IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

AI on the frontlines: Transforming border security in the fight against drug and arms smuggling

Mansoor G. Al-Thani

Technical Affairs Department, Ministry of Interior, Qatar.

(*Email: mbgalthani87@gmail.com*)

Abstract

Transnational drug and arms smuggling has evolved into a multidimensional challenge, increasingly enabled by advanced technologies that outpace traditional border security systems. This review offers a comprehensive and original synthesis of how Artificial Intelligence (AI) is reshaping global counter-smuggling efforts across land, maritime, and cyber domains. Unlike prior literature that often focuses on narrow technical or regional applications, this review uniquely integrates interdisciplinary perspectives, drawing from computer science, international security, ethics, and policy. It distinguishes itself by exploring a wide spectrum of cutting-edge AI tools, such as federated learning, quantum machine learning, swarm robotics, and explainable AI, within real-world border control operations. The review also addresses adversarial AI threats rarely examined in depth, including deep-fake documentation and subterranean drone deployments. These forward-looking insights set the review apart as both a technological analysis and a strategic foresight exercise. Furthermore, this work critically evaluates the ethical, legal, and infrastructural challenges of AI deployment, particularly in low- and middle-income countries, an angle largely neglected in existing literature. It highlights disparities in technological access, the risks of algorithmic bias, and the tensions between national security and individual privacy, offering concrete mitigation strategies such as decentralized machine learning models. Ultimately, this review is distinctive for its depth, breadth, and policy relevance through comparative case studies. It goes beyond technical functionality to underscore the ethical and geopolitical implications of AI in border security, positioning technology not only as a powerful defense tool but also as a strategic domain requiring global cooperation, responsible governance, and sustained innovation.

Keywords: AI ethics, Arms trafficking, Artificial intelligence, Border security, Computer vision, Drug smuggling, Machine learning, Predictive analytics, Surveillance technologies, Transnational crime.

DOI: 10.53894/ijirss.v8i4.8277
Funding: This study received no specific financial support.
History: Received: 29 April 2025 / **Revised:** 4 June 2025 / **Accepted:** 6 June 2025 / **Published:** 4 July 2025

Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.
Transparency: The author confirms that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Organized criminal networks, with an estimated annual turnover of around US$870 billion, make money by selling illegal items wherever there is a need. These massive illicit revenues are equivalent to 1.5% of the world's GDP or 7% of worldwide merchandise exports and are worth more than six times the amount of official development assistance [1]. Moreover, the global drug trade and illicit arms trafficking have escalated into some of the most pervasive threats to national and international security. According to the United Nations Office on Drugs and Crime [2], the international drug trade is currently valued at over $320 billion annually, with similar patterns of proliferation evident in the movement of firearms and military-grade equipment [2]. These networks not only finance organized crime but also contribute to political destabilization, transnational violence, and systemic corruption across borders [2].

Conventional border security mechanisms, such as manual inspections, rule-based surveillance, and patrol-centric monitoring, are increasingly insufficient in mitigating these evolving threats. Smugglers now exploit advanced technologies, including AI-guided drone delivery systems [3], 3D-printed firearms that evade conventional detection [4] and decentralized, blockchain-enabled logistics that obscure the traceability of illicit transactions [5]. These developments demand a paradigm shift in the methods and tools utilized by border control agencies.

AI offers transformative potential in addressing these challenges. Its core strength lies in the capacity to analyze vast and complex multi-modal datasets [6] ranging from satellite imagery [7] and X-ray scans [8] to social media chatter and encrypted dark web communications [9]. Furthermore, AI systems possess adaptive learning capabilities, enabling them to evolve in response to shifting smuggling patterns and adversarial tactics [10]. When integrated effectively, AI can provide strategic foresight, enhance situational awareness, and support faster and more accurate interdictions [11].

This review aims to provide a comprehensive synthesis of how AI is being leveraged to counteract the global drug and arms smuggling crisis. It critically assesses the state-of-the-art technologies and operational frameworks employed at national borders, seaports, and customs facilities, while also identifying key gaps in their deployment. Specifically, the review seeks to explore three major dimensions. First, it investigates technological disparities, particularly the challenges faced by developing countries in deploying low-resource AI solutions. Second, it addresses the ethical implications of AI deployment, such as balancing privacy rights with national security imperatives. For example, facial recognition systems at border crossings raise serious concerns under data protection regulations such as the General Data Protection Regulation (GDPR) in Europe [12]. Third, it examines the growing role of interagency and international collaboration, including platforms like INTERPOL's AI-enhanced threat analysis toolkit [13] and the World Customs Organization's risk management systems [14].

This review distinguishes itself within the current body of literature through its interdisciplinary breadth, original perspectives, and strong policy relevance. Unlike previous works, such as those by Cani et al. [15], Ige et al. [16], Jejelola [17] and Mademlis et al. [18], which often focus on singular domains or regional scopes, this paper offers a more integrative analysis that bridges technical innovations, ethical considerations, and geopolitical imperatives (Table 1). Among its notable strengths are the incorporation of cutting-edge AI technologies such as federated learning, swarm robotics, and quantum machine learning within operational border security contexts. The review also advances the discourse on ethics by engaging with GDPR compliance, explainable AI (XAI), and decentralized privacy-preserving architectures. Furthermore, it provides practical value through forward-looking policy recommendations, advocating for globally harmonized AI standards, enhanced cross-border intelligence sharing, and scalable AI solutions tailored for low- and middle-income countries. By exploring these themes, the review seeks to inform both practitioners and policymakers on the strategic integration of AI into border security operations. Ultimately, it stresses the urgent need for proactive innovation, ethical governance, and cross-border intelligence sharing to ensure that technological advantages remain with law enforcement rather than criminal enterprises.

Table 1.
Comparative analysis of AI-driven reviews in border security and smuggling detection.

Criteria	**This review**	Cani et al. [15]	Jejelola [17]	Mademlis et al. [18]	Ige et al. [16]
Focus Area	AI in border security for drug and arms smuggling	AI for combating illicit firearms in the EU	General AI applications in transnational crime	Illicit trafficking and AI-enabled countermeasures	Computer vision for contraband detection
Technologies Reviewed	ML, CV, Predictive Analytics, UAVs, NLP, Federated Learning, QML, Swarm Robotics	Cyber-patrolling, Predictive Modeling, Network Analysis	ML, Crime Pattern Recognition, Risk Profiling	AI surveillance, Dark Web analysis, Adaptive systems	Deep learning, Object recognition
Novel Aspects	Deepfake threats, subterranean drones, quantum AI, federated learning, ethics & policy integration	Emphasis on EU law enforcement needs	Broad thematic synthesis of AI-crime interactions	Dark web trafficking trends and counter-AI tools	Focused use of CV at border checkpoints
Ethical Discussion	Extensive: GDPR, algorithmic bias, data governance, explainable AI	Limited to EU regulatory context	Brief mention of AI risks and privacy	Moderate ethical concerns raised	Limited/no ethical dimension covered
Geographical Scope	Global (U.S., EU, Africa, Middle East, Latin America)	EU-centric	Global (academic view)	International (EU + U.S. focused)	Global (technology-centric)
Policy & Governance Recommendations	Reflected on UN-led AI standards, cross-border data trusts, capacity building, and public-private R&D	Limited to EU frameworks	Lightly touched	Briefly mentioned	None
Application Depth	Detailed case studies, real-time systems, UAVs, customs scanning, NLP in encrypted apps	Project-focused, development-phase AI tools	Thematic and conceptual overview	Tactical uses with emphasis on digital environments	Technical applications only

2. Methodology

To enhance transparency and ensure reproducibility, this review followed a structured literature selection process consistent with PRISMA guidelines. An initial search across academic databases such as Scopus, Google Scholar, and Web of Science yielded 89 records, with an additional 3 sources identified through manual searches of policy reports and other literature. After removing 2 duplicates, a total of 90 records were screened based on title and abstract. Of these, 11 were excluded either because they were not fully accessible or because the content did not provide the needed information. The remaining 79 full-text articles were assessed for eligibility and were ultimately included in the qualitative synthesis.

The search included articles published in the English language using the following keywords: “Artificial Intelligence; Border Security; Drug Smuggling; Arms Trafficking; Machine Learning; Computer Vision; Predictive Analytics; AI Ethics; Surveillance Technologies; Transnational Crime.” The inclusion criteria were set to include peer-reviewed journal articles, policy reports, and systematic reviews in English without limiting the date of publication. Conversely, an exclusion criterion was implemented to avoid blog posts or opinion pieces, duplicates, and inaccessible full-text resources. A PRISMA flow diagram summarizing the selection process is provided in Figure 1.

