사이버안보연구, 1집 2호 2024 가을, 007-051

퀀텀 위협 대비 사이버공간의 신뢰 기반 구축 방향 :

미-중 전략경쟁과 사이버 안정성을 중심으로

0102-007051

김정호 | 국방대학교, 1저자
강봉호 | ICTK㈜, 교신저자

* 이 논문 작성을 위해 아낌없는 조언과 지도·편달을 해주신 전(前) 주미(駐美) 국방무관 예.소장 표세우님과 ICTK㈜ 대표 이정원님에게 깊은 감사를 드립니다.

논문접수일 2024년 6월 10일 | 논문심사일 2024년 8월 22일 | 게재확정일 2024년 9월 5일

논문 요약

본 논문의 논지는 사이버공간에 내재된 두 개의 의미 상충적 축을 중심으로 구성되어 있다. 첫째는 미-중 전략경쟁 속에서 미래 패권을 위한 경쟁의 공간이면서 인류 편익 증대를 위한 공존의 공간이라는 축이며, 둘째는 안정적 운영을 위해 보안성이 필수적인 공간인 동시에 효과적인 시스템·데이터 활용성이 요구되는 공간이라는 축이다.

'경쟁↔공존'과 '보안성↔활용성'이라는 두 개의 축으로 사이버공간의 새로운 창(미래 퀀텀 위협)과 방패(ZTA, PQC)의 발전 추이를 진단한 결과, 효율적이고 안정적인 디지털 생태환경을 위해 새로운 보안 아키텍처의 신속한 추진이 긴요한 것으로 판단되었다.

이 논문은 이러한 진단 결과를 바탕으로, PQC 사용의 의무화, 디지털 정보의 보호 등급 분류 기준 정립 및 등급별 차등적 암호화 알고리즘 적용 기준 등 세부 보안대책 제시, 사이버 보안활동 단위의 최소화(micro-segment), 방화벽 중심의 기존 보안정책을 데이터 중심으로 전환할 필요성 등 보안성과 활용성을 동시에 고려한 ZT 기반 MLS 및 PQC 구축 개념과 방향을 대안으로 제시하였다.

주제어 미-중 전략경쟁, 사이버공간, 경쟁-공존, 보안성-활용성, 미래 퀀텀 위협, 제로 트러스트(ZT), 다층적 보안 체계(MLS), 양자내성암호(PQC)

Ⅰ. 서론

인류 역사 속 안보와 번영의 역사는 창과 방패 간 싸움의 기록이었다. 누군가가 효과 좋은 창(공격수단)을 개발하면, 그 상대방은 그 창을 무력화할 수 있는 방패(방어수단)를 개발했고 또 다른 누군가는 그 창과 방패의 능력을 뛰어넘는 도구를 개발하는 데 집중했다. 결국, 국가의 이익 또는 인류의 편익을 증진하는 새로운 도구/기술 또는 제도가 생겨나면 이의 효용을 지키고 더욱 극대화하려는 노력(방어)과 기존 도구/제도의 효용을 자신의 이익에 맞춰 변형하거나 극복하려는 새로운 시도(공격)가 끊이지 않았다.

이러한 역사의 기록은 21세기 핵심 이익 영역 중 하나인 '사이버공간'[1]에서도 적용된다. 군사적 수단이 주요한 실현 도구로 간주되는 기존의 전통적인 안보 개념과 달리, 사이버공간의 안보에는 군사적, 비군사적 수단이 모두 작동하는 등 사이버안보는 현실 안보와 밀접하면서도 확장적으로 연결(Nye 2011, 9)되어 있으며 '화웨이 사태' 등 공급망 안보 차원의 배타적 갈등에서도 볼 수 있듯이, 미국과 중국은 사이버공간에서의 주도권을 안정적으로 확보하기 위해 막대한 예산·인력을 투입하고 우방·동맹국과 연대를 강화하는 등 경쟁하고 있다.

1) 본고에서 '사이버공간'은 전자 통신 네트워크를 통해 연결된 사회적 공간(Castells 1996)으로써, 정보 생성·저장·전송·처리를 위한 기반 구조를 제공(Denning 2000, 498)하는 과정에서 국가·기업·개인 간 새로운 권력관계를 형성(Timmers 2023, 578)하며 이를 통제·감시하는 도구를 수반(Zittrain 2002, 15)하는 영역으로 정의한다.

더욱이 영역이 날로 확장하는 이 공간에서의 '편익 의존성'[2] 급증에 따라, 이 공간을 자신의 이익 극대화에 맞춰 운영하기 위한 공존·협력적 행위와 함께, 기존 제도·규범을 자신에게 유리하게 변형시키거나 기존 틀 속에서 이를 조작/파괴하려는 경쟁·갈등적 행위가 동시에 나타나는 등 현재와 같은 전략경쟁 시기 사이버공간은 미래 핵심적인 갈등·경쟁 또는 상생·협력의 장으로 주목받고 있다.

특히, 정치·경제·사회·개인적 편익 의존성이 높아진다는 것은 상대방을 효과적으로 통제·제압하는 수단으로서의 가치가 높아진다는 것 또한 의미하기에, 사이버공간에서의 주도권을 쥘 수 있는 창과 방패를 확보하려는 경쟁과 협력이 나타나고 있으며 공존·협력적 행위는 이 공간의 활용성 제고에, 경쟁·갈등적 행위는 보안성 확보에 각각 초점이 맞춰진 행태를 자연스럽게 촉발한다.

한편, 향후 양자컴퓨터의 위협이 본격화되면 RSA(Rivest-Shamir-Adleman), ECC(Elliptic Curve Cryptography) 등 현재 널리 사용되는 공개키 기반 암호체계 붕괴와 기존 암호화 데이터의 복호화를 통해 현실화할 민감 정보의 광범위한 탈취, 디지털 서명 위조를 통한 사이버 공격의 증거 은폐 등 퀀텀 시대는 미래 사이버공간의 안정성을 교란하는 심각한 위협(Dam et al. 2023, 2)이다.

하지만, 미래 퀀텀 위협[3]은 비단 양자컴퓨팅뿐만이 아니다. 특정

2) 현재 인류는 인터넷은 물론, 클라우드 컴퓨팅, 각종 시뮬레이션, VR, AR, 국제 금융·경제(결재)망 운용, 정치·사회적 이슈 생성 등 네트워크가 연결된 사이버공간 속에서 다양한 편익을 누리고 있으며 이 공간이 제대로 기능하지 못할 경우, 심각한 정치·경제·사회·개인적 공황이 도래할 것이다. 본고는 이러한 의미에서 '편익 의존성'이라는 용어를 사용한다.

3) 본고에서 사용하는 '미래 퀀텀 위협'은 양자컴퓨팅 기술의 디지털 암호체계 해독 능력뿐만이 아니라, 날로 정교화되고 있어 어디까지 발전할지 알 수 없는 해킹 기술 등 미래 사이버공간의 위

대상을 지향한 지능형 지속 공격(Advanced Persistent Threat, 이하 APT)으로 진화하고 있는 해킹 기법/기술 등을 고려할 때, 그 창날의 날카로움이 어디까지 정교화될지 쉽게 예단할 수 없으며 사이버 영역의 최대 맹주인 미국 정부를 비롯한 세계 각국과 기업들은 이에 대응하기 위한 새로운 방패로써, 모든 컴퓨팅 과정을 '절대 신뢰하지 말고, 항상 검증하라(Never Trust, Always Verify)'라는 ZT 개념을 기반으로 하는 Zero Trust Architecture(이하 ZTA)와 양자컴퓨터의 암호 해독능력에 대항할 양자내성암호(PQC)[4]를 앞다투어 도입(The White House 2023, 7)하고 있다.

본 논문은 이러한 순환적 역사와 최근 추세를 고려하여, 사이버공간상 미래 퀀텀 위협의 대응 방향으로써 ZT 기반 다층적 보안체계(Multi-level Security, 이하 MLS) 구축과 PQC의 제도화를 주장하고자 한다.

이러한 논지에 따라, 2장에서는 미-중 전략경쟁의 특징과 유형을 먼저 살펴본 후 현재와 미래의 핵심 이익 영역인 사이버공간 안에 공존하는 갈등-협력적 기능에 관한 선행연구를 분석함으로써, 사이버공간이 안고 있는 '미래 핵심 이익 확보를 위한 갈등 영역 vs 인류 편익 의존성 확대를 위한 협력 공간', '보안성 확보 vs 활용성 제고'라는 두 가지 딜레마를 확인할 것이며, 3장부터는 사이버공간의 가장 대표

협을 통칭한다.

4) 양자컴퓨팅 기술에 대응하기 위해 개발된 양자내성암호(Post-Quantum Cryptography, 이하 PQC)는 강력한 암호화 알고리즘 제공과 함께, 보안정책을 위배하는 액세스가 추정·식별되면 고유의 암호화 민첩성(Crypto-agile)을 통해 시스템 인프라를 크게 변경하지 않고도 새로운 암호화 프로토콜로 신속하게 변경·통합함으로써, 시스템을 안정적으로 보호할 수 있도록 설계되었다.

적인 위협(창)인 양자컴퓨팅 기술과 새로운 보안체계(방패)인 ZTA 및 PQC를 미-중 전략경쟁의 틀로 진단한 후 앞선 두 가지 딜레마를 보완할 수 있는 기술·정책적 방향과 고려 요소를 제시할 것이다.

특히, ZTA에 큰 영향을 미치는 미국과 중국 정부의 공식 정책(발표) 및 추진 동향에 현행 국가(軍)급 암호화 정보 소통 체계에 대한 일선 현장의 경험을 투영함으로써, 보안성과 활용성을 동시에 보장할 수 있는 대안 제시에 집중할 것이다.

Ⅱ. 미-중 전략경쟁과 사이버공간

1. 미-중 전략경쟁의 특징과 사이버공간의 역할

2013년 시진핑 국가주석 등장 이후 미-중 간의 전략경쟁은 표면화되었으며, 특히 트럼프 전 대통령 취임 이후 양국의 갈등은 무역 및 공급망 확보 등 경제 분야는 물론, 탄소중립 및 인권 등 환경·사회 문제, 대만·북핵 등 안보·군사 문제 등 국제적 이슈 전반에서 노골화하고 있다.

이러한 전략경쟁은 사이버공간에서도 예외 없이 적용되고 있다. 현재 사이버공간에서는 미국과 중국 간 뚫으려는 자(창)와 지키려는 자(방패)의 치열한 싸움이 진행되고 있으며, 그 중심에는 미래 퀀텀 위협(창)과 불확실한 미래 사이버공간의 안정성 확보를 위한 ZTA(방패)가 자리를 잡고 있다.

하지만, 사이버공간에서 작동하는 미-중 간의 갈등·경쟁 동향을 다

루기 전에 현재 국제 이슈 전반에 작동하는 미-중 전략경쟁이 안보 측면에서 어떤 특징이 있는지를 먼저 살펴볼 필요가 있다.

