Technical fundamentals - 10%
- AI in IoT devices - 10%
- AI-enabled surveillance - 5%
- AI-predictive Policing - 5%
- AI-Assisted Investigations - 5%

As for future research areas, participants voted on their preferences as indicated below:

- Border Security & Surveillance - 30%
- Counter-terrorism - 20%
- Cybercrime Detection & Prevention - 20%
- Drones, Robotics & Autonomous Systems - 15%
- Data Localization & Sovereignty - 15%

The following word cloud illustrates responses to a query about the deficiencies and essential AI-related positions within the law enforcement sector. These responses were collected from law regional law enforcement specialists.

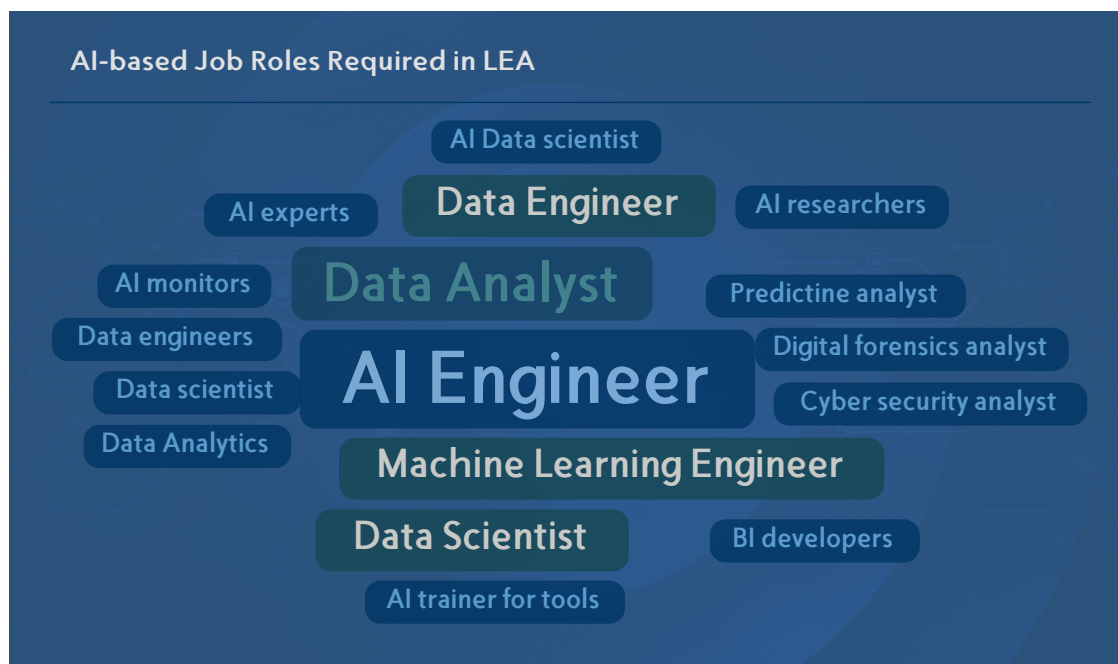


Figure. 7. Word cloud of AI-based job roles required in LEA

Finally, when participants were prompted to discuss the strategies that law enforcement agencies in the region could adopt and implement to remain abreast of AI technology advancements, they tabled the topic in an open group discussion and took into account the following considerations:

- International experts & specialized staff,
- Capacity building,
- Development of courses & training material,
- Conferences, Forums & Workshops,
- Increased investment in AI R&D



5(c1). Key Findings of Theme 2

- i. Data Availability is a Major Hurdle:** The primary challenge in adopting AI technologies for crime prevention and investigation in the Arab region is the lack of data availability. The majority of participants in surveys identified this issue.
- ii. Institutional Obstacles:** Participants also pointed out various institutional obstacles to AI implementation in law enforcement. These obstacles include a lack of legislative frameworks, concerns about citizen privacy, limited legal and technical knowledge, institutional resistance, inadequate funding, and resources, insufficient AI skills and awareness, a scarcity of available data, and limited work experience.
- iii. Gap in Regulatory Frameworks:** Over 75% of regional participants flagged the absence of regional or international frameworks or guidelines related to law enforcement's use of AI. This highlights a clear gap in regulatory and legislative frameworks.
- iv. AI Literacy of Law Enforcement Experts:** Law enforcement experts in the region generally rated their experience and knowledge in AI as falling within the rudimentary to intermediate range. This suggests a need for further training and education in AI and data analytics.
- v. Recommendations for Skill Development:** To cultivate a highly skilled regional workforce in AI and data analytics, participants recommended integrating AI training into law enforcement agency training programs, enhancing education in relevant fields, establishing standardized AI academic and training programs, offering training at various skill levels, and providing training on both the malicious and responsible uses of AI.
- vi. Future Training and Research Priorities:** Participants expressed interest in future training topics such as AI Tools & Software, AI in Drones & Robotics, and technical fundamentals. In terms of research areas, the priorities include Border Security & Surveillance, Counter-terrorism, Cybercrime Detection & Prevention, and Drones, Robotics, & Autonomous Systems. These topics reflect the growing relevance of AI in various aspects of law enforcement.

5(d). Theme 3: The Malicious Uses of AI

In the context of this theme, speakers focused on the malicious applications of AI, providing examples of how ChatGPT can be misused for criminal purposes. They also discussed the consequences of generating fake content to provoke disunity and unrest.

i. Presentation: An Overview of Malicious Use and Abuse of AI – by a professor from the University College London (UCL), UK.

The concern regarding the malicious uses of AI has gained critical momentum but insufficient immediate attention. Before delving into the intricacies of malicious applications, the professor from UCL initiated the discussion by shedding light on both the “Unintended” and the actively “Malicious” uses and the resulting harms arising from the recent AI advancements. Please see Table 6 for further details.

Table 6. Unintended & malicious uses of AI

Unintended	Malicious
Employment turmoil	National Security: - Kinetic Warfare - Information Warfare - Psychological Warfare
Truth Decay: undermining the status of evidence as rational basis for decision-making.	
Maintenance and creation of bias	Crime & Terrorism: - Disinformation - Fraud - Radicalization - Harassment - Child Exploitation - Terrorism
Weakening of social fabric due to: - Personalized synthetic media reducing common grounds - Human-AI relationships displacing human-human	
Devaluation of human creativity	
Destabilizing changes to sexual behaviour arising from optimized generative pornography	
Widening of inequality	Misdemeanours: - Academic cheating
Creation of powerful AI agents without human values	

Under the Crime & Terrorism branch, the professor elaborated on the various effects of those crime categories. **Disinformation** can have significant impacts, as some may believe it, and even if not believed, it can still exert influence through the Illusory Truth Effect. Additionally, disinformation can displace real news and contribute to Truth Decay. The utilization of AI contributes to the emergence of complex new **fraud** types (such as AI-enhanced family emergency scams). These scams employ Generative AI to voice-clone audio messages and/or engage in real-time voice-cloning conversations. Furthermore, there is a growing concern that bots may soon replace human agents, enabling large-scale automated calling attacks.