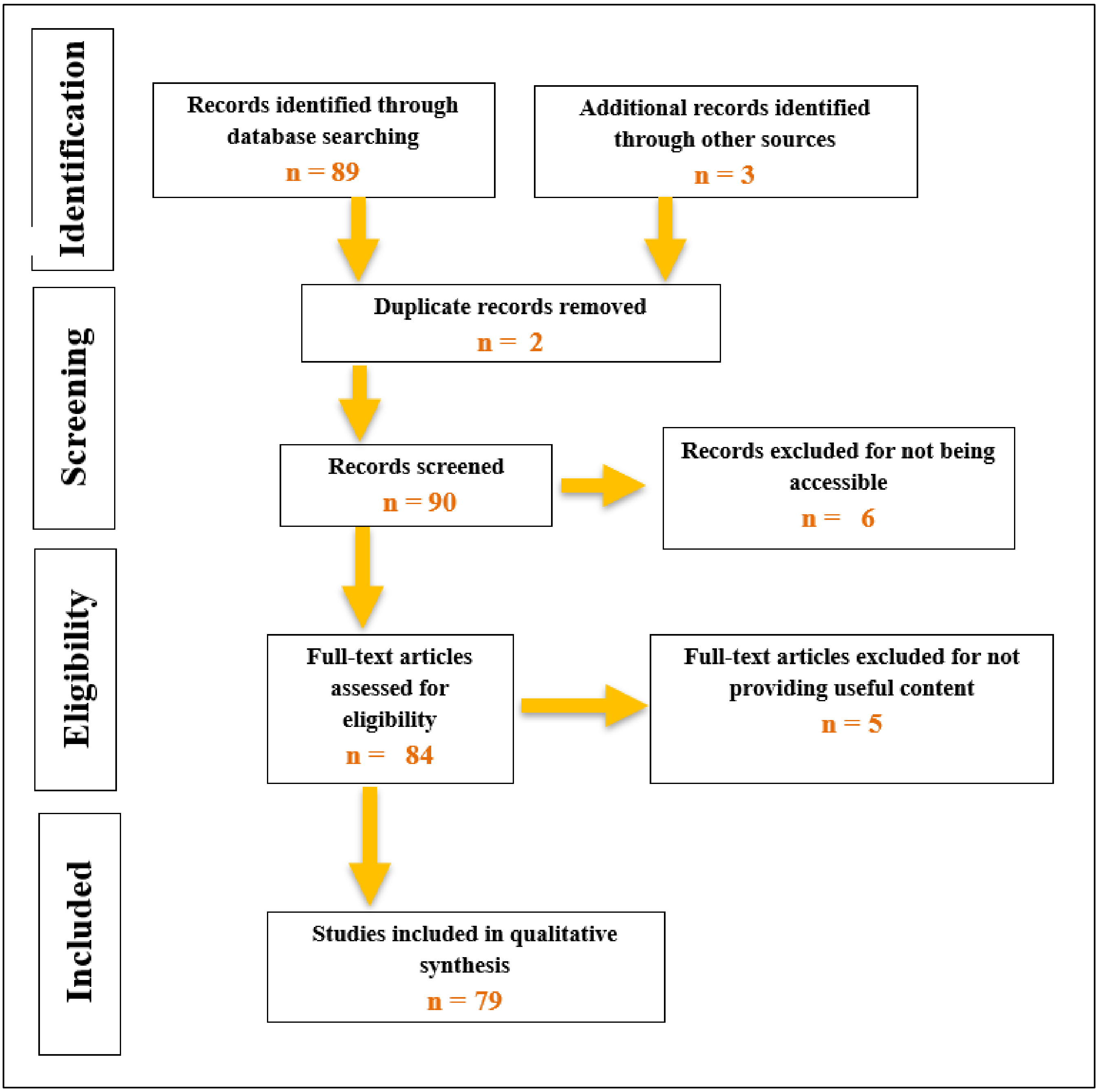

Identification
Screening
Eligibility
Included
Records identified through database searching
n = 89
Additional records identified through other sources
n = 3
Duplicate records removed
n = 2
Records screened
n = 90
Records excluded for not being accessible
n = 6
Full-text articles assessed for eligibility
n = 84
Full-text articles excluded for not providing useful content
n = 5
Studies included in qualitative synthesis
n = 79

Figure 1.
PRISMA diagram of the literature selection process.

3. The Technological Landscape of AI in Border Security

An innovative step in how countries address transnational crime concerns is the integration of artificial intelligence into border protection. AI provides border control organizations with the ability to identify, intercept, and stop smuggling operations with unprecedented speed and accuracy by replacing reactive, labor-intensive approaches with data-driven, autonomous systems. The key technological applications of AI in border operations are examined in this section, with particular attention paid to three interconnected areas: autonomous enforcement platforms, predictive analytics, and intelligent surveillance systems.

3.1. AI-Powered Surveillance

AI-driven surveillance technologies have become indispensable in securing national borders, especially in regions characterized by difficult terrain, limited manpower, or high traffic. These systems leverage advances in machine vision, edge computing, and real-time data fusion to monitor vast stretches of border with minimal human intervention [19].

One of the most prominent applications is facial recognition and biometric verification at border checkpoints [20]. AI algorithms trained on vast biometric databases can instantly compare a traveler's face with passport or visa records to confirm identity, flag anomalies, and detect forged documentation. The U.S. Department of Homeland Security's Biometric Exit Program, for example, demonstrated that AI-based facial recognition can achieve accuracy rates exceeding 97% in identifying overstayed visa holders and fraudulent identities [21]. These systems reduce processing time, minimize human error, and mitigate the risk of identity theft or alias-based border crossings. In addition to static checkpoint technologies, smart CCTV systems employing deep learning algorithms can detect behavioral anomalies such as loitering, rapid movements, or suspicious item transfers [22]. These systems are capable of learning patterns from recorded footage and flagging irregularities without manual input [22]. Through integration with national crime databases, they also support real-time alerts to intercept known smugglers or persons of interest.

AI also enhances thermal and multi-spectral imaging, particularly in terrain where visual surveillance is limited, such as deserts, mountainous regions, or densely forested areas [23]. AI-enabled drones equipped with thermal cameras can identify human body heat signatures, movement patterns, or vehicle trails that are otherwise invisible to conventional optical sensors [24]. Such capabilities have proven crucial in preventing unauthorized crossings along remote parts of the U.S.–Mexico border [25].

3.2. Predictive Analytics and Threat Forecasting

Beyond immediate surveillance, one of the most powerful applications of AI lies in its predictive capacities. By aggregating and analyzing diverse data sources, including shipping logs [26], migration patterns [27], criminal records[28], satellite data [29] and geopolitical events [30]. AI systems can anticipate smuggling attempts and direct enforcement actions accordingly. Cargo risk profiling and anomaly detection are fundamental tools in modern customs enforcement [31]**.** Learning algorithms trained on historical inspection data can detect discrepancies in shipping manifests, unusual trade routes, or cargo weight and volume inconsistencies. These systems are increasingly used alongside advanced scanning technologies, enabling automated identification of illegal imports hidden within containers or vehicles [32]. Global trade has been transformed by shipping containers, which are now essential to supply chain infrastructure. To ensure the contents are properly safeguarded, shipping containers must be inspected regularly. Inspection of shipping containers involves monitoring their safety and security during transit to confirm they have not been tampered with and are maintained in good condition throughout their lifecycle. Currently, human observation is used to manually inspect containers, which is labor-intensive and prone to errors [32].

To address this challenge, Bahrami [32] has used data-driven analytics for the automated inspection of shipping containers [32]. First, the security of shipping containers is examined. The automated security examination of shipping containers uses a deep learning-based architecture to analyze security seals on the back of the container. An attention-based memory bank is used to extract long-range spatial relationships, and a multi-scale, multi-depth image pyramid network is used to extract feature representations. The terminals receive a very precise and effective security inspection solution from these two modules. After that, a comprehensive inspection of the containers' safety status is conducted to keep them in good condition. Lastly, a deep learning-based supervised architecture is suggested for identifying and describing surface flaws in shipping containers [32]. To achieve high performance in defect identification, the suggested framework combines two attention-based memory banks with a multi-scale, multi-depth picture pyramid network. To determine the proportion of flaws on a container's surface, the framework also presents a novel optical flow-based picture stitching technique for defect characterization. Finally, an architecture based on unsupervised deep learning is developed to check shipping containers for safety [32]. Human annotators are required to prepare a significant amount of data and its ground truth, which is expensive and time-consuming. To identify anomalous areas on the surface of containers, the proposed system uses Siamese networks and multi-scale, multi-depth networks for feature extraction and defect formation. The suggested architecture functions well at terminals with different conditions and is broadly applicable. The results of the study will help standardize and strengthen container management and logistics at terminals, which will benefit the worldwide transportation sector [32]**.**

Another application was recently published Emaani and Saghaei [33]. About 500,000 owner-operator drivers comprise the Iranian road transportation industry, which is experiencing an increase in syndication issues, causing interruptions and driver refusals in certain provinces. Drivers emphasize the urgent need to improve terminal load distribution. The assessment of driver assumptions begins with the use of K-means clustering. Emaani and Saghaei [33] explore anomaly detection by drivers in cargo terminals [33]. According to the survey, drivers who handle more freight in less time are more reliable. After that, data mining techniques are used to identify anomalous activity utilizing the Isolation Forest, KNN, and Histogram-Based Outlier Score (HBOS) algorithms. The findings show three different driving groups, with one group accounting for a significant percentage (98%) of the abnormalities. Researchers and shipping professionals can learn a lot from that study, which clarifies the crucial systemic problem of drivers detecting anomalies in cargo terminals. The underutilization of clustering in earlier literature reviews centered on case study analysis is further evidenced by the fact that the paucity of research on theft prevention makes traditional approaches ineffective [33].

Another key innovation is the ability of AI systems to predict smuggling routes based on dynamic risk modeling. These models incorporate real-time variables, such as enforcement activity, climate conditions, or political instability, to forecast shifts in trafficking routes [34] A novel framework was developed combining a dynamic Bayesian network to assess the risk performance of maritime shipping routes. To accomplish this, the authors have created a useful framework that uses a Dynamic Bayesian Network (DBN) model to probabilistically represent the interacting relationships between significant components. To address the issue of unbalanced marine accident reports, this framework combines the edited closest neighbor method with the synthetic minority over-sampling strategy. The framework identifies major influencing factors at various time intervals and allows for dynamic consideration of the risk performance of maritime routes [34]. According to their scientific research, the catastrophic effects of terrorism on shipping routes are classified in declining order of severity, followed by other risk factors, including piracy, armed conflicts, and numerous induced dangers. Using the suggested methodology, the case study on the Indian Ocean shipping route shows a period of varying gains at first, followed by a dominant decreasing trend from 2009 to 2019. The results and approach offer marine stakeholders important assistance in making well-informed decisions [34].

