

국방 양자기술 전문인력 양성 및 활용 방안

서형식, 민진식, 허준*

고려대학교

suhhsik@korea.ac.kr, mgs3351@korea.ac.kr, *junheo@korea.ac.kr

Defense Quantum Technology Workforce Development and Utilization Strategies

Hyeong-Sik Seo, Gun-Sik Min, Heo Jun*

Korea Univ.

요약

군 내 양자기술 전력화는 장비 도입만으로는 한계가 있으며, 운용·보안·획득·정비 전 주기에서 임무 중심으로 기술을 이해·적용할 전문인력 양성이 선행되어야 한다. 본 논문은 군 조직 특성을 반영해 인력 수요를 직무 관점에서 분류하고, 직무-역량 기반의 단계적 교육·훈련 체계와 교육-실습-평가 연계 절차를 제안한다. 특히, 기반 실습 장비/플랫폼을 활용해 “개념 이해 → 운용 절차 체득 → 시나리오 평가”로 이어지는 실습 모듈을 구성하고, 시범-체계화-확장 로드맵과 KPI를 통해 제한된 시간·예산 하에서도 지속 가능한 전문인력 양성 방안을 제시한다.

I. 서론

군은 통신·지휘통제·사이버보안 등 핵심 기능을 기반으로 임무를 수행하며, 기술 변화가 운용 방식과 전력 구조에 직접적인 영향을 미친다[1]. 최근 양자기술은 양자통신, 양자센싱, 양자컴퓨팅을 축으로 빠르게 발전하고 있으며, 특히 보안·탐지·최적화 등 군 운용과 연결되는 적용 가능성이 지속적으로 확대되고 있다[2-3]. 그러나 군 내 양자기술 전력화는 장비를 도입하는 것만으로 구현되기 어렵고, 임무와 제약을 이해한 인력이 체계적으로 확보되지 않으면 성능·효율·안전 측면에서 기대효과가 제한될 수 있다. 즉, 양자기술을 “보유”하는 것과 “운용 가능한 전력”으로 만드는 것 사이에는 인력 역량이라는 핵심 간극이 존재한다[4,6]. 군 조직은 임무 우선, 안전·규정 준수, 장비 교체의 제약, 제한된 교육시간과 인사 순환 등 고유한 조건을 갖는다[6]. 이러한 조건에서는 최신 기술을 단순 교육으로 확산하기보다, 직무별로 요구되는 역할과 책임을 먼저 정의하고 그에 맞는 역량을 단계적으로 축적하는 방식이 효율적이다[6]. 예를 들어 동일한 ‘양자기술’이라도 작전·운용 인력은 임무 적용과 의사결정 지원 관점의 이해가 필요하고, 보안 인력은 키·인증·정책과 같은 통제 요소를 중심으로 숙련되어야 하며, 획득·정책 인력은 표준·요구도·성과지표 기반으로 사업을 설계·관리할 수 있어야 한다. 따라서 군 내 전문인력 양성은 단일 과정의 이수 여부가 아니라, 직무 기반 역량 모델과 교육-실습-평가가 연계된 체계로 설계되어야 한다[4]. 본 논문은 이러한 문제의식에 기반하여 군 내 양자기술 전문인력 양성을 위한 실용적 프레임워크를 제안한다. 구체적으로, 군 내 양자기술 인력 수요를 직무 관점에서 분류하고, 직무-역량 기반의 단계적 교육·훈련 체계와 교육-실습-평가 연계 절차를 제시하며, 시범-체계화-확장으로 이어지는 전력화 로드맵과 성과지표(KPI)를 제안한다[4,6]. 이를 통해 제한된 시간·예산·인사 구조 하에서도 지속 가능한 전문인력 양성 체계를 구축할 수 있는 방향을 제시하고자 한다.

