PROJECTS PLAN

MINISTRY OF INTERIOR
STATE OF QATAR

وزارة الداخليـــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

وزارة الداخليـــــــــة

Ministry of Interior

State of Qatar • دولـــة قطـــر

Introduction

Under the patronage of His Highness Sheikh Tamim Bin Hamad Al Thani, Amir of the State of Qatar, the 16th edition of the Global Exhibition for Homeland Security & Safety – Milipol Qatar will be held from 20th to 22nd October 2026 in Doha, State of Qatar.

Recognized internationally as one of the most prominent specialized security exhibitions, Milipol Qatar provides an exceptional platform to explore the latest technologies in the field of security. The event addresses the growing security needs of the State of Qatar and the wider Middle East region. It also serves as a gateway to security markets across the region, enabling leading international industry players to engage in a dynamic environment shaped by medium-and long-term economic and strategic projects.

This esteemed patronage aligns with the aspirations of the Qatar National Vision 2030, which is built on strong social foundations that advocate for a peaceful and prosperous society. It signifies His Highness's steadfast commitment to global initiatives that seek to enhance peace and security amid a period of growing international challenges.

On this occasion, this booklet has been designed to highlight selected projects of the Ministry of Interior departments and their future security requirements. In line with the rapid development witnessed by the State of Qatar, the role of the Ministry of Interior and its departments continues to expand in maintaining security and stability. Through strategic planning and the adoption of advanced technologies, the Ministry strives to meet the requirements of comprehensive national growth and development by providing cutting-edge security systems, equipment, and services to the public, addressing both the present and future needs of the nation.


MILIPOL QATAR
EXHIBITION
2026
Milipol
QATAR
Th
Edition
16
20 - 22
OCTOBER
2026
THE GLOBAL EVENT FOR
HOMELAND SECURITY & SAFETY
وزارة الداخلية
Ministry of Interior
State of Qatar • دولة قطر
www.milipolqatar.com
milipolqatar

وزارة الداخليـــــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

Ministry of Interior Projects

Summary

وزارة الداخليـــــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

@moi_qatar | moigovqatar | moigovqa | www.moi.gov.qa

The Strategy of the Ministry of Interior

The Ministry of Interior through its duties and functions aspires the community and the state to be blessed with stability and well-being. Therefore, it is keen to put in place its strategy that reflect a deep understanding of the security challenges and threats and ways to counter its effects, and the adoption of the effective means to overcome them.

These challenges consists of the internal challenges, from within the ministry environment, and external challenges, and at the same time, these challenges brings out several threats, direct or indirect, visible or hidden, targeting the security and stability of the State of Qatar.

The strategic vision, mission and its mainstays embodied in the four pillars, all intend to identify the ways to confront those challenges and threats to ensure protection of the security and stability of the State of Qatar.

Strategy Theme

Outstanding Performance – Active Participation - Permanent Security

Vision

Achieve the maximum degree of security and stability under the rule of law.

Mission

Establishment of security and safety in the country, through the security performance with a high degree of efficiency and professionalism, in the framework of a true partnership with the community.

Sources of the Strategy

- The Permanent Constitution of the State of Qatar
- Qatar Vision 2030
- Military Service Law No. 31/2006, Emiri Decree No. 16/2009
- Other Laws and Legislative Tools
- Arabic and Islamic Culture and Heritage
- Authentic Qatari Norms and Traditions
- Understand the elements of security and stability and ways of strengthening them.
- Comprehend the challenges and threats faced by the State of Qatar.

Pillars of the Strategy

- Public Security
- Relationship with the Community
- Human Resources
- Material Resources and Technological Development.

General Directorate of Coasts and Borders Security

Night Vision Google

1X Magnification Gen 3 Auto-Gated Black & White Image FULL MIL SPEC Night Vision binoculars, Minimum 64 Lp/Mm Resolution, Waterproof, Built in 'IR On' And 'Low Battery' indicators Supplied with following standard accessories 1/Soft carrying case 2x AA Battery 2/Objective Lens cover, Lens cleaning kit 3/ Operation Manual.

Dayvision binoculars

The binoculars are lightweight, compact instruments intended for use in general field observation and fire direction.

Bulletproof Helmets

Material :Aramid Composite

Color: Black, Olive Green, Desert

Protection Area - 1250cmt

Size :S/M/L/XL/XXL/XXL

Net weight :1.45 kg/ pc

Features :

- To defeat 9mm FMJ, 124 grain, bullet velocity 1400+1-50 FPS
- To defeat .44 Magnum SWC-GC, 240 grain, bullet velocity 1400 +/- 50 FPS
- Defeat Level (MJ STD 0106.01)
- Interior: Webbing suspension "ith sweatband 3 or 4 point strap-harness suspension system.

Bulletproof Vest with life jacket

Bulletproof Vest with life jacket
Tactical bullet proof floating jacket
Protection level : NIJ IIIA
Buoyancy approximately : 15 Kg
Protection capability :protection against hand gun round and fragment .
Material: Water Resistant outer cover with removable soft ballistic panel.

Purpose: Design for tactical use and water operation provide both water operation - Provide both ballistics protection and floating support.

Intended for protection in tactical and marine environment.

Plastic handcuff

Made from nylon material. Used by law enforcement to restrain individual by securing their wrists to prevent escape, harm or escalation. It is also used in the security contest.

Hearing Protection Earmuff

Hearing Protection Earmuff Primary Use

Shooting ranges, hunting, firearm training, military, or law enforcement environments

Key Performance Criteria:

- High attenuation to protect against impulse noise from firearms.
- Comfortable fit for long shooting sessions.
- Durable materials resistant to impact and environmental exposure.
- Replaceable ear cushions for hygiene and extended service life.

