양자 이전(Pre-Quantum) 세계에서 양자 수준 보안 주장

(2022.04.28., 양자정보연구지원센터)

□ 미, 양자 컴퓨팅 기술 대비 정부 차원 법안 도입

○ 선제적 사이버 보안 조치로 **양자 내성(Quantum-resistant) 암호화**를 통해 미국 온라인 네트워크 보호 지지

- 양자 기술로부터 데이터를 보호할 표준 설정 필요
- 미 기반 시설 대규모 해킹을 배경으로, 공공 및 민간 산업 리더는 강력한 양자 알고리즘 사용하여 네트워크 보호 위한 선제적 조치 취함
- 해커들 또한 양자 기반(Quantum-enabled) 암호화 파괴 소프트웨어 사용할 수 있음

○ **양자 컴퓨팅 사이버 보안 대비법**(Quantum Computing Cybersecurity Preparedness Act) 도입

- 포스트-퀀텀(Post-Quantum) 암호화 표준으로 대규모 전환을 위한 연방 정부의 네트워크 준비 목표
- 양자 해킹의 대상이 되는 중요한 데이터 인프라 보호에 필요한 소프트웨어 업그레이드 안내에 필수적인 준비과정
- 국립표준기술연구소(NIST) 통해 새로운 장치 표준 설정
- IBM, Google, QuSecure, Maybell Quantum, Quantinuum 민간 기업 지지

○ 선제적 양자 해킹에 대비한 **포스트-퀀텀 암호화로 마이그레이션**

- 해킹과 랜섬웨어 공격의 급격한 증가 속에서 양자 알고리즘 암호화에 대한 전국적 디지털 정밀 검사는 도전이 될 것임
- NIST와 예산 관리국은 연방 기관 내 모든 디지털 네트워크에 포스트-퀀텀 지침 주도, 국토안보부(DHS)는 양자 알고리즘 해킹에 대해 컴퓨터 네트워크 강화 로드맵 발행

(원문)

1. https://www.nextgov.com/emerging-tech/2022/04/lawmaker-argues-quantum-level-security-pre-quantum-world/366026/