AI has also started to play a role in increasing **radicalization**, as very basic methods enable chatbots to learn how to prolong conversations, leading to the emergence of hyper-engaging chatbot communities that can effectively persuade individuals into radicalization, with AI continually improving in this regard. Another malicious use is the increase in AI use for sextortion and **harassment**, where an individual's publicly available images are manipulated to explicit content and used to harass or blackmail them. The issue is widespread, extending from nightmarish celebrity harassment campaigns to school-level bullying, where children exploit sexually explicit generated images for bullying. This directly feeds into the malicious use of AI for **child exploitation**, where evidence has emerged of online guides for those interested in creating abuse images using AI circulating online. Using sophisticated image-generation tools, strikingly realistic pictures of children as young as three years old are produced. Lastly, **terrorism** - the UCL professor highlighted how AI serves as an enabler, bridging the expertise gap in areas like cyber, chemical, and biological terrorism. These types of criminal activities typically have a high technical entry barrier, but AI has been rendered readily accessible to anyone with AI technology at their disposal.

ii. Presentation: ChatGPT & Large Language Models, the ever-changing threat landscape – by a Senior Threat Researcher, Forward-looking Threat Research Team, Trend Micro

The Trend Micro expert presented large language models as ever-changing threat landscapes and divided the GPT threats into the following categories:

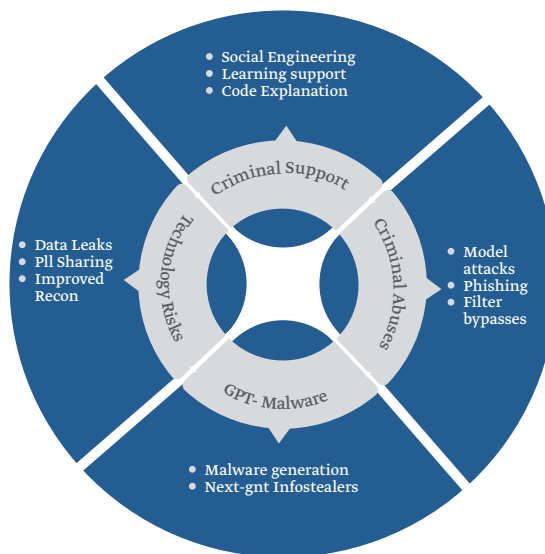


Figure. 8. LLM threat categories

The implications of advancing LLM technology are manifold, particularly in the realm of cybersecurity. With the rise of large language models, the risk of sensitive and personal information being leaked and exploited increases significantly. Additionally, these models lower the entry barrier to the criminal market, making it more accessible to non-English speakers, potentially giving rise to a global criminal economy. Furthermore, the advent of next-generation malware is set to take the concepts of “polymorphic” and “targeted” attacks to new heights, posing formidable challenges to cybersecurity efforts.

iii. Presentation: The Evolving Threat Landscape of Deepfakes - by a Senior Threat Researcher, Forward-looking Threat Research Team, Trend Micro

In the subsequent presentation on deepfakes, the cybersecurity expert started by presenting the current and existing types of deepfakes:

- **Face Replacement:** replacing one’s face with a different one
- **Face re-enactment:** manipulating one’s face to make them say something they are not
- **Face generation:** generating new, convincing synthetic faces
- **Speech synthesis:** generating audio content using a deepfake voice
- **Shallowfakes:** audio-video forgeries using less sophisticated techniques

The presentation highlighted a distinct parallel between the anticipated threat landscapes in 2020 and 2023 as shown in Fig. 9, underscoring the significant impact of technology’s evolution on the entire domain.

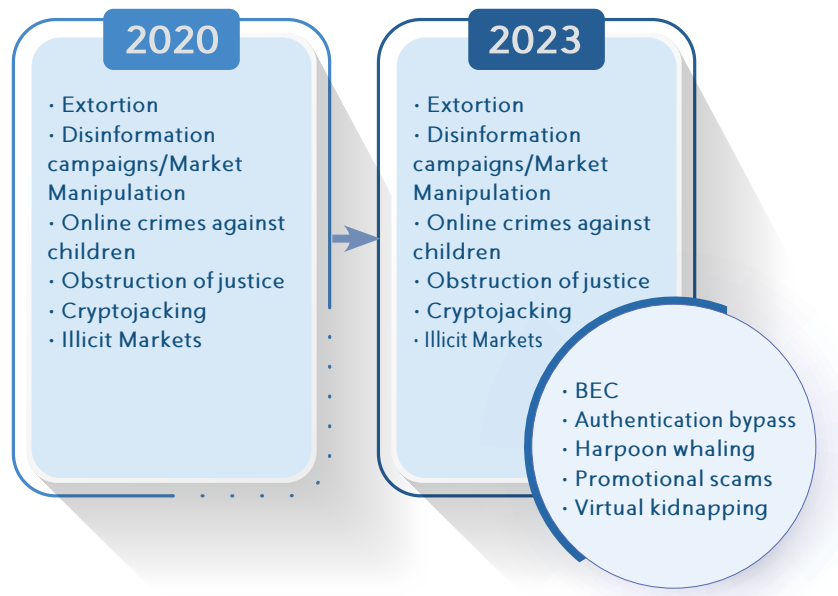



Figure. 9. Threat Development 2020-23



The landscape of deepfakes has undergone a profound transformation since its initial emergence. While initial concerns revolved around mass manipulations, the reality has witnessed the proliferation of more precise and targeted attacks. The real catalyst behind these developments lies in the widespread accessibility of biometric data, which facilitates the seamless impersonation of victims. This trend aligns with the evolving preferences of the criminal market, which is increasingly favouring fraud over traditional malware-based activities.

iv. Presentation: United Nations Perspective and the Malicious Use of AI for Terrorist Purposes
– by the Programme Management Officer, Cyber-Security & New Technologies Unit, United Nations Office of Counter-Terrorism (UNCCT).

The UN representative commenced by drawing a parallel between the myriad positive technological advancements that have shaped contemporary society, including the internet, IoT, social media, biometrics, and augmented & virtual realities, among others. Nevertheless, these advancements also open doors for malevolent actors to exploit and harness technology for harmful purposes. Notably, a survey conducted by UNOCT-UNICRI in 2021 gauging the perceived likelihood of AI’s malicious use for terrorist purposes revealed that 44% found it very likely, with 56% considering it somewhat likely. However, in striking contrast, the same survey conducted in 2023 yielded dramatically different results, with 69% expressing a belief in its very likely occurrence and 31% regarding it as somewhat likely. This shift indicates the escalating utilization and growing concerns regarding the malicious exploitation of AI. In both instances, no respondents indicated that the threat was unlikely.

AI has been identified as enhancing Cyber Threats, Physical Threats, and Political Threats of terrorism, enhancing the effectiveness of cyber-attacks, widening target demographics, and augmenting fake news and disinformation capabilities.