Eyes Protective Glasses

It is used for protecting eyes to guard projectile impacts against ballistic. Protection, shielding the eyes from both the front and the sides. Protection distortion free vision and high wearing comfort.

National Command Centre (NCC)

Najm System

The primary system for handling all reports received by the Emergency Services Department (999).

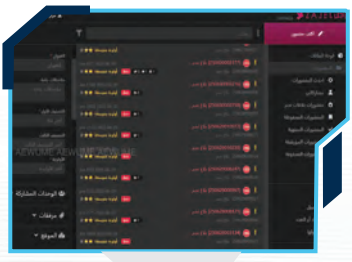
Key features include:

- Integrates all responding departments within a unified and centralized platform.
- Provides real-time tracking of patrols affiliated with the Ministry of Interior.
- Used by patrols to process reports and communicate with the Command and Control Operations Center.

Zajel System

The system provides a range of capabilities, including:

- Creating incident reports with precise location mapping.
- Sharing reports with relevant departments and tracking their actions.
- Generating analytical and operational reports.
- Displaying communication plans and hotline numbers for each event.
- Receiving incident reports from the Najm System based on duty area.
- Compatible with iPhone and iPad devices.



Tabie System

This system offers a variety of features, such as:

- Creating and scheduling events and activities for institutions, teams, VIPs, and other groups.
- Defining the time duration for each event or activity.
- Assigning patrols and personnel supervising each event.
- Monitoring the status of ongoing and upcoming events.
- Tracking patrol movements related to events on the map.
- Compatible with iPhone and iPad devices.

Task Planning System

This system includes several key features:

- Creating and designing strategic and security plans.
- Sharing general plans across departments and entities.
- Supporting multiple geographic layers.
- Providing 2D and 3D map views.
- Comparing planned deployment with actual field conditions to ensure accuracy.
- Adding notes and comments across all parts of the plan.

Unified Voice Communication System

The system offers a wide range of features, including:

- Adding and activating communication channels for various Ministry of Interior departments and security entities.
- Using multiple channels simultaneously.
- Instant playback of recorded communications across all channels.
- Receiving incoming calls on numbers assigned by the National Command Center (NCC).
- Making calls through landlines, mobile networks, and international lines

General Directorate of Civil Defence

Rapid Intervention Vehicle (Off Road):

- Classified as a light – duty specialized vehicle.
- Designed for small rescue and firefighting operations in Non-urban areas.
- Fast responding to accident seen.
- It has limited equipment for firefighting and rescue.

Medium Fire Fighting And Rescue:

- Classified as a medium – duty specialized vehicle.
- Designed for medium rescue and firefighting operations.
- It has firefighting and rescue equipment.
- It has firefighting pump and water – foam tank.

Heavy Emergency Rescue:

- Classified as a medium – duty specialized vehicle.
- Designed for search and rescue operations.
- It has rescue equipment only.
- It has a crane can bear a weight of 5.750kg and maximum height of 18m.

42 Meters Ladder:

- Classified as a medium – duty specialized vehicle.
- Designed for rescue from height places.
- It can used for medium – duty firefighting operation.
- It has rescue equipment.
- Maximum height for the ladder 40m.
- The rescue basket can handle 450kg change according to the height of ladder.

Hazmat Vehicle:

- Classified as a heavy – duty specialized vehicle.
- Used for rescue from accident and leaks chemical.
- Designed for industrial areas.
- Can used for searching, detecting and decontaminating chemical.

General Directorate of Telecommunications and Information Systems

1. Digital Electronic Passport Initiative

ePassport technology combines a smart chip, short-range wireless communication (NFC), strong encryption (such as RSA or ECC), digital signatures, and international standards (such as ISO/IEC 14443 and ICAO 9309) to ensure security and global interoperability.

2. Project to Modernize Standard and Digital National ID Cards

The ordinary identity card is used to represent official identity through a printed document featuring the individual's photograph and basic information, while it has evolved into the digital identity card, which integrates a smart chip, short-range wireless communication (NFC), strong encryption (such as RSA or ECC), digital signatures, and international standards (such as ISO/IEC 14443 and ICAO 9309), making it a secure and efficient means of digital identity for government services, financial services, and access to facilities, enabling users to verify their identity securely and quickly without the need for paper documents.

3. Private Networks for Camera Coverage (Wired and Wireless)

Network solutions for wired and wireless camera coverage are used to build integrated surveillance systems, relying on wired network connections such as cables for wired cameras and wireless networks (Wi-Fi per IEEE 802.11a/b/g/n/ac/ax standards) for wireless cameras. These systems support local area network (LAN) connectivity, video management systems (such as ONVIF), cloud server integration, and secure communication protocols (such as WPA3 or IPsec), ensuring security and consistency in the transmission of images and video from cameras to storage units or monitoring stations.

4. Artificial Intelligence Data Centers

AI data centers are dedicated to collecting, storing, and analyzing vast volumes of structured and unstructured data through advanced artificial intelligence systems, leveraging technologies such as machine learning (ML) and deep learning (DL), natural language processing (NLP), and big data analytics. These centers are supported by robust infrastructure—including multi-core processing units (GPUs/TPUs), high-speed networking (such as InfiniBand or 100G Ethernet), and cloud or hybrid cloud environments—enabling efficient data processing and real-time AI model training. They empower AI systems to make intelligent decisions, continuously improve through automated learning, and ensure security via data encryption (AES-256), role-based access control, and comprehensive audit logging to maintain transparency and compliance with standards such as GDPR and ISO 27001.