그동안 미-중 전략경쟁의 특징 연구는 다양하게 진행(주재우 2022; 전가림 2023)되었으며, 대체로 안보적 측면에서 다음과 같은 특징(김정호 2023, 43-45)이 담겨 있다. 첫째, 진영논리에 입각한 집단적 대응이다. 중국은 아프리카 지역과 이른바 반미 국가들과의 연대를 통해 에너지 및 핵 능력 확산 등 미국이 민감하게 반응하는 사안에서 미국의 국력 소모와 리더십 손상을 추구하고 있으며, 미국도 우방·동맹국들과 '역할 분담과 향후 실익 분배' 방식으로 다자간 포괄적 안보협력을 확대하는 등 중국 진영에 대한 대응력을 강화하고 있다.

둘째, 경제를 안보와 연동하는 경제 안보 추구 행태다. 지금의 세계경제는 글로벌 네트워크로 밀접하게 연동되어 있어 미-중의 자원·원료·부품 공급망은 서로 얽혀있는 등 미-중 진영은 필연적으로 대립하거나 협력할 수밖에 없는 상호 연동성의 틀에 묶여 있다.

셋째, 전략경쟁 방향의 예측 불가성이다. 비록 미-중 전략경쟁에서 양 진영 간 대립-갈등 논리가 지배적이기는 하지만, 다국적 기업 등 비국가적 주체와 첨단 과학·기술 등 비인격적 주체가 글로벌 상호 연동성 속에서 각자의 생존과 번영에 집중하고 있어 전략경쟁의 방향과 결과를 쉽게 예단할 수 없다. 특히, 미래 핵심 성장동력인 인공지능, 양자컴퓨팅, 우주·사이버 분야 등에서 우위를 선점한 진영은 향후 국제질서를 주도할 수 있기에 미-중 전략경쟁의 방향과 결과는 언제든 달라질 수 있다.

넷째, 경제 안보 중심의 경쟁이 다른 영역으로 확대될 수 있는 확장성이다. 중국의 '위안화 국제화' 시도 등을 볼 때, 현 전략경쟁은 궁극적으로 미국 주도의 기존 국제질서에 대한 중국의 도전이기도 하다.

특히, 자유, 개방, 민주, 인권 등 자유민주주의 체제 미국의 가치·규범은 공산당 일당 독재 체제인 중국의 그것과 공존하기 어렵기에 향후 전면적인 체제 경쟁으로 확장될 가능성은 충분하다.

다섯째, 신냉전이라는 용어가 어울리는 군사 안보적 특징이다. 현재 미-중 양국은 군사적 영역을 지상·해상·공중에서 수중·우주·사이버 등으로 확장한 가운데 인공지능이 연결된 신속한 지휘 결심 능력을 바탕으로, 원거리 자율·무인 무기체계를 이용한 선제적 타격을 지향하는 등 전략·전술적 목표가 매우 유사하기에, 매사 충돌할 가능성이 크며 양측 진영으로 집단화될 가능성 또한 농후하다.

한편, 사이버공간은 앞선 미-중 전략경쟁의 수위와 유형(김정호 2023, 46-49)에도 영향을 미치는데, 첫째 사이버공간은 세계를 연동시키는 '글로벌 네트워크'로써 전략경쟁의 긴장 수위를 조절하는 기능을 한다. 만약, 사이버공간이 갈등을 촉진하는 역할을 하면 전략경쟁의 긴장도는 높아질 것이나, 공존의 역할을 하게 되면 그 긴장도는 낮아질 것이다. 또한, 미-중의 진영논리보다 독자적인 이익과 신념을 우선 고려하는 비국가, 비인격적 행위자들의 역할에 따라, 그 긴장의 수위는 고조 또는 완화된다.

둘째 사이버공간은 미-중 전략경쟁이 발현되는 전장(戰場)으로써, 전략경쟁 속에서 벌어지는 각종 불법 활동을 촉진하는데 사이버공간의 가상화폐 및 첨단 기술의 불법 탈취 행태는 기존 국제질서를 교란한다. 또한 '가짜 뉴스' 등 특정한 목적에 따라 특정 국가·단체·경제·사회를 왜곡하며 각국 정부가 가짜 뉴스를 국가 안보영역으로 다룰 정도(오일석 2022, 46)다. 특히, 민감 정보를 무분별하게 유통-수집 및 악용하는 공간으로써, 경쟁 상대국의 중요 정책 결정자를 목표로 한 APT 등 의도적 정보탈취 및 악용은 물론, 일반인의 개인정보와 민감

정보에 대한 탈취 시도가 끊이지 않고 있다.

2. 미-중 전략경쟁 시대 사이버공간의 딜레마

사이버공간은 앞선 특징과 역할들이 발현 또는 심화하는 근원이자 매개체이며 이러한 사이버공간의 특징과 역할에 관한 관심을 크게 두 가지로 구분하면, 미래 핵심 이익 추구 영역에서의 경쟁·갈등 배경과 대응(신경수·신진 2018, 29), 그리고 인류 삶의 질 제고를 위해 이 영역의 안정성과 활용성을 어떻게 확대(유지영 2020, 5-6)할 것인지로 나눌 수 있다.

1) 미래 이익 추구를 위한 경쟁 공간: 보안성 우선

미국 정부가 사이버공간의 디지털 생태환경 구축에 대한 국가 차원의 전략을 담은 2023년 『National Cybersecurity Strategy, 이하 NCS』에서도 밝혔듯이, 사이버공간은 인류의 모든 영역과 밀접하게 연결되어 강력한 영향(The White House 2023, 1)을 미치고 있으며, 미-중 간 전략경쟁 역시 전통적인 이익 영역을 넘어 사이버공간에서도 격화되는 등 사이버공간은 국제정치적 측면에서도 중요한 영역으로 자리매김하고 있다.

경쟁·갈등적 시각에서, 사이버공간의 역할/기능에 관한 연구는 크게 3개의 분야로 나누어져 진행되었는데, 첫째는 사이버공간이 국가 간 전통적인 갈등을 왜, 어떤 형태로 변화시키는지에 대한 연구로써, 정보화 시대에서 사이버공간은 군사 전략과 전쟁의 핵심 영역이기에 사이버상의 공격과 방어가 국가 간 갈등과 전략경쟁의 장(Geers 2009; Zilincik 2012; Allison 2021)이 될 수밖에 없으며, 이 공격과 방어에

Deep/Machine 러닝과 같은 AI 기술 등 새로운 위협(신기술)이 계속 개발·활용되는 경향(Diogenes·Ozkaya 2019; Sindiramutty 2023)이 있음을 밝히고 있다.

둘째, 사이버공간상 의도적 정보 확산과 그 영향력에 관한 연구로써, 가짜 뉴스의 확산, 온라인 홍보-선전 등 상대방의 이익 영역에서의 여론을 자신에게 유리하게 바꾸려는 사이버 공격의 효과성(Buchanan 2017; 김상배 2023)과 같은, 사이버 공작의 패턴과 동향을 분석하여 효과적인 대응 전략을 모색하는 데 집중한다.

셋째, 사이버 정책 및 국제적 협력 강화와 관련된 연구로써, 사이버공간과 관련된 국제법과 규칙 등 사이버 정책의 국제적 표준화로부터 우방·동맹국 간의 협력 강화 방안(Touré 2011; 채재병·김일기 2020; Digital Watch 2020; Kim 2023; The White House 2023)까지, 미-중 진영 간의 배타적인 제도·협력에 관한 다양한 내용을 다룬다.

이러한 연구 동향을 볼 때, 사이버공간은 이미 현재와 미래 이익을 위해 첨예하게 갈등하는 핵심 이익 공간으로 기능하고 있음이 명백하며, 보안성 확보가 이 공간에서의 이익 극대화와 경쟁에서 유리한 위치 점유를 위한 중요한 관심사로 다뤄지고 있음을 알 수 있다.

다만 이러한 연구들은 미-중 전략경쟁 시기 사이버공간의 갈등과 경쟁이라는 국제정치의 제로섬(Zero-sum)적 특징에 집중함으로써, 이 공간에서 활동하는 다양한 행위자들로 인해 공존·협력 활동 또한 존재한다는 점을 간과하고 있으며 이는 인류 편익 증대를 위한 기술·정책적 대비 노력을 세밀하게 조명하지 못하는 이유가 된다.

사이버공간에는 미-중 진영의 진영논리에 집중하는 국가적 행위자와 함께, 사이버 해커와 다국적 기업 같은 비국가적 행위자, 그리고 첨단 과학기술과 컴퓨터 바이러스와 같은 비인격적 행위자 등 국가/

진영보다 개인/단체의 이익을 우선 고려하는 행위자들로 인해 경쟁·갈등뿐만 아니라, 공존·협력 또한 존재(김정호 2023, 46)하며 이들로 인해 사이버공간의 예측 불가능성은 더욱 커진다.

2) 인류 편익 증대를 위한 공존의 공간: 활용성 중시

사이버공간이 품고 있는 예측 불가능성은, 사이버공간에 대한 인류 편익 의존성의 급격한 증가와 어우러져 이 영역의 안정적인 디지털 생태환경(Digital Ecosystem) 조성에 관한 연구를 촉진했다. 왜냐하면, 사이버공간은 인류 편익을 증진하는 방향으로 발전할 경우, 삶의 질을 더 없이 높일 수 있지만, 그럴수록 국가·경제·사회·개인의 편익 의존성이 높아짐으로써 특정 대상을 의도적으로 교란하거나 무력화하는데 더 없이 유용한 공간이기 때문이다.

안정적인 디지털 생태환경 조성에 관한 연구들은 첫째, 사이버 공격의 패턴·의도 등을 연구하는 사이버 위협 분석·예측에 관한 연구(Patel 2019; Freas et al. 2002; Leszczyna 2021; Taherdoos 2022) 둘째, 암호화 기술과 네트워크 보안 및 AI 보안 등 기술적 측면의 연구(Khan et al. 2021; Moore·Brown 2016; Scott 2016) 셋째, 랜섬웨어, 데이터 유출 등 사이버공간에서 벌어지는 다양한 범죄와 대응에 관한 연구(정태진·이광민 2019; Vasoya et al. 2022; Prasanna·Prakash 2023) 넷째, 5G 등 안정적인 Cyber Infrastructure 구축 방안에 관한 연구(Friedman·Singer 2014; William et al. 2014; Ahmed et al. 2022; 임재혁·최인수 2024) 등이며 이 분야의 연구들은 디지털 생태환경의 안정성이 확고해야 한다는 점을 넘어, 과거 보안성 위주로 구축되던 사이버 보안 체계가 점차 보안성과 활용성을 동시에 고려하는 방향으로 전환되어야 함을 강조한다.

이렇듯 보안 취약점의 반복적 발생과 이에 대한 탐지·대응에 관한

연구가 끊임없이 진행되는 것은, 사이버공간 속 새로운 창(공격수단)과 방패(방어수단) 간의 악순환 등 '사이버공간의 영구적 불안정성'이라는 인식이 일반화되어 있음을 방증한다.

특히 사이버 보안 정책에서 보안성과 활용성을 동시에 고려해야 한다는 주장은, 안전하고 안정적인 운영 환경 보장(보안성)을 기본 전제로 하는 사이버공간에서의 활용성 확대가 정보 유통 단위의 급증[5] 및 편익 의존성 확대 속에서 공존 공간의 효용 증대를 위한 시급한 해결 과제(임재혁·최인수 2024, 1)로 대두되고 있음을 말하고 있다.