AI is also transforming how agencies monitor online and encrypted communication platforms, including social media, messaging apps, and the dark web [35]. Cybercrimes on the Dark Web have significant and wide-ranging economic effects. Fraud, identity theft, and ransomware attacks are examples of cybercrimes that cause substantial financial damage to individuals, companies, and governments. For example, identity theft can deplete personal and business accounts, and ransomware attacks can result in large ransom payments. To prevent, identify, and address cybercrimes, organizations must also make significant investments in cybersecurity solutions. This includes the cost of employing cybersecurity experts, purchasing security software, and conducting regular security assessments. Cybercrimes also have broader economic repercussions, such as reduced customer trust in online transactions, disruptions to corporate operations, and impacts on national economies [35].

Besides, natural language processing (NLP) models can identify linguistic markers, coded slang, or behavioral cues indicative of illicit transactions. These systems can scan thousands of digital interactions in multiple languages to identify patterns preceding trafficking events [36]. Importantly, these tools must be deployed with attention to privacy and legal safeguards to prevent overreach or wrongful profiling.

3.3. Autonomous and Semi-Autonomous Systems

The operational burden of border enforcement can be significantly reduced through the use of AI-integrated autonomous systems. These platforms provide continuous monitoring capabilities across vast or hazardous areas where human patrols would be inefficient or dangerous.

Unmanned aerial vehicles (UAVs), equipped with AI-based navigation and analytics, can autonomously patrol borders, identify irregular movements, and relay live data to command centers. Applications of UAVs have grown in popularity recently due to their adaptability to a wide range of sensors, low operating costs, ease of deployment, and superior mobility. Remotely operating UAVs in complicated environments, however, restricts their capabilities and lowers system efficiency. As a result, numerous academics are focusing on autonomous UAV navigation, which allows UAVs to move and carry out duties according to their environment. Recent technical developments have led to a proliferation of AI applications.

One application where AI is essential in providing basic human control features is autonomous UAV navigation. To improve the efficiency of autonomous UAV navigation, numerous researchers have implemented various AI techniques [37]. Thoroughly examining and classifying several AI techniques for autonomous UAV navigation that have been suggested by various researchers. Model-based learning and mathematical optimization are two examples of many AI techniques (Figure 2). Their paper discusses the foundations, guiding ideas, and salient characteristics of various optimization-based and learning-based methodologies. To make AI implementation more comprehensible, the features, varieties, navigation models, and uses of UAVs are also discussed. Furthermore, the authors explore open research directions to provide researchers with clear and precise ideas for future research [37].

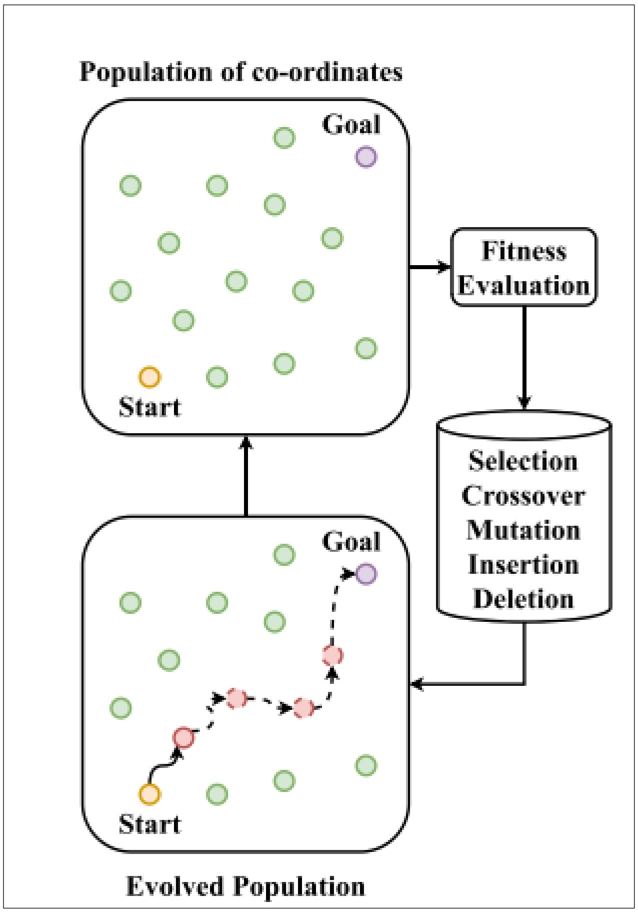


Figure 2.
A taxonomy of the artificial intelligence approaches for UAV navigation.
Source: Rezwan and Choi [37]

On land, robotic ground patrol units are being trialed in areas prone to smuggling tunnels, hidden compartments, and rugged terrain. These robots are outfitted with sensors and AI software that detect disturbances in soil, vibrations, or changes in subsurface structures, allowing them to uncover illicit underground networks used for arms and drug trafficking [38]. At inspection hubs such as seaports and customs terminals, AI-integrated inspection systems now employ robotic arms, automatic scanners, and decision-support algorithms to inspect cargo with high speed and accuracy. These tools automate vehicle and container checks, allowing customs agents to focus only on flagged anomalies. Such systems reduce inspection times while increasing detection rates.

4. The Evolving Landscape of Smuggling

The strategies and resources employed by transnational criminal organizations change along with enforcement technologies. Today's drug and weapons smuggling scenes are more complicated than ever, involving not only physical concealment but also digital deception, cyber-physical strategies, and AI-enabled evasive maneuvers. The most well-known new smuggling methods are examined in this section, along with important regional hotspots where there is a particularly fierce battle between law enforcement and illegal trade.

4.1. Emerging Tactics

Modern smugglers now integrate sophisticated technological infrastructure into their operations. One alarming trend is the use of cyber-physical smuggling, where traditional concealment methods are augmented by smart devices. For example, GPS-enabled cargo containers with encrypted IoT components can obscure their location or transmit false data, misleading customs authorities and enabling seamless transshipment across jurisdictions [39]. These methods complicate tracking efforts, especially when shipments traverse poorly governed or high-traffic regions.

An even more technologically advanced tactic involves AI-generated deepfake documentation [40]. The creation, identification, and attribution of synthetic media are among the uses of deep learning. To address this issue, Khoo et al. [40] developed a technique to characterize deepfake attribution as a way to not only identify phony photos but also to determine their origin and generation method (Figure 3**)** [40].

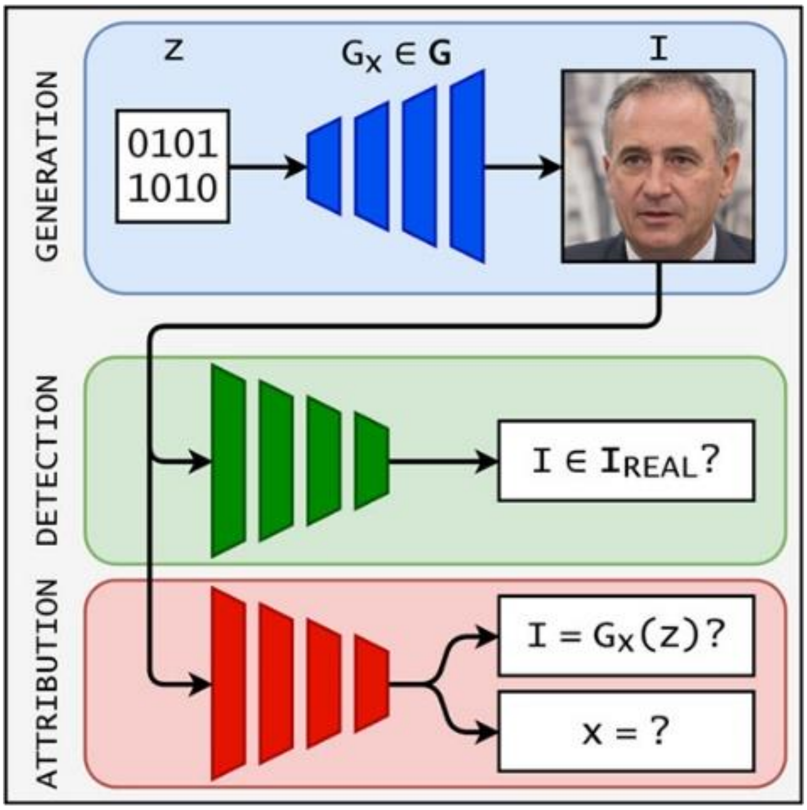
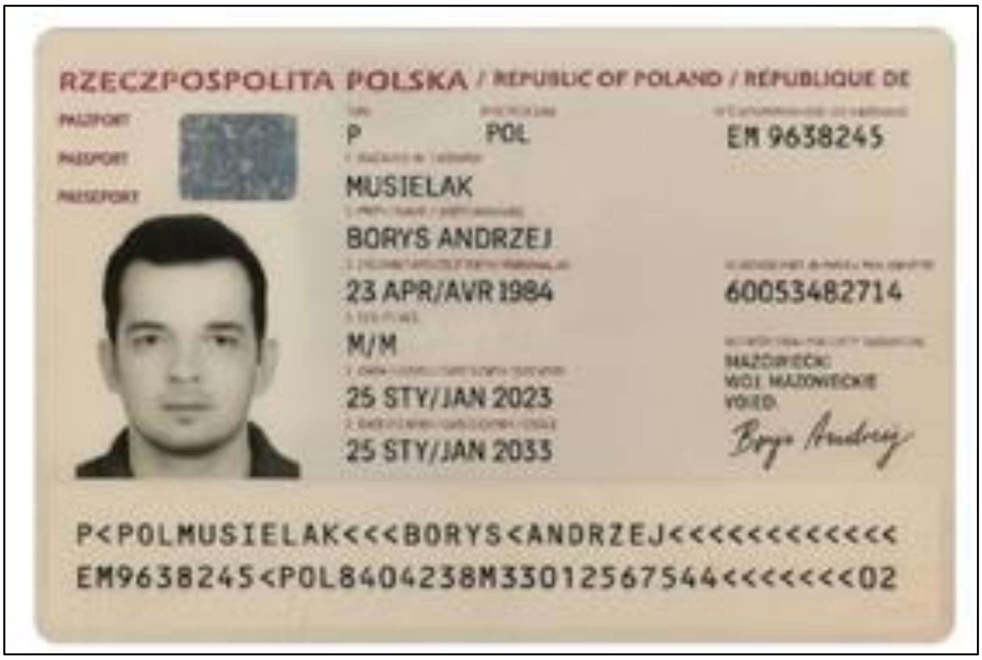


Figure 3.
Attribution, detection, and generation of deepfake documentation Khoo et al. [40].