Table 7 details the malicious uses of AI for Terrorism:

Table 7. Terrorist uses of AI

Malicious Uses of AI for Terrorist Purposes	
Enhancing Cyber Capabilities	DDoS Attacks, Malware, Ransomware, Password Guessing, CAPTCHA Breaking, Encryption & Decryption
Enabling Physical Attacks	Autonomous Vehicles, Drones with Facial Recognition, Genetically Targeted Bio-Weapons
Providing Means for Financing Terrorism	Audio Deepfakes, Crypto-trading
Spreading Propaganda & Disinformation	Deepfakes and other Manipulated Audio-Visual Content
Other Operational Tactics	Surveillance, Fake Online Identities & Human Impersonation of social networking platforms, Morphed Passports, Online Social Engineering

v. Group Discussion – Dark Side of AI for Malicious Activities in the Arab Countries

In the group discussion, a diverse gathering of regional law enforcement experts, academic and industry professionals collaborated to enhance their comprehension of the threats posed by malicious AI usage and the institutional and capacity deficits in addressing these issues within the region. Right from the outset, when asked about the likelihood of malicious AI use by terrorists, an overwhelming **98%** of participants voted **high** or **very high**. A majority subsequently reported their concern about the misuse of deepfakes, LLMs, and generative AI. The conversation then led to exploring the best methods for LEAs to stay one step ahead of malicious actors, and participants suggested the following:

- Research & Development,
- Training & Education,
- Enhanced Infrastructure (Cyber & Real) Security,
- Best practices & knowhow exchange,
- International Collaboration,
- Using AI to combat (misuse of) AI.

In the context of effectively detecting & responding to malicious AI-driven activities, group participants suggested the following:

- Legislation,
- Specialist Training,
- Monitoring & Surveillance,
- (International/Regional) Collaborations,
- Live Simulations & Trainings,
- Continued Research & Development,
- Develop unified response mechanisms, protocols, and techniques.

In response to the moderators’ inquiry regarding the primary challenges and constraints associated with covering AI-driven malicious activities, participants indicated they faced restricted knowledge and experience, inadequate infrastructures, limited capacity, and struggled to keep pace with the rapidly advancing technology.

Fig. 10 shows the word cloud generated from the conversation regarding instances of malicious AI activity identified by members of the regional law enforcement community.



Figure. 10. Word cloud on examples of AI-based malicious activities

Below is another word cloud (Fig. 11) generated from the conversation regarding strategies to combat AI-based malicious activities.

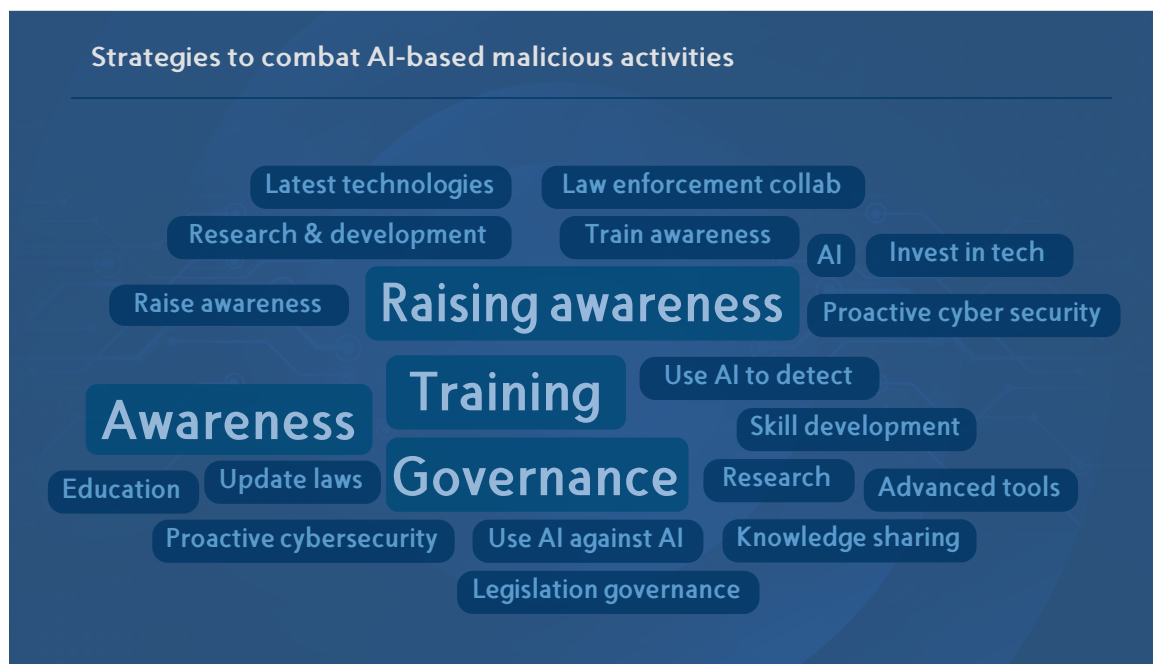


Figure. 11. Word cloud on strategies to combat malicious AI

vi. Regional Perspective

In the survey questionnaire, participants were asked to evaluate their knowledge of different AI-based applications and malicious uses of AI. Figure 12 illustrates the extent to which law enforcement experts have varying levels of familiarity with these areas.

How aware are you of the potential malicious use of AI technologies?