II. 본론

A. 군 내 양자기술 인력 수요와 직무 분류

군에서 양자기술은 단일 장비나 단일 과업으로 한정되기보다, 통신·보안·감시·의사결정 등 여러 기능에 걸쳐 새로운 성능과 새로운 위협을 동시에 형성하는 기술군으로 논의되고 있다[1-3]. 일부 국가 및 방위 관련 문헌에서는 양자기술을 국방 역량과 연계되는 전략 기술로 제시하며, 기술 생태계뿐 아니라 숙련 인력의 확보와 보호를 중요한 축으로 포함한다

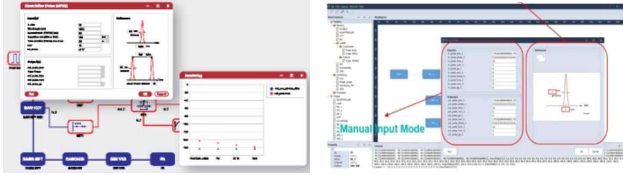
[4,6]. 또한, 국제적으로도 양자 분야 인력 부족과 직무 수요 증가가 반복적으로 언급되고 있어, 군 역시 제한된 인사 구조 안에서 필요 직무를 먼저 정의하고 역량을 단계적으로 축적하는 접근이 요구된다[3-4].

군 내 양자기술 전문인력 수요는 연구개발 인력만을 의미하지 않는다. 전력화 관점에서 핵심은 기술을 임무 환경에서 실제로 운용하고, 보안·정책과 연동하며, 기존 체계와 통합해 가용성을 유지하는 전 주기 역량이다. 이를 고려하면, 먼저 임무 적용과 운용 절차를 설계·개선하는 운용 중심 인력이 필요하다. 이들은 기술의 내부 원리를 깊게 증명하는 것보다, 운용 조건에서의 성능 한계와 실패 모드, 장애 발생 시 대체 절차, 규정 준수 요소를 이해하고 임무 목표에 맞게 적용하는 능력이 중요하다. 다음으로 암호 전환과 키 수명주기, 접근통제와 감사, 컴플라이언스 등 통제 기능을 수행하는 보안·기관리 중심 인력이 필요하다. 양자컴퓨팅 위협에 대비한 전환은 알고리즘의 선택만이 아니라 전환 절차, 운영 규칙, 검증과 감사까지 포함하므로, 보안 인력의 역할이 확대되는 영역으로 볼 수 있다[7-8]. 이어서 기존 통신체계와의 연동, 자동화, 모니터링과 장애 대응을 구현하는 네트워크·소프트웨어 중심 인력이 필요하며, 요구도 정의와 성능지표 설계, 시험평가와 표준 적용을 통해 전력화 리스크를 낮추는 획득·정책 중심 인력도 필수적이다. 마지막으로 장비·소프트웨어·절차의 고장을 현장에서 복구하고, 교정·점검과 예방정비로 가용성을 관리하는 정비·유지보수 중심 인력이 뒷받침되어야 한다. 이와 같은 직무 관점 분류는 양성체계를 설계할 때 “누구에게 무엇을 가르칠 것인가”를 명확히 해준다. 군 조직은 순환보직과 제한된 교육시간이 구조적으로 존재하므로, 모든 인력에게 동일한 심화 교육을 제공하기보다 직무별 필수 역량을 정의하고 단계적으로 확장하는 방식이 현실적이다[3-4]. 또한, 국방 분야 인력 개발은 목표 대비 진척을 측정·관리하는 체계가 약할 경우 지속성이 낮아질 수 있으므로, 교육의 결과를 임무 적용 가능 역량으로 환산해 관리하는 기준이 필요하다[7].

B. 직무-역량 기반 교육·훈련 체계 설계

군 내 양자기술 전문인력 양성은 이론 교육을 넘어서 교육-실습-평가가 연계된 훈련 체계로 설계되어야 한다. 양자기술은 개념 난이도가 높고 현업 적용 간극이 커 단발성 교육만으로 임무 적용 능력으로 이어지기 어렵기 때문에, 직무-역량 기반의 단계적(초·중·고급) 구조가 필요하다[4,6]. 초급단계는 전 직무군 공통의 공통 기초역량(기술 소양)을 확보하는 구간으로, 양자 개념과 운용 제약, 그리고 양자컴퓨팅 위협에 대비한 암호 전환과 표준화 동향을 포함해 제도·운영 관점까지 연결한다[5,7]. 이 공