5. New Data Centers and Hybrid Cloud Infrastructure (Local and Public)

Modern data centers—whether public, private, or hybrid—serve as integrated environments for storing, processing, and intelligently analyzing vast volumes of data. They combine public cloud infrastructure (such as AWS, Microsoft Azure, Google Cloud), on-premises data centers, or hybrid architectures, leveraging advanced storage technologies (such as SAN/NAS), modern database management systems (including NoSQL, NewSQL, and in-memory databases), and predictive and retrospective analytics powered by artificial intelligence and machine learning. High-speed networking (such as 100G Ethernet or InfiniBand), DevOps automation, and integrated IT service management (ITSM) platforms ensure operational efficiency and scalability. Built on virtualized or cloud-native infrastructures, these centers support elastic, secure, and high-performance computing environments. They enforce stringent security standards—including AES-256 data encryption, multi-factor authentication, role-based access control, and secure audit logging—to enable organizations to make fast, accurate, and secure strategic decisions while maintaining flexibility, compliance with regulations (such as GDPR and ISO 27001), and end-to-end data integrity.

6. Digital Transformation of Infrastructure Systems

Digital transformation in critical infrastructure systems is a comprehensive process that modernizes traditional infrastructure—such as communication networks, power grids, transportation, water supply, and essential facilities—into intelligent, interconnected, and remotely manageable environments. This transformation integrates advanced technologies including cloud computing, the Industrial Internet of Things (IIoT), sensor-based data acquisition, high-speed connectivity (5G, fiber optics), big data analytics, and artificial intelligence/machine learning (AI/ML). It leverages distributed computing models such as edge computing, high-performance networking (e.g., 100G Ethernet, InfiniBand), and integrated automation systems like BMS. The result is a unified, intelligent control environment enabling predictive maintenance, real-time anomaly detection, and optimized system performance. Robust security standards—such as AES-256 encryption, multi-factor authentication, and SIEM-based security monitoring—are enforced to ensure resilience, operational efficiency, scalability, and long-term sustainability. This transformation empowers smart cities and enterprises to make data-driven strategic decisions, enhance service quality, reduce operational costs, and achieve environmental sustainability through intelligent, secure, and interconnected infrastructure ecosystems.

7. Digital Forensics and Incident Response Capabilities

Digital forensics is a structured, scientifically rigorous process for collecting, preserving, and analyzing digital evidence from electronic devices, networks, and digital systems—including smartphones, computers, storage drives, cloud environments, communication networks, and surveillance systems—to support criminal investigations and provide legally admissible evidence in court. It follows a standardized methodology involving forensic acquisition using validated dedicated tools, strict chain-of-custody documentation to ensure evidence integrity, and advanced analysis of encrypted data, login records, log files, location data, temporary storage, and network traffic. Techniques include recovery of deleted files, decryption of protected accounts, time-stamped log correlation, behavioral analysis of user activity, and intelligent data filtering. International standards such as ISO 27037 for digital forensic practices are applied, ensuring compliance with national and

international laws, including GDPR and criminal evidence regulations. Modern forensic platforms—such as Autopsy, Cellebrite, and Magnet AXIOM—support automated documentation, interactive timeline analysis, and real-time evidence correlation, enabling precise reconstruction of digital events. This ensures high reliability, legal admissibility, and transparency in court, making digital forensics a cornerstone of modern criminal justice and cybercrime investigations.

8. Digital forensics Laboratory equipment

Specialized equipment for digital evidence laboratories forms a critical part of the national forensic response infrastructure, ensuring accurate data acquisition, legal chain-of-custody integrity, and full traceability. These tools include forensic dumps and write blockers for cloning storage devices without altering data; mobile phone acquisition tools capable of extracting information from locked Android and iPhone devices; high-speed storage media readers supporting SSDs, HDDs, SD cards, and USB drives; forensic workstations equipped with powerful CPUs, 64GB+ RAM, NVMe SSDs, and clean operating systems like Windows Forensic Edition or customized Linux; cloud forensics devices for extracting logs, emails, files, and communications from platforms such as Microsoft 365, Google Workspace, and iCloud; secure storage lockers with surveillance systems to preserve evidence in controlled environments; time synchronization devices to unify timestamps across sources like computers, cameras, and phones; power conditioners to stabilize electricity during sensitive operations; and EMI/EMC test equipment to shield evidence from electromagnetic interference. All devices operate within certified digital forensic labs that comply with international standards such as ISO/IEC 27037 and ANSI/NIST-ITL 1-2020, ensuring precision, traceability, and admissibility of digital evidence in court.

9. Augmented and Interactive Reality Services for End Users

Augmented reality (AR) and interactive user services represent a cutting-edge digital experience that seamlessly blends the physical world with digital content through real-time, interactive spatial awareness. These services rely on advanced technologies such as computer vision, inertial measurement units (IMU), GPS, and LiDAR scanning to enable precise spatial mapping and real-time tracking. They are powered by high-speed connectivity (5G, Wi-Fi 6) and edge computing to deliver low-latency, responsive experiences.

Applications include interactive AR navigation, voice and gesture recognition, real-time 3D spatial mapping, interactive product visualization (e.g., placing virtual furniture in real homes), interactive educational simulations (e.g., medical training with AR), and multiplayer AR gaming. Security is ensured through TLS 1.3 encryption, user authentication, and secure identity management, while intuitive, responsive interfaces support cross-platform deployment—on smartphones, AR glasses, and Windows-based mixed reality devices. Development is powered by leading platforms such as ARKit, ARCore, Unity 3D, and Unreal Engine, enabling immersive, secure, and scalable AR experiences across education, retail, healthcare, vocational training, and entertainment.