In a recent case that has gained attention and calls into question the limits of AI's application, a Polish researcher, Borys Musielak, created a realistic-looking fake passport in five minutes using ChatGPT-4 (Figure 4). Most automatic Know Your Customer (KYC) systems could quickly detect the phony paper since it was so plausible [41].


RZECZPOSPOLITA POLSKA / REPUBLIC OF POLAND / RÉPUBLIQUE DE

PASZPORT
PASSPORT
PASSEPORT

P POL EM 9638245

MUSIELAK

BORYS ANDRZEJ

23 APR/AVR 1984

60053482714

M/M

MAZOWIECKI
WOJ. MAZOWIECKIE
VOIED

25 STY/JAN 2023

25 STY/JAN 2033

P<POLMUSIELAK<<<BORYS<ANDRZEJ<<<<<<<<<<<<
EM9638245<POL8404238M33012567544<<<<<<<02

Figure 4.
Image of the fake generated passport as posted by the researcher, Times of India AI Getting Dangerous [41].

Furthermore, with generative adversarial networks (GANs), smugglers can fabricate high-resolution passports, IDs, and bills of landing that evade both human scrutiny and basic digital verification. These falsified documents are increasingly being detected only through forensic AI models capable of analyzing pixel anomalies or text inconsistencies [42]. The implications are profound, as identity fraud becomes more scalable and accessible through open-source AI tools. Another evolving strategy includes the deployment of subterranean drones, which are compact, AI-navigated machines used to map and traverse drug tunnels [43]. Mexican cartels and other trafficking networks have reportedly begun deploying robotic platforms underground to identify structural weaknesses, map cross-border passages, and transport contraband while evading aerial surveillance [44]. These tactics pose a direct challenge to traditional counter-tunneling methods and demand a recalibration of detection frameworks.

4.2. Global Hotspots

The dynamics of smuggling vary considerably by region, shaped by geography, governance, and socio-economic factors. Nevertheless, several global hotspots stand out as critical pressure points where technological interventions have either succeeded or struggled. At the U.S.-Mexico border, smugglers have increasingly relied on aerial drone deliveries to circumvent ground patrols. These drones can carry high-value drug payloads across rural terrain and drop them via GPS coordinates to waiting recipients. In response, U.S. Customs and Border Protection (CBP) has implemented AI-powered radar systems and aerial threat classifiers capable of detecting low-flying drones in real time [45]. However, the cat-and-mouse dynamic continues as smugglers adopt stealthier flight paths and jamming countermeasures.

In the ports of the European Union (EU), particularly those in the Netherlands, Belgium, and Spain, smuggling networks exploit the high volume of maritime containers [46]. Concealed compartments within legal cargo are used to hide weapons, narcotics, and counterfeit goods [47]. The EU’s iBorderCtrl system has trialed AI-driven behavioral biometrics to screen individuals for deception, using facial micro-expressions and keystroke analysis during customs interviews [48].

In Africa’s Sahel region, arms trafficking is exacerbated by porous borders, political instability, and weak state infrastructure. Informal trade routes crisscross the region, facilitating the illicit movement of weapons from Libya to West Africa and the Horn of Africa [49]. The United Nations has responded by deploying satellite-AI fusion systems to monitor heat maps and vehicle patterns in contested regions. These systems help detect convoys or unusual movement patterns that could signal arms shipments, although a lack of infrastructure and training often impedes real-time interdiction (Table 2).

Table 2.
Comparative analysis of common AI-driven approaches to border security and smuggling prevention.

Title	**Main Focus**	**Technology Highlighted**	**Region/Agency**	**Source**
CEASEFIRE Project: An AI-Powered System for Combating Illicit Firearms Trafficking	Development of AI tools to support EU law enforcement in combating illicit firearms trafficking.	AI analytics, cyber-patrolling, predictive modeling	European Union (Horizon Europe Project)	Cani et al. [15]
The Role of Artificial Intelligence in the Eradication of Transnational Crime	Explores AI potential in dismantling transnational crime networks, including drug and arms smuggling.	Machine learning, predictive analytics, risk profiling	Global scope (Academic research)	Jejelola [17]
The Invisible Arms Race: Digital Trends in Illicit Goods Trafficking and AI-Enabled Responses	Analyzes the digital evolution of illicit goods trafficking and AI-enabled enforcement countermeasures.	AI surveillance, dark web monitoring, adaptive learning	International (Law enforcement and customs)	Mademlis et al. [18]
Enhancing Border Security and Countering Terrorism Through Computer Vision	Application of computer vision for border control and detecting contraband at checkpoints.	Computer vision, deep learning, object recognition	Global (Springer conference publication)	Ige et al. [16]
DHS Use of AI in Border Security	Overview of AI use cases in U.S. border security operations, including scanning, identification, and threat detection.	Machine learning, facial recognition, anomaly detection	United States (Department of Homeland Security)	U.S. Department of Homeland Security [50]

5. AI Technologies in Action

Artificial intelligence is actively influencing actual interdiction and intelligence operations; it is not only a theoretical or experimental instrument for border protection. This section explores the main artificial intelligence (AI) tools being used to stop the smuggling of drugs and weapons, with a particular emphasis on machine learning, computer vision, and predictive analytics. Although each technology operates in a different operational domain, they all work together to support an all-encompassing enforcement strategy.

5.1. Machine Learning (ML)

Machine learning, a subset of AI that enables systems to learn from data patterns and make predictions, is central to modern risk-based enforcement strategies. One key application lies in anomaly detection in financial transactions [51] Particularly in uncovering illicit financing routes tied to arms and narcotics trade. Algorithms such as random forests and gradient boosting machines are used to identify deviations from expected financial behaviors, flagging transactions that may indicate Hawala transfers or smuggling-related payments [52] developed an abnormal point scale is a concept that is proposed to assess the degree of abnormality in a sample based on its similarity. The abnormal samples are filtered out based on this scale, and the random forest method is introduced to discover abnormal samples. Simulation tests demonstrate that the random forest-based abnormal sample detection method outperforms the other two distance-based abnormal sample detection techniques in terms of increasing model accuracy and reducing computation time [52].

In addition, advanced ML models, especially transformer architectures like Bidirectional Encoder Representations from Transformers (BERT), have also proven effective in text-based threat identification [53]. These models can scan and interpret unstructured data from encrypted messaging apps, forums on the dark web, or multilingual social media platforms to detect suspicious activity. For example, in 2023, Europol collaborated with several AI research centers to apply BERT to track evolving slang terms and trafficking codes used by drug cartels, resulting in the interception of planned smuggling operations in Eastern Europe [54].

Furthermore, reinforcement learning algorithms are being employed to optimize inspection protocols at customs checkpoints. These systems dynamically adjust scanning intensity or selectivity based on real-time risk scoring, improving detection rates without overburdening border personnel.

5.2. Computer Vision (CV)

Computer vision, a field of AI that enables machines to interpret and act on visual input, has become indispensable in automated inspection and surveillance. At border crossings and seaports, hyperspectral imaging integrated with AI algorithms enables the detection of chemical residues that are invisible to traditional X-ray scans [55]. This allows for the identification of narcotics, explosives, or concealed firearms hidden within dense or metallic objects [56]. A notable implementation of CV is found in the Port of Rotterdam's "Smart Port" initiative, which combines image recognition, machine learning, and sensor fusion to accelerate and improve the inspection process [57]. These models cross-reference visual data with shipping manifests and customs databases, flagging inconsistencies and identifying patterns suggestive of smuggling. CV is also used in UAVs and fixed surveillance towers to automatically classify threats, distinguish between authorized and unauthorized movements, and detect tampering with infrastructure such as fencing or tunnels [58]. The use of edge computing allows these systems to function in bandwidth-constrained environments, such as border deserts or remote ports.

5.3. Predictive Analytics

One of the most critical applications of AI in border security is predictive analytics. These systems can determine the probability of illegal conduct linked to shipments, carriers, or people by examining customs reports, seizure records, and open-source intelligence. One notable model developed by the World Customs Organization (WCO) uses supervised learning techniques to generate risk scores for shipping containers, achieving up to 85% accuracy in identifying high-risk shipments based on prior data inputs [59]. The model incorporates a range of variables, including cargo origin, transit route, company history, and previous violations. These insights enable enforcement officers to prioritize inspections and allocate resources more effectively.

Predictive analytics also aids in geo-spatial threat modeling, where data from satellite imagery, drone surveillance, and ground sensors are used to map smuggling trends. These systems generate heat maps and risk gradients (Figure 5), allowing authorities to preemptively deploy resources to high-threat areas [60]. For instance, Colombia's national anti-narcotics directorate used predictive analytics to monitor shifts in coca cultivation and optimize drone deployment, accordingly, resulting in a reduction in new coca production [61]. Hence, the integration of ML, CV, and predictive analytics technologies offers a powerful triad for tackling the multifaceted challenges of smuggling. However, each tool must be calibrated for operational reliability, data bias mitigation, and legal compliance issues, further explored in subsequent sections.