Strongly Unaware 1 2 3 4 Strongly Aware 5

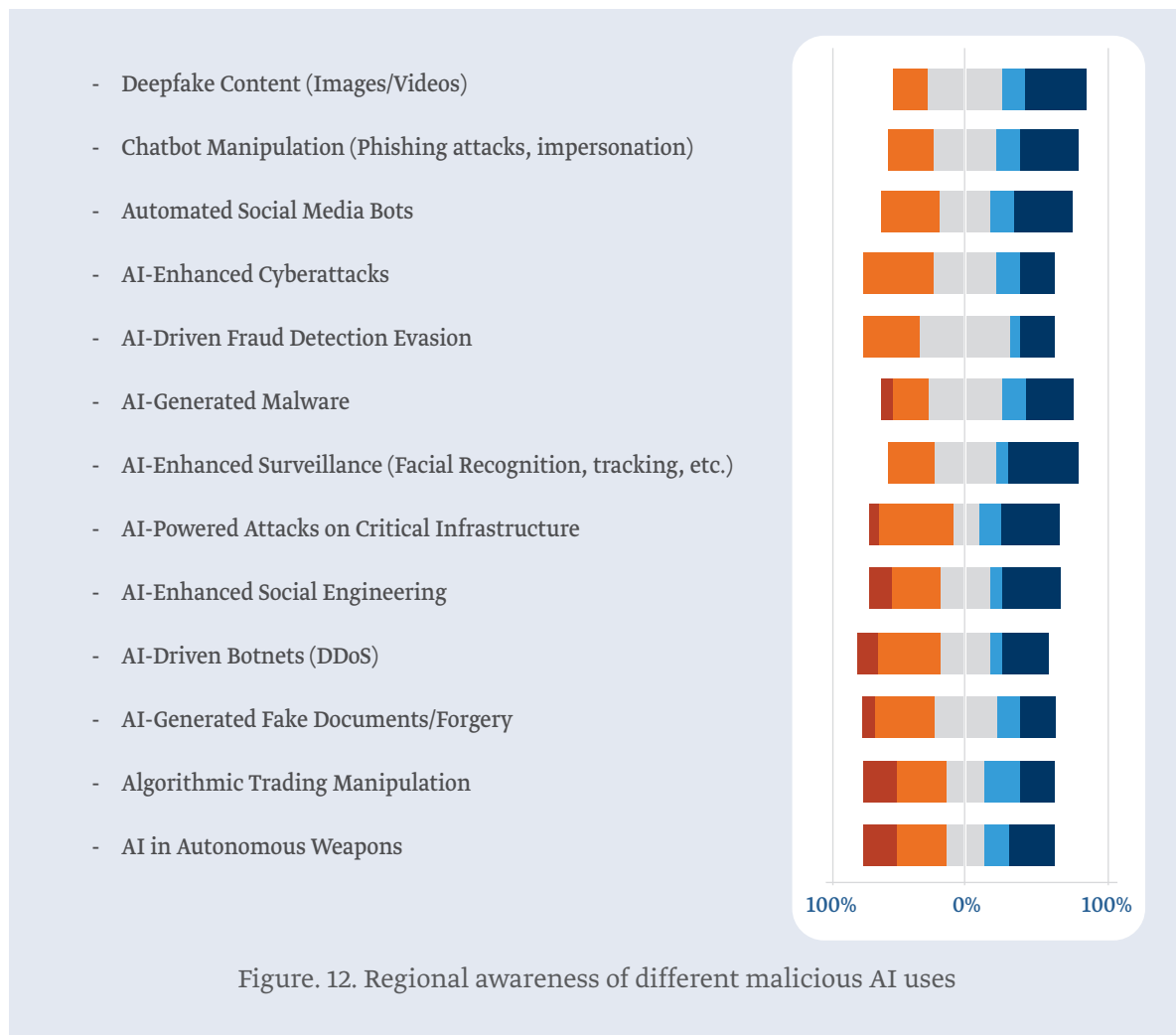



Figure. 12. Regional awareness of different malicious AI uses



Participants conveyed that their organizations and agencies have taken steps to keep their personnel informed about emerging AI-driven threats, utilizing methods such as cybersecurity training, simulations, expert speakers, and inter-agency exercises. Nevertheless, they expressed a strong interest in further enhancing their expertise and knowledge in countering malicious AI, particularly in the following areas:

- Cybersecurity Expertise - 75%
- Data Analysis - 62.5%
- Threat Intelligence - 56%
- AI Forensics - 43%
- Ethical Hacking - 43%
- Machine Learning - 56%

Delegates emphasized the significance of progressing research related to AI-driven attacks during the forum. They placed particular emphasis on deepfake content (highlighted by over 80% of participants), AI-generated disinformation (75%), attacks targeting critical infrastructure (75%), cyberattacks (62%), social engineering (62%), and malware (50%). However, the statistics revealed that just over 60% of the organizations or agencies had established internal regulations, guidelines, or protocols dedicated to addressing the malicious applications of AI. Surprisingly, less than 40% of them had implemented tools for detecting or preventing potential malicious uses of AI.

5(d1). Key Findings of Theme 3

- i. Diverse Malicious Applications:** AI technology, particularly LLMs like ChatGPT, is maliciously employed in various criminal activities. Examples include disinformation campaigns, AI-enhanced fraud such as voice cloning scams, radicalization through hyper-engaging chatbots and harassment using manipulated images, child exploitation facilitated by AI-generated abusive images, and terrorism activities aided by AI, bridging expertise gaps in cyber, chemical, and biological terrorism.
- ii. Increasing Accessibility:** Advances in LLMs have significantly lowered the entry barrier for criminals, allowing non-English speakers to participate in the global criminal economy. This increased accessibility poses a severe threat to cybersecurity as sensitive and personal information becomes more vulnerable to exploitation.



- iii. **Evolving Threat Landscape of Deepfakes:** Deepfake technology has evolved from mass manipulations to precise and targeted attacks. Criminals exploit biometric data to impersonate victims, leading to more convincing and dangerous deepfake attacks. Different types of deepfakes, including face replacement, face re-enactment, face generation, speech synthesis, and shallowfakes, are being employed for various malicious purposes.
- iv. **Escalating Concerns:** There is a growing concern among experts and law enforcement agencies regarding the malicious use of AI. Surveys conducted by organizations like the UNCCT and UNICRI show a significant increase in the perceived likelihood of AI's malicious use for terrorist purposes. This escalating concern highlights the urgent need to address these threats.
- v. **Collaborative Strategies:** Law enforcement experts, academics, and industry professionals recognize the importance of collaboration to combat malicious AI activities. Strategies include research and development, training, enhanced infrastructure security, best practices exchange, international collaboration, and utilizing AI to counteract misuse.
- vi. **Challenges and Constraints:** Law enforcement faces limited knowledge and experience, inadequate infrastructures, and capacity constraints in dealing with rapidly advancing AI technology. To effectively respond to AI-based malicious activities, efforts must focus on legislation, specialist training, monitoring, international and regional collaborations, live simulations, continued research, and developing unified response mechanisms and protocol.

5(e). Theme 4: Responsible AI Innovation and Building Capacities for Responsible Use

Within this concluding theme, the speakers explored the concept of responsible AI innovation and the need for law enforcement to employ AI in a manner that aligns with human rights principles and ethical standards. This was identified as a prerequisite for law enforcement agencies to ensure it preserves public trust in the performance of its function. Discussions during this session also delved into measuring organizational readiness to implement AI and to do so in a responsible manner, as well as the development of processes to bring this vision to fruition.



i. Presentation: What is responsible AI Innovation? – by a Programme Officer at UNICRI.


AI has emerged as a powerful tool in law enforcement, enhancing efficiency and capabilities. However, its use poses significant risks, both to the public and the law enforcement community itself. Unethical outcomes and human rights violations are possible, which can cause direct harm and challenging fundamental legal principles like the presumption of innocence. Biases can creep in, affecting the system's performance, especially in sensitive areas like identifying victims or perpetrators of crimes. Additionally, due to the scalability of AI systems, while boosting efficiency, it can amplify the impact of flawed systems or outputs. The “black box” problem equally raises concerns in cases where the AI systems are so intricate that humans cannot comprehend their workings. This is particularly concerning from a law enforcement perspective when it comes to adjudication of an investigation in the courts. The concept of ‘Responsible AI innovation’ therefore is crucial for law enforcement agencies to take onboard as a framework to navigate these challenges. Adhering to the principles of responsible AI innovation as a framework for navigating AI is pivotal for law enforcement and will aid it fostering confidence among the public.

ii. Presentation: An Introduction to the Toolkit for Responsible AI Innovation in Law Enforcement – by the Head of INTERPOL Responsible AI Laboratory.

The “Toolkit for Responsible AI Innovation in Law Enforcement,” developed by INTERPOL and UNICRI, aims to provide specific guidance for law enforcement agencies on using AI responsibly. It was developed in a consultative manner which included expert consultations in various subject areas such as law enforcement, human rights, criminal justice, and technology providers. The toolkit is designed for senior police management, law enforcement officers, R&D officers, legal advisors, and more, and it offers resources like guidance documents, an introduction to responsible AI innovation, principles for responsible AI, an organizational roadmap, and practical tools. The toolkit's primary purposes are to offer strategic and operational support, address human rights and ethical considerations, outline AI capabilities, and promote public trust in AI use within law enforcement. Each resource in the toolkit can be used independently to suit the specific needs of law enforcement agencies.

iii. Responsible AI Workshop: Putting Responsible AI innovation into Practice – Scenario-based Discussion.