10. Quantum Computing and Supercomputing Solutions

High-performance computing (HPC) and quantum computing represent the forefront of modern computing, delivering unprecedented processing power for complex scientific and industrial workloads. HPC systems aggregate hundreds or thousands of multi-core CPUs, GPUs, or specialized TPUs within purpose-built, high-density data centers, interconnected via ultra-fast networks (such as InfiniBand or 100G/400G Ethernet) and supported by advanced storage solutions (e.g., NVMe flash, storage fabrics). These systems are essential for computationally intensive tasks such as climate modeling, molecular simulation, drug discovery, and large-scale AI training. Quantum computing, on the other hand, leverages core principles of quantum physics—quantum superposition and quantum entanglement—to solve problems intractable for classical computers, such as breaking modern encryption or optimizing complex combinatorial problems. Current implementations rely on Noisy Intermediate-Scale Quantum (NISQ) devices, with hybrid quantum-classical algorithms like QAOA and VQE enabling practical applications. These systems are supported by secure environments, including quantum key distribution (QKD) for encryption, and specialized software platforms such as Qiskit, Cirq, and Microsoft Azure Quantum. With strong scalability, high precision, and robust security protocols—including AES-256 encryption, multi-factor authentication, and zero-trust architectures—these advanced computing platforms are accelerating breakthroughs in fields like cybersecurity, healthcare, materials science, and AI, while ensuring reliability, compliance, and resilience in mission-critical applications.

11. Hazardous Materials Detection Tools and Sensors

Advanced detection tools and sensors for hazardous materials integrate precision sensing with secure communications, leveraging a multi-modal approach combining electrochemical gas sensors, long-wave infrared (LWIR) thermal imaging, mass spectrometry, advanced spectroscopic systems (e.g., FTIR, Raman), and radiation detectors (gamma, beta, alpha). These systems are enhanced with intelligent data analytics and AI-driven anomaly detection to accurately identify and differentiate hazardous substances—including toxic gases, explosives, and radiological materials—across high-risk environments such as nuclear facilities, chemical plants, airports, and emergency response units. Compliant with international standards such as ISO 17025 and IEC 61000-6-2, these tools feature standardized communication interfaces (e.g., Modbus, CAN Bus, MQTT) and secure wireless connectivity (e.g., TLS 1.3, Zigbee 3.0), ensuring data integrity and interoperability. They support multi-factor authentication, automated audit logging, and real-time identity verification, forming a fully integrated system that combines multi-spectral sensing, edge computing, and predictive analytics for early, accurate, and scalable threat detection. Designed for resilience and compliance with strict technical and legal standards, these solutions significantly enhance safety, operational efficiency, and incident response capabilities in critical infrastructure and high-risk operations.

12. Smart Reservation and Tracking Systems for Vehicles and Sensitive Materials

Smart reservation and hazardous materials tracking systems represent end-to-end digital solutions deployed in industrial facilities, hospitals, critical infrastructure, and large-scale warehouses to ensure secure, efficient, and auditable management of both procedural workflows (e.g., staff schedules, medical procedures, operational tasks) and hazardous substances (chemical, radioactive, or explosive materials). These systems integrate advanced platforms—including Electronic Health Records (EHR), Enterprise Resource Planning (ERP), smart scheduling and reservation systems, and real-time monitoring dashboards—leveraging technologies such as Industrial Internet of Things (IIoT), smart time-stamping, biometric authentication, unique item identification (UID),

AI/ML-based risk prediction, and AES-256 encryption. RFID, QR codes, and NFC enable precise, real-time tracking of materials and work orders. Integrated with cloud-based or on-premises platforms, the systems support automated alerts when thresholds are exceeded (e.g., temperature, chemical concentration, or time windows), enabling proactive risk mitigation. Compliance with international standards—such as ISO 22301 (Business Continuity), ISO 27001 (Information Security), and IEC 62443 (Cybersecurity for Industrial Automation)—is ensured through chain-of-custody logging, secure audit trails, and role-based access control. Interactive dashboards, integration with video management systems (VMS), and real-time anomaly detection enhance transparency, reduce human error, and support data-driven strategic decision-making in complex, high-risk environments. The result is a resilient, intelligent, and auditable ecosystem that strengthens safety, compliance, and operational efficiency across critical operations.

13. (5G) Mobile services

The latest advancements in 5G networks represent a transformative shift in modern telecommunications, delivering unprecedented performance through ultra-high-speed data rates (up to 10 Gbps), ultra-low latency (under 1 millisecond), and massive device connectivity (up to 1 million devices per km²). These capabilities are enabled by cutting-edge technologies such as millimeter-wave (mmWave) communications, network slicing, edge computing, dynamic spectrum sharing (DSS), and intelligent radio access (Smart Radio Access). The technology supports diverse use cases—mMTC (massive Machine-Type Communications), URLLC (Ultra-Reliable Low-Latency Communications), and eMBB (Enhanced Mobile Broadband)—with high-precision location tracking via downlink reference signals (DRL) and AI-driven network optimization (AIOps) for adaptive quality of service (QoS) and self-healing capabilities. Security is reinforced through multi-layered protection—including packet-level encryption, mutual authentication, and intrusion detection systems (IDS)—ensuring resilience against cyber threats. Seamless handover, multi-connectivity support, and compliance with strict international standards (3GPP Release 18/19) further enhance reliability and scalability. These advancements enable mission-critical applications such as autonomous vehicles, remote healthcare, smart manufacturing (Industry 5.0), and high-definition augmented reality (AR). With energy-efficient power management and sustainable design, 5G networks deliver consistent performance, reliability, and scalability—paving the way for a next-generation digital economy, immersive virtual-physical experiences, and secure, intelligent, and sustainable digital infrastructure.

14. Modernization of TETRA Communication Systems Through 5G Network Integration

The evolution of telecommunications through 5G networks marks a paradigm shift—from simple data transfer to a fully intelligent, adaptive, and secure digital infrastructure. This transformation is driven by advanced technologies such as millimeter-wave (mmWave) connectivity delivering ultra-high speeds up to 10 Gbps, network slicing enabling the creation of multiple virtual networks on a single physical infrastructure—each tailored for specific use cases (e.g., ultra-reliable low-latency communications for autonomous vehicles, or massive connectivity for industrial IoT), and edge computing reducing latency to under 1 millisecond, thereby enhancing Operational response.

