Journal of the KNST

2024; Vol.7, No.3; pp.284-289

ISSN: 2635-4926 https://doi.org/10.31818/JKNST.2024.9.7.3.284

Check for updates

Received: 2024/08/30
Revised: 2024/09/06
Accepted: 2024/09/27
Published: 2024/09/30

*Corresponding Author:
Dae-Seon Choi
Tel: +82-2-820-0943
E-mail: sunchoi@ssu.ac.kr

Abstract

북한의 정찰위성이 주로 핵미사일 공격 목표를 설정하기 위한 목적으로 사용되는 반면, 우리 군의 정찰위성은 정찰 및 감시용으로 활용되고 있다. 이에 따라, 본 연구에서는 북한이 우리 군의 정찰 및 감시 기능을 저해하기 위해 위성 시스템을 공격할 가능성이 있는 시나리오를 분석하였다. 이러한 위협과 침해 사례에 대한 보안 대책으로 양자기술을 제안하며, 이를 통해 위성체계의 안전성을 강화할 수 있는 방안을 제시한다.

In this paper, North Korea's reconnaissance satellites are mainly used for the purpose of setting targets for nuclear missile attacks, while the ROK military's reconnaissance satellites are used for reconnaissance and surveillance. Accordingly, this study analyzes a possible scenario in which North Korea may attack a satellite system in order to undermine the reconnaissance and surveillance capabilities of the ROK military. Quantum technology is proposed as a security measure against such threats and infringements, and a way to strengthen the safety of satellite systems is proposed.

Keywords

인공위성(satellite), 보안(Security), 양자기술(Quantum Technology), 해킹(Hacking)

Acknowledgement

이 논문은 2024년도 한국해군과학기술학회 하계학술대회 발표 논문임

북한의 인공위성 공격에 대비한 양자기술 연구

Research on Quantum Technology in Preparation for North Korea's Satellite Attack

김승우[1], 최대선[2*]

[1]해병대사령부 전투모의분석센터 M&S발전담당 사무관/숭실대학교대학원 소프트웨어학과 박사과정
[2]숭실대학교 소프트웨어학과 교수

Seung-Woo Kim[1], Dae-Seon Choi[2*]

[1]M&S development manager, Battle Simulation & Analysis Center, ROK Marine Corps HQ/Ph.D. candidate, Dept. of Software Doctorate Program, Soongsil University
[2]Professor, Dept. of Software, Soongsil University

1. 서론

북한은 최근 군사정찰위성 '만리경-1호'의 우주궤도 진입에 성공했다고 주장했으며, 우리나라도 첫 번째 군사정찰위성을 성공적으로 발사함으로써 남북한 간의 위성 경쟁과 기술 축적이 본격화되고 있다. 북한의 조선중앙통신은 만리경-1호가 촬영한 미국 백악관과 국방부(펜타곤)의 사진을 확보했다고 주장하며, 버지니아주 노포크 해군기지를 촬영한 위성사진에서 미 해군의 핵항공모함 4척과 영국 항공모함 1척이 포착되었다고 보도했다. 그러나 북한은 이와 같은 군사정찰위성이 촬영했다는 위성사진을 공개하지 않았다.

한편, 우리나라는 미국 캘리포니아주 반덴버그 공군기지에서 군사정찰위성 1호기를 발사하였으며(Fig. 1 참조), 이 위성은 발사 후 성공적으로 우주궤도에 안착하고 해외 지상국과의 첫 교신을 성공적으로 수행하였다. 이러한 위성무기체계의 발전과 함께 위성 분야에서의 사이버보안 중요성이 점점 더 커지고 있으며, 중요한 정보와 데이터가 사이버공간에서 교환되는 상황이 증가하고 있다. 특히, 위성체계에서 유통되는 정보와 데이터는 사이버 공격자에게 큰 경제적 이익의 기회를 제공할 수 있으며, 국가적으로는 중요한 정보의 유출과 육·해·공 전투에 필요한 자원의 부재 등 국가 안보에 직결되는 사이버전 수행에 대한 주요 표적이 될 수 있다.

Fig. 1. ROK's military reconnaissance satellite no. 1

사이버전 기술은 공격과 방어 양측면에서 지속적으로 발전하고 있으며, 위성체계의 보안 대응 방안을 강화하는 것은 필수적이다. 이에 따라 위성체계의 사이버보안 능력을 제고하고, 이를 기술개발과 위성 운용에 반영하는 것이 필요하다. 본 연구에서는 위성체계에서의 보안 필요성과 잠재적인 위협, 그리고 실제 침해 사례를 논의하며, 이러한 위협에 대응하기 위한 보안 방안으로서 양자기술을 제시한다. 이는 위성 시스템의 안전성을 강화하고 국가 안보를 보장하기 위한 중요한 전략적 대책이 될 것이다.