통 기반은 초기 인력(장교·부사관·군무원 등) 양성 과정에 내재화될 때 확산 효과가 크며, 이후 직무 교육이 동일한 용어와 기준 위에서 누적되어 보직 순환에 따른 교육 효과의 단절을 줄일 수 있다[6]. 평가는 암기보다 임무 맥락에서 조건·한계·위험요인을 설명할 수 있는지에 초점을 둔다. 중급단계는 직무군별 과업 수행 능력을 중심으로 훈련을 분화한다. 운용 인력은 시나리오 기반 적용 판단과 절차 수행, 보안·키관리 인력은 키 수명주기 통제와 정책·감사, 네트워크·SW 인력은 연동과 모니터링·장애 대응, 획득·정책 인력은 요구도-시험평가-KPI 설계, 정비 인력은 점검·교정·복구 절차를 중심으로 숙련도를 높인다[6]. 고급 단계는 교관·설계자 역할을 수행할 핵심 소수를 양성해 과정 운영과 평가 체계를 지속 가능하게 만드는 데 목적을 둔다[6]. 실습은 교육용 시뮬레이터·모의 망·테스트베드를 활용해 구성하되, 링크/노드 구성과 상태 모니터링, 키 생성-분배-사용(암호 적용) 등의 운용 절차, 그리고 환경 변동·장애 상황을 포함한 시나리오 평가로 연결한다. 수행 시간, 오류율, 기록 완전성, 복구 소요시간 등 현장형 지표로 숙련도를 정량화하면, 교육 이수율 임무 적용 가능 역량으로 환산해 관리할 수 있다[4].



< 상용 양자 시뮬레이터 기반 실습 환경의 구성·시각화 화면[9] >

C. 운영 모델과 전력화 로드맵

군 내 양자기술 전문인력 양성은 보직 순환과 제한된 교육시간이라는 구조적 제약을 전제로, 과정 운영의 표준화와 교관 풀 유지, 실습 환경의 상시 운영을 포함한 운영 모델로 설계되어야 한다[4]. 이를 위해 교육·실습·평가를 통합 관리하는 조정 기능을 두고, 직무군별 현업 부서가 요구도와 시나리오를 제공하는 구조가 필요하며, 과정 이수 결과는 최소한의 인증과 기록 체계를 통해 지속 가능하게 관리되어야 한다[4]. 성과지표(KPI)는 운영 가능성을 위해 단순화하는 것이 합리적이다. 본 논문에서는 ‘수료-실습-시나리오 숙련-현장 복구’의 흐름을 반영하여 핵심 직무 충원율, 과정 수료율, 실습 수행률, 시나리오 평가 통과율, 현장 문제 해결시간(복구 소요시간)을 제안하며, 각 지표는 정의와 측정 방법, 측정 주기와 책임 주체를 함께 설정해 관리 가능한 체계로 운영되도록 구성한다[4]. 또한, 암호 전환과 같은 정책 과업은 표준 채택만으로 완료되지 않고, 현장의 절차 수행 능력과 예외 통제, 갱신·폐기 오류 방지, 변경 시 적응성이 함께 확보되어야 한다[7-8]. 예를 들어 전환 시점을 정하더라도 현장에서 이중 운용 규칙이나 키·인증서 갱신 절차를 숙지하지 못하면 예외 운용이 누적되어 전환이 형식화될 수 있으므로, 전환 절차 실습 통과 여부(교육 이수 지표)와 함께 예외 유지 기간, 만료 키·인증서 사용 건수, 변경 소요시간과 같은 적용 지표를 전환 일정과 연계해 관리하는 방식이 타당하다[7-8]. 전력화 로드맵은 시범-체계화-확장의 3단계로 제시할 수 있으며, 시범 단계에서는 훈련 루프와 평가 기준을 안정화하고, 체계화 단계에서는 직무를 위한 전문가격 인증을 정규화하며, 확장단계에서는 성능 이득이 불명확할 경우 즉시 기존 체계로 전환 가능한 운영 규칙을 포함해 현장 수용성과 안전성을 확보해야 한다[4,6].