In collaboration with moderators from UNICRI, a senior law enforcement expert played a pivotal role in orchestrating an insightful workshop that marked the culmination of the NAUSS-UNICRI convened forum. During the workshop, the initial exercise focused on a comprehensive analysis, delving into identifying challenges, training gaps, and the requisite skills and processes essential for the effective implementation of Responsible AI innovation. Participants actively engaged in discussions, drawing from their expertise to address pertinent issues and map out strategic approaches.




The second exercise proved equally impactful, centered on the practical application of Responsible AI innovation using the Responsible AI Toolkit. The objective of this session was to enhance preparedness among participants by presenting real-life cases for utilizing the toolkit. The goal was to guide attendees through the intricacies of integrating Responsible AI into law enforcement practices, offering practical insights and hands-on experiences.

The collaborative efforts of attending experts ensured that participants left the workshop equipped with actionable insights and tangible resources, fostering a heightened level of preparedness for the evolving landscape of AI innovation within the law enforcement domain.

iv. Regional perspective

The survey conducted among law enforcement professionals unveiled crucial insights into the awareness and preparedness for responsible AI innovation. Here are the key findings:

- i. Awareness of Responsible AI Innovation:** participants were asked to rate their awareness of the importance of responsible AI innovation and building capabilities for responsible use. The average rating for this question was an impressive **4/5**, indicating a high level of awareness and recognition of the significance of responsible AI in law enforcement.
- ii. Established Guidelines or Principles:** regarding the presence of established guidelines or principles for the responsible development and deployment of AI, 2 out of 3 respondents affirmed that their organizations do not have such guidelines.
- iii. Ongoing AI Education Programs:** when it comes to AI education programs or training initiatives to keep personnel informed about best practices and ethical considerations, the majority of respondents (2 out of 3) confirmed that their organizations do not provide ongoing AI education.
- iv. Steps to Ensure Responsible AI Use:** participants were asked about the steps they believe should be taken to ensure responsible and ethical AI use in law enforcement. The vast majority expressed that all options presented should be implemented, demonstrating a comprehensive approach to responsible AI usage. These steps included policy and regulation, transparency, data security and quality management, third-party audits and assessments, human oversight, training and education, community engagement, ethics committees, regular reviews and updates, and international collaboration.
- v. Training Areas in Need of Improvement:** in the context of law enforcement, capacity building, and the responsible use of AI, respondents identified key training areas that require improvement. These areas included AI fundamentals, ethical considerations, data privacy and security, and bias detection and mitigation. Each of these areas received equal attention from participants, underlining their significance.

- 
- vi. **Research Focus Area:** for research, participants identified several crucial areas that require more attention and improvement. These included algorithm transparency, AI-enhanced investigations protocols, incident response and accountability, data privacy and security, and bias mitigation, detection, and auditing.
 - vii. **Skills and Skillsets:** in the context of law enforcement, capacity building, and the responsible use of AI, participants highlighted specific skills or skillsets that demand more attention and improvement. These included data handling, bias detection and mitigation, risk assessment, the use of AI tools, ethical awareness, legal and regulatory knowledge, and transparency and accountability.

5(e1). Key Findings of Theme 4

- i. **High Awareness of Responsible AI Innovation:** Law enforcement professionals exhibit a high level of awareness and recognition of the importance of responsible AI innovation and the significance of building capacities for its responsible use. On average, participants rated their awareness at an impressive 4/5, reflecting a strong understanding of this concept within the field.
- ii. **Lack of Established Guidelines:** The majority of law enforcement organizations surveyed do not have established guidelines or principles for the responsible development and deployment of AI. Two out of three respondents confirmed the absence of such guidelines, highlighting a need for clear legal and ethical frameworks in AI implementation.
- iii. **Insufficient AI Education Programs:** A significant gap exists in AI education and training initiatives within law enforcement agencies. Approximately two out of three respondents reported that their organizations do not provide ongoing AI education, indicating the need for improved training programs to keep personnel informed about best practices and ethical considerations.
- iv. **Comprehensive Approach to Responsible AI:** Law enforcement professionals recognize the complexity of ensuring responsible, legal and ethical AI use. The majority of respondents expressed the importance of implementing multiple steps to achieve this, including policy and regulation, transparency, data security, and quality management, third-party audits, human oversight, training and education, community engagement, ethics committees, regular reviews and updates, and international collaboration. This comprehensive approach underscores the multifaceted nature of responsible AI implementation.
- v. **Key Training Areas in Need of Improvement:** Respondents identified specific training areas that require improvement for capacity building and the responsible use of AI in law enforcement. These areas include AI fundamentals, ethical considerations, data privacy and security, and bias detection and mitigation. The equal attention given to these areas emphasizes their critical importance in the responsible use of AI within law enforcement.




6. Conclusion

This report aspires to facilitate the progress of law enforcement agencies in Arab countries as they embrace AI technology and confront its potential misuse. Drawing upon the insights derived from presentations, practical cases, and group discussions, it becomes evident that law enforcement agencies have a considerable distance to cover to keep pace with the rapidly evolving AI technological landscape. It is crucial to examine these findings at an institutional level before addressing their global implications.

At both an institutional and local level, participants started by highlighting a deficiency in organizational support and adaptability for the integration of such technologies. Technological endorsement is not unanimous, and numerous institutional barriers frequently hinder progress, setting some countries behind already. Adequate resources, or the lack of, was also identified as one of the most crucial challenges. The technological infrastructure required for setting up, operating, and maintaining AI systems is deemed to be a substantial burden. Furthermore, even in cases where the necessary technical infrastructure is available, issues concerning data quality and accessibility persist. Many agencies struggle to acquire high-quality data suitable for AI applications. In addition to infrastructure and data, the know-how, skills, and education are consistently underscored as imperative for equipping current agencies with the requisite AI expertise and ensuring that upcoming generations of law enforcement experts are well-prepared. Priority areas for training include AI tools and software, AI in drones and robotics, as well as research in border security and surveillance, counter-terrorism, cybercrime detection and prevention, drones, robotics, and autonomous systems.

Zooming out, these shortcomings exacerbate the knowledge gap between countries that have adopted AI and those that have not. This, in turn, has prompted the very few countries or regions to develop regulatory frameworks. This discrepancy complicates the sharing of information, expertise, and know-how. Repeatedly emphasized is the crucial role of regional and international collaboration and collective efforts as the cornerstone of successful AI adoption in law enforcement. Currently, there appears to be a shortage of cooperation and joint initiatives in this regard.

From a malicious perspective, it is apparent that all sectors concur on the urgent necessity to address, stay ahead of, and proactively counter the myriad malevolent applications of AI. The increasing accessibility and lowered entry barriers, coupled with the ever-evolving and multi-faceted nature of AI-driven crimes, present a disconcerting trend that warrants considerable concern.



