논문접수 2023.04.06 | ISSN 1738-6144 | Journal of The Korea Association of Defense Industry Studies Vol. 30, No. 1(2023)
논문확정 2023.04.24 | http://journal.kadis.or.kr/ | 한국방위산업학회지 제30권 제1호 | https://doi.org/10.52798/KADIS.2023.30.1.3

미국 사이버사령부의 임무와 역할 분석

Analysis of the mission and role of the USCYBERCOM

이용석*, 최정민**
Yongseok Lee*, Jeongmin Choi**

ABSTRACT

Established on May 21. 2010, the U.S. Cyber Command achieved its full operational capability(FOC) in 2018 and becomes the united combat command. USCYBERCOM uses 133 cyber missions teams to perform its mission. The cyber mission team is organized into a national mission team(13), a cyber protection team(68), a combat mission team(27), and a support team(25). And USCYBERCOM accepts the concept of 'Defence Forward' to carry out its mission. Forward defense is an effort to prevent enemy attacks in the early stages by physically deploying them abroad against enemy cyber activities and is an active way to cooperate with allies. Recently, the United States plans to add 14 "space operations teams" to its 133 cyber mission teams to support combatant commanders in space operations. Protecting the nation, the lives and property of its people in cyberspace is an important task for those in charge of national defense. This study analyzes the mission, role, and recent activities of USCYBERCOM, which is responsible for the cyber domain of national defense, to contribute to improving our nation's cyber warfare capabilities.

초 록

2010년 5월 21일에 창설된 미 사이버사령부(USCYBERCOM)는 2018년 완전작전능력(FOC)을 달성하고 통합전투사령부가 되었다. USCYBERCOM은 133개의 사이버 임무 팀을 활용하여 임무를 수행한다. 사이버 임무 팀은 국가임무팀(13), 사이버보호팀(68), 전투임무팀(27), 지원팀(25)으로 편성되고, 임무 수행을 위하여 '전진 방어(Defence Forward)'개념을 도입하고 있다. 전진 방어란 적의 사이버 활동에 대항하여 물리적으로 해외에 배치하는 것으로 초기 단계에 적의 공격을 방해하기 위한 노력이며 동맹국과 협력하기 위한 적극적인 방법이다. 최근 미국은 133개 사이버 임무 팀에 우주작전에서 전투지휘관을 지원하고자 '우주작전팀' 14개를 추가할 계획이다. 새로운 영토인 사이버공간에서 국가와 국민의 생명과 재산을 보호하는 것은 국방을 담당하는 이들에게는 중요한 임무이다. 본 연구는 국방상의 사이버 영역을 책임지는 USCYBERCOM의 임무와 역할, 최근 주요 활동 등을 분석하여 우리나라의 사이버전 대응력을 향상시키는데 기여하고자 한다.

Key Words : USCYBERCOM(미 사이버사령부), National Mission Team(국가임무팀), Cyber Warfare(사이버전), Space Operations Team(우주작전팀)

* 이용석, 국방부(주저자, E -mail: lyskms@korea.ac.kr)
** 최정민, 국회입법조사처(공동저자)

Ⅰ. 서 론

사이버공간은 물리적 행동에 수반되는 물리적 장애와 자원에 대한 우려 없이 목표에 대해 행동할 수 있는 사실상 제약이 없는 영역이다. 사이버공간을 전장 지역으로 하는 사이버군은 키(key) 입력만으로 언제 어디서나 공격할 수 있는 능력을 갖추고 있다.[1] 또 병력을 특정 연령, 신체조건으로 제한할 필요가 없다. 값비싼 부대 건물과 시설, 연료에 대한 접근, 광활한 훈련지역, 광범위한 탄약 비축이나 보장이 필요 없다.

2022년 러시아-우크라이나 전쟁 등 글로벌 안보환경의 불안정성 심화, 북한의 핵·미사일 역량 강화 등의 군사적 위협에 신속히 대응하기 위한 군사적 역량 확보 필요성이 높아지고 있다.[2] 앞으로의 전쟁은 러시아-우크라이나 전쟁에서처럼 사이버전이 물리적 전쟁 전에 수행될 것이며, 사이버전으로 시작해서 사이버전으로 끝나는 상황이 될 것이다.[3]

한편 사이버공간은 사이버 범죄(국가)자로 인한 금전적 피해는 날이 갈수록 증가하고 있다. 2022년에 북한은 16억 5천만 달러를 암호화폐 해킹으로 탈취했다. 이는 2022년 전 세계 암호화폐 탈취금액 총 38억 달러의 43%가 넘는 금액이며 2021년보다 4배 증가한 것이다. 북한의 2020년 총 수출액이 1억 4,200만 달러인 것을 감안한다면 11배가 넘는 금액이다.[4] 대부분의 북한 전문가들은 해킹으로 획득한 자금이 북한의 핵무기 및 미사일 개발 프로그램에 사용된다는 의견에 동의한다.[5]

사이버공간에서의 군은 군대와 작전에 대한 글로벌 지휘 및 통제를 가능하게 하며, 현대 물리적 군사작전에서는 불가능한 전 세계적으로 분산된 물류 시스템에 대한 접근도 가능하게 한다. 정보 커뮤니티와 지휘관 및 전투원 등은 중단 없는 정보 흐름의 이점을 모두 누릴 수 있지만, 정보는 보안을 유지하기가 점점 더 어려워졌고 훔치기는 더 쉽고 간편해졌다.