2. 관련 기술

2.1 우리나라 최초 정찰위성

2023년 12월 2일, 국방부는 정찰위성 1호기가 해외 지상국과의 첫 교신을 통해 궤도에 성공적으로 안착했으며, 위성의 상태가 양호하다는 것을 확인했다고 발표했다. 이 정찰위성 1호기의 발사는 일론 머스크가 설립한 스페이스X의 '팰컨9(Falcon 9)' 로켓을 통해 이루어졌다.

우리 군의 군사정찰위성 1호기는 전자광학(EO)과 적외선(IR) 기능을 포함한 고해상도 카메라를 장착하고 있다. 이 정찰위성은 지상 표적의 감시와 정찰 임무를 수행하는 데 중요한 역할을 할 것으로 기대된다. 또한, 우리 군은 2025년까지 800 kg급 SAR(합성개구레이더) 위성 4기와 EO·IR 위성 1기를 추가로 발사할 계획이다. 이로써 우리나라의 군사정찰위성 체계는 더욱 강화될 것이며, 다양한 정찰 및 감시 임무를 수행할 수 있는 능력을 갖추게 될 것이다.

2.2 북한 만리경 1호 수준

북한은 위성 발사 직후부터 송·수신 능력을 대외적으로 과시하고 있으나, 미국 국방부는 북한이 대내 결속을 강화하기 위해 감시·정찰 능력을 과장했을 가능성을 제기했다. 미국 국방부는 북한의 성공 보도가 과장되었을 수 있으며, 설령 위성이 정상 궤도에 진입했다고 하더라도 정상적인 정찰 임무를 수행하려면 상당한 기간이 필요할 것으로 분석하고 있다.

북한은 옛 소련제 RD-250 트윈엔진 2세트를 모방하여 개발한 백두산 액체 엔진을 Fig. 2에서 볼 수 있듯이 발사체(천리마-1형) 1단 로켓으로 사용했다. 2·3단 로켓은 러시아 엔진 등을 토대로 북한이 자체 제작한 신형일 가능성이 있다. 북한의 만리경-1호가 목표 궤도인 저궤도(500 km 고도 태양동기궤도)에 진입하여 정상 작동할 경우, 하루 3~4회 한반도를 지나갈 것으로 예상된다. 그러나 이는 우리나라 지역의 특정 목표물을 하루에 3회 정도 관찰하는 것으로, 정찰 목표를 충분히 달성하기에는 한계가 있을 것이다.

북한이 다수의 군집위성을 궤도에 진입시킨다면, 핵미사일을 위한 정찰위성 역할이 본격화될 가능성이 있다. 특히 러시아 등으로부터 부품을 조달하고, 위성 카메라의 해상도를 향상시킨 뒤 지속적으로 정찰위성 발사를 시도할 것이다.

Fig. 2. Reconnaissance satellite 'Cheollima-1' launched from West Sea Satellite Launching Station in Cheolsan, North Pyongan Province, North Korea

한편, 북한이 위성 요격이나 랑데부 근접 작전을 수행할 역량이 부족하기 때문에, 위성에 대한 직접적인 물리적 공격을 추진할 가능성은 낮다고 평가된다. 그러나 북한의 GPS 재밍 능력과 우주 자산에 대한 공격 역량은 심각한 위협으로 인식되고 있다. 실제로 2016년 북한의 GPS 재밍 공격으로 인해 다수의 우리 민항기가 피해를 입은 사례가 있으며, 또한 북한은 인도의 달 탐사선 찬드라얀 2호 발사 중 인도우주연구소에 대한 사이버 공격을 감행한 바 있다.

2.3 남북한 정찰위성의 차이점

한국과 북한이 비슷한 시기에 각각 첫 정찰위성을 발사했으나, 두 나라의 정찰위성은 성능과 활용 목적에서 상당한 차이를 보인다. 북한의 정찰위성은 주로 핵미사일 공격 목표를 선정하기 위한 용도로 사용되며, 공격적인 목적을 띠고 있다. 반면, 한국의 정찰위성은 주로 북한의 군사 활동을 감시하고 정찰하는 데 활용될 것이다.