15. Distributed Data Architecture and Blockchain-Based Service Platform

Distributed data and blockchain software form the foundation of transparent, secure, and decentralized digital systems, built on Distributed Ledger Technology (DLT)—a peer-to-peer architecture that stores data across multiple nodes in a network, eliminating single points of failure. This model ensures data consistency and integrity through consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). The technology leverages strong cryptography (e.g., SHA-256, Elliptic Curve Cryptography), digital identity systems, immutable timestamping, and open-source code to enable trustless environments. It powers applications across finance (decentralized payments), healthcare (secure patient records), supply chains (end-to-end traceability), voting systems (tamper-proof elections), and smart contracts—self-executing agreements triggered automatically upon predefined conditions. Advanced features include decentralized queries, secure inter-node communication, and time synchronization via NTP or GPS-enabled clocks. The system ensures complete transparency, data immutability, and resilience against tampering, protected by cryptographic integrity, identity verification, and role-based access control (RBAC). Deployed in sensitive sectors such as finance, healthcare, and government, it preserves privacy through zero-knowledge proofs (ZKP) and encrypted queries, enabling secure, peer-to-peer interactions without intermediaries. This creates a future-ready digital ecosystem—secure, auditable, scalable, and trust-based—driven by decentralization, transparency, and cryptographic integrity.

16. Unmanned Aerial Vehicles (UAVs) for Operational Missions

Unmanned Aerial Vehicles (UAVs) for operational tasks represent a technological revolution in industrial monitoring, remote sensing, and autonomous operations. Widely deployed in industrial plants, hospitals, large warehouses, power stations, and critical infrastructure, they enhance efficiency, reduce operational costs, and improve safety by enabling automated inspections and logistics. Key applications include routine facility monitoring, remote sensing, early defect detection, critical infrastructure inspections, and internal transport of hazardous or sensitive materials. These systems rely on an integrated ecosystem combining autonomous flight systems, secure network connectivity (5G, Wi-Fi 6, LoRaWAN), RTK-GNSS for centimeter-level positioning, multi-sensor fusion (LiDAR, thermal imaging, distance sensors), and indoor positioning via IMU and SLAM (Simultaneous Localization and Mapping). Real-time AI analytics enable anomaly detection, while centralized command and control, UAS fleet management platforms, and secure communications (TLS 1.3, mutual authentication) ensure operational reliability. Time synchronization, identity verification, and compliance with FAA and EASA regulations are enforced, along with adherence to ISO 27001 and IEC 62443 for cybersecurity. Integrated with VMS, CMMS, and EAM systems, UAVs provide real-time data, predictive insights, and automated alerts—reducing human error, enhancing maintenance planning, and accelerating digital transformation across high-risk, mission-critical environments.

17. Counter-Drone Defense Systems

Counter-drone systems represent a cornerstone of advanced protection for critical infrastructure, military installations, airports, hospitals, and sensitive facilities, where they detect, track, and neutralize unauthorized unmanned aerial vehicles (UAVs) posing direct security threats. These systems employ a multi-layered defense architecture combining long-range radar, RF signal detection, EO/IR cameras, LIDAR and thermal imaging, GNSS spoofing detection, acoustic sensing, and automated airspace monitoring. Advanced AI-driven capabilities—including machine learning-based classification, behavioral pattern prediction, and RF fingerprinting for identity

verification—enable precise discrimination between drones and non-threatening airborne objects (e.g., birds). Active countermeasures include RF jamming, GPS spoofing, laser-based interception, and drone net launchers, all supported by secure, encrypted communication (TLS 1.3, mutual authentication), time synchronization (PTP), and command channel integrity. Integrated with SIEM, SOAR, incident management, and chain-of-custody logging, these systems ensure full auditability and compliance with international standards such as IEC 62443, ISO 27001, and NIST SP 800-83. They seamlessly integrate with VMS, building alarm systems, and SCADA networks, offering real-time situational awareness, automated threat response, and resilience in high-risk environments. This results in a secure, scalable, and intelligent defense ecosystem—driven by predictive analytics, secure communications, and automated control—ensuring operational safety and sovereignty against evolving aerial threats.

18. Advanced Radar Systems(Including Traffic Violations Detection, Facial Recognition, Object Tracking, Thermal Imaging, and Land & Maritime Surveillance)

Advanced radar systems used for traffic violation monitoring, facial and object recognition, and terrestrial and maritime thermal radar integration are characterized by a sophisticated fusion of high-precision sensing, intelligent analytics, and secure communications. These systems employ multi-frequency radar technologies—including X-band, K-band, Ka-band, and FMCW—offering speed measurement accuracy within ±1 mph, enhanced by integration with long-wave infrared (LWIR/MSIR) thermal imaging and AI/ML-based image analytics to detect movement, classify objects, and perform advanced identification tasks such as gait recognition and behavioral pattern analysis. Key capabilities include micro-Doppler analysis for detecting subtle motion signatures and multi-spectral fusion to improve detection reliability in complex environments. Secure high-speed connectivity via 5G, TLS 1.3, and mutual authentication ensures data integrity, while PTP/IEEE 1588 time synchronization, identity verification, and chain-of-custody logging maintain auditability and compliance. Fully compliant with stringent security standards such as ISO 27001, NIST SP 800-53, and IEC 62443, these systems are deployed in high-risk environments—including highways, critical infrastructure, borders, and maritime zones.