사이버는 적군과 그 능력을 표적으로 삼는다는 측면에서 다른 군사작전과 유사하다. 사이버 도구는 명령 및 제어 노드와 그룹의 배포능력을 교란하는 기존 작전의 형태로 사용될 수 있다. 사이버 작전은 표적 제거를 위해 사용되며 특수작전과 같이 은밀한 방식으로 사용된다. 재래식 작전에서의 사이버 작전은 적보다 우위를 점하는 데 사용된다. 이를 위해 사이버는 아군이 사이버공간에서 방해받지 않도록 작전하며, 적의 작전능력을 방해함으로써 아군과 지휘관을 지원한다. 사이버는 세계 어느 곳에서나 공격을 시작하고 매우 빠르게 공격할 수 있다.[6]

미국은 이러한 국방상의 사이버 영역을 책임지는 사이버 공격 대응 조직을 설치, 발전을 거듭하여 2010년에는 사이버사령부를 창설하였고 최근에는 우주전 대응을 위해 또 다른 변화를 시도하고 있다. 그러나 미 사이버사령부의 임무나 역할 등에 대한 연구는 거의 찾기 어려웠다. 따라서 본 연구는 미 사이버사령부 임무 및 최근 동향 등을 면밀히 분석하여 우리나라 사이버 공격 대응과 우주작전 능력 향상 등을 위한 참고자료로 활용되는데 기여하고자 한다.

Ⅱ. 미 사이버사령부의 임무와 역할

2.1. 미국의 사이버 업무 관련 조직[7]

미국에서 사이버 업무를 전담하는 정부 조직은 국토안보부(DHS), 법무부(DOJ), 국방부(DoD)다. 첫째, 국토안보부는 사이버 침해사고에 대한 국가적 보호, 예방 및 완화와 복구를 조정하며 국내 사이버 위협의 중요한 보호와 취약성 분석을 전파한다. 둘째, 법무부(DOJ, 구체적으로는 FBI)는

1) 미래전 양상은 전장영역이 지·해·공에서 우주·사이버 공간으로 확장되고, 첨단과학 기술의 발전과 함께 무기체계의 혁신적인 기반 체계로 변화로 전쟁 본질의 변화를 가져올 것이다.〈장상국, "미래전을 대비하는 차기자주포의 화력강화방안". 『한국방위산업학회지』 제29권 제3호, 2022.〉

2) 장원준·송재필, "디지털 전환시대에 걸맞은 한국형 신속획득 프로세스 정립방안 연구". 『한국방위산업학회지』 제29권 제3호, 2022.

3) 박동휘, 『사이버전의 모든 것』, 플래닛미디어, 2022.

4) 『nbcnews』 "Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups", 2023.2.2. https://www.nbcnews.com/tech/crypto/crypto-hacks-stole-record-38-billion-2022-led-north-korea-groups-rcna68602(검색일: 2023.2.14.)

5) 『The Korea times』, "Ranking US official visits South Korea to discuss cyber security: NSC," 2022.7.29.

6) James Di Pane, *Cyber Warfare and U.S. Cyber Command in 2023 Index of U.S. Military Strength,* Washington: The Heritage Foundation, 2022.

7) G. Alexander Crowther, *National Defense and the Cyber Domain, in 2018 Index of U.S. Military Strength, ed. Dakota L. Wood,* Washington: The Heritage Foundation, 2017.

사이버 범죄를 조사하고 속성을 지정하며 기소를 통해 국내 국가 안보 활동을 주도한다. 사이버 위협정보의 국내 수집과 분석 및 배포에 관여한다. 사이버 침해에 대한 국가적 보호, 예방 및 완화와 복구를 조정하는 국토안보부의 업무를 지원하기 위해 사이버 위협조사를 조정한다. 셋째, 국방부(DoD)는 사이버공간에서 국가 행동의 자유를 보장하며 사이버공간에 대한 의존도가 높아짐에 따른 국가 안보에 대한 위험을 완화하는 활동을 한다.