하지만 이런 연구들은, 앞선 사이버공간의 갈등·경쟁적 측면의 기존 연구와는 반대로, 사이버공간에서 식별되는 다양한 위협에 관한 기술·제도적 대응에 집중함으로써, 이 공간의 위협 행태가 미-중 전략경쟁 측면의 원인에 크게 영향을 받는다는 점을 주목하지 못한다.

사이버공간상 다양한 위협은 개인/단체의 이익을 추구하는 비국가적·비인격적 행위자들에 의해 촉발되기도 하지만, 미-중 진영이 사이버공간에 대한 상대방의 편익 의존성을 공략 지점으로 삼아 상대를 제어·압박하거나 미래 이익 실현을 위한 도구(Golota 2023, 175)로도 활용하기 때문에 이를 간과할 경우, 사이버공간의 역동성과 미래의 위협 방향을 예측하는 데 한계를 가진다.

5) 한 민간 통신장비 회사가 발행한 『글로벌 네트워크 트래픽 2030 보고서』에 따르면, AI/ML, AR/VR 등 데이터 소통량을 큰 폭으로 증가시키는 차세대 기술의 영향으로 데이터 트래픽은 향후 2030년까지 매년 평균 22~25% 확대될 것으로 예상(Hill 2023)된다.

Ⅲ. 사이버공간의 새로운 창과 방패

1. 대표적인 새로운 창: 양자컴퓨팅 기술

현재 사이버공간의 안정성을 위협하는 창들은 일일이 열거할 수 없을 정도로 다양하다. 특히, 과거 불특정 다수를 향했던 공격 패턴이 점차 특정 기관 또는 인물, 직업군 등 공략 목표를 지향한 APT 형태로 변화하는 추세(The UN Cyber Groups 2022)이다.

하지만, 이 논문에서 양자컴퓨팅 기술을 가장 대표적인 새로운 창으로 주목하는 것은, 이 분야가 향후 사이버공간에 미칠 엄청난 미래 파괴력을 가지고 있기도 하지만, 여타 해킹 기술·기법 대비 미-중 전략경쟁의 메커니즘이 가장 뚜렷하게 나타나기 때문이다.

양자컴퓨팅이란, 양자역학의 원리를 활용하여 계산을 수행하는 새로운 컴퓨팅 방식으로, 0 또는 1중 하나만을 저장·처리할 수 있는 기존 컴퓨터의 비트(bit) 단위 대신 0과 1이라는 두 가지 정보뿐만 아니라 중첩이라는 두 상태의 조합도 가질 수 있는 큐비트(qbit)를 정보 처리 단위로 채택함으로써 기존 컴퓨터보다 연산 능력이 획기적으로 개선되는 기술을 말한다(IBM 2024). 특히 이 큐비트를 활용한 연산 방식은 ECC, RSA 등 현행 키 기반의 디지털 암호체계를 해독하는 데 강력하게 사용될 수 있어 미-중 전략경쟁의 주요 전장인 사이버공간의 미래 주도권을 획득할 수 있는 핵심 기술(창)로 주목받고 있다.

1) 양자컴퓨팅 기술 개발 속 미-중 전략경쟁

현재 중국, 러시아, 북한, 이란 등 반미 성향의 국가들이 서로의 협

력관계를 강화하고 있으며, 이들은 벨라루스에 대한 러시아의 전술핵 확산, 우크라이나 전쟁에 대한 중국·북한의 지원, 북-러 및 북-이란 간 첨단 무기 분야 기술협력 강화, 북핵에 대한 중·러의 유·무형적 지원 및 국제적 여론전에서의 옹호 등 미국 진영의 세계 전략에 반발하고 있다.

사이버공간에서도 이러한 미-중 진영 간 전략경쟁 메커니즘이 여실히 작동하고 있다. 중·러·북·이란은 모두 사이버공간에 대한 교란 능력과 의지를 가진 나라들이며, 실제 국가 주도로 사이버공간을 교란하는 등 사이버안전의 최대 위협 국가(Jaikaran 2023, 5)들이다.

특히 중국은 미래 사이버안전에 대한 최대 위협 중 하나인 양자컴퓨팅 기술 개발에 막대한 인력·예산을 집중하고 있다. 중국은 양자컴퓨팅 기술 개발에 미래 기술패권 경쟁의 사활을 거는 분위기다. 2006년 발표한 '국가 중장기 과학기술발전계획'에 양자컴퓨팅 기술 분야를 처음 포함하면서 국가 정책으로 추진하겠다는 의지를 밝혔으며, 2011년 양자통신, 2016년 양자컴퓨터 개발을 '중대 과학기술 프로젝트'로 지정하여 2030년까지 개발을 완료(서행아 2016, 19)한다는 목표연도까지 명시했다.

또한, 2021년 제14차 과학기술혁신계획 발표 시에는 양자통신 및 양자 컴퓨터 분야 기술 발전에 집중할 수 있도록 연구 개발비를 매년 7% 이상 증액(한중과학기술협력센터 2021, 4)하는 계획을 수립하는 한편, 탄탄한 천연자원 공급망과 위안화의 자금력을 앞세워 제3세계 국가들과 기술동맹(이선재 외 2023, 51)을 맺는 등 이른바 미국의 기술동맹 및 기술·부품 선진국 간의 다자협의체에 대응하고 있으며, 하드웨어에 집중하고 있는 미국 정부와 차별적 우위를 점할 수 있는 소프트웨어 중심의 기술 개발에 집중하고 있다.

미국 역시 '중국의 과감하고 지속적인 R&D 분야 투자로 인해 첨단 산업 분야의 독보적 위상이 흔들리고 있다'라는 판단(이선재 외 2023, 47-48)에 따라 양자컴퓨팅 분야를 기술 패권 경쟁의 핵심 영역 중 하나로 삼고 있다.

미국은 2008년 국가 차원의 '양자 정보 과학 비전'을 수립하면서 양자 컴퓨터 기술 개발을 본격화한 이후 2018년 '국가 양자 이니셔티브 법안(NQI)'으로 최대 12억 달러를 투자하는 등 미-중 양자컴퓨팅 분야 기술패권 경쟁에서 우위를 유지(이선재 외 2023, 50)하고 있는데, 미국의 이 분야 우위 전략은 첫째, 정부 주도로 정부와 민간의 역할을 구분하여 기술을 개발하는 것이다. 현재 미국 정부는 하드웨어 중심의 연구개발에 집중하면서 구글, IBM, 인텔 등 민간 빅테크 기업과의 협력 및 기업 간의 기술 개발 경쟁을 유도하고 있다.

둘째, 미국 중심의 기술동맹 및 다자간 기술협의체를 활성화하여 중국의 기술 개발을 방해하는 것이다. 현재 미국은 대한민국·미국·일본·대만 등 이른바 'Chip 4 동맹'을 통해 양자 컴퓨터 개발에 필수적인 10nm급 이하(Sub-10 nm)의 초정밀·고성능 반도체 및 관련 기술의 중국 유입 차단하는 등 우방·동맹국을 중심으로 대중국 기술 장벽을 넓게, 그리고 높게 펼치고 있다.

셋째, 대중국 기술 견제가 가능한 국내법을 입안하고 이를 지키면 혜택을, 위반하면 큰 페널티를 주는 방식으로 이해 당사자를 견제하는 것이다. 현재 미국은 '수출관리 개혁법(EAR)', 'Chip and Science Act' 등 양자컴퓨팅 관련 기술과 물자의 대중국 수출을 법률로써 제한하고 이를 위반하는 국가·법인·개인에 대한 과감한 페널티 부과를 제도화했다.

이렇게 미국과 중국이 양자컴퓨팅 분야를 미래 전략경쟁의 핵심

이슈로 바라보는 이유는 양자컴퓨팅 기술 속에 잠재된 불투명성과 파괴력에 주목하기 때문이다. 양자컴퓨팅은 기술 개발에 관한 관심과 투자가 집중된 지 얼마 되지 않은 분야이기에, 다른 첨단 기술 분야와 달리 미국의 우위가 독보적이지 않으며 그만큼 누가 얼마나 효과적으로 기술을 개발하느냐에 따라 기술 패권이 누구에게 돌아갈지 알 수 없는, 불투명성이 잠재된 분야이다. 실제로도 미국은 중국의 이 분야의 기술 추격에 위기감(Sayler 2024, 5-6)을 느끼고 있다.

또한, 양자컴퓨팅 기술은 현행 사이버공간의 안정성을 유지하는 핵심 기술이자 군사적으로도 널리 활용(The White House 2023, 12)되는 RSA, ECC 등 현 디지털 암호체계를 무력화(암호 해독)하는 데 최적화되어 있기에 이 분야의 기술 우위를 선점하는 쪽은 한동안 사이버공간은 물론, 정치·군사·경제 영역에서 확고한 우위를 점하거나 유지할 수 있는 등 양자컴퓨팅 기술에는 이른바 게임 체인저로서의 파괴력이 내재되어 있다.

2) 양자컴퓨팅 기술의 위험성과 미래 퀀텀 위협

현재 사이버공간에서는 'Store now, Decrypt later(SNDL)' 공격 기법이 활성화되고 있는데, 이는 현행 디지털 암호체계로 암호화된 데이터가 지금은 정보로서의 가치가 없지만 향후 양자 컴퓨터 기술이 큐비트(qbit)를 충분히 증가시킬 수 있을 정도로 발전하면 기존에 사이버공간에서 사용되던 디지털 암호를 해제하여 활용할 수 있을 것이라는 전망에 따라, 일단 무작위로 수집·저장해 놓는 미래 예측형 공격 기법(QuSecure 2024)을 말한다.

이 공격 방식이 지금은 의미가 없어 보일 수도 있지만, 현실 세계 거의 모든 영역이 사이버공간과 접점을 가지고 있으며 그 공간에 저

장·유통되는 데이터 대부분이 현행 키 기반의 디지털 암호체계로 암호화되어 있다는 점을 고려한다면, 그 정보들을 어렵지 않게 해독할 수 있는 양자 컴퓨터의 활용이 본격화되었을 때의 파급력은 클 수밖에 없다. 특히, 적대적 의도를 가진 상대방이 기존에 수집·저장한 수많은 정보와 데이터를 해독하여 상대방의 정치·경제·금융·군사적 취약점을 공략한다면 그 파괴력은 상상을 초월할 것이다.