19. Safe City Systems with Live Integration to Operations Rooms, Civil Defense, and Early Warning Networks

The Smart City Security Ecosystem, integrated in real time with centralized command centers, represents a holistic model of urban intelligence, unifying real-time data from diverse sources—such as CCTV networks, IoT sensors, license plate recognition (LPR), facial recognition, 5G and fiber-optic networks, edge computing, and AI-powered real-time analytics—into a single, secure, and intelligent operational platform. This system enables real-time situational awareness, predictive risk modeling, automated incident response, and intelligent decision-making through interactive dashboards, smart maps, and early warning systems. It supports secure communications (TLS 1.3, mutual authentication), precise time synchronization (PTP/IEEE 1588), identity verification, chain-of-custody logging, and SIEM-based monitoring, ensuring compliance with international standards such as ISO 27001, IEC 62443, and NIST SP 800-83. The ecosystem integrates seamlessly with EAM, VMS, BAS, ATMS, counter-drone systems, and advanced radar, enabling rapid, coordinated responses to threats. With robust cybersecurity, role-based access control, and end-to-end encryption, it ensures resilience against cyber threats while enhancing public safety, operational efficiency, and emergency response. This fully integrated, AI-driven, and secure architecture empowers smart cities to proactively detect risks, adapt to dynamic threats, and build a safer, more sustainable, and intelligent urban future—grounded in interoperability, real-time intelligence, and trusted digital transformation.

20. Robotics for Reconnaissance, Surveillance, Rescue, and Civil Defense Missions

Search and rescue (SAR) robots represent a cutting-edge advancement in emergency response, disaster management, and military operations, serving as intelligent, adaptable, and highly effective solutions for hazardous or inaccessible environments. These robotic systems integrate multi-spectral sensing, real-time AI analytics, secure network connectivity (5G, LoRaWAN, mesh networking), autonomous navigation, and edge computing to operate in extreme conditions such as collapsed buildings, nuclear accident zones, or chemical spill sites. They include aerial drones (UAVs), ground robots, marine drones, and underground tunnel/pipeline robots, equipped with advanced sensors—including LiDAR, thermal and infrared (IR) cameras, gas detectors, and acoustic/accelerometer sensors—to detect survivors, assess structural integrity, and map hazardous zones in real time.

These robots generate 3D spatial maps on-the-fly, support automated emergency response protocols, and use machine learning-based risk prediction to prioritize rescue operations. With secure communications (TLS 1.3, mutual authentication), precise time synchronization (PTP), identity verification, AES-256 encryption, and chain-of-custody logging, they ensure data integrity and compliance with ISO 27001 and IEC 62443 standards. Integrated with centralized command centers, early warning systems, and critical infrastructure control platforms, they enable rapid, coordinated actions while minimizing human exposure. This transformation from human-dependent to technology-driven rescue operations enhances speed, precision, safety, and scalability—delivering a future of intelligent, secure, and resilient disaster response powered by AI, connectivity, and real-time decision-making.

21. Software Solutions for Sensitive Data Leak Detection and Prevention

Data Loss Prevention (DLP) software forms the cornerstone of modern data protection, safeguarding sensitive information in government agencies, industrial enterprises, financial institutions, and healthcare providers from internal and external data breaches. These systems employ an integrated architecture combining User and Entity Behavior Analytics (UEBA), real-time data monitoring, Identity and Access Management (IAM), content inspection (including encrypted data), AI-driven anomaly detection, network traffic analysis, and multi-factor authentication (MFA). Advanced capabilities include real-time policy enforcement, automated incident response, secure communication (TLS 1.3, AES-256), chain-of-custody logging, and integration with SIEM/SOAR platforms for automated threat detection, alerting, and investigation. The solution monitors user behavior—flagging suspicious actions such as large-scale data transfers to cloud storage or USB drives, or unauthorized access to medical records or intellectual property. Compliant with international standards such as ISO 27001, GDPR, HIPAA, and NIST SP 800-53, DLP tools are deployed across critical sectors including banking, healthcare, and critical infrastructure. With support for secure communication, time synchronization (PTP), and role-based access control (RBAC), they enable precise threat detection, rapid incident response, and full compliance.

This empowers organizations to enforce data governance, prevent breaches proactively, and maintain confidentiality in a secure, transparent, and intelligent digital environment—built on real-time analytics, end-to-end encryption, and centralized control.

22. Cyber Intrusion Detection and Resilience Systems

Cybersecurity intrusion detection and prevention systems form the backbone of modern digital defense, enabling early threat detection, real-time response, and proactive mitigation across enterprise and critical infrastructure environments. These systems integrate Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) with Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), and Security Orchestration, Automation, and Response (SOAR) platforms to deliver comprehensive threat visibility. Advanced capabilities include real-time network traffic analysis, predictive threat analytics, AI/ML-driven anomaly detection for identifying sophisticated attacks such as zero-day exploits, Advanced Persistent Threats (APTs), and cloud-targeted breaches, and automated incident response with secure communication (TLS 1.3, mutual authentication), time synchronization (PTP/IEEE 1588), identity verification, and chain-of-custody logging. Fully compliant with international standards—ISO 27001, NIST SP 800-53, IEC 62443, and GDPR—these solutions support integration with AES-256 encryption, Identity and Access Management (IAM), VMS, and SCADA systems, ensuring end-to-end security. With support for interactive threat hunting, behavioral profiling, and real-time response orchestration, they enable organizations to detect threats with precision, respond at scale, and maintain compliance. This holistic, AI-powered, and secure approach ensures resilience, transparency, and operational continuity—building a future of intelligent, proactive, and data-driven cybersecurity.