한국의 정찰위성은 대북 킬체인(Kill Chain)의 핵심 전력 중 하나로, 북한의 핵 개발 및 무기 배치 동향을 독자적으로 감시하고 정찰하는 데 주력할 것이다. 이 위성은 고도 400 km – 600 km의 저궤도에 위치하며, 전자광학(EO) 및 적외선(IR) 촬영 장비를 탑재하고 있다. 이를 통해 지상 30 cm 크기의 물체를 식별할 수 있는 수준의 고해상도를 제공한다.

국방부는 위성의 해상도와 EO·IR 동시 운영 능력을 고려할 때, 한국의 정찰위성 성능을 세계 5위 이내로 평가하고 있다. 이는 북한의 정찰위성에 비해 월등한 성능을 보유한 것으로 판단된다. 이러한 기술적 우위는 한국이 북한의 군사적 위협에 효과적으로 대응하고, 실시간으로 중요한 정보를 확보할 수 있는 능력을 강화시킬 것이다.

2.4 북한의 양자암호 연구

북한이 양자컴퓨터로도 풀 수 없는 차세대 암호기술을 연구 중이라는 사실이 확인되었다. 이 연구는 김일성종합대학이 발행한 학보 '수학' 2019년 제65권 제1호에 실린 논문(Fig. 3 참조)에서 밝혀졌으며, 미국 암호학자 다니엘 J. 번스타인의 연구를 기반으로 하고 있다.


김일성종합대학학보
수 학
주체108(2019)년
제65권 제1호

근사최대공약수문제에 기초한 한가지 공개열쇠암호체계

곽위성, 김철은

우리는 량자콤퓨터로도 풀수 없는 철단암호로서 안전성이 근사최대공약수문제의 계산복잡성에 기초한 한가지 공개열쇠암호체계를 연구하였다.

씨인수분해문제나 리산로그문제의 곤난성에 의거하고있는 RSA암호나 타원곡선암호들을 비롯한 공개열쇠암호들이 량자콤퓨터에 의한 단축공격법으로 쉽게 풀린다는데로부터 최근 안전성이 담보되는 새 세대 암호를 개발하기 위한 연구가 본격적으로 진행되고있다.[4]

현재 널리 연구되고있는 새 세대 암호들중 실용화의 측면에서 주목을 끌고있는것은 암복호화알고리듬이 단순한 옹근수모듈연산들로 정의되고 암호문들에서의 문자렬검색을 비롯한 다양한 연산을 안전하게 보장하는 공개열쇠암호체계이다.

이런 암호체계의 안전성은 근사최대공약수(AGCD)문제의 계산복잡성에 의거하고있다.

AGCD문제는 어떤 씨수 혹은 몇개의 씨수들의 적의 근사공배수가 여러개 주어졌을때 그것들의 공약수를 계산하는 문제로서 현재 오유동반학습(LWE)문제보다 더 어려운 문제로 알려져있다.

선행연구[1]에서 처음으로 제기된 AGCD문제에 의거하면서 옹근수연산으로 정의되는 공개열쇠암호체계는 1bit단위로 암, 복호화가 진행된다는 결함을 가지고있다.

선행연구[2, 3]에서는 AGCD변종문제(주어진 근사공배수들중에 근사값이 0인 수가 1개 끼워있는 경우의 AGCD문제)에 기초하여 한번에 여러bit들을 처리할수 있는 다중비트공개열쇠암호체계를 제기하였지만 안전성의 기초로 되는 AGCD변종문제의 계산복잡성이 AGCD문제보다 떨어지므로 량자콤퓨터에 의하여 비공개열쇠의 일부를 쉽게 알아낼수 있다는 약점을 가지고있다.

론문에서는 AGCD문제에 안전성의 기초를 두고있으면서 옹근수연산으로 정의되는 공개열쇠암호체계에 대한 선행연구들에서 나타난 결함들을 극복할수 있는 새로운 다중비트공개열쇠암호체계를 제기하였다.

Fig. 3. The paper "A Public Key Cryptosystem Based on the Approximate Greatest Common Divisor Problem," published in Mathematics, a journal of Kim Il Sung University

해당 논문은 기존의 RSA와 타원곡선 암호체계는 양자컴퓨터의 공격에 취약하다는 점을 지적하며, 안전성을 보장할 수 있는 새로운 공개열쇠암호체계의 필요성을 주목했다. 이 연구에서는 근사최대공약수(approximate greatest common divisor, AGCD) 문제의 계산 복잡성을 바탕으로 한 암호체계를 제안했으며, 이는 양자컴퓨터에 의한 공격에도 안전하다고 주장한다.