Advancements in AI and its integration into law enforcement have also spurred discussions on responsible AI usage and the need to ensure transparency, accountability, and safeguard privacy when fighting crime with AI. The debate between harnessing AI for safety and security versus the legal and ethical concerns looms large. While participants demonstrated a commendable level of awareness regarding responsible AI use, it was evident from the group discussions, survey results, and Responsible Use of AI Workshop that there is substantial work to be done in terms of educating and training law enforcement officers in the practical implementation of responsible AI practices. The most critical training areas identified encompass data privacy, as well as the detection and mitigation of bias.

In conclusion, the challenges and opportunities presented by AI adoption in law enforcement uses are multi-faceted and intricate, extending from institutional hurdles to international collaboration. Bridging the knowledge gap and fostering responsible AI practices are central to harnessing the potential of this technology for both security and ethics. As law enforcement agencies navigate this transformative landscape, it is imperative to invest in comprehensive training, remain vigilant against misuse, and nurture a global cooperation network to address the ever-evolving AI landscape collectively.



7. Recommendations

Based on the compilation of contributions from presentations and discussions from AI experts in law enforcement, industry, and academia, the following fundamental recommendations have been identified for Arab countries to consider in relation to the future of AI in the region:

- i. **Training, Education & Skills:** Prioritizing and investing in AI literacy and training for LEA personnel in the region is crucial. To address the significant skills gap and facilitate the effective adoption of AI in policing, authorities should develop comprehensive educational training programs emphasizing technical capabilities, AI tools, software, applications, data handling, privacy protection and responsible AI as a whole. Furthermore, given the increasing relevance of technologies like drones, robotics, and AI-based crime prevention, it is imperative to incorporate these topics into training curricula to ensure LEAs are prepared for future challenges. As a strategic initiative, NAUSS is introducing the Master in AI for Security (MAIS) Program, scheduled to commence in August 2024. This master's program is designed to address the specific requirements of security and law enforcement agencies, aiming to narrow the gap by incorporating specialized content. The program's curriculum is meticulously crafted to ensure its direct applicability to real-world security and law enforcement challenges.
- ii. **Research Areas:** Given the paramount importance of AI implementation in law enforcement, it is imperative to prioritize rigorous research in key areas with significant national and international security implications. Focus areas for research should encompass AI in border security, surveillance, counter-terrorism, cybercrime detection, and prevention, as well as the advancement of AI in drones, robotics, and autonomous systems, as well as research into data sovereignty and localization. Robust research in these critical domains will enhance strategic deployment and position law enforcement at the forefront of technological advancements in AI, enabling them to address the evolving challenges better and ensure our society's safety and security.
- iii. **Resources:** To address the budget limitations and resource constraints when integrating AI into their operations, law enforcement agencies should consider exploring partnerships and collaborations with academic institutions, private-sector companies, and other government agencies. Such partnerships can facilitate access to shared resources, expertise, and funding to support the development and implementation of AI systems. Additionally, seeking government grants and funding opportunities tailored to AI technology in law enforcement can offer the essential financial support to overcome these challenges and enhance the effectiveness of law enforcement operations.



- iv. **Regulation & Guidelines:** To address the absence of agreed-upon AI regulations and guidelines in law enforcement and to foster consistent and ethical integration, it is imperative to establish a comprehensive approach. This strategy should encompass the development of unified policies, regulations, transparency measures, data security protocols, and quality management standards. Such an approach will not only help bridge existing gaps but also facilitate and encourage data-sharing and cross-border collaboration, promoting a more standardized and responsible use of AI technologies across diverse jurisdictions.
- v. **Job Roles:** To fully harness the potential of AI technology in law enforcement, it is essential to establish specialized job profiles that cater to AI-related functions and seek to attract the relevant expertise into the agency. Based on the survey results, agencies see a need for creating roles for AI engineers, data analysts, machine learning engineers, data scientists, and data engineers. These positions will be instrumental in ensuring the effective integration and application of AI within LEA.
- vi. **Collaborations:** To address the challenges stemming from the lack of collaboration among LEA in AI integration, it is necessary to establish a comprehensive framework for knowledge sharing and best practices. This framework should prioritize the development of standardized methods, facilitate cross-border collaboration, and the promotion of data availability and sharing. By fostering seamless cooperation at regional and international levels, LEA can unlock the full potential of AI for crime prevention and investigation.
- vii. **Malicious AI:** Given the AI threat landscape and the widespread consensus among experts regarding the potential malicious use of AI, LEAs, academia, and industry stakeholders must collaborate closely. Prioritizing investments in education, research, training, and technology is highly recommended to bolster cybersecurity expertise, data analysis capabilities, and threat intelligence. Additionally, organizations should concentrate on developing advanced tools for detecting and preventing malicious applications of AI. Through these collaborative efforts and innovative approaches, LEAs can effectively mitigate the risks associated with AI-related criminal activities and safeguard digital ecosystems.
- viii. **Responsible AI:** To ensure the responsible, legal and ethical use of AI in law enforcement while safeguarding data, preventing misuse, and addressing biases, LEAs should establish comprehensive guidelines for responsible AI use. These guidelines should encompass critical domains such as policy and regulation, transparency, data security, and ethical considerations. Additionally, LEAs are encouraged to develop and implement responsible AI education programs and training programs that focus on AI fundamentals, ethics, data privacy and security, bias detection, and mitigation. Decision-makers should consider collaborating with



international organizations to align their responsible AI mechanisms with internationally recognized standards. Furthermore, research efforts should concentrate on algorithm transparency, AI-enhanced investigation protocols, incident response and accountability, data privacy and security, bias mitigation, and detection and auditing.

- ix. **Data Availability:** It is recommended to prioritize and advocate for the proactive integration of AI technologies within LEA while emphasizing transparency, accountability, and the mitigation of privacy and bias concerns. This should be accompanied by a combined effort to address data availability challenges through initiatives that facilitate data collection and sharing within the law enforcement community.



References:

Chiancine, C. (2023). The Role of Artificial Intelligence in Law Enforcement. [\(3\) The Role of Artificial Intelligence in Law Enforcement | LinkedIn](#)

Heinemeyer, M. (2023). Tackling the Soft Underbelly of Cyber Security - Email Compromise. Darktrace. [Tackling the Soft Underbelly of Cyber Security - Email Compromise | Darktrace Blog](#)

McKinsey. (2023). The state of AI in 2023: Generative AI's breakout year. [The state of AI in 2023: Generative AI's breakout year | McKinsey](#)

United Nations Interregional Crime and Justice Research Institute (UNICRI), (2019). Artificial Intelligence and Robotics for Law Enforcement. [ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW ENFORCEMENT_WEB_0.pdf \(unicri.it\)](#)

United Nations Office of Counter-Terrorism (UNOCT), (2021). Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes. [Malicious Use of AI - UNCCT-UNICRI Report_Web.pdf](#)

Appendix 1

Use-Case Title	Country/Organization
Gait Recognition for Security Purposes to Improve Investigations based on Deep Learning	Hashemite Kingdom of Jordan
Abusive Content Detection on X Using Machine Learning	Kuwait
On Predictive Models	London School of Economics
Traffic Management System (TMS)	Hashemite Kingdom of Jordan
Smart Hotlines Processing - Using Arabic NLP	Internal Security Forces, Lebanon
The Integrated Fan Journey at the FIFA World Cup Qatar	Ministry of Interior, Qatar
AI for Large Event Management and Public Safety	Nanyang Technological University, Singapore
AI-enabled Social Network Analysis Capabilities for Counter-Terrorism	Kulindalytics
AI-enabled Phishing Websites Detection Tool	Naif Arab University for Security Sciences, KSA
AI-Drone Object Detection and Surveillance	Naif Arab University for Security Sciences, KSA



1st Artificial Intelligence Forum for Law Enforcement Uses

List of Use-Cases

Gait Recognition for Security Purposes to Improve Investigations based on Deep Learning

Hashemite Kingdom of Jordan

In this poster presentation, the law enforcement expert discussed his research results regarding the use of deep learning in analyzing human gait patterns.