23. Systems for Identifying and Mitigating Manipulated AI-Generated Media (Visual, Auditory, and Video Content)

AI-generated media detection systems represent the vanguard of digital trust, combining advanced forensic analysis with cryptographic integrity to combat deepfakes and synthetic media. These systems employ a multi-layered approach using high-precision micro-feature analysis—leveraging state-of-the-art deep learning models such as Vision Transformers, 3D-CNNs, and audio-visual fusion networks—to detect subtle, human-invisible anomalies such as irregular eye movement, inconsistent lighting angles, temporal instability between video frames, and audio-visual misalignment. They support time-resolved analysis, frame-level synchronization detection, and generation artifact identification (e.g., texture repetition, unnatural facial edges). Advanced capabilities include digital watermarking via specialized algorithms (e.g., neural watermarks, sparse signatures), provenance tracking through metadata analysis (device type, timestamp, digital signature), and automated threat response via SIEM/SOAR integration. With support for TLS 1.3, mutual authentication, PTP/IEEE 1588 time synchronization, multi-factor authentication, and chain-of-custody logging, these systems ensure data integrity and compliance with international standards such as NIST SP 800-157, ISO/IEC 27001, and the EU AI Act. Deployed in high-stakes environments—including official media, medical records, and electoral systems—these tools enable precise discrimination between authentic and synthetic content, ensuring authenticity, transparency, and trust in digital information. By combining AI-powered forensic analysis, robust encryption, secure authentication, and end-to-end auditability, they form a critical defense layer against digital disinformation—ensuring a secure, reliable, and accountable digital ecosystem in the age of synthetic media.

General Directorate of Industrial Security

Taser Gun

Specifications:

- Lightweight design
- Smart targeting technology
- Replaceable cartridges
- Advanced safety features
- Compliant with safety and security standards in oil and gas zones

Police Patrol Car Interior Camera

Specifications:

- High-definition video recording
- Automatic data analysis
- Real-time tracking
- Simultaneous interior and exterior recording
- Automatic license plate recognition
- Supports night vision

Glasses-Mounted Camera

Specifications:

- High-definition video recording
- Waterproof design
- Wide viewing angle
- Long-lasting battery
- Supports night vision

Body Cam

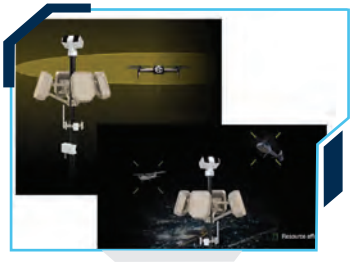
Specifications:

- High-resolution video recording
- Wide viewing angle
- Battery life suitable for a full work shift
- Live streaming support
- High-quality night vision
- Waterproof
- Operates in high-temperature environments

Anti-Drone System

Specifications:

- Long-range LED illumination
- Lightweight design
- Shock resistant
- USB rechargeable
- Long battery life
- Waterproof
- Operates in high-temperature environments



Police Tactical Flashlight

Specifications:

- Long-range LED illumination
- Lightweight design
- Shock resistant
- USB rechargeable
- Long battery life
- Waterproof
- Operates in high-temperature environments

Police Tactical Baton

Specifications:

- 60 cm length, foldable design
- Quick deployment with one-hand motion
- Lightweight
- Steel construction
- Vehicle glass-breaking capability
- Comfortable, anti-slip grip

Tactical Weapon Light for Rifles

Specifications:

- Long-range LED illumination
- Lightweight
- Quick mounting on rifles
- Rechargeable battery
- Waterproof and shock resistant
- Operates in high temperatures

Pistol-Mounted Tactical Flashlight

Specifications:

- Long-range LED illumination
- Lightweight
- Quick weapon mounting
- Rechargeable battery
- Waterproof and shock resistant
- Operates in high temperatures

Tactical Pepper Spray

Specifications:

- Strong concentration
- Long spray range
- Safety cap
- Ergonomic, easy-to-carry design
- Waterproof
- Heat resistant
- Long shelf life

Portable Drug and Explosive Detector

Specifications:

- Advanced sensing technology
- Instant data analysis
- Lightweight, handheld, and portable design
- Detects narcotics and explosives
- High sensitivity for trace detection
- Fast response with digital display and user-friendly interface
- Long-lasting battery
- Operates in harsh terrain and high temperatures

Security Under-Car Inspection Camera

Specifications:

- Automatic image analysis
- Rapid threat detection
- Advanced vehicle scanning system
- Night vision capability
- Operates in high-temperature environments

Portable Hydrogen Sulfide (H_2S) Gas Detector

Specifications:

- Long-range and safe gas leak detection
- Audible, visual, and vibration alerts
- Waterproof
- Operates in high temperatures
- Self-calibration support
- Easy-to-read display
- Battery life of at least two years

Security Screening Gate

Specifications:

- Compliant with international safety standards
- Thermal detection capability
- Durable construction
- Easy installation and operation
- Simple user interface
- Operates in high temperatures

Metal detector handheld

Specifications:

- Deep detection area
- Easy to use
- Audio, visual, or vibration alarms
- Long battery life
- Extremely durable design
- Headphone jack
- Waterproof and heat resistant

Tactical Night Vision

Specifications:

- Clear visibility in low-light environments
- Infrared illumination
- Durable, lightweight, water- and dust-resistant
- Digital zoom, photo, and video recording
- High-temperature tolerance
- Infrared target identification
- Long battery life

Tactical Helmet

Specifications:

- Impact protection
- Mounting points for accessories (lights, night vision, etc.)
- Padded inner cushions for comfort
- Adjustable straps for a secure fit
- Lightweight construction

Tactical Goggles

Specifications:

- High durability and impact resistance
- Anti-fog lenses
- UV protection
- Ventilation system
- Adjustable strap
- Comfortable inner padding
- Interchangeable lenses

X-Ray Bag Scanner

Specifications:

- Detects bag contents without opening
- Large tunnel size
- High-resolution imaging
- Explosive detection capability
- Safe radiation levels for people and baggage
- Integrated computer system
- User-friendly interface