AGCD 문제는 현재 널리 연구되고 있는 오유동반학습(LWE) 문제보다 더 어려운 것으로 알려져 있으며, 이를 기반으로 한 새로운 다중 비트 공개열쇠암호체계가 기존 연구의 결함을 극복할 수 있다고 논문은 설명하고 있다.

3. 위성시스템의 취약점과 북한 공격 시나리오

3.1 위성통신 시스템의 취약점

위성 해킹은 실제로 발생할 수 있는 심각한 위협이며, 위성통신 시스템이 국방, 외교, 안보 분야에서 핵심 자산으로 자리 잡으면서 전 세계 여러 국가가 위성 전용 보안 정책과 기술을 개발하고 있다. Table 1에 제시된 바와 같이, 위성시스템에 대한 공격은 다양한 형태로 발생할 수 있다. 주파수 대역에 간섭신호를 방사하여 통신을 방해하는 주파수 재밍, 민감

한 데이터 도청, 비인가자의 위성 신호 도용, 데이터 불법 변경 또는 허위 데이터 전송, 탈취한 신호의 재전송 등이 그 예다.

실제로, 러시아 군용 통신위성 및 위성통신 업체 비아샛(Viasat)은 악성 소프트웨어를 이용한 해킹 공격을 받은 사례가 있다. 이러한 공격은 위성시스템의 취약점을 악용하여 민감한 정보를 유출하거나, 통신을 방해하며, 나아가 중요한 인프라에 피해를 줄 수 있는 가능성을 보여준다. 또한, 위성항법시스템을 탈취하여 테슬라의 레벨 2 자율주행 차량에 오동작을 유도하려는 시도도 있었다. 이는 위성시스템 해킹이 실제로 발생할 수 있는 위협이며, 특히 민간 및 군사 분야에서 그 파급력이 클 수 있음을 시사한다.

Table 1. Satellite communication features[7]

Item	Description
Feature	▪ Uses radio waves to transmit information ▪ Uses satellites located in space ▪ Long-distance communication in most cases
Merit	▪ Extensive area coverage ▪ Regardless of topography
Disadvantages	▪ Delay in reporting ▪ Security issues ▪ Interference issues ▪ High-cost ▪ Unstable data transfer speeds

3.2 북한의 위성 공격 유형 및 시나리오

북한은 위성통신 시스템을 대상으로 한 다양한 형태의 공격을 시도할 수 있으며, 이는 국가 안보에 직접적인 위협이 될 수 있다. 이러한 공격에는 Table 2에 제시된 바와 같이 신호 교란, 데이터 해킹, 서비스 거부 공격(DoS) 등이 포함될 수 있다. 예를 들어, 북한의 정찰총국이나 라자루스와 같은 조직들은 사이버전을 통해 타국의 통신 시스템에 침입하고, 이를 통해 정보를 유출하거나 군사적 목적으로 신호를 방해하는 활동을 수행할 수 있다. 특히 국가 간의 갈등 상황에서는 이러한 통신 시스템을 통한 정보 유출이나 군사적 목적을 위한 신호 방해가 더욱 빈번해질 가능성이 크다.

위성통신의 중단은 국가의 중요한 기반 시설과 서비스에 심각한 영향을 미칠 수 있으며, 이는 국가 안보를 심각하게 위협할 수 있다. 예를 들어, 군사 작전의 지휘 통제 시스템이 위성통신에 의존하는 경우 이러한 시스템에 대한 공격은 작전 수행에 치명적인 장애를 초래할 수 있다. 따라서, 위성통신 시스템의 보안 강화는 국가 안보를 보장하는 데 필수적이다.

이러한 위협에 대응하기 위해서는 탈린 매뉴얼과 같은 국제적인 사이버전 법률 및 규범을 참고하여 효과적인 대응 전략을 수립하고 실행하는 것이 중요하다. 탈린 매뉴얼은 사이버전에서의 법적 대응 기준을 제공하며, 위성통신 시스템에 대한 공격 등 국가 안보 위협에 대처하기 위한 중요한 지침이 될 수 있다.

따라서, 위성통신 시스템의 보안을 강화하기 위해서는 지속적인 보안 평가와 기술적 대응 전략의 개발 및 업데이트가 필요하다. 또한, 국제 협력을 통해 정보 공유와 공동 대응을 강화하는 것이 중요하다. 이러한 조치들은 위성통신 시스템에 대한 위협을 효과적으로 관리하고, 국가 안보를 보호하는 데 중요한 역할을 할 것이다.