Gait recognition can identify individuals by their walking patterns, unaffected by appearance changes or low-light conditions. Traditional methods include Appearance-based and Skeleton-based approaches, but the expert's research introduced a sensor-based approach using smartphone signals for rapid identification in security applications.

The research shows that using sensors notably improves gait recognition, addressing issues in other methods. This approach, utilizing smartphones, offers potential benefits for law enforcement, enabling the collection of time-series gait data for security purposes.

Abusive Content Detection on X Using Machine Learning

Kuwait

A law enforcement expert emphasized a crucial problem during their presentation: the vast amount of big data produced on social media, which cannot be effectively managed using manual methods. They pointed out that criminals using social media to display illegal activities can harm law enforcement's image and public trust. Additionally, this criminal content on social media can have a significant impact on a large part of the population, necessitating automated investigation by authorities.

The project developed by law enforcement expert aimed to develop a machine learning model to detect abusive or hate speech content in social media accounts, specifically on a platform like Twitter. This detection would help identify users potentially engaged in criminal activities.

To achieve this goal, the expert employed three distinct machine learning algorithms: Logistic Regression (LR), Random Forest (RF), and Support Vector Machine (SVM). The approach involved converting raw data into meaningful features using the Bag of Words (BOW) technique, which focused on the presence and frequency of words to create a vector representation. Additionally, Term Frequency-Inverse Document Frequency (TF-IDF) was used to assess the significance of each word, considering its prevalence within a specific document and its rarity across a broader collection of documents. The model development process was carried out using Python, and two datasets, one containing hate speech and the other abusive content, were used to train and test the machine learning models.

The achieved results were promising for all three machine learning algorithms, but Logistic Regression emerged as the most effective choice, showing superior performance in identifying abusive Twitter accounts.



On Predictive Models

London School of Economics

This poster presentation focuses on data-driven methods for understanding and predicting crime and incidents, using both bottom-up and top-down approaches. It emphasizes machine learning techniques, challenges in assessing police service demand, determinants of demand, and the use of data from 18 police forces. Additionally, it introduces a new approach for understanding road traffic accidents and explores top-down data applications for crowd counting and organized crime prediction.

Part II: Balanced Policing

The presentation introduces “Balanced Policing,” which aims to efficiently allocate police resources by balancing fairness and deterrence. It recognizes the challenge of distributing resources fairly while maintaining public safety. Key points include identifying areas with excessive or inadequate policing, utilizing data analysis for resource allocation, and outlining future steps for improvement, including forecasting demand, testing dynamic deployment, expansion, automation, and enhancing the understanding of deterrence effects.

In summary, this use case poster presentation primarily focuses on enhancing the allocation of police resources by harmonizing fairness and deterrence through data-driven methods, ensuring that officers are deployed where their presence is most crucial. It also highlights the importance of continual improvement and assessment of the policing strategy.

Traffic Management System (TMS)

Public Security Directorate/Dept. of Communications and Information Technology/AI Team, Hashemite Kingdom of Jordan

During the presentation, the law enforcement specialist discussed the development of an intelligent traffic management system. They utilized artificial intelligence to collect road condition data, implemented Python and Java for database creation, and focused on relevant traffic information. Machine learning and deep learning techniques were employed to predict traffic conditions. The system integrated data from multiple sources, including weather and traffic factors, aiding in congestion management and finding alternate routes.

This project aims to offer traffic organizers important statistics using surveillance camera data instead of GPS data from vehicles. It can also connect with the licensing department to detect expired or unlicensed vehicles.

The presentation highlights AI benefits in traffic analysis, focusing on accuracy, feedback, security, minimal human involvement, and ethical alignment with national AI strategy. It's the first project from the Public Security AI Team, in line with the National AI Strategy for digital transformation.

Smart Hotlines Processing - Using Arabic NLP

Internal Security Forces, Lebanon

In this use-case presentation, a law enforcement specialist detailed their use of Arabic Natural Language Processing (NLP) to process heterogeneous multisource information in the context of hotlines.

The purpose behind implementing such technology was to address the issue of misclassified reports in cases of incidents, crimes, and investigations. The classification deficiencies had resulted in incorrect actions, incomplete analysis, and defective decision-making. The following NLP process schema illustrates the steps involved in utilizing this technology:

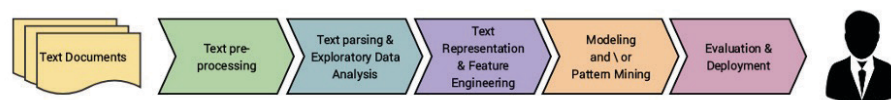


Figure. 6. Step-by-step NLP process


Some of the key findings from this use case concerning the execution methodology were:

- iv. The Arabic language is intricate and challenging,
- v. There is a lack of official free annotation tools,
- vi. There is a shortage of training data.

The Arabic crime tests fell into classification under eleven different labels as shown in Table 3:

Table 3. Classification of crimes

أفعال ضد الملكية	Acts against poverty
أعمال ضد السلامة العامة وأمن الدولة	Acts against public safety & state security
اعمال تسبب الضرر للشخص	Acts that cause harm to the person
أعمال التي تنطوي على المؤثرات العقلية أو المخدرات	Works involving psychotropic substances or drugs
أعمال ضد النظام العام والسلطة وأحكام الدولة	Acts against public order, authority and state provisions
افعال تسبب الوفاة	Acts causing death
أعمال التي تنطوي على احتيال أو الخداع أو الفساد	Acts involving fraud, deception or corruption
أفعال الضارة ذات الطابع الجنسي	Harmful acts of a sexual nature
اشتباه بجرم	Suspicion of a crime
مخالفات و حوادث اخرى	Other violations & different accidents
مختلف	Different



Among all the classification models employed, AraBERT demonstrated a testing accuracy of 85.82%. It excelled in comprehending the meaning and context of Arabic sentences, as well as in understanding the semantic relationships between Arabic words.