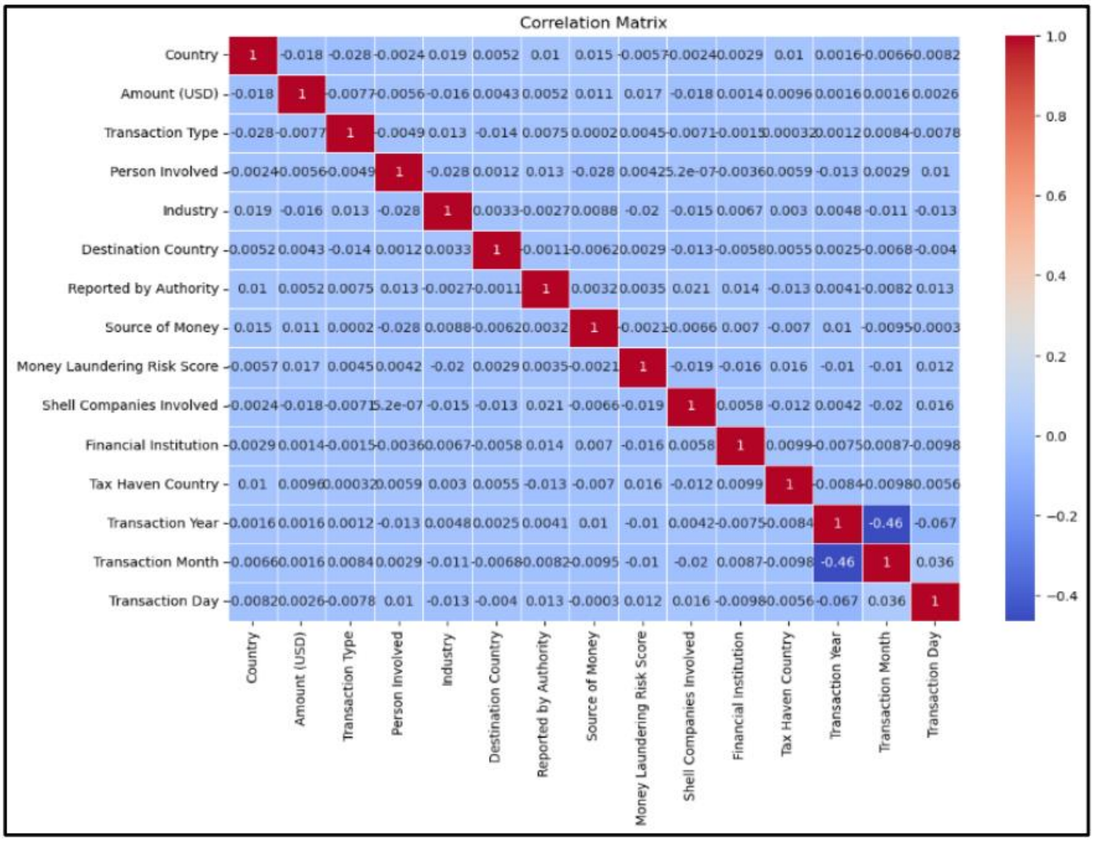


Figure 5.
The Correlation Heatmap between Various Factors in the Dataset Rahman et al. [60].

6. Ethical and Operational Challenges

The application of artificial intelligence presents serious operational, ethical, and legal issues despite its remarkable potential to enhance border security. When AI is used to track people, profile their behavior, or make judgments that impact basic rights such as privacy and freedom of movement, these issues become more evident. In the absence of strong protections, AI-enabled enforcement risks perpetuating discrimination, violating civil liberties, and eroding public confidence in law enforcement agencies.

6.1. Privacy Concerns

Among the most contentious issues in the application of AI to border control is the risk of mass surveillance and overreach. The widespread adoption of facial recognition technology and biometric data collection at ports of entry, while instrumental in combating identity fraud, has drawn criticism from civil liberties organizations and privacy advocates. Concerns stem from the possibility of non-consensual data capture, indefinite data retention, and lack of transparency in how biometric data is processed or shared [62].

These issues are particularly salient in jurisdictions governed by data protection regulations such as the European Union's GDPR, which mandates strict conditions for personal data processing, including biometric identifiers. In 2022, for instance, the European Data Protection Board flagged several EU-funded AI border trials for lacking adequate impact assessments and safeguards [63].

One promising mitigation strategy is the use of federated learning, a decentralized machine learning technique that allows AI models to be trained on local devices or servers without transferring raw data to central authorities [64]. Federated learning is a decentralized machine learning technique that enables AI models to be trained directly on local devices or servers, eliminating the need to transfer raw data to a central authority. This approach enhances data privacy and security by ensuring that sensitive information remains on the local device.

In federated learning, a central server first initializes a global machine learning model. This model is then distributed to multiple client devices, such as smartphones, edge devices, or institutional servers. Each device trains the model using its local dataset and subsequently sends back only the updated model parameters, not the underlying data. These updates are then aggregated at the central server to refine the global model. This iterative process continues until the model reaches satisfactory performance, all while ensuring that individual data never leaves its origin.

Federated learning has been successfully applied across various sectors. In healthcare, it enables hospitals to collaboratively train diagnostic models without sharing sensitive patient records. Financial institutions utilize it to develop fraud detection systems while maintaining client confidentiality. On mobile devices, federated learning enhances features such as predictive text and voice recognition without uploading personal data to the cloud. Similarly, autonomous vehicles can share driving insights without transmitting raw sensor data. The benefits of federated learning are significant. It improves user privacy by keeping data localized, reduces bandwidth usage since only model updates are transmitted, and facilitates the development of personalized models based on individual user data. Furthermore, federated learning supports compliance with strict data protection regulations such as the GDPR.

Despite its advantages, federated learning does present several challenges. Data heterogeneity across different clients can impair model consistency and performance. The system also incurs communication overhead due to frequent model update exchanges. Moreover, it is susceptible to certain security threats, such as model inversion attacks. Lastly, coordinating training across many distributed devices increases the complexity of implementation.

To support the deployment of federated learning, several open-source tools and frameworks are available. TensorFlow Federated facilitates federated learning within the TensorFlow ecosystem. PySyft extends PyTorch to support secure and private computations [64]. Practically, the International Criminal Police Organization (INTERPOL) has begun piloting federated learning models that enable cross-border collaboration on threat detection without compromising individual privacy [65]. This approach aligns with the principle of data minimization and reduces the risk of large-scale breaches.

6.2. Bias and Fairness

Another critical concern is algorithmic bias, which can result in discriminatory outcomes if AI systems reflect and reinforce prejudices embedded in historical data. For instance, natural language processing tools used to monitor digital communications have been shown to disproportionately flag individuals from certain ethnic or linguistic backgrounds, due to unbalanced training datasets or context-insensitive keyword detection.

In natural language processing (NLP) applications, demographically grounded bias has garnered increased attention recently. Providing an overview of prejudice from a broader perspective and characterizing bias have been the main topics of many recent studies. Hovy and Prabhumoye [66] offered a straightforward, useful synopsis of their research (Figure 6) [66]. They listed five potential sources of bias in NLP systems: (1) the data; (2) the annotation procedure; (3) the input representations; (4) the models; and (5) the study strategy. Their article provided a detailed analysis of each bias source, along with examples, references to relevant research, and possible countermeasures [66].

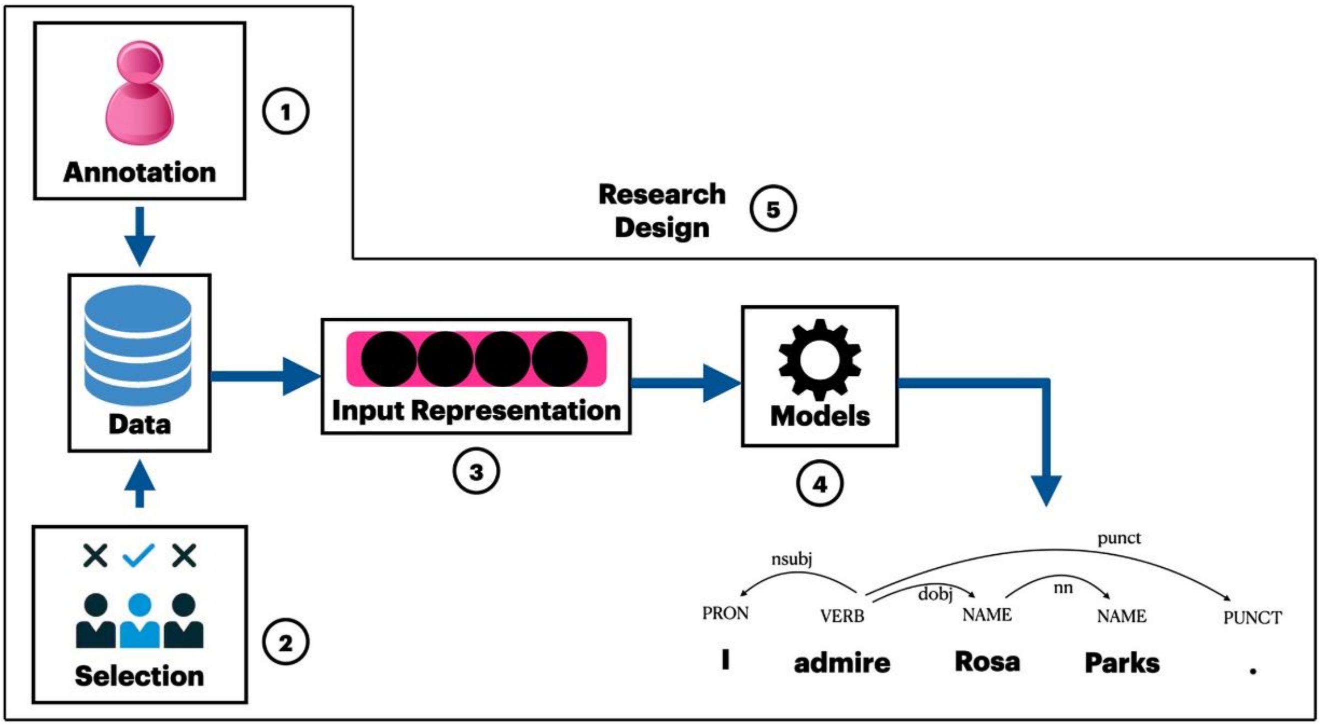


Figure 6.
A diagram showing the five causes of bias in the pipeline for broad natural language processing Hovy and Prabhumoye [66].