Table 2. Types and scenarios of attacks by North Korea

Item	Description	Damage assessment
Signal jamming	Interference with communication signals in order to hinder normal operations	Interference with critical communications relevant to national security
Hacking	Unlawful access or manipulation of information	Increased security threats due to information breaches
DoS	Generation of a large amount of traffic in order to hinder services	Devastating impact on services and infrastructure
Information exposure	Leakage of sensitive information	Leakage of state secrets
Interruption of military signals	Disruption of signals from communication system in the midst of conflicts between countries	Reduced effectiveness in military operations and security threats

4. 양자기술 보안 대책

4.1 양자기술 미래전 게임체인저 기술

무기체계는 현재 더욱 정밀한 탐지 및 항법 기술,

인공지능 기반의 지능화, 그리고 초신뢰 통신 기술을 중심으로 발전하고 있다. 기존의 네트워크 중심 정밀타격(C4ISR+PGM) 작전 환경은 고전 물리 이론에 기초한 결정론적 정보 상태에 의존하고 있다. 이와 같은 환경에서는 정보가 결정된 상태에 도달하면 무기체계나 기반 환경에 대한 공격과 기만이 가능해진다. 예를 들어, 전자기파의 주파수 스펙트럼을 활용한 재밍 기술을 통해 특정 주파수 대역을 방해할 수 있으며, 항공기와 미사일의 정밀 항법을 방해하는 다양한 GPS 교란도 가능하다.

그러나 양자기술의 도입은 이러한 패러다임을 근본적으로 변화시킬 수 있다. 양자기술은 아인슈타인이 '유령 같은(spooky)' 현상이라 불렀던, 상태가 사전에 정해지지 않은 중첩과 얽힘 등 확률론적 양자역학에 기반을 두고 있어 예측이 매우 어렵다. 또한, 양자컴퓨팅의 병렬 연산 능력을 통해 초고속 연산이 가능해지며, 스텔스 기체처럼 전파로 탐지가 어려운 목표물도 탐지할 수 있는 잠재력을 가지고 있다. 이러한 기술적 발전은 기존의 무기체계와 작전 환경의 패러다임을 혁신적으로 변화시킬 수 있다.

4.2 양자통신 국방적용 분야

국방 분야에서 통신은 매우 높은 신뢰성을 요구하며, 적의 도청 및 감청으로부터 완벽한 보안을 보장해야 한다. 이러한 요구에 부응하기 위해, 양자통신 기술의 국방 분야 적용 가능성은 매우 다양하고 잠재력이 크다.

먼저, 양자 암호통신을 통해 안전한 양자 키 분배와 암호통신이 가능하다. 유선망을 기반으로 하는 양자 암호통신은 국방의 핵심 통신망인 국방 광대역 통신망이나 작전사-군단 이상급 제대 간의 중요 통신망에 적용될 수 있다. 이러한 기술을 통해 기존 통신망의 보안성을 획기적으로 향상시킬 수 있다.

또한, 자유 공간 양자 암호통신 기술은 지상 무인체계 간 또는 드론 간의 통신에서 암호화된 데이터를 안전하게 주고받는 데 활용될 수 있다. 이와 더불어, 양자 암호화 기술은 위성통신에서도 적용 가능하여, 미래 우리 군의 다양한 위성통신에 대한 보안을 강화할 수 있다.

얽힘 기반의 양자 네트워크는 미래 전술통신체계에서 기존의 무선통신을 대체하거나 보완하는 통신 수단으로 활용될 수 있다. 그러나 현재 이러한 기술은 개념적 연구 단계에 있으며, 실제 국방 분야에 적용하기 위해서는 향후 기술 개발 추세를 면밀히 분석하고, 실용화 가능성을 신중히 판단해야 한다.

따라서 양자통신 기술은 국방 통신의 보안을 혁신적으로 강화할 잠재력을 지니고 있지만, 실질적인 적용을 위해서는 추가적인 연구와 기술 성숙도가 필요하다.

4.3 양자컴퓨터 국방적용 분야

양자컴퓨터의 가장 강력한 장점은 병렬처리이다. 기존의 비트(bit) 기반 고전 컴퓨터가 $2n$가지 경우 중 하나의 연산만을 수행하는 데 비해, 양자컴퓨터는 모든 $2n$가지 경우를 동시에 계산할 수 있다. 이는 n의 값이 커질수록 양자컴퓨터의 컴퓨팅 능력이 지수적으로 증가함을 의미하며, n이 50을 넘어가면 특정 계산 분야에서 현재 존재하는 디지털 슈퍼컴퓨터를 능가하는 양자 우위를 가질 수 있다.