Riot Shield

Specifications:

- Lightweight
- Shock resistant
- High transparency
- Easy to carry

Tactical Goggles

Specifications:

- Shock resistant
- Built-in rechargeable light with long battery life
- Multi-directional wheels
- Ability to inspect upper vehicle areas

Mobile Platform Ladder

Specifications:

- Minimum height: 4 meters
- High safety standards
- Equipped with multi-directional, lockable wheels
- Waterproof and heat resistant

Mobile Truck & Cargo Scanner

Specifications:

- Fully mobile, vehicle-mounted unit
- Meets international safety standards
- Safe radiation levels
- High safety design
- Adjustable scanning arm for all vehicle types
- User-friendly interface

Handheld Backscatter X-Ray Imager

Specifications:

- Deep penetration detection capability
- Easy-to-use interface
- Long battery life
- Lightweight
- Operates in high temperatures
- Waterproof
- Safe radiation level

Ballistic Vest

Specifications:

- Lightweight
- Bullet- and shrapnel-resistant
- Adjustable shoulder and waist straps
- Compatible with additional tactical accessories

General Directorate of Criminal Investigation

Mobile Laboratory

The mobile laboratory represents a qualitative addition to investigation capabilities, its flexibility to move directly to incident sites and its high level of readiness through the integration of the latest technologies and specialized digital forensics software. It provides a secure work environment for preserving evidence in accordance with forensic chain-of-custody standards, while enabling rapid incident response. In addition, it is equipped with independent power sources and fully integrated workspaces for experts.

The objectives of the laboratory include expediting digital investigations, protecting evidence from tampering or loss, and supporting field teams in carrying out their tasks with high efficiency. It also contributes to the development of national capacities by serving as a practical platform for training and awareness in the field of digital forensics.

Digital Forensics Hardware and Software

As part of strengthening the digital laboratory and observation room infrastructure, it is essential to provide advanced forensic devices that align with the latest international standards and meet the needs of electronic criminal investigations. devices with ability to handle various digital media and devices, extract and analyze data with high accuracy, and ensure the integrity of evidence and preservation of the legal chain of custody. They also support the recovery of deleted or encrypted data and enable fast and efficient analysis processes, thereby accelerating investigations.

In addition, specialized software for examining computers, smartphones, and tablets forms a vital component, enabling the extraction and analysis of digital data in accordance with the highest standards. This includes retrieving deleted files, messages, and communications, as well as dealing with modern operating systems and applications. Such software also provides advanced tools for decryption and intelligent analysis, while issuing certified reports admissible in court and ensuring the preservation of evidence integrity.

The integration of these devices and software enhances both the speed and accuracy of digital investigations, supporting efforts to combat various forms of cybercrime, including fraud, extortion, financial crimes, and online child exploitation.

RapID3

RapID3 is the third generation of IDEMIA's handheld biometric devices, enabling police officers to identify suspects directly in the streets against a central ABIS or search them against a watchlist stored locally on the device, saving them the time to return to the police station.

MTop Mobile

The slimline MTop Mobile enables officers to verify the identity of Person of Interest (PoIs) quickly and easily in the field by providing high-quality biometric capture. Cumbersome paperwork is now a thing of the past and officers have more time to dedicate to protecting their communities.

BERLA

System for Examining Digital Forensic Evidence and Extracting Data from Vehicles.

The system is from the American company Berla.It enables the extraction of data and information from the vehicle's computer. In addition, it retrieves data and information from devices connected to the vehicle's infotainment system, such as calls, text messages, location tracking, and more.

Smart Lane For Vehicle Technical Inspection

Smart vehicle technical inspection lanes based on AI to conduct technical inspection without human interference.

- Control room systems, especially those related to traffic data analysis.
- Upgrade of fixed in-vehicle speed radar units installed in patrols (IN-Vehicle Radar).
- Upgrade of tripod-mounted mobile speed radar units (Tripod Radar).

وزارة الداخليــــــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

Ministry of Interior
Departments Contact Information

Department Name	Contact number	Email
General Directorate of Coasts and Borders Security	+974 2354666	Coast@moi.gov.qa
National Command Center	+974 2345999	ncc@moi.gov.qa
General Directorate of Civil Defence	+974 2355555	civildefence@moi.gov.qa
General Directorate of Telecommunications and Information Systems	+974 2342000	it@moi.gov.qa
General Directorate of Industrial Security	+974 2361444	info@moi.gov.qa
General Directorate of Criminal Investigation	+974 2347444	cid@moi.gov.qa
General Directorate of Traffic	+974 2344444	traffic@moi.gov.qa
Milipol Qatar committee	+974 44411818	milipol@moi.gov.qa

www.moi.gov.qa
@moi_qatar | moigovqatar | moigovqa


Milipol
QATAR
TONNJES
وزارة الداخلية
Ministry of Interior
State of Qatar
MILIPOL
QATAR
EXHIBITION
2026
20 - 22
OCTOBER
2026
THE GLOBAL EVENT FOR
HOMELAND SECURITY
& SAFETY
www.milipolqatar.com
milipolqatar

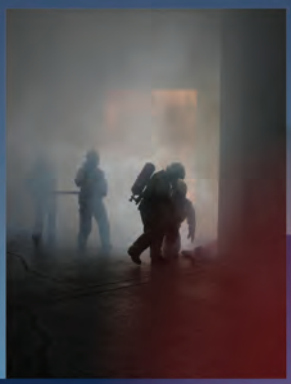
International Conference on Ai For Homeland Security

2nd Edition
20-21 October
2026 DECC
Doha - Qatar

Milipol Qatar

International
Ai Conference

AI



With Best Compliments of Milipol Qatar Committee
Ministry of Interior - State of Qatar

www.milipolqatar.com milipolqatar