Similarly, computer vision systems may underperform for darker skin tones or non-Western facial features, raising the risk of false positives or wrongful detentions at border checkpoints. This was illustrated when an AI inspection system might misclassify imported medical supplies as narcotics due to skewed training data. Hence, the FDA has recently proposed a framework to advance the credibility of AI models used for drug and biological product submissions [67].

The FDA's draft guidance on the use of artificial intelligence to support regulatory decision-making for drugs and biological products offers critical insights that align with the risks posed by misclassification of imports, such as the hypothetical case where an AI system at a major EU airport erroneously flagged 20% of imported medical supplies as narcotics [67]. At the core of the FDA's guidance is the acknowledgment that AI systems, while powerful, are inherently vulnerable to the quality and diversity of their training data. If an AI model is trained on datasets that fail to capture the full range of product variations, such as packaging styles used by African and Asian manufacturers, it can result in significant misclassifications when deployed in real-world environments like customs inspections [67].

The guidance strongly emphasizes the concept of "fit for use" data, which refers to data that is both relevant and reliable. In the context of import inspections, relevance would mean including data that accurately reflects global manufacturing and packaging norms, while reliability implies the data must be accurate, complete, and traceable. A lack of such data diversity increases the likelihood of algorithmic bias, where the model performs well on familiar inputs but poorly on new or underrepresented ones. This is especially problematic in global trade settings, where the diversity of goods is vast and any misclassification can disrupt supply chains, delay medical treatments, or trigger regulatory violations [67].

To mitigate such risks, the FDA proposes a risk-based credibility assessment framework. This framework encourages developers to define the AI model's specific question of interest and context of use, then assess the associated model risk. In a high-risk setting, such as detecting narcotics in imported goods, any classification error could have significant legal, economic, or public health consequences. Therefore, models used in such environments must undergo a higher level of scrutiny, validation, and regulatory engagement. The FDA's framework includes steps such as documenting model development processes, describing and justifying training datasets, detailing model evaluation methods, and addressing the limitations and biases of the modeling approach [67].

One of the key challenges discussed in the guidance is "data drift," where a model's performance declines over time or across new environments because the data it encounters deviates from its training set. This phenomenon is particularly relevant in the customs context, where products and suppliers continually change. The FDA recommends a strategy of lifecycle maintenance, continual monitoring, retraining, and updating of AI systems to ensure sustained accuracy and appropriateness over time. Without such maintenance, AI systems risk becoming obsolete or dangerously inaccurate as they process evolving inputs [67].

Moreover, to address these challenges, experts advocate the implementation of explainable AI (XAI), which enables end-users and auditors to trace the logic behind AI decisions. XAI tools not only help detect and correct biases but also support regulatory compliance by enhancing the transparency and accountability of algorithmic processes [68].

Beyond technical fixes, there is also a need for multi-stakeholder governance frameworks that include input from civil society, data protection authorities, and marginalized communities. Ethical deployment of AI in border security requires more than functional efficiency; it demands a commitment to human dignity, legal proportionality, and social equity.

7. Future Directions

Since smugglers themselves are increasingly using AI and digital tools to improve their operations, border security technology must continue to be flexible, forward-thinking, and morally sound. Advanced innovation, strategic foresight, and cross-border cooperation are all necessary to ensure AI's sustained efficacy in drug and weapon interdiction. This section describes new technologies that have the potential to influence AI-assisted border control in the future, along with the regulatory frameworks that will be required to guarantee their responsible application.

7.1. Next-Generation AI Technologies

The next phase of AI in border enforcement will likely be defined by the convergence of quantum computing, autonomous systems, and collective machine intelligence.

Quantum machine learning (QML) represents a transformative leap in data processing capacity [69]. By leveraging qubits and quantum entanglement, QML systems can process vast and complex datasets at exponentially faster speeds than classical computers. This capability has significant implications for real-time decryption of smuggler communications, particularly those protected by advanced encryption or obfuscation schemes. While QML remains in early research stages, pilot programs by institutions such as MIT and IBM have shown promise in accelerating pattern recognition in security datasets [70].

Equally promising is the development of swarm robotics, where fleets of small, autonomous drones communicate with one another to patrol large, unstructured border environments [71]. These systems mimic the collective behavior of biological swarms, enabling dynamic formation changes, cooperative target tracking, and real-time coverage of high-risk zones [71]. Such systems are particularly useful in terrain that is difficult to secure via static infrastructure, such as archipelagic borders or mountainous regions.

Another frontier involves [72] where data from multiple sources, thermal cameras, acoustic detectors, ground-penetrating radar, and satellite imagery is integrated into a single, real-time decision-support platform. These multi-modal systems improve situational awareness and reduce false positives, enabling more informed tactical responses.

While these technologies hold significant potential, their deployment must be tempered with robust ethical governance and legal oversight. As the capabilities of AI systems grow, so too does the risk of abuse, error, or mission creep into areas of civil liberty.

7.2. Policy Recommendations

Several policy directions are essential to guide the ethical, effective, and globally harmonized use of AI in border security.

First, there is an urgent need to establish international AI standards specific to law enforcement and border control. Current frameworks, such as the OECD AI Principles [73] and UNESCO's Recommendation on the Ethics of AI [74], provide a normative foundation but lack sector-specific guidance. The creation of an UN-led regulatory charter for AI in border contexts, similar to the International Civil Aviation Organization (ICAO) standards for biometric passports, would help align enforcement protocols across jurisdictions while ensuring compliance with human rights norms.

Second, the formation of cross-border data trusts could greatly enhance intelligence sharing among national and regional agencies. These trusts would serve as secure, GDPR-compliant platforms for exchanging structured and unstructured data relevant to smuggling threats. By standardizing metadata formats, anonymizing personal identifiers, and applying federated learning, such systems could mitigate the risks of data breaches and sovereignty violations while promoting operational synergy [75].

Third, sustained investment in capacity building for low- and middle-income countries is crucial to ensure equitable access to AI tools. Many trafficking corridors intersect with nations that lack the technological infrastructure or trained personnel to implement advanced surveillance or analytics. International aid mechanisms should prioritize funding for scalable, low-cost AI applications, such as mobile-based NLP threat detection or modular drone kits, that can be customized to local conditions [76].

Finally, fostering public–private research partnerships is key to keeping pace with the rapidly evolving tactics of criminal organizations. Industry stakeholders, including AI firms, logistics companies, and telecom operators, often possess the technical expertise and data resources that governments lack. Structured collaborations underpinned by clear legal and ethical guidelines can accelerate innovation while ensuring accountability and public interest alignment.

To enhance the practical utility of AI applications in border security, future research should incorporate quantitative benchmarks that assess system performance across diverse contexts. For instance, the U.S. Department of Homeland Security’s Biometric Exit Program has reported facial recognition accuracy rates exceeding 97% in real-time identity verification at border checkpoints [77]. Similarly, a supervised machine learning model developed by the World Customs Organization achieved up to 85% accuracy in identifying high-risk shipments based on cargo origin, transit history, and known violations [78]. Meanwhile, anomaly detection algorithms applied to financial transactions, such as Random Forest or Isolation Forest, have demonstrated precision rates of 98% in experimental smuggling-related fraud detection scenarios [79]. These figures not only highlight the operational potential of AI systems but also underscore the importance of standardized performance metrics, such as accuracy, false positive rates, and real-time processing capabilities, to guide procurement, deployment, and evaluation strategies.

8. Conclusion

The global fight against drug and arms smuggling has entered a new technological era—one where the stakes are not only geopolitical and economic but also algorithmic. Artificial intelligence, when effectively integrated, offers law enforcement and customs agencies unprecedented capabilities for surveillance, detection, prediction, and interdiction. From machine learning models that flag anomalous cargo patterns to computer vision systems that reveal concealed weapons, AI has proven itself to be a transformative force multiplier in border security operations.

Yet, the battle is far from one-sided. Smuggling networks are not only reacting to enforcement innovations but are increasingly leveraging AI themselves, deploying encrypted IoT devices, fabricating deepfake documents, and coordinating illicit trade through anonymized digital platforms. This adversarial dynamic highlights the urgent need for proactive and anticipatory innovation, rather than reactive adaptation.

The review has underscored that while AI technologies such as hyper-spectral imaging, predictive analytics, and federated learning offer immense promise, their success depends on thoughtful and ethical implementation. Privacy concerns, algorithmic bias, and infrastructural disparities pose real and present challenges. These issues must be addressed through robust governance frameworks, transparency tools such as explainable AI, and inclusive policy design that considers the diverse socio-political contexts of AI deployment.

Ultimately, this review calls for action. The arms race between AI-driven border security and AI-enabled smuggling is no longer a hypothetical scenario; it is our current reality. In this high-stakes contest, complacency is not an option. Governments, researchers, and private sector actors must align their efforts to stay ahead of adversaries who are equally agile and technologically informed. Investing in ethical AI systems, building cross-border trust, and supporting global AI literacy are not supplementary strategies; they are indispensable imperatives. To secure our borders in the age of intelligent threats, we must be equally intelligent in our response.