이렇듯 가장 대표적인 미래 퀀텀 위협인 양자 컴퓨터의 위험성은 첫째, 사물·모바일 인터넷 기술의 발전과 데이터의 디지털화에 힘입어 사이버공간이 현실 세계 전반과 연결되는 극단적인 편익 의존성 증가 추세에 기반한다. 가령, 군사적 영역에서는 교전 중에 발생하는 전장·전투 정보 등 다양한 기밀·일반 정보들이 정보·전산화되면서, 군 전용망이든 일반 위성·인터넷망이든, 디지털 체계에 의해 제어되는 사이버공간 속에서 디지털 형태로 저장·유통된다. 이러한 정보·전산화를 통해 디지털화된 정보의 유통 및 제어는 비단 군사적 영역뿐만 아니라, 다양한 정책과 기밀정보를 다루는 정부 기관, 신기술을 개발·운영하는 민간 기업, 원자력 등의 발전소, 전자화된 화폐 유통·관리 및 신용 거래(결재)와 같은 경제 원천을 운용하는 금융 기관과 기업, 일반인 간의 원거리 통신·소통 등 거의 모든 일상생활과 연동되어 있으며, 현 시대는 사이버공간과 접점 없이 일상생활을 영위할 수 없을 정도이다.

둘째, 편익 의존성이 극단적으로 확장되고 있는 사이버공간이 안정성 유지를 위해 채택하고 있는 현행 암호체계가 소인수분해 문제(RSA, Rabin) 또는 이산대수 문제(EIGamal, KCDSA, ECC)에 기반한 암호화 알고리즘으로써, 언젠가는 양자 컴퓨터에 의해 암호체계가 무력화될 수 있다는 점에 기반한다. 군사·국방용 암호를 비롯하여 블록체

인, 암호화폐, CBDC(Central Bank Digital Currency), 인터넷 및 모바일 뱅킹, 암호화 통신(TLS/SSL), HTTPS, VPN, 보안 토큰, 스마트카드, 공인인증서, FIDO(Fast Identity Online) 및 심지어 해킹 도구 중 하나인 랜섬웨어조차도 앞서 언급한 키 기반의 디지털 암호체계를 적용한 공개키 암호를 사용하고 있다.

결국, 기존 암호체계 해독에 특화된 양자컴퓨팅 기술이 큐비트의 양을 충분히 증가시킬 수 있을 만큼 발전하면, 사이버공간은 현재의 운영·관리 시스템만으로 더는 안정성을 도모할 수 없을 뿐만 아니라, 미래 세계 패권을 놓고 벌어지는 온·오프라인상의 갈등·경쟁, 그리고 분쟁의 원인이자 공간이 될 것이다.

더욱이, 미래 퀀텀 위협은 양자컴퓨팅 기술에서 멈추지 않는다. 향후 이를 활용·접목한 해킹 기법·기술이 새롭게 진화하거나, 상대의 방패를 뚫을 전혀 새로운 형태의 창이 다시 태어날 수도 있다. 따라서, 미지의 해킹 방식/기술을 특정하여 거기에 최적화된 방패를 선제적으로 구상할 수도 없는 사이버공간에는 여전히 '영구적 불안정성'이 잠재되어 있다.

2. 새로운 방패: 제로 트러스트 아키텍처(ZTA)와 양자내성암호(PQC)

이미 1960년대 'ARPANET'이라는 최초의 컴퓨터 네트워크가 구축되면서 인류의 실생활에 발을 들여놓은 사이버공간은 그동안 다양한 프로토콜 등 소통 방식/원칙을 정립해 나갔고, 그에 따라 다양한 기술·부품·제품이 표준화되어 실생활에 적용되었다. 따라서, 그 공간에서 통용되었던 기준을 대신하여 새로운 신뢰의 기반을 정립하는

것은 많은 시간과 노력, 비용이 소요될 수밖에 없다.

하지만 미국과 중국은 모두, 새로운 기준과 기반을 재설정하기가 쉽지 않음에도 불구하고, 사이버공간에서의 갈등·경쟁에 대비하면서 보안성이 담보된 활용성을 구현하기 위해 사이버공간의 새로운 신뢰 기반이 되는 ZTA 구현과 독자적인 PQC 적용을 앞다투어 추진하고 있으며, 이 구상에는 단순히 사이버공간에서의 안전성을 확보하려는 의도뿐만 아니라, 미래 핵심 이익을 놓고 경쟁하는 상대방에 대한 완벽한 방어체계 구축이라는 전략경쟁 측면의 인식 또한 자리 잡고 있다.

1) 새로운 방패 설계·구축 과정 속 미-중 전략경쟁

미래에 어떤 형태로 나타날지 모르는 창에 대응하기 위해 'Never Trust, Always Verify'라는 ZT 개념을 기반으로 나타난 새로운 방패가 ZTA이고, 퀀텀 컴퓨터의 암호 해독력에 대응하기 위한 새로운 암호화 알고리즘이 PQC이다. 그리고, 이의 설계·구현 과정에서도 미-중 전략경쟁의 메커니즘은 작동한다.

ZTA란 사이버공간상 모든 사용자·장치·애플리케이션을 끊임없이 검증하고, 필요에 따라 액세스 권한을 최소로 부여하며, 침해사고 시에도 문제 범위를 최소화할 수 있도록 네트워크를 최소화 단위로 구성 및 데이터 암호화와 손실 방지 등 데이터를 가장 중요한 자산으로 간주하는 사이버 보안 아키텍처(Rose et al. 2020, 4-7; 이진용 외 2022, 210-211)로써, APT 공격 추세, 클라우드 및 모바일 기기 사용 확대, 데이터 유출 및 침해사고 증가 등 최근의 위협 변화에 기민하게 대응하기 위해 구상되었다.

미국 정부는 2023년 『NCS』를 발표하면서, ZTA 구현과 PQC 적용

을 미래 사이버공간의 안정성 확보의 핵심적인 요소로 다루고 있으며 침해사고 발생 시 신속한 복원력(Resilience)을 갖추는 것에도 많은 관심을 기울이고 있다. 또한, 현재 사이버공간의 안정을 해치는 악의적 행위자(Malicious Actors)로 '미국의 이익과 국제적 규범을 침해함으로써 현 사이버공간의 질서를 재편하려는 중국, 러시아, 이란, 북한 및 그 밖의 권위주의 국가'라고 명시하면서 이들의 사이버 능력과 과거 공격 사례를 일일이 소개하는 등 이들의 위협이 미국과 미국 진영의 이익을 침해(The White House 2023, 3-4)하고 있다는 인식 또한 명확히 했다.

2023년 『NCS』에서 특히 주목해야 할 부분은, 미국과 우방국 군대 간의 데이터 상호운용성을 포함한 사이버공간의 새로운 방패를 미국 정부 주도로만이 아니라, 신기술을 빠르게 발전시키는 민간 빅테크 기업은 물론, 동맹·우방국과 함께 구축한다는 계획(The White House 2023, 19-20, 29-33)을 밝히는 등 사이버공간의 안정성 구축 과정에서 미국 진영 대 반미 진영의 경쟁·대립 구도를 국가전략에 공개적으로 명시했다는 점이다.

중국 정부 역시 미래 번영의 핵심 이익 영역인 사이버공간에서의 안정성 확보를 미국 진영의 위협에 대한 대응 개념으로 접근하고 있다.

중국의 디지털 경제 규모는 중국 전체 GDP의 39.8%, 데이터 생성량은 2021년 전 세계의 약 9.9%에 해당하는 6.6ZB(오종혁 2023, 3)로써, 사이버공간은 이미 중국의 핵심 이익 공간으로 자리를 잡았으며 중국 당국은 2023년 미래 사이버 환경 발전 방향과 계획을 명시한 '디지털 중국 건설 규획(数字中国建设整体布局规划)'을 발표(오종혁 2023, 4)하는 등 이 핵심 이익 공간의 미래 가치 확장을 위해 노력하고

있다.

이러한 노력에는 이익 공간으로서의 가치가 지속 확대되는 사이버 공간의 안정성에 대한 국가 차원의 우려와 대비 방향이 반영되어 있는데, 2018년 시진핑은 사이버안보정보화 전국회의에서 '정보화와 사이버 보안은 한 몸의 두 날개와 두 바퀴의 추진력이다. 사이버안보 없이는 국가 안보도 없고 경제사회도 안정되지 않으며 광범한 인민의 이익을 수호하기 어렵다'라면서 정보화가 미-중 전략경쟁에서 우위를 점할 파격적인 기회를 제공하지만, 사이버공간에서의 완벽한 보안 환경 구축은 정보화의 전제조건임을 명확히 했다.

또한, 2023년 4월 중국의 사이버 보안 이론·기술 연구 및 제품 개발·공급 업체들로 구성된 중국 사이버보안산업연맹(中国网络安全产业)은 2010년 이후 중국을 향한 사이버 공격·감시, 기밀 도용, 악성 코드 및 해킹 툴 유포 사례 10여 건을 공개하면서 이를 미국 국가안보국(NSA) 등 정보기관의 소행으로 특정(国家信息中心 2023)하는 등 사이버공간에 대한 대미 경쟁적 갈등 의식을 표면화했다.

특히, 안정적인 디지털 생태환경 구축 배경에 대한 중국 국가사회과학재단의 연구 논문(单志广a 2023; 单志广b 2023)에 따르면, 중국은 사이버공간을 '다양한 공격과 방어가 빈번한 첫 번째 전장으로써, 군사·외교적 활용성 증대 등 국가 이익 보호를 위한 정치적 수단'으로 간주하고 있으며, '미국 등 적대 세력이 강력한 사이버 공격 기술을 사용하여 중국의 사이버공간을 DDos 공격, 도메인 삭제, 네트워크 시스템 공격과 기밀 탐지/도용 및 사이버 여론전 같은 방식으로 끊임없이 교란하고 있으며 갈수록 심화하고 있다'라고 인식하고 있다. 학술 활동조차 당국의 간섭이 일반화된 중국의 사정을 고려한다면, 중국 내부에는 '정보화 추진에 따라 편익 의존성이 커지는 사이버공간

이 미-중 전략경쟁의 취약점이며 이 공간에서의 안정성 확보는 미-중 전략경쟁 환경을 유리하게 조성하는 것'이라는 인식이 보편적임을 알 수 있다.

한편, 사이버 안정성 확보 방향은 2023년 '디지털 중국 건설 규획(数字中国建设整体布局规划)'과 2024년 공산당 제20차 전국대표대회 보고서에 잘 담겨 있는데, 이 두 발표에는 디지털 생태환경 조성 목표를 '경제, 주요 인프라, 금융, 네트워크, 데이터, 생물학, 자원, 원자력, 우주, 해양 등 제반 국가 이익 영역과 연결된 사이버 영역에서 신뢰할 수 있고 통제할 수 있는 디지털 보안 장벽 구축'(国家信息中心 2023)이라고 제시하는 등 ZTA와 PQC의 개념을 적용하고 있으며, 현재는 정부 주도로 이의 발전 추세에 대한 소개 자료를 당국 홈페이지에 게재(信息网络安全公安部重点实验室 2024)하는 등 일반 대중 여론의 친숙화를 도모하고 있다.

2) 미-중 양국의 ZTA 구축 방향

미국 정부는 미래 디지털 생태환경 구축 목표를 '시스템 공격 비용이 방어 비용보다 많고 민감한 정보 또는 개인정보가 안전하게 보호되며 사이버 공격이나 오류가 재앙적인 결과로 가지 않도록 막을 수 있는 방어·복원력 확보'(The White House 2023, 1)로 설정하고 있으며, 이를 ZTA로 구현한다는 계획이다.