In this presentation, the speaker explained how Qatari MOI deployed the 'Hayya' platform, a connected and integrated IT platform aimed at centralizing the entire fan experience in one place. The platform integrated 20+ systems for fan convenience and safety, including their information, security check, border control, transport system, hotels/residences, mobile cards, FIFA ticketing system, stadium access, FAN zone access, health services, and security profiling information and data. MOI, Qatar representative went on to explain the use of AI (data science & analytics) in various components of the World Cup Organization, such as:

- Queue Management at the airport & stadiums, reducing queues, screenings, and managing the 40,000-80,000 daily fans visiting stadiums.
- Video Analytics (Computer Vision), supporting significantly in improving crime prevention (by 60%), detection, management of security operations, and increasing efficiency in incident response x10. The same systems were used for (1) Offender Search & Identification (80% accuracy), (2) Enhanced Security, (3) Prevent Terrorism & Violence, and (4) Monitor Access to Restricted Areas. Using AI, it took, on average, 0.3 seconds to search in a database of 1,500,000,000 faces.
- Intelligent Radar System (URS), technology was used for wanted vehicle identification (stolen vehicles, offender vehicle), to detect drivers using phones or not wearing seatbelts and alerting relevant authorities, and to identify vehicles parked in prohibited spots.
- Health Care Capacity Planning & Operation, used AI tools for demand and capacity forecasting, connecting all healthcare organizations, clinics, mobile medical units, ambulances, and staff across Qatar.
- Using AI for Health Care, using *Avey* this innovative healthcare solution (1) self-diagnosed instantly with the most accurate AI diagnostic algorithm in the world, (2) connected with the right doctors physically or virtually, (3) order medicines and more follow-up procedures effectively.



AI for Large Event Management and Public Safety

Nanyang Technological University, Singapore

Within the Digital Trust Centre framework, the speaker showcased AI research in the realm of large event management and public safety. The presentation delved into typical machine learning applications, such as object detection, face recognition, and machine translation, emphasizing the effectiveness of deep neural networks in these tasks. The discussion expanded to video analytics and deep learning, covering areas like object classification, pedestrian detection, cross-camera person re-ID, visual anomaly detection, action recognition, and person tracking. The speaker introduced topics like 'Deep Learning for Multi-Object Tracking,' 'Multi-media in Analytics in LE Operations,' and 'Intelligence Analytics & Decision Support,' leading into AI for next-generation law enforcement operations. The speaker also highlighted AI's potential in the legal industry, pointing out the key benefits of Generalized Boosted Trees (GBT), including automating routine tasks, swiftly and accurately analyzing large unstructured text data, uncovering hidden insights, and ensuring contract quality consistency among different parties.

The presentation also featured a segment on 'AI for Cyber Threat Intelligence,' exploring AI-enabled tools like document analytics, auto-summarization, NLP, and text-mining in the context of cybersecurity operations. The speaker shared lessons from translational research, including the importance of developing AI through systems engineering, leveraging domain-specific AI with machine learning and domain knowledge, and prioritizing human intelligence in designing complex intelligence systems to mirror user work processes.

AI-enabled Social Network Analysis Capabilities for Counter-Terrorism

Kulindalytics

In the use case presented by Kulindalytics, an expert explained the application of AI in social media network analysis, surpassing the limitations of human experts conducting manual analysis. The expert described the utilization of AI techniques, including:

- Algorithms for identifying abnormal activity within networks,
- Automated data collection and alerts at scale,
- Machine Learning for languages, sentiment analysis, and keyword trends,

These AI techniques enabled the execution of methods and approaches such as network and pattern analysis, direct engagement, network infiltration, and the analysis of themes, narratives, and content. These tasks, traditionally performed manually by human experts, were now automated.

However, while integrating AI into these previously manual domains, automating processes for real-time insights, new outputs, and data streams, the expert also identified certain AI limitations or “blind spots,” which include:


Table 4. AI limitations in Social Network Analysis

Area of understanding	Example weaknesses of AI	How AI sees the world	How humans see the world
Context and nuance	Understanding languages, slang, humor, satire, history, tribalism, and intertwined emotions such as anger, fear, and resentment	Seeks to understand how facts fit into history	Harbors emotions that cause the past to affect the present and the future
Human connections and communication	Understanding the human desire for purpose and the need to feel understood	Interprets communication at face value	Seeks deeper meaning and subtle messages in words, tone, phrases, and body language
Intentions	Differentiating between threats vs. the exploration of ideas, organic interactions vs. motives	Does not assume ulterior motives, interprets information at face value, and is not suspicious	Almost always suspicious and expects ulterior motives
The human experience	Viewing information through a lens that reflects a human perspective	Does not make real-life / on-the-ground connections and is objective without empathy	Constantly aware of real-life connections, self-centered but also empathetic

The expert characterized AI as perceiving the world through facts and statistics, in contrast to humans, who see it through stories and emotions. When AI lacks a complete understanding of the contextual aspects of a narrative, it can make incorrect recommendations and decisions and occasionally miss potential threats. Nonetheless, AI proves highly valuable when employed within specific bounds of social network analysis. The expert described the current state of AI as “just smart enough to be dangerous unless implemented with great care. Incredibly powerful when correctly placed.”

In terms of crafting an AI implementation strategy, the expert outlined the following key applications of AI that offer low risk and high benefits:

- Collect information: scrape social media and crawl websites, combine geospatial data,

- 
- Process information: generate social networks, categorize media content, and combine with OSINT,
 - Identify anomalies: flag accounts that consistently interact with or post content in VE networks.

To ensure that AI remains within its designated scope, the expert advised establishing safeguards such as “no-go zones” and rules of engagement for AI usage in social network analysis. These safeguards include:

- Setting specific goals and desired outcomes
- Setting human context boundaries to create “givens”
- Identifying areas where AI and other technologies are best placed
- Assess the four category blind spots.

AI-enabled Phishing Websites Detection Tool

Naif Arab University for Security Sciences, KSA

An AI Expert from NAUSS delivered a use-case presentation on AI-Enabled Phishing Websites Detection Tool. Phishing is the malicious act of stealing personal information online with the intent to commit financial fraud. It typically involves unsolicited communications via email, SMS, or websites, where the attacker poses as a trustworthy third party to trick victims into revealing sensitive data, like login credentials and payment information. In the fourth quarter of 2022, APWG observed a record-breaking 1,350,037 phishing attacks, marking a concerning trend. A project at NAUSS is underway to combat this issue by developing a robust phishing website detection system utilizing machine learning and deep learning techniques. This system aims to create its dataset focused on phishing websites in the Arab region and analyze existing benchmark data. The goal is to empower law enforcement agencies and cybercrime investigators with a tool to detect phishing websites effectively. Currently in the conceptual phase, the project’s completion is expected to benefit law enforcement agencies, cybercrime investigators, and financial institutions and enhance community awareness through sharing its findings with local and international law enforcement agencies.

AI-Drone Object Detection and Surveillance

Naif Arab University for Security Sciences, KSA

A professor from NAUSS gave an informative presentation on their advanced drone technology work, primarily focused on R&D for law enforcement. They emphasized AI and drone training, showcasing the NAUSS Drone Laboratory, which integrates AI with drones to detect dangerous objects at crime scenes, even in low-light conditions. They discussed their use of Large Language Models and Transformer architecture for object detection, outperforming the popular YOLO version 5. They also high-



lighted the development of a fully automated Dangerous Object Detection Recognition (DFR) command center system that works with drones, offering promising security solutions. Ongoing research aims to enhance this technology's performance.