Future advances in this research, ranging from quantum-enhanced threat detection to autonomous drone swarms, suggest a rapidly evolving frontier. However, technological superiority alone will not be sufficient. Institutional readiness, international coordination, and a commitment to civil liberties will determine whether AI becomes a tool for empowerment or a vector for overreach.

Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
BERT	Bidirectional Encoder Representations from Transformers
CBP	Customs and Border Protection
CCTV	Closed-circuit Television
CV	Computer Vision
DBN	Dynamic Bayesian Network
EU	European Union
FDA	Food and Drug Administration
GAN	Generative Adversarial Networks
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HBOS	Histogram-Based Outlier Score
ICAO	International Civil Aviation Organization
INTERPOL	International Criminal Police Organization
IoT	Internet of Things
KNN	k-nearest Neighbor Algorithm
KYC	Know your customer
ML	Machine Learning
NLP	Natural language processing
QML	Quantum Machine Learning
R&D	Research and Development
UAV	Unarmed Vehicles
U.S.	United States
XAI	explainable AI

References

[1] United Nations Office on Drugs and Crime, *New UNODC campaign highlights transnational organized crime as a US$870 billion a year business*. Vienna: UNODC, 2012.

[2] United Nations Office on Drugs and Crime, *Global report on cocaine 2023: Local Dynamics*. New York: Global Challenges. United Nations Publications, 2023.

[3] D. Rassler and Y. Veilleux-Lepage, "On the horizon: The Ukraine War and the evolving threat of drone terrorism," *CTC Sentinel,* vol. 18, no. 3, pp. 1–24, 2025.

[4] J. B. Jacobs and A. Haberman, "3D-printed firearms, do-it-yourself guns, & the Second Amendment," *Law and Contemporary Problems,* vol. 80, no. 2, pp. 129-147, 2017.

[5] M. El Midaoui, E. B. Laoula, M. Qbadou, and K. Mansouri, "Logistics tracking system based on decentralized IoT and blockchain platform," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 23, no. 1, pp. 421-430, 2021.

[6] Y. Wang, "Survey on deep multi-modal data analytics: Collaboration, rivalry, and fusion," *ACM Transactions on Multimedia Computing, Communications, and Applications,* vol. 17, no. 1s, pp. 1-25, 2021.

[7] O. L. Ojo *et al.*, "AI applications in satellite image processing: Enhancing earth observation and environmental monitoring," in *Proceedings of the 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON); November 2024; pp. 1–5*, 2024.

[8] S. J. Adams, R. D. Henderson, X. Yi, and P. Babyn, "Artificial intelligence solutions for analysis of X-ray images," *Canadian Association of Radiologists Journal,* vol. 72, no. 1, pp. 60-72, 2021.

[9] A. Tubaishat, M. Aljouhi, and A. Maramara, *Unveiling challenges and solutions with intelligence in the dark and deep web. In Proceedings of the Intelligent and Fuzzy Systems; Kahraman, C., Cevik Onar, S., Cebi, S., Oztaysi, B., Tolga, A.C., Ucal Sari, I., Eds.* Cham: Springer Nature Switzerland, 2024.

[10] T. Kabudi, I. Pappas, and D. H. Olsen, "AI-enabled adaptive learning systems: A systematic mapping of the literature," *Computers and education: Artificial intelligence,* vol. 2, p. 100017, 2021.

[11] A. A. Qader Ismail Alnajem *et al.*, "AI-driven strategic foresight: Anticipating future trends and modelling business strategies," in *Proceedings of the 2024 International Conference on Decision Aid Sciences and Applications (DASA); December 2024; pp. 1–6*, 2024.

[12] A. Mantelero, "AI and big data: A blueprint for a human rights, social and ethical impact assessment," *Computer Law & Security Review,* vol. 34, no. 4, pp. 754-772, 2018.

[13] INTERPOL, "Artificial intelligence toolkit," Retrieved: https://www.interpol.int/How-wework/Innovation/Artificial-Intelligence-Toolkit, 2025.

[14] World Customs Organization, "World customs organization," Retrieved: https://www.wcoomd.org/en/Topics/Facilitation/Instrument%20and%20Tools/Tools/Risk%20Management%20Compendium, 2025.

[15] J. Cani *et al.*, "CEASEFIRE: An AI-powered system for combating illicit firearms trafficking," in *Proceedings of the 2024 IEEE International Conference on Big Data (BigData) (pp. 2697–2705). IEEE. https://doi.org/10.1109/BigData62323.2024.10825989*, 2024.

[16] T. Ige, A. Kolade, and O. Kolade, "Enhancing border security and countering terrorism through computer vision: A field of artificial intelligence," in *Proceedings of the Computational Methods in Systems and Software (pp. 656-666). Cham: Springer International Publishing.*, 2022.

[17] F. O. Jejelola, "The Role of Artificial Intelligence in the Eradication of Transnational Crime," *International Journal of Research and Innovation in Social Science*, vol. 8, no. 11, pp. 867-882, 2024.

[18] I. Mademlis *et al.*, "The invisible arms race: Digital trends in illicit goods trafficking and AI-enabled responses," *IEEE Transactions on Technology and Society,* 2024. https://doi.org/10.1109/TTS.2024.3514683

[19] T. Singh, "AI-driven surveillance technologies and human rights: Balancing security and privacy," presented at the International Conference on Smart Systems: Innovations in Computing (pp. 703-717). Singapore: Springer Nature Singapore, 2023.

[20] L. R. Carlos-Roca, I. H. Torres, and C. F. Tena, "Facial recognition application for border control," in *Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN); July 2018; pp. 1 –7,* 2018.

[21] U.S. Customs and Border Protection, "Biometric entry-exit program: H-1B and L-1 Fee Spend Plan (FY 2022)," *U.S. Department of Homeland Security,* 2022.

[22] K. B. Lee and H. S. Shin, "An application of a deep learning algorithm for automatic detection of unexpected accidents under bad CCTV monitoring conditions in tunnels," in *In Proceedings of the 2019 International Conference on Deep Learning and Machine Learning in Emerging Applications (Deep-ML);*

August 2019; pp. 7–11, 2019.

[23] P. Anu, P. Sharma, H. Kumar, N. Sharma, P. Rani, and K. I. A. James, "Machine learning in multi-spectral thermal imaging for enhanced detection of neurological disorders through thermoplasmonics," *Journal of Thermal Biology,* vol. 129, p. 104102, 2025. https://doi.org/10.1016/j.jtherbio.2025.104102

[24] S. Dhakal, A. Parvez, P. Das, S. Saxena, and M. Memoria, "An analysis of ai -driven technologies for enhancing security along the India-nepal border," in *In Proceedings of the 2024 International Conference on Computing, Sciences and Communications (ICCSC); October 2024; pp. 1–6,* 2024.

[25] L. Arya, Y. K. Sharma, H. Padmanaban, S. Devi, and R. Kumar, "Eyes in the sky: Safeguarding borders security with ai-powered aerial monitoring and iot integration," in *In Proceedings of the Proceedings of International Conference on Recent Innovations in Computing; Illés, Z., Verma, C., Gonçalves, P.J.S.,*

Singh, P.K., Eds.; Springer Nature: Singapore, 2024; pp. 863–873, 2019.

[26] W. Mao and S. Larsson, "Increase shipping efficiency using ship data analytics and AI to assist ship operations," Lighthouse Swedish Maritime Competence Centre. Report, 56 pp., 2023.

[27] Y. O. Adebayo, O. O. Adeusi, J.-P. Adjadeh, S. M. Obiono, and R. O. Abdulsalam, "Artificial intelligence and predictive analytics to develop evidence-based migration policies for optimal integration and economic empowerment of migrants," *World Journal of Advanced Research and Reviews,* vol. 25, no. 1, pp. 2147-2155, 2025. https://doi.org/10.30574/wjarr.2025.25.1.0286

[28] J. W. Brahan, K. P. Lam, H. Chan, and W. Leung, "AICAMS: Artificial intelligence crime analysis and management system," *Knowledge-Based Systems,* vol. 11, no. 5-6, pp. 355-361, 1998.

[29] R. Kotawadekar, *Satellite data: Big data extraction and analysis. In Artificial intelligence in data mining*. Amsterdam: Academic Press, 2021.

[30] R. E. R. Shawon *et al.*, "Assessing geopolitical risks and their economic impact on the USA using data analytics," *Journal of Economics, Finance and Accounting Studies,* vol. 6, no. 6, pp. 05-16, 2024. https://doi.org/10.32996/jefas.2024.6.6.2

[31] A. Biiak and Y. Lindskog, "Leveraging technologies of Industry 4.0 for risk management in sea freight forwarding operations," Master's thesis, University of Gothenburg, Sweden. GUPEA., 2023.

[32] Z. Bahrami, "Data-driven analytics for the automated inspection of shipping containers ", Doctoral Dissertation University of British Columbia, 2022. https://doi.org/10.14288/1.0422985

[33] S. Emaani and A. Saghaei, "Driver anomaly detection in cargo terminal," *Heliyon,* vol. 11, no. 2, 2025.

[34] H. Fan, H. Jia, X. He, and J. Lyu, "Navigating uncertainty: A dynamic Bayesian network-based risk assessment framework for maritime trade routes," *Reliability Engineering & System Safety,* vol. 250, p. 110311, 2024. https://doi.org/10.1016/j.ress.2024.110311

[35] A. Adel and M. Norouzifard, "Weaponization of the growing cybercrimes inside the dark net: The question of detection and application," *Big Data and Cognitive Computing,* vol. 8, no. 8, p. 91, 2024.