미국 상무부 산하 국립표준기술국(NIST)이 발표한 자료(SP 800-207 2020)에 따르면, ZTA 구현에 필요한 7가지 필수 기능은 첫째, 사이버 공간의 모든 사용자, 장치 및 S/W에 대한 반복 검증 체계 둘째, 액세스 권한 최소화 정책 셋째, 모든 액세스 시도에 대한 실시간 모니터링 기능 넷째, 정보보호 활동 단위의 최소화 구성(micro-segment) 다섯째,

데이터 암호화 등 강력한 손실 방지 대책 여섯째, 시스템 이상 탐지 체계의 상시 가동 일곱째, 앞선 일련의 시스템 보호 활동에 대한 자동화 분석·통제 시스템 운영 등(Rose et al. 2020, 11-21)이다. 특히, SP 800-207에는 정보보호 활동 단위를 최소화(micro-segment)함으로써 사이버공간의 안정성을 확보하려는 의도가 반영(Rose 2020, 6-12)되어 있다.

이는 ZTA 구현에 있어 데이터를 가치의 중심으로 다루려는 인식에 따라, 여러 데이터와 장치, 애플리케이션 등이 함께 존재하는 일정한 크기의 영역을 방화벽으로 묶어 보호하는 기존 보안 활동을 단일 또는 최소화된 데이터 영역 중심으로 전환하려는 것으로, 사이버공간상 디지털 데이터의 활용성을 증진하려는 데이터 중심의 다층적 보안체계(Multi-level Security)에 큰 시사점을 준다.

이미 미국 정부는 ZTA 개념을 본격적으로 도입하기 이전부터 사이버공간에 저장·유통되는 보안 등급별 데이터의 보호 대책을 차등적으로 구체화하는 등 데이터 중심 보안 활동 개념을 적용하기 시작했는데, 국가 안보 시스템을 관장하는 CNSS(Committee on National Security System)는 2010년 CNSSI 4009를 발행하여 보안 등급별 데이터를 사이버공간에서 저장·소통할 때 적용할 암호화 알고리즘과 암호화 장비의 개발·획득·검증·운용 기준을 4개 등급으로 구분·규정(CNSS 2010, 78-79)하였다.

또한, 미국의 암호화 장비/체계 업무를 수행하는 NSA는 앞선 CNSSI의 데이터 등급별 암호화 장비가 충족해야 할 세부 기준을 제시하면서, 빠르게 발전하는 민간의 공개/표준 암호 알고리즘 기술을 효과적으로 활용할 수 있는 CIS(Cryptographic Interoperability Strategy)를 추진해 왔으며, 이는 2022년 발표된 CNSA(Commercial National Se-

curity Algorithm) 2.0 계획으로 이어지고 있다(임재혁·최인수 2024, 4-6).

가령, CNSSI 4009의 규정에 따라 미국 국가 안보 관련 자료 중 비밀로 분류(Classified)된 민감(Sensitive)한 데이터는 국가(NSA)가 개발·검증·관리(Government Off-The-Shelf, GOTS)하는 비공개 암호 알고리즘이 적용된 암호화 장비(Type 1)를 통해서만 사이버공간에서 소통하도록 강제하지만, 국가 안보 관련 정보 중 SBU(Sensitive But Unclassified)는 NSA가 평가·인증·관리하는 Type 2 암호화 알고리즘과 장비로, 안보 이외의 미국 정부 업무와 관련된 SBU는 연방정부 표준인 FIPS(Federal Information Processing Standard)를 준용하면서 NIST가 승인한 Type 3 암호화 알고리즘과 장비로 소통하되, Type 2~4[6] 암호화 알고리즘과 장비는 민간에서 개발한 공개/표준 알고리즘(Commercial Off-The-Shelf, COTS)을 적극 활용하는 것이다.

중국 역시 매우 유사한 목표를 제시·추진하고 있다. 중국 당국이 지향하는 정보화와 이에 대한 보안 환경 구축의 지향점에 관해 시진핑 경제사상연구센터가 2023년 국가발전계획위원회에게 보고한 '새로운 시대 네트워크 보안의 발전 동향, 과제 및 대책(新时代网络安全的发展趋势、面临挑战与对策建议)'이라는 연구보고서에 따르면, 중국은 '정보화 전략의 전제조건인 사이버 보안의 완성을 위해 향후 선제적 보안 위험 분석 체계, 사이버공간에 대한 협력-통제 메커니즘, 지능형 통제 기술 및 유사시 긴급 대응 능력을 중점적으로 구축할 것'이며 기존의 패치, 부분-사후 수정 등의 사이버 보안 활동과 일정한 규모를 유지하는 방화벽 등 도메인 중심의 보안 아키텍처는 더 이상

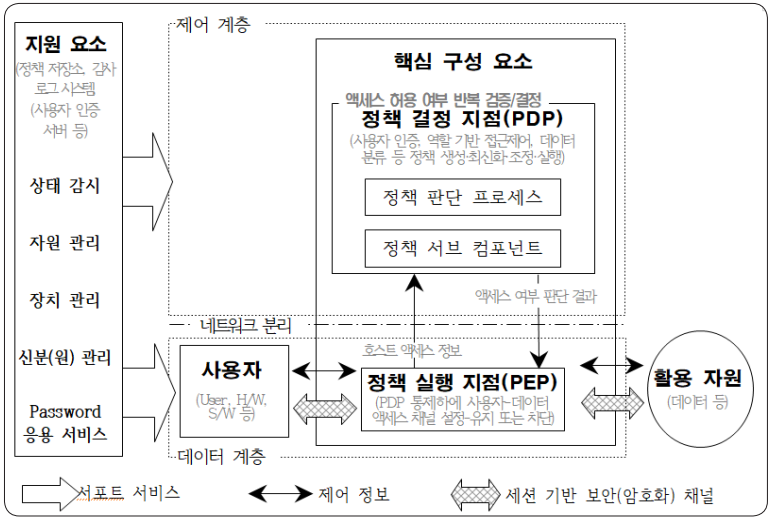
6) Type 4는 국가 기관의 인증을 받지 않는 순수 민간 및 상업 용도로 사용되는 암호화 제품이다.

신뢰할 수도 없고 미래 정보화 환경에 적합하지도 않기에, 활용성 증대 등의 세계적 추세를 반영한 새로운 보안 아키텍처 설계를 거쳐 사이버 안정성 확보에 필요한 기반 체계를 구축(国家信息中心 2023)하겠다고 밝혔다.

또한, 클라우드 컴퓨팅을 위해 특별히 설계된 AI 기반 보안 활동 등 다양한 환경에서 데이터를 모니터링하고 분석하는 하이브리드 사이버 보안 솔루션 및 데이터의 암호화-전송-저장 및 변조 문제를 개선하는 새로운 암호화 기술 등에, 과거와 같은 사후 관리가 아닌 사전 예측 및 처리라는 능동적 선제 감시-대응 메커니즘을 적용할 것이라고도 밝혔다.

이러한 ZTA 개념이 반영된 중국의 미래 사이버 보안 아키텍처의

〈그림 1〉 중국 학술 논문에 제시된 ZTA 구축 개념



출처: 中国国家标准化管理委员会(중국국가표준화관리위원회). 2022.『中华人民共和国国家标准 GB/T 42046-2021』. p 3.

지향점은 중국 국가표준화관리위원회가 2022년 ZTA의 개념, 요구사항, 설계 및 평가 등에 대한 국가 표준 규격으로 제시한 『中华人民共和国国家标准 GB/T 42046-2021(Information Security Technology - Zero Trust Architecture)』에도(〈그림 1〉) 잘 나타나며, 이는 미국 NIST가 이미 2020년에 제시한 ZTA 개념과 매우 흡사하다.

3) 미-중 양국의 PQC 구축 방향

미국은 2016년경 기존 주요 암호 알고리즘이 양자 컴퓨터 공격에 안전하지 않다는 사실을 인지한 이후 CNSA 2.0 계획에 따라 향후 10년 이내에 모든 비대칭 암호 시스템의 기반 알고리즘을 교체할 예정이다. 또한, 양자 컴퓨터의 암호 해독력에 체계적으로 대응하기 위해 2024년 8월 아래 〈표 1〉과 같이 첫 번째 PQC 표준을 독자적으로 공표했다.

〈표 1〉 美 NIST the first three PQC standards

FIPS Standard	Description	Derived From	Purpose
FIPS 203	**ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism) Standard	CRYSTALS-KYBER	Defines a cryptographic scheme that allows two parties to establish a shared secret key over a public channel.
FIPS 204	**ML-DSA** (Module-Lattice-Based Digital Signature Algorithm) Standard	CRYSTALS-Dilithium	Defines a digital signature scheme used to detect unauthorized data modifications and to authenticate the identity of the signer.

FIPS Standard	Description	Derived From	Purpose
FIPS 205	SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) Standard	SPHINCS+	Defines a stateless hash-based digital signature algorithm.

출처: 美 NIST 홈페이지 내용을 참고하여 저자가 작성

하지만, 아래 〈그림 2〉에서도 볼 수 있듯이, 중국[7]은, 미국의 PQC 알고리즘 표준을 따라가는 세계 대부분 국가와는 달리, 독자적인 표준을 채택하는 방향으로 PQC의 제도화를 진행하고 있는데 이는 향후 퀀텀 위협의 현실화에 독자적인 방향으로 대응하겠다는 의지의 천명이자, 향후 암호화-복호화 과정의 호환성 부족으로 인해 사이버공간이 미-중 양국 진영으로 구분될 수도 있다는 의미가 담겨 있다.

〈그림 2〉 세계 각국의 PQC 표준 채택 동향

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	CTPCO (2021)	Start planning; early implementation 2025-2026
Canada	NIST	Cyber Centre (2021)	Start planning; impl. from 2025
China	China Specific	CACR (2020)	Start Planning
European Commission	NIST	ENISA (2022)	Start planning and mitigation
France	NIST (but not restricted to)	ANSSI (2022)	Start planning; Transition from 2025
Germany	NIST (but not restricted to)	BSI (2022)	Start planning
Japan	Monitoring NIST	CRYPTREC	Start planning; initial timeline
New Zealand	NIST	NZISM (2022)	Start planning
Singapore	Monitoring NIST	MCI (2022)	No timeline available
South Korea	KpqC	MSIT (2022)	Start competition First round (Nov.'22-Nov.'23)
United Kingdom	NIST	NCSC (2020)	Start planning;
United States	NIST	NSA (2022)	Implementation 2023-2033

출처: GSMA Post Quantum Telco Network Impact Assessment Whitepaper. 2023.

7) 미국의 동맹·우방국인 대한민국은 독자적인 PQC 알고리즘 표준(KpqC)을 채택하고 있다.

Ⅳ. 새로운 사이버 보안 아키텍처의 방향; 보안성과 활용성의 배합

미래 퀀텀 위협과 이에 대비하기 위한 ZTA 구현의 전반에 미-중 전략경쟁의 메커니즘이 작용하고 있음을 볼 때, 이에 대한 독자적 대응 방향을 마련하여 조기에 적절히 실행하는 것은 미래 국익을 위해 매우 시급한 과제일 것이다.