이러한 특징 때문에 양자컴퓨터는 국방 분야에서 고속 병렬처리를 통해 방대한 데이터를 신속하게 분석하고, 최적의 해답을 도출할 수 있는 경로 최적화 문제나 수학적 복잡성에 기반한 고전 암호분석 분야에 특히 유용하다. 또한, 양자컴퓨터는 양자 기반 기계학습 분야에서도 큰 잠재력을 가지고 있다.

양자 기반 기계학습 알고리즘에는 QCNN 모델과 하이브리드 모델 두 가지 주요 접근 방식이 있다. QCNN 모델은 기존의 기계학습 알고리즘을 완전히 양자 알고리즘으로 대체하는 것을 목표로 한다. 반면 하이브리드 모델은 특정 구간에서만 양자 알고리즘을 사용하는 방식이다.

양자 기반 기계학습 알고리즘은 고전적인 컴퓨팅 방식으로는 해결하기 어려운 문제를 빠르게 처리할 수 있으며, 국방을 비롯한 여러 분야에서 혁신적인 도구로 활용될 수 있다.

5. 결론

인공위성 보안 위협은 현재에도 실질적인 위험으로, 우리나라의 11개 인공위성이 다양한 용도로 활용되고 있으나 보안 체계가 완벽하지 않다. 위성통신 방해 및 마비는 국방 C4I 체계에 큰 영향을 미치

며, 군사 정보의 정확성과 안정성을 저해할 수 있다. 이를 해결하기 위해서는 위성 방해전파 방지 시스템(OCX) 개발과 같은 대응책이 필요하다.

양자통신기술(QKD)을 활용하면 인공위성의 사이버보안을 강화할 수 있으며, 외부 공격에 대한 높은 안정성을 제공한다. KT, SK텔레콤, LG유플러스 등 국내 기업들이 양자통신 기술과 양자 내성 암호를 연구 및 상용화하면서, 군사 정보 보안에 적용해 뛰어난 안정성과 기밀성을 보장할 수 있다. 우리 군은 이러한 기술적 발전을 통해 위성 보안에 대한 대비책을 마련하고, 정보 및 기술 우위를 확보하는 데 집중해야 한다.

참고문헌

[1] Hankyung.com, "South Korea's First Military Reconnaissance Satellite on Launch Pad," 2023. 12. 2. https://www.hankyung.com/article/2023120187011
[2] Hyeonseong Yoon, "SpaceX's Falcon 9 Ushers in the Era of Rocket Recycling, Loading with Spaceship Danuri," Newsis, 2022. 8. 5, https://www.newsis.com/view/?id=NISX20220804_0001968332
[3] Seol Lee, "Why 'Chonma' not 'Chollima' on the North Korean Projectile? ... Why was North Korea's Announcement Different?," News1, 2023. 6.16., https://www.news1.kr/articles/?5079353
[4] Richard Kim, "South Korea Launches Reconnaissance Satellite Too After North Korea... What are Differences Between North and South Korean Military Reconnaissance Satellites?", 2023. 12. 2., BBC News Korea, https://www.bbc.com/korean/67388919
[5] Hyeonho Lee, "Military 'Space War' Has Been Realized Already: ASAT Destructs and Neutralizes Enemy Satellites," Seoul Economic Daily, 2024. 5. 6., https://www.sedaily.com/NewsView/2D92ZPZ8J4
[6] Gwangha Park, "KRIT "Quantum Technology Changes Changes the Future Battlefield"," Information & Communication Daily, 2022. 9. 4., https://www.koit.co.kr/news/articleView.html?idxno=102383
[7] Jong Yeong Kim, "A Review on the Defense Application of Game-Changer Quantum Technology in the Future Battlefield," Defense & Technology Monthly, 2023. 6. 21., https://bemil.chosun.com/nbrd/bbs/view.html?b_bbs_id=10008&branch=&pn=1&num=358
[8] Davide Castelvecchi, "Quantum Network is Step Towards Ultrasecure Internet," 2021, Nature, 590, pp. 540-541, https://www.nature.com/articles/d41586-021-00420-5
[9] Google TensorFlow, "Quantum Convolutional Neural Network," https://www.tensorflow.org/quantum/tutorials/qcnn?hl=ko.