[36] P. Sarzaeim, Q. H. Mahmoud, A. Azim, G. Bauer, and I. Bowles, "A systematic review of using machine learning and natural language processing in smart policing," *Computers,* vol. 12, no. 12, p. 255, 2023.

[37] S. Rezwan and W. Choi, "Artificial intelligence approaches for UAV navigation: Recent advances and future challenges," *IEEE Access,* vol. 10, pp. 26320-26339, 2022.

[38] X. Hu and R. H. Assaad, "The use of unmanned ground vehicles (mobile robots) and unmanned aerial vehicles (drones) in the civil infrastructure asset management sector: Applications, robotic platforms, sensors, and algorithms," *Expert Systems with Applications,* vol. 232, p. 120897, 2023.

[39] D. Kaur Sohi and R. Raman, "Advanced IoT-driven freight management for enhanced cargo security and efficiency in transit using decision tree algorithm," in *Proceedings of the 2024 3rd International Conference for Innovation in Technology (INOCON); March 2024; pp. 1–6,* 2024.

[40] B. Khoo, R. C. W. Phan, and C. H. Lim, "Deepfake attribution: On the source identification of artificially generated images," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery,* vol. 12, no. 3, p. e1438, 2022.

[41] Times of India AI Getting Dangerous, "Times of India AI getting dangerous: Polish researcher uses ChatGPT-4.o to generate fake passport in 5 minutes!," 2025.

[42] A. Najee-Ullah, L. Landeros, Y. Balytskyi, and S. Y. Chang, "Towards detection of AI-generated texts and misinformation," presented at the International Workshop on Socio-Technical Aspects in Security (pp. 194-205). Cham: Springer International Publishing, 2021.

[43] B. He, X. Ji, G. Li, and B. Cheng, "Key technologies and applications of UAVs in underground space: A review," *IEEE Transactions on Cognitive Communications and Networking*, vol. 10, no. 3, pp. 1026-1049, 2024.

[44] T. X. Hammes, *Criminal enterprises, private military companies, smart robots and their implications for national sovereignty in global criminal and sovereign free economies and the demise of the western democracies*. Abingdon, UK: Routledge, 2014.

[45] V. R. Singh, *Navigating the complexities: AI, security, and liberty at the border in artificial intelligence for cyber security and industry 4.0*. Boca Raton: CRC Press, 2025.

[46] J. Serra Ferràndiz, "Analysis of strategies used to smuggle illicit drugs into Europe via shipping containers, current and future trends, and what counter-measures are being implemented in ports to seize them," Bachelor's thesis, Facultat de Nàutica i Transport Marítim, Universitat Politècnica de Catalunya). UPCommons, 2023.

[47] J. de Carvalho Ponce, "Novel strategies in drug concealment." Hershey: IGI Global, 2024, pp. 31-49.

[48] K. Kalodanis, P. Rizomiliotis, G. Feretzakis, C. Papapavlou, and D. Anagnostopoulos, "High-risk AI systems—lie detection application," *Future Internet*, vol. 17, no. 1, p. 26, 2025.https://doi.org/10.3390/fi17010026

[49] J. J. Forest, "Crime-terror interactions in sub-Saharan Africa," *Studies in Conflict & Terrorism*, vol. 45, no. 5-6, pp. 368-388, 2022.

[50] U.S. Department of Homeland Security, "Using AI to secure the homeland," Retrieved: https://www.dhs.gov/ai/using-ai-to-secure-the-homeland, 2025.

[51] M. Thilagavathi, R. Saranyadevi, N. Vijayakumar, K. Selvi, L. Anitha, and K. Sudharson, "AI-driven fraud detection in financial transactions with graph neural networks and anomaly detection," in *Proceedings of the 2024 International Conference on Science Technology Engineering and Management (ICSTEM);*

April 2024; pp. 1–6, 2024.

[52] Q. Zhang, "Financial data anomaly detection method based on decision tree and random forest algorithm," *Journal of Mathematics*, vol. 2022, no. 1, p. 9135117, 2022.

[53] H. Kheddar, "Transformers and large language models for efficient intrusion detection systems: A comprehensive survey," *Information Fusion*, p. 103347, 2025.https://doi.org/10.1016/j.inffus.2025.103347

[54] Europol New Accountability, "Europol new accountability framework to use artificial intelligence in a transparent and accountable manner," Retrieved: https://www.europol.europa.eu/media-press/newsroom/news/newaccountability-framework-to-use-artificial-intelligence-in-transparent-and-accountable-manner, 2025.

[55] S. Sifnaios, G. Arvanitakis, F. K. Konstantinidis, G. Tsimiklis, A. Amditis, and P. Frangos, "A deep learning approach for pixel-level material classification via hyperspectral imaging," *arXiv preprint arXiv:2409.13498,* 2024. doi.org/https://doi.org/10.48550/arXiv.2409.13498

[56] I. Mademlis *et al.*, "The invisible arms race: Digital trends in illicit goods trafficking and AI-enabled responses," *IEEE Transactions on Technology and Society*, pp. 1-19, 2024.

[57] Port of Rotterdam Authority, "Artificial intelligence in the port," Retrieved: https://www.portofrotterdam.com/en/port-future/innovation/artificial-intelligence-port, 2025.

[58] E. Kakaletsis *et al.*, "Computer vision for autonomous UAV flight safety: An overview and a vision-based safe landing pipeline example," *Acm Computing Surveys*, vol. 54, no. 9, pp. 1-37, 2021.

[59] World Customs Organization, "WCO cargo targeting system," Retrieved: https://www.wcoomd.org/en/topics/enforcement-and-compliance/instruments-and-tools/cargo-targetingsystem.aspx, 2025.

[60] A. Rahman *et al.*, "Machine learning and network analysis for financial crime detection: Mapping and identifying illicit transaction patterns in global black money transactions," *Gulf Journal of Advance Business Research*, vol. 2, no. 6, pp. 250-272, 2024.

[61] D. M. Gerstein, B. Pardo, A. C. Davenport, and I. A. Chindea, "An overview of the effectiveness of U.S. counternarcotics efforts in Colombia, 2000–2020, and recommendations for the future," Research Report RRA-A1389-3, 20 pp.). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1389-3.html, 2022.

[62] S. Bor and N. C. Koech, "Balancing human rights and the use of artificial intelligence in border security in africa," *Journal of Intellectual Property & Information Technology Law*, vol. 3, p. 77, 2023.

[63] European Data Protection Board, "Data protection issues arising in connection with the use of artificial intelligence," European Data Protection Board, 2022.

[64] Google Inc, "Federated learning tensorflow federated," Retrieved: https://www.tensorflow.org/federated/federated_learning, 2025.

[65] Dialogue on an Effective, "Dialogue on an effective multilateral policing architecture against global threats," Retrieved: https://www.interpol.int/en/How-we-work/Dialogue-on-an-effective-multilateral-policing-architectureagainst-global-threats, 2025.

[66] D. Hovy and S. Prabhumoye, "Five sources of bias in natural language processing," *Language and Linguistics Compass*, vol. 15, no. 8, p. e12432, 2021.

[67] U.S. Food and Drug Administration, "FDA proposes framework to advance credibility of AI models used for drug and biological product submissions," U.S. Food and Drug Administration, 2025.

[68] A. Bertrand, R. Belloum, J. R. Eagan, and W. Maxwell, "How cognitive biases affect XAIassisted decision-making: A systematic review," in *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (pp. 78–91). Association for Computing Machinery*, 2022, doi: https://doi.org/10.1145/3514094.3534164.

[69] E. Vaz, "Quantum machine learning in spatial analysis: a paradigm shift in resource allocation and environmental modeling," *Letters in Spatial and Resource Sciences*, vol. 17, no. 1, p. 11, 2024.

[70] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195-202, 2017.

[71] M. Brambilla, E. Ferrante, M. Birattari, and M. Dorigo, "Swarm robotics: a review from the swarm engineering perspective," *Swarm Intelligence*, vol. 7, pp. 1-41, 2013.

[72] C. Tian, Y. Cho, Y. Song, S. Park, I. Kim, and S.-Y. Cho, "Integration of AI with artificial sensory systems for multidimensional intelligent augmentation," *International Journal of Extreme Manufacturing*, vol. 7, no. 4, p. 042002, 2025.

[73] Organisation for Economic Co-operation and Development, "What are the OECD principles on AI?," *OECD Observer*, 2019. doi.org/https://doi.org/10.1787/6ff2a1c4-en

[74] UNESCO, "Recommendation on the ethics of artificial intelligence," Retrieved: https://unesdoc.unesco.org/ark:/48223/pf0000381137, 2021.

[75] J. Hardings, "Data trusts in 2020 the open data institute," Retrieved: https://theodi.org/news-and-events/blog/data-trusts-in-2020/, 2020.

[76] N. Mohamed, "A comprehensive framework for cyber threat detection: leveraging AI, NLP, and malware analysis," *International Journal of Information Technology*, pp. 1-8, 2025. https://doi.org/10.1007/s41870-025-02466-4

[77] U.S. Department of Homeland Security, *Customs and border protection comprehensive biometric entry/exit plan: Fiscal year 2016 report to Congress (Report to Congress)*. Washington, D.C: U.S. Department of Homeland Security, 2016.

[78] World Customs Organization, "WCO A-CIP Programme: Customs Integrity Perception Survey (CIPS) iterations demonstrate improvements over time world customs organization," Retrieved: https://www.wcoomd.org/en/media/newsroom/2024/february/wco-a-cip-programme-cips-iterationsdemonstrate-improvements-over-time.aspx, 2024.

[79] A. M. Aburbeian and H. I. Ashqar, "Credit card fraud detection using enhanced random forest classifier for imbalanced data. In K. Daimi & A. Al Sadoon (Eds.)," 2023.