특히, 이미 2023년 '캠프 데이비드 회담' 등을 통해 사이버공간에서의 협력 및 공동 대응을 약속한 동맹국 미국이 ZTA 등 안정적인 디지털 생태환경을 미국 정부 단독으로만이 아니라, 이른바 빅텍크 기업이라고 불리는 첨단 기술 보유 기업 및 우방·동맹국 정부와 함께 구축하는 기조를 유지하고 있기에, ZTA의 출발점인 ZT 개념을 기반으로 한 새로운 보안 아키텍처를 조기에 효율적으로 구축하는 것은 미-중 전략경쟁에서 이익을 주장·확보하는 데에도 유익할 것이다.

하지만 미-중 전략경쟁의 경쟁·갈등적 측면에만 집중할 수도 없다. 사이버공간은 경쟁·갈등의 영역이기도 하지만 인류 편익 증대를 위한 공존·협력이 필요한 곳이며, 이러한 사이버공간의 딜레마적 이슈는 보안성과 활용성이 배합된 새로운 보안 아키텍처를 요구하고 있다.

1. ZT 기반 다층적 보안 체계(MLS)와 PQC의 구축 방향과 과제

미국 NIST가 발행한 SP 800-207에는 ZTA 구축에 대한 7가지 필수적 기능이 제시되어 있으나 이를 두 가지로 요약한다면, 첫째 신뢰

성을 반복적으로 확인·검증할 수 있는 시스템 구축 둘째, 정보보호 활동을 데이터 자체에 집중하는 체계 마련으로 정리할 수 있으며 사이버공간상에 존재하는 데이터의 방대한 양(量)과 실시간 소통의 필요성 등을 고려한다면, 새로운 보안체계 구축 작업에는 보안성과 활용성이 동시에 고려되어야 한다.

특히 데이터 보호 활동 측면에서는, 미국의 CNSA 계획처럼, 모든 디지털 데이터를 국가(軍)가 개발한 비공개 암호화 알고리즘으로 완벽하게 보호하는 것보다 빠르게 발전하는 민간의 공개/표준 암호화 알고리즘을 활용하면서도 데이터의 정보 가치에 따라 적절히 보호될 수 있도록 구분하여 보안대책을 적용하는 것이 효과적이다. 사이버공간에 저장·유통되는 모든 정보에 국가가 개발한 암호 알고리즘·장비를 적용하여 보호한다면 막대한 비용이 소요되며 알고리즘 유지·보수·관리 등으로 인해 그 암호 알고리즘의 안정성을 장기간 유지하기도 어렵다. 그렇다고 모든 데이터에 민간의 공개/표준 암호화 알고리즘을 적용하는 것도 유출 시 국가 안보에 치명적 역할을 하는 민감정보의 보호 대책으로 적합하지 않다.

따라서, 사이버공간상에서 저장·유통되는 데이터에는 적절한 이용(활용성)과 보호(보안성)를 보장할 수 있는 ZT 기반의 보안 아키텍처가 필요하며, 이것이 바로 MLS 개념의 출발점이 되어야 한다.

ZT 기반 MLS 구현의 첫걸음은 퀀텀 위협에 대응할 수 있는 PQC의 의무적 사용을 조기에 제도화함으로써, 비록 현재는 디지털 암호체계로 암호화되어 보호될 수 있으나 향후 양자컴퓨팅 기술에 의해 언제든 복호화(유출)될 수 있는 데이터의 범주를 빠르게 감소시키는 것이다. 미국은 이미 2022년 말 연방정부 디지털 시스템에 PQC 적용을 강제하는 '양자컴퓨팅 사이버 보안 준비법(H.R.7535-Quantum

Computing Cybersecurity Preparedness Act)'을 발효하는 등 퀀텀 위협의 현실화에 대비하기 시작했다.

둘째, 사이버공간상 저장·유통되는 데이터의 보호 등급을 개별 가치와 활용 소요를 동시 고려한 분류 기준을 정립하는 것이다. 특히, 국방(무기) 부분에서는 무기체계의 속도와 파괴력, 그리고 회피 전술·기술이 하루가 다르게 발전하는 현실을 고려하여, 사이버공간상 유통되는 정보를 보안성 우선 분야와 신속성 우선 분야로 구분해야 한다.

가령, 북한이 우리를 향해 탄도미사일을 발사했을 때, 이를 요격해야 할 동맹·우방국 군대 간의 요격 정보 소통·결심에는 보안성보다는 신속성이 우선되어야 한다. 하지만 누구나 접근할 수 있는 비암호화(평문) 상태로 교환한다면, 동맹·우방국의 작전 패턴과 소통 채널이 노출됨으로써 향후 작전 성공률을 낮추고 역공격을 당하는 결정적 원인이 될 것이기에 보안성 또한 고려해야만 한다. 물론, 이러한 소통 체계를 별도의 망으로 구성할 수도 있지만, 탐지~지휘 결심~요격 등 민감 정보의 소통 과정은 사이버공간과 접점이 있을 수밖에 없고, ZT의 관점에서 망 중심의 보호 활동만으로는 데이터의 보안성 완벽하게 확보할 수 없다.

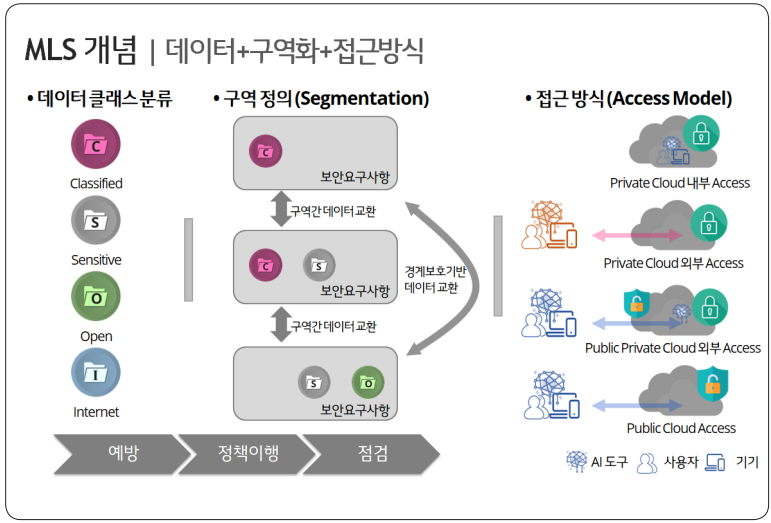
따라서, 국가의 사이버 보안 업무를 총괄하는 주무 기관을 중심으로 각 정부 기관이 참여한 가운데 데이터별 보안 측면의 가치 대비 신속한 소통 필요성, 대국민 활용성 등을 고려한 정부 보관·활용 데이터의 등급 분류 기준을 마련하고, 이를 각급 기관별로 적용할 수 있는 세부 기준으로 구체화하는 작업이 필요하다. 이것은 현재 정부에서 추진하는 '세계 최고 디지털 플랫폼 정부 구현' 기조에도 부합한다.

셋째, 각각의 보호 등급별로 구체적인 보호 대책 및 활용 방안을 정립하는 것이며, 이는 등급별 보호 영역(segment)을 제시된 보안정책에 따라 보호하되, 데이터의 활용 소요에 따라 등급별 구역 이동이 필요할 경우, 이와 관련된 체계·절차를 마련하는 것이다. 이때 각각의 등급별 데이터의 저장·소통에 적용할 암호화 알고리즘과 암호장비의 보안 수준과 인증 절차·정책 역시 정립되어야 한다.

특히, 보호 단위를 최소화해 유사시에도 파급력을 최소화하려는 ZTA의 개념을 적용하여 보호 영역을 세밀화(micro-segment)할 필요가 있으며, 정보보호 활동의 출발점인 세밀화된 보호 영역에서부터 저장 데이터를 보호할 수 있는 신뢰점(Root of Trust, RoT)을 구축해야 한다. 예를 들어, 해킹 포인트 중 하나인 반복적 암호키 주입(Key Injection) 대신 사람의 지문처럼 물리적으로 복제 불가능한 고유의 루트 키(Root Key)를 생성하고, 이 복제 불가능한 루트 키로 보호되는 안전한 저장소(Secure Storage)에 개인 키(Private Key)를 저장하는 PUF(Physically Unclonable Function) 기술[8] 적용 등 하드웨어 기반의 신뢰점(RoT)을 구현한다면 보안성과 활용성을 혁신적으로 높일 수 있다.

8) PUF 기반의 H/W RoT 기술은 대한민국의 ICTK(주)가 VIA PUF 기술을 통해 세계 최초로 양산했는데, ICTK의 PUF 기술은 수동소자를 사용하여 온도·습도 등의 환경 변화에도 PUF 값이 변하지 않고(신뢰성 보장), 침투(Invasive)-비침투(Non-Invasive) 공격에 대한 저항력(Tamper Resistance)까지 갖춘 것으로 평가받는다.

〈그림 3〉 MLS 구축 개념 구상도(데이터+구역화+접근방식)



출처: 저자 작성

위 〈그림 3〉은 향후 MLS의 구축 방향을 도시한 것으로, 그 중점은 각종 데이터의 개별 보호 가치에 따라 보호 등급을 다층화하고, 이에 따른 보안 측면의 준수 절차와 요구 사항을 별도로 정립하되 필요할 경우, 각 등급(구역)의 데이터가 호환(교환)될 수 있는 특정한 절차를 규정함으로써 활용성을 높이는 것이며, 각 등급의 데이터가 저장되는 공간과 접근(인증) 자격을 차별화해 보안성을 높이는 것이다.

한편, 대한민국은 양자컴퓨터 위협에 대응하기 위해 2035년까지 기존 사이버공간의 암호 알고리즘을 독자적인 PQC 알고리즘(KpqC)으로 전환할 계획이며, 수차례의 공모와 분석·평가를 통해 2023년 12월 차기 공모에 도전할 PQC 알고리즘이 선정하는 등 KpqC 제도화에 박차를 가하고 있다.

하지만, 미국의 동맹·우방국인 대한민국은 군사적인 상호운용성은

물론, 다양한 정보 유통망에서 미국의 동맹·우방국들과 호환성을 유지해야 한다는 점을 고려해야만 하며 최근 중국과의 전략경쟁 속에서 동맹·우방국과의 긴밀한 협력·연결을 중시하는 미국의 전략·정책 기조를 고려한다면, 향후 퀀텀 위협에 대응하는 과정에서 미국이 제시하는 기술 표준과의 호환성은 매우 중요한 고려 요소가 될 것이 분명하다.

따라서, 미국이 진행하고 있는 NIST PQC와 우리가 독자적으로 구축하려는 KpqC 모두를 충족하는 암호화 알고리즘을 계속 개발·적용함으로써 보다 높은 보안성을 추구할 것인지, 아니면 미국의 기준을 수용하는 것이 효율적인지를 깊이 있게 고민해야 한다.

2. 보안업무 환경의 개선·정비

그동안 보안 활동의 중심은 국가(軍)였다. 하지만, 사이버공간의 영역이 지속 확대되고 그곳에서 극단적으로 편익을 의존하는 대상이 일반인으로 확대되고 있는 상황에서 사이버공간에서의 보안 활동을 더 이상 국가(軍)에만 의존할 수 없다.