국방 사이버 영역에서 미 사이버사령부(USCYBERCOM)는 네 가지 분야에 대한 활동에 책임을 진다. 첫째, 비밀을 탈취하고 출처를 개발하는 정보활동이다. 둘째, 피·아 활동에 대한 데이터를 획득하는 첩보 활동이다. 셋째, 사이버보안과 중요 인프라 보호, 법 집행과 대응, 문서와 미디어 착취, 대테러 활동을 수행한다. 넷째, 인지 형성(Shaping cognition) 분야로 사이버 감시정찰, 여건조성작전, 사이버 방어작전, 사이버 공격작전 등의 네 가지 작전으로 구분된다. 구체적으로 데이터수집을 위한 '사이버 감시정찰(CSR : Cyber Surveillance Reconnaissance)', 'Backdoor' 설치 등 후속 활동을 위해 환경을 구체적으로 준비하는 '여건조성작전(OPE: Operational Preparation of the Environment)', 사이버 작전 활동의 대다수를 구성하는 '사이버 방어작전(DCO: Defensive cyber operations)', 목적달성을 위한 수단 및 VIP와 전장 지휘관에게 추가 기능을 제공하는 도구인 '사이버 공격작전(OCO: Offensive Cyber Operations)'이다.

2.2. 미 사이버사령부 창설 이전의 사이버 공격 대응 조직

미국은 사이버사령부가 창설되기 전인 1997년 6월 9일~13일에 ELIGIBLE RECEIVER 97 훈련[8]을 수행하였다. 해당 훈련에는 국가(정보)기관(NSA, CIA, DIA, FBI, NRO, DISA, DOS, DOJ)과 민간 통신회사도 참여하였으며, NSA가 레드팀으로서 사전에 계획된 사이버 공격 임무를 담당하였다. 이 훈련을 통해 NSA(National Security Agency: 국가안보국)는 다양한 사이버 침해 활동에 대한 시나리오[9]를 점검하였고, 결과적으로 국가적인 사이버 취약성에 대응할 방안을 모색하게 되었다.

국방부는 곧 정보체계보안을 위한 작전 접근방식을 개발하여 1998년 DISA (Defense Information Systems Agency)와 함께 운영되는 'JTF-CND(Joint Task Force-Computer Network Defense: 컴퓨터 네트워크 방어 합동임무부대)'를 창설했다.

JTF-CND는 1999년 말에 미 우주사령부(USSPACECOM) 예하의 '컴퓨터 네트워크 작전 합동임무부대(JTF-CNO)'로 발전했으며, 2002년 10월 USSPACECOM 해체 후에는 JTF-CNO가 미 전략사령부(USSTRATCOM)로 통합되었다.

미 합참은 2004년 국가급 군사전략에서 사이버공간을 육지, 바다, 공중 및 우주 영역과 함께 분쟁의 "영역"으로 선언했으며 국방부는 이 새로운 영역에서 적 행위자를 방어하고 교전할 수 있는 능력을 유지해야 한다고 언급했다. 같은 해 도널드 럼스펠드(Donald Rumsfeld) 국방장관은 JTF-CNO를 방어 및 공격팀으로 나누었으며, 공격적인 사이버공간 작전을 위한 'JFCC-NW (Joint Functional Component Command-Network Warfare: 합동기능구성군사-네트워크전)팀'으로 발전시켰다.

2.3. 미 사이버사령부 창설 및 통합전투사령부로 승격

2009년 6월까지 미 전략사령부에서 테스크포스로 임무를 수행하던 JFCC-NW와 'JTF-GNO(Joint Task Force-Global Network Operations: 합동임무부대-범세계 네트워크 작전)'는 당시 국방부 장관인 로버트 게이츠(Robert Gates)의 메모를 통해 'DoD 사이버 부대'로 재편성[10]되었다가 2010년 5월 21일 '미 사이버사령부(USCYBERCOM)'로 창설되었다.

8) "Eligible Receiver 97", https://en.m.wikipedia.org/wiki/Eligible_Receiver_97(검색일: 2023. 2.16)

9) NSA는 모의 사이버 공격, 인질극, 특별습격작전 등과 기반시설 침해, 군 지휘통제권 확보 시도, 미군 네트워크 거부 및 DDoS 공격, 이메일 조작 및 변경, 피싱, 통신 방해 활동 등을 하였다. 이 같은 사이버 중심훈련에서 네트워크 취약성이 입증되고 악용과 관련된 잠재적 위험이 강조되면서 침해사고에 대한 우려가 극적으로 증가했다.

10) 미 육군 문장학 연구소가 2010년에 제작한 USCYBERCOM의 문장에는 USCYBERCOM에 속한 두 조직인 JFCC-NW와 JTF-GNO를 기리며 사이버공간 작전을 통합, 동기화 및 수행하기 위한 임무를 표현했다. 〈U.S. Cyber Command homepage, https://www.cybercom.mil/About/History/ (검색일: 2023.2.20.)〉

당시 국가안보국(NSA) 국장이었던 크리스 알렉산더(Krith Alexander) 육군 대장이 초대 USCYBERCOM의