구분 (단계)	시범단계	체계화단계	확장단계
내용	<ul style="list-style-type: none"> 핵심직무 구분 및 시나리오 선정 교육-실습-평가기준 확정 시뮬레이터 실습 검증 	<ul style="list-style-type: none"> 직무 정규화 실습 인프라 상시 운영 최소역량 기준 도입 	<ul style="list-style-type: none"> 합동/연합 시나리오 확대 암호 전환 방안 적용 리스크 발생에 따른 대책 마련

< 군내 양자기술 전문인력 양성 3단계 전력화 로드맵(저자 작성) >

III. 결론 및 정책제언

본 논문은 군 내 양자기술 전문인력 양성을 ‘교육 프로그램’이 아니라 ‘전력화 가능한 역량 체계’로 정의하고, 직무-역량 기반으로 초·중·고급의 단계적 교육·훈련 구조와 운영 모델을 제안하였다[4,6]. 특히, 초기 인력(장교·부사관·군무원 등) 양성 과정에 공통 기초역량(기술 소양)을 내재화하고, 이후 직무 트랙별 실습·시나리오 평가를 통해 현장 적용 능력을 정량화함으로써, 보직 순환 환경에서도 전문성이 누적될 수 있는 구조를 제시했다[6]. 또한, 암호 전환과 같은 정책 과업은 표준 채택만으로 달성되지 않으며, 절차 수행 능력과 예외 통제, 갱신·폐기 오류 방지와 같은 운영 요소가 결합되어야 하므로, 전환 일정과 연계한 교육 이수 지표 및 현장 적용 지표를 함께 관리하는 접근이 타당함을 논증하였다[7-8]. 정책적으로는 첫째, 양자기술 관련 직무를 운용·보안·키 관리·네트워크·SW·획득·정책·정비로 구분하고, 각 직무별 최소 역량 기준과 교육 성취 기준을 공식화할 필요가 있다[6]. 둘째, 교육·실습·평가를 통합 운영할 전담 기능을 설정하여 교관과 실습 인프라를 안정적으로 유지하고, 과정 결과가 현장 산출물(절차서, 점검표, 장애 대응 가이드)로 축적되도록 운영 규칙을 마련해야 한다[4]. 셋째, 성과관리는 운영 가능성을 고려해 KPI를 단순화하되, 수료-실습-시나리오 숙련-현장 복구로 이어지는 흐름으로 구성하여 교육 성과가 가용성과 임무성으로 연결되는지를 지속적으로 점검해야 한다[4]. 넷째, 암호 전환과 같이 정책적 요구가 강한 과업은 표준·전환 일정과 교육·적용 지표를 연동해 ‘문서 준수’가 아니라 ‘운용 준수’로 이행되도록 관리 체계를 설계해야 한다[7-8]. 마지막으로 확산 단계에서는 성능 이득이 불명확하거나 운용 리스크가 확인될 경우 즉시 기존 체계로 전환 가능한 롤백 규칙을 포함해, 현장 수용성과 안전성을 동시에 확보하는 방향이 바람직하다[6].

ACKNOWLEDGMENT

본 논문은 2026년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원(IITP-2026-RS-2021-II211810, 50%)과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396, 50%)

참 고 문 헌

- [1] Ministry of Science and ICT (MSIT), “Quantum Science and Technology Strategy of Korea,” Jun. 27, 2023.
- [2] UK Department for Science, Innovation and Technology (DSIT), “National Quantum Strategy,” 2023.
- [3] OECD, “An Overview of National Strategies and Policies for Quantum Technologies,” OECD Publishing, 2025.
- [4] U.S. Government Accountability Office (GAO), “Quantum Technologies: Defense Laboratories Should Take Steps to Improve Workforce Planning,” GAO-24-106284, Dec. 5, 2023.
- [5] National Quantum Initiative Advisory Committee (NQIAC), “National Strategy for Quantum Information Science,” Oct. 27, 2020.
- [6] Quantum Flagship, “Strategic Research Agenda,” 2019.
- [7] W. Barker, W. Polk, and M. Souppaya, “Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms,” NIST Cybersecurity White Paper (CSWP) 15, 2021.
- [8] UK National Cyber Security Centre (NCSC), “Timelines for migration to post-quantum cryptography,” 2025.
- [9] Qsimplus, “QSIM Pro : Quantum Simulator”