이제는 국가 기관뿐만이라, 일반인들에게 다양한 애플리케이션과 프로그램을 제공하는 민간 기업, 특히 다양한 보안체계를 제공하는 우수한 보안 기술 기업들도 적지 않은 만큼 이들의 선진 보안 기술을 적극적으로 활용할 필요가 있다. 특히, 미국 NSA의 CIS와 CNSA 2.0처럼, 빠르게 발전하는 민간 첨단 기술을 국가 차원의 새로운 보안 아키텍처인 ZTA 구현에 적극적으로 도입할 수 있는 체계를 마련해야 한다.

이러한 작업은 첫째, 그동안 국가 주도로 이뤄져 왔던 디지털 데이

터 보호 활동에 민간 기업이 참여할 수 있도록 암호 알고리즘·장비 개발·운용·정비 시장을 민간에 파격적으로 개방하는 등 국가(軍)의 암호 알고리즘 및 암호장비 획득 체계를 개선에서부터 시작될 수 있다.

엄격한 암호화 알고리즘과 암호장비 관리로 정평이 난 미국도 그동안 공개되지 않은 암호 기술과 장비만을 운용해 왔던 보안정책을 포기했다. 현재 미국 정부는 정보 소통에 관여된 모든 사용자·장치·체계가 디지털 네트워크화되고 있는 정보통신 환경을 고려하여, 자신들이 제시한 암호화 수준을 충족하는 국제표준 상용 암호 기술들을 소통 대상 정보의 보안도에 따라 등급별 디지털 정보 저장·소통에 차등적으로 적용·활용함으로써 디지털 데이터와 보안 활동의 활용성을 제고시키고 있다.

따라서, 우리 정부도 민간에서 개발된 암호화 알고리즘·장비가 정부의 제시 기준 충족 여부를 엄격히 검증·평가·승인하면서 민간에서 생산된 제품이 국가 단위의 새로운 보안 아키텍처에 확산·활용될 수 있도록 유도해야 한다. 이는 정부 보안 주무 부서가 국가 단위의 사이버 보안 정책에 집중할 수 있도록 과중한 업무 부담 경감과 사이버 보안 분야 핵심 기술력 확보를 동시에 모색할 수 있는 등 국가 차원의 사이버 보안 활동과 데이터 활용의 활용성을 혁신적으로 개선할 것이다.

특히, 이를 앞선 '디지털 정보별 보호 등급 구분 및 등급별 보호 기준 정립' 작업과 연동하여, 정부는 국가 사이버 보안 활동의 아키텍처 등 정책 구상 및 핵심적으로 보호해야 할 디지털 데이터에 대한 암호화 알고리즘·장비 개발·운용에 집중하고, 핵심 민감 정보 외 대다수 디지털 데이터에 적용할 암호화 알고리즘·장비 개발을 민간에 과감

히 위임할 때, 시너지 효과를 발휘할 수 있다.

둘째, 동맹·우방국과의 디지털 데이터의 상호운용성(interoperability)을 개선함으로써, 사이버공간의 업무 활용성을 높이는 것이다. 상호운용성이란 두 개 이상의 시스템 간 원활한 정보·서비스·데이터 교환을 통해 주어진 임무를 달성하는 데 시너지 효과를 창출(한창근 2015)하는 것을 말하며 현재 우방·동맹국 간, 특히 그 군대 간의 임무 수행 체계는 디지털 데이터를 주고받는 사이버 네트워크로 연동되어 있어 양자 또는 다자 간 시스템 사이에는 암호 장비·알고리즘 운용 단계가 불가피하게 연동되어야 한다.

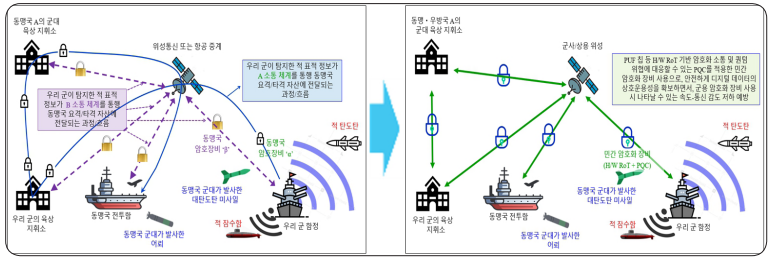
하지만, 우방·동맹국 군대가 공동의 목표 달성을 위해 디지털화된 정보·서비스·데이터를 소통하는 체계가 특정 국가 일방의 암호화 알고리즘 또는 체계를 이용해야 한다면, 그 국가의 독특하거나 엄격한 암호 알고리즘·장비 관리체계로 인해 상대국 군대는 시의적절한 정보 소통에 애로를 겪을 수밖에 없다.

가령, 특정 국가는 디지털 데이터의 상호운용성 확보를 위해 자신들이 직접 개발·생산한 암호장비를 별도의 예비 장비 없이 동맹·우방국에 대여하면서 자신들이 직접 정비·관리하도록 강제하는 한편, 운용 기준에 대한 사전 승인 절차를 엄격히 적용한다면, 그 우방·동맹국들은 장비 고장 및 성능 저하 등 장비의 고유 결함에 기인한 문제 발생 시 상호운용성을 보장할 수 없는 상황이 빈번하게 발생할 수밖에 없다. 실제로도 암호화 장비를 거쳐 디지털 데이터를 송수신하면 송신 속도 및 질의 감소가 불가피하며, 이는 보안도의 향상을 위해 보안 알고리즘 또는 장비의 성능을 높일수록 속도·질의 소실량은 커진다.

따라서, 미국 NSA가 CIS에 따라 민간 암호화 알고리즘·장비의 세

부 도입 기준을 정립한 후 이를 충족할 경우, 정부의 보안 데이터 소통에 활용할 수 있도록 한 CNSA 절차 등을 참고하여, 우방·동맹국 모두가 합의한 상업 암호화 알고리즘·장비 승인 기준을 정립한 후 이를 국가 안보를 위해 보안성보다 신속성이 우선되는 분야의 디지털 정보 상호운용성 확보를 위한 보조적 소통 채널(vice communication channel)에 적용할 필요가 있다.

〈그림 4〉 상업 암호화 기술 적용을 통한 동맹·우방국 군대 간 상호운용성 극대화 개념



출처: 저자 작성

특히, 우리만의 다층적 보안체계를 선제적으로 구축한 후 이를 위 〈그림 4〉처럼, 동맹·우방국 간의 사이버공간상 정보·서비스·데이터 상호운용성 확대·개선을 제안함으로써, 우리의 선제적 보안체계가 미래 사이버 보안의 새로운 기술표준으로 자리매김한다면, 다양한 토종 기술·제품의 부가가치는 물론, 추가적인 기대 이익도 창출할 수 있을 것이다.

Ⅳ. 결론

우리 대부분은 하루를 살면서 스마트폰과 PC 등의 장치로 연결된 사이버공간과 끊임없이 소통하며 정보를 주고받고 있다. 만약 사이버공간과의 접속이 강제로 끊길 경우, 정신·심리적 공황은 물론, 국가 기관이든 개별 기업이든 업무 프로세스 진행이 어렵거나 아예 중단될 가능성이 매우 크다.

인터넷의 개발로부터 시작된 이러한 디지털 대전환은 모바일과 클라우드 시대를 지나서 양자와 AI의 시대에 접어들었다. 이제는 기존의 편리성 도모와 강력한 보안을 통한 데이터 통제의 시대를 넘어 데이터의 활용성과 더불어 보안성을 새로운 각도로 보완해야 하며, 그동안 쌓아온 데이터가 거대언어모델(LLM)과 같은 AI 도구를 통해 상생적 편익을 증진할 수 있도록 데이터의 접근과 보안에 대한 새로운 모델을 만들어야 할 시점이다.

하지만, 현재 사이버공간에는 개인/단체의 이익 극대화를 위한 침해 행위 이외에도, 핵-미사일 개발 및 경제발전에 필요한 자금과 핵심 기술, 그리고 각국의 기밀 정보를 탈취하는 북한처럼, 정부 차원에서 사이버 공격을 장려하는 국가들도 있으며, 지금도 누군가는 사이버공간에서 이익 획득 또는 탈취를 위해 활동하거나 준비하는 등 현재와 미래의 핵심 이익 추구가 일상적인 사이버공간에는 현실 세계 전반에 영향을 미치는 미-중 전략경쟁 메커니즘을 비롯한 복잡한 갈등-협력의 동력이 작동하고 있기에, 우리는 사이버공간의 위협과 미래 불확실성에도 대비해야만 한다.

이 논문은, 인류 편익 증진을 위한 공존의 영역이자 심각한 편익 의존성에 기반한 안보의 최대 취약점 중 하나로써 갈등의 영역인 사이

버공간에서 미국과 중국이 미래 패권 경쟁에서의 유리한 위치를 점유하기 위해 벌이고 있는 창과 방패의 싸움에 주목하고 있으며, 그 대안을 모색하는 데 있어 상생적 가치를 높이기 위한 보안성과 활용성의 동시 극대화를 고려하고 있다.

특히, 앞선 창과 방패에 대응하여 우리의 국익 보호와 확보에 유리한 보안 아키텍처 구축 방향으로써, 양자컴퓨팅의 암호 해독 기능에 대응하기 위한 PQC 의무 사용 조기 제도화, 디지털 데이터의 보호 등급 분류 및 등급별 보호 대책 세부화와 디지털 데이터의 등급별 보호 단위 최소화(micro-segment), 디지털 데이터의 활용 소요에 따른 등급 간 데이터 이동·인증 절차 정립 등 보안성과 활용성의 동시 추구 방안, 최소 보호 단위에서부터 PUF 기술이 적용된 신뢰점(RoT) 구축, AI 기반 액세스 컨트롤 및 유사시 비상조치 기능 등이 포함된 ZT 기반 MLS 구축 방향을 제시했다. 또한, 민간 암호화 알고리즘·장비 기술 활용성 증대, 동맹·우방국과의 상호운용성 확보와 같은 사이버공간 업무 활용성 제고 등 사이버 보안 업무 환경 개선 필요성도 제안했다.

이러한 사이버공간의 안정성 확보를 위한 새로운 사이버 보안 아키텍처의 첫걸음은 오늘 당장 내딛지 않아도 되며, 그렇다고 내일 당장 사이버공간의 안정성이 붕괴하는 것도 아니다. 하지만, 미-중 전략 경쟁 속 우리의 안보 환경이 빠르게 변화하는 이때 '초고속 인터넷 선진국'이라는 과거 현실에 안주하여 새로운 방패를 굳건히 하지 않는다면, '삶은 개구리 증후군(boiled frog syndrome)'과 같은 비극은 부지불식간에 우리를 엄습할 것이다.

물론, 새로운 보안체계를 구축하는 데에는 엄청난 시간, 비용, 인력과 노력이 소요된다. 하지만, 백년지대계라도 하루빨리 준비하는 자

에게 미래의 주도권 확보 또는 안정적 번영의 기회가 조금 더 많이 주어지기에, ZT 기반 MLS 구축과 PQC의 조기 제도화와 같은 사이버공간의 미래 안정성 확보 노력은 우리만의 철옹성을 쌓아 올리기 위해 꼭 필요한 것이며, 미래 세대에 부끄럽지 않을 선택 또한 하루빨리 진행되어야 한다.

