UAE 국가 사이버보안 전략 2025-2031 발표와 AI 기반 방어체계 구축 계획

날짜 : '25년 12월 23일	무역관명 : 두바이	작성자 : 김경화 대리	
		TEL : +971)4-450-4360	EMAIL : khkim99@kotra.or.kr

□ 개요

○ (**추진 배경**) 2025년 9월, UAE 사이버보안 위원회(CSC)는 디지털 경제 전환 가속화와 고도화되는 사이버 위협에 대응하기 위한 국가 사이버보안 전략 (National Cybersecurity Strategy) 2025-2031을 공식 발표함.

○ 이는 기존의 방어 중심 체계에서 AI 기술을 접목한 능동형 방어(Active Defense) 및 회복 탄력성(Resilience) 확보로 패러다임을 전환하는 국가 최상위 도큐먼트임.

○ **(핵심 목표) 국가 중요 인프라(CNI) 보호를 위한 UAE 사이버 아이언돔 (Cyber Iron Dome) 구축과, 전세계 사이버 보안 지수(GCI) 1위 수성 및 데이터 주권(Data Sovereignty) 확립.**

□ UAE 사이버 위협 현황 및 전략의 주요 골자

AI 기반의 **초연결(Hyper-connected) 위협 현실화**

○ (**공격 유형**) UAE 내 사이버 공격은 일평균 20만 건 이상 차단되고 있으며, 최근 생성형 AI를 악용한 딥페이크(Deepfake) 피싱, 자동화된 랜섬웨어 공격이 급증하는 추세 (CSC, 2025.02).

○ (**주요 타겟**) 정부 기관(30%) 외에 에너지, 금융, 의료 등 국민 생명·재산과 직결된 운영 기술(OT) 및 핵심 인프라에 대한 공격 시도가 집중됨.

전략 '2025-2031 '의 5대 핵심 기둥(Pillars)

1. **AI 기반 사이버 방어**(AI-Driven Defense): 머신러닝을 활용한 실시간 위협 탐지 및 자동 대응 체계(SOAR) 의무화.
2. **데이터 주권 및 클라우드 보안**: 정부 및 공공 데이터의 UAE 내 저장(Local Hosting) 원칙 강화 및 암호화 표준 상향.
3. **사이버 회복 탄력성**(Resilience): 침해 사고 발생 시 차단을 넘어 최단 시간 내 시스템을 복구하는 연속성(BCP) 확보.
4. **국내 역량 강화**(Capacity Building):' Cyber Pulse' 캠페인을 통한 전 국민 보안 인식 제고 및 4만 명의 사이버 보안 전문가 양성.
5. **글로벌 협력**(Global Partnership): ITU, 인터폴 및 우방국과의 실시간 위협 정보 공유(Intelligence Sharing) 채널 가동.

□ 세부 실행 계획: '사이버 아이언돔' 구축

통합 관제 및 제로 트러스트 (Zero Trust) 도입

○ (**통합 대응**) 연방 정부와 각 토호국(아부다비, 두바이 등)에 분산된 보안 관제 센터 (SOC)를 하나로 연결하는 연방 사이버 통합 관제 플랫폼을 구축하여 국가 단위의 가시성 확보.

○ **(보안 아키텍처)** 기존의 경계 보안 (Perimeter Security) 한계를 극복하기 위해, 모든 접근을 신뢰하지 않고 검증하는 '제로 트러스트 (Zero Trust)' 아키텍처를 전 공공기관에 도입 의무화.

AI vs AI: 지능형 위협 대응

○ 공격자가 AI를 사용하여 취약점을 탐색하듯, 방어 측에서도 AI를 활용한 자동 모의해킹(BAS) 및 취약점 점검을 상시 수행하여 방어 태세를 선제적으로 강화.

□ 국제 협력 현황 및 한국 관련 동향

글로벌 빅테크 및 우방국 협력

○ 마이크로소프트(MS), 구글 등 글로벌 기업과 데이터 센터 보안 협력을 강화하고 있으며, 2025년 2월 '인터내셔널 사이버 보안 컨퍼런스(Insec 2025)를 개최하여 기술 표준을 주도.

한-UAE 사이버 안보 파트너십

○ (**전략적 제휴**) 2025년 1월 尹 대통령 국빈 방문 후속 조치로, 양국 인터넷진흥원(KISA-CSC) 간' 사이버 위협 정보 자동 공유 시스템 '구축 합의.

○ (**기업 진출**) 한국의 우수한 양자 암호 통신(Quantum Cryptography) 및 OT 보안 기술에 대해 UAE 측의 관심이 높으며, Barakah 원전 보안 협력을 모델로 스마트시티 보안 분야로 협력 범위 확장 중.

□ 검토 의견 및 시사점

[시장 기회] 규제 준수 (Compliance) 시장의 폭발적 성장

○ UAE의 새로운 전략에 따라 공공 및 민간 기업들의 보안 규제 준수가 의무화되면서, 보안 컨설팅, 모의해킹, 보안 관제 서비스 (MSSP) 수요가 급증할 전망. 단순 솔루션 납품을 넘어' 규제 대응 패키지 '형태의 진출이 유리.

[진출 전략] AI 보안과 OT 보안 투트랙 (Two-Track) 접근

○ (AI) UAE가 가장 공을 들이는' AI 기반 탐지 '분야에서 한국의 AI 보안 스타트업과 UAE 국영 기업 (G42 등) 간의 기술 실증 (PoC) 협력 추진 필요.

○ (OT) 석유·가스·전력 등 핵심 인프라 시설의 노후화된 제어 시스템을 보호하는 OT/ICS 보안 솔루션은 진입 장벽이 높으나 장기적인 수익 창출이 가능한 블루오션임.

□ 출처:

과학기술정보통신부 (2025.01) 한-UAE 정상회담 후속 조치:사이버보안 분야 전략적 동반자 관계 심화 방안 발표.

IDC Middle East. “UAE Security Operations Center (SOC) Market Analysis and Forecast 2025-2029”

PwC Middle East. “Digital Trust Insights 2025: The Compliance Imperative in the GCC”

UAE Cyber Security Council (CSC). “National Cybersecurity Strategy 2025-2031:Securing the Digital Economy”

UAE Cyber Security COuncil (CSC) (2025.02). “Monthly Cyber Threat Landscape Report: The Rise of AI-Driven Attacks”

UAE Ministry of AI & Digital Economy. “The Digital Economy Strategy: Data Sovereignty and Cloud Regulations”

Gulf Business. “UAE Government launches unified ‘Cyber Eye’ platform to connect federal and local SOCs”

Microsoft News Center (2025). “Microsoft and G42 Expand Partnership to Secure UAE’ s AI and Cloud Infrastructure.

The National, “UAE unveils 2031 roadmap for cyber resilience and digital growth”

WAM (Emirates News Agency) (2025.09) “UAE Cyber Security COuncil launches new strategy to safeguard digital infrastructure and accelerate economic transformation”

Zawya (Thomson Reuters) “UAE to implement ‘Cyber Iron Dome’ using AI to protect critical infrastructure.