〈참고문헌〉

김상배. 2023. “플랫폼 지정학 시대의 중견국 전략: 한국의 디지털 플랫폼 전략이 주는 함의.”『국가전략』 제29권 4호.

김정호. 2023. “미-중 전략경쟁 시대 사이버공간의 역할.” 한국사이버안보학회 추계 학술대회 기술정책연구위원회 논문집. pp. 41-49.

서행아. 2016. “중국 13차 5개년 국가 과학기술혁신 계획 특징 및 시사점.” 한국과학기술기획평가원 Issue Paper 2016-20.

신경수, 신진. 2020. “국제사회와 사이버공간의 안보문제.”『국제 지역연구』 27권 3호. pp. 27-55.

오일석. 2022. “바이든 정부의 사이버안보 정책과 시사점.”『INSS 연구보고서』 2022-13.

오종혁. 2023. “‘디지털 중국’ 추진 전략의 주요 내용과 평가.” KIEP(대외경제정책연구원) 세계 경제 리포트 Vol. 6 No. 8.

유지영. 2020. “사이버안보 이슈의 글로벌 쟁점과 전략적 시사점.” STEPI Insight(과학기술정책연구원) 제262호.

이선재, 정선화, 조병선. 2023. “미중 기술패권 경쟁과 양자컴퓨팅 정책 동향.”『전자통신동향분석』 제38권 제4호. pp. 47-57.

이진용, 조원배, 장형진. 2022. “제로 트러스트 아키텍처 기반의 정보보호 관리체계 구축에 대한 연구.” 한국정보처리학회 학술대회논문집 29(2). pp. 210-212.

임재혁, 최인수. 2024. 미국의 암호 발전 동향과 시사점.『국방논단』 제1979호(24-6).

전가림. 2023. “미·중 전략경쟁 분석: 구조와 경쟁 그리고 대결.”『신아세아』 30(4). pp. 60-82.

정태진, 이광민. 2019. “사이버범죄 대응을 위한 부다페스트협약 가입과 국제공조 연구.”『경찰학논총』 제14권 제2호. pp. 65-84.

주재우. 2022. “미중전략경쟁 격화와 한국의 선택.” 주재우『계간 외교』 2022-01(140). pp. 34-49.

채재병, 김일기. 2020. "사이버안보 역량 강화를 위한 국제협력 방안." 『INSS 전략보고』 No. 96.

한중과학기술협력센터. 2021. "14차 5개년 계획 내 과기동향 분석." Issue Report vol. 3.

한창근. 2015. "무기체계 상호운용성의 효율적 확보방안." 『주간 국방논단』 제1587호 (15-40). p. 2.

Ahmed, Elshweikh,, Mattar, Ahmed., Hussein, Mohamed., Ashraf, Dina. 2022. "Literature Survey for Cybersecurity for Internet of Things (IoT)." pp. 1-5.

Allison G., Klyman, Kevin., Barbesino, Karina., Yen, Hugo. 2021. "Great tech rivalry: China vs the US." Belfer Center, Avoiding Great Power War Project.

Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press.

Castells, M. 1998. *The information age: Economy, society and culture*. Oxford, UK: Blackwell.

CNSS. 2010. CNSS Instruction No. 4009.

Dam D-T, Tran T-H, Hoang V-P, Pham C-K, Hoang T-T. "A Survey of Post-Quantum Cryptography: Start of a New Race." *Cryptography*. 2023; 7(3):40.

Denning, D. E. 1999. *Information warfare and security*. ACM Press.

Digital Watch. 2020. "Digital Watch newsletter - Issue 47 - February 2020." https://dig.watch/newsletter/february2020 (검색일: 2024.05.21.).

Diogenes, Yuri., Ozkaya, Erdal,. 2019. *Cybersecurity: Attack and Defense Strategies*. Packt Publishing.

Freas, R. L., Adair, H. F., Hammad, E. 2022. "An Engineering Process Framework for Cybersecurity Incident Response Assessment." IEEE Conference on Dependable and Secure Computing (DSC). Edinburgh,

United Kingdom. pp. 1-8.

Friedman, Allan., Singer, P. W. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Geers, Kenneth. 2009. *Cyberspace and the Changing Nature of Warfare.* Strategic Studies Institute (U.S. Army War College).

Golota, Lukasz. 2023. "The Role of 5G Technology in Superpower Rivalry between the United States and China: An Offensive Realist Approach." *Polish Political Science Yearbook* 52. pp. 173-190.

Hill. Jürgen. 2023. "데이터 트래픽, 2030년까지 연평균 25% 증가 : 노키아 트래픽 보고서." https://www.itworld.co.kr/news/314786#csidx3ae61755e4c2075a1030bfc80fc5045 (검색일: 2024.05.21.).

IBM. "양자컴퓨팅이란 무엇인가요?." https://www.ibm.com/kr-ko/topics/quantum- computing (검색일: 2024.5.17.).

Jaikaran, Chris. 2023. "Cybersecurity: Selected Cyberattacks, 2012-2022." Congressional Research Service.

Nye, Joseph S. 2011. "Power and National Security in Cyberspace." *America's Cyber Future: Security and Prosperity in the Information Age*. vol. 2 (Center for a New American Security, June 2011)

Khan, M. N., Rao, A., Camtepe S. 2021. "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey." *IEEE Internet of Things Journal*. vol. 8, no. 6, pp. 4132-4156.

Kim, Jeong-ho. 2023. "The ruling strategy of Kim Jong-Un and North Korea's last 10 years." *The Korean Journal of International Studies*. 21-1 pp. 113-142.

Leszczyna, Rafał. 2021. "Review of cybersecurity assessment methods: Applicability perspective." *Computers & Security*. Volume 108.

Moore, Sandra., Brown, Sheena. 2019. Bringing the Humanities to STEM. https://www.researchgate.net/publication/349441132_Bringing_

the_Humanities_to_STEM/citation/download (검색일: 2024.05.11.)

Patel, K. 2019. "A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication." 3rd International Conference on Trends in Electronics and Informatics (ICOEI). Tirunelveli, India. pp. 320-325.

Prasanna, Kumar., Prakash, Ashwini. 2023. "Machine Learning in Cybersecurity: A Comprehensive Survey of Data Breach Detection." Cyber-Attack Prevention and Fraud Detection.

QuSecure. 2024. "The Quantum Threat: SNDL - The Urgent Need for Quantum-Resilient Data Security." https://www.qusecure.com/store- now-decrypt-later-sndl/ (검색일: 2024.05.11.)

Rose, S., Borchert, O., Mitchell, S., Connelly, S. 2020. *Zero Trust Architecture*. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207 (검색일: 2024.05.21.).

Sayler, K. M. 2020. "Emerging military technologies: Background and issues for congress." Congressional Research Service.

Scott, H. S., Natarajan, S., Sezer, S. 2016. "A Survey of Security in Software Defined Networks." *IEEE Communications Surveys & Tutorials*. vol. 18, no. 1, pp. 623-654.

Sindiramutty, S. R. 2023. *Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence*. ArXiv abs/2401.00286.

Taherdoost, H. 2022. "Understanding Cybersecurity Frameworks and Information Security Standards-A Review and Comprehensive Overview." *Electronics* 1(14):2181.

The UN Cyber Groups. 2022. "UN GGE and OEWG 2019-2021." Digital Watch. https://dig.watch/processes/un-gge (검색일: 2024.05.17.).

The White House. 2023. *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (검색일: 2024.05.15.)

Timmers, P. 2024. “Sovereignty in the Digital Age.” *Introduction to Digital Humanism*. pp. 571–592.

Touré, I. Hamadoun, 2011. *The Quest for Cyber Peace: Cybersecurity and the International Digital Order*. International Telecommunication Union, Geneva.

Vasoya, Shweta., Bhavsar, Krishna., Patel, Nishtha. 2022. *A systematic literature review on Ransomware attacks*. 10.48550/ArXiv 2212.04063.

William, Hurst., Merabti, Madjid., Fergus, Paul. 2014. *A Survey of Critical Infrastructure Security*.

Zilincik, Samuel., 2023. Duyvesteyn Isabelle. “Strategic studies and cyber warfare.” *Journal of Strategic Studies* 46(4):1–22.

Zittrain, J. L. 2009. *Future of the Internet: And How to Stop It.* Yale University Press.

国家信息中心. 2023. “新时代网络安全的发展趋势、面临挑战与对策建议.” https://www. ndrc.gov.cn/wsdwhfz/202311/t20231129_1362347.html (검색일: 2024.05.21.).

单志广a. 2023. “智慧城市智能数据治理创新机制研究.”『人民论坛·学术前沿』. https:// www.ndrc.gov.cn/wsdwhfz/202311/t20231129_1362347.html (검색일: 2024.05.21.).

单志广b. 2023. “智能物联网系统自进化统一安全机制.『人民论坛·学术前沿』. https:// www.ndrc.gov.cn/wsdwhfz/202311/t20231129_1362347.html (검색일: 2024.05.21.).

信息网络安全公安部重点实验室. 2024. 零信任安全架构发展趋势. https://www.secrss. com/articles/63177 (검색일: 2024.05.21.).

中国国家标准化管理委员会. 2022.『中华人民共和国国家标准 GB/T 42046–2021』.

Building a Trust Foundation in Cyberspace amid the Era of Quantum Threats:

Focusing on US-China Strategic Competition and Cyberspace Stability

Jeong-ho Kim | Korea National Defence University
Bongho Kang. | ICTK Co., Ltd.

This paper is centered around two conflicting axes inherent in cyberspace. The first axis represents cyberspace as both a competitive arena for future hegemony amidst the US-China strategic rivalry and a space for coexistence aimed at enhancing human welfare. The second axis portrays cyberspace as a domain where security is essential for stable operations, yet availability is required for effective utilization of systems and data.

Diagnosing the development trends of a spear (quantum threats) and a shield (ZTA, PQC) technologies in cyberspace through these axes of 'competition↔coexistence' and 'security↔availability,' it is deemed crucial to swiftly advance a new security architecture to build an efficient and stable digital ecosystem.

Based on these findings, this paper proposes detailed security measures such as the mandatory use of PQC, establishing classification standards for the protection levels of digital information, and applying differentiated encryption algorithms based on these levels. It also highlights the need to minimize the units of cybersecurity activities (micro-segmentation) and shift the existing firewall-centric security policies to a data-centric approach. The paper presents the concept and direction for building a ZT-based MLS and PQC that simultaneously considers security and usability.

Keyword U.S-China Strategic Competition, Cyberspace, Competition- Coexistence, Security-Availability, Future Quantum Threats, Zero Trust, Multi-Level Security, Post-Quantum Cryptography

* I would like to extend my heartfelt gratitude to former U.S. Defense Attaché and Reserve Army Major General SeWoo Pyo, as well as ICTK Co., Ltd.'s CEO Justin J. Lee, for their invaluable guidance and mentorship throughout the research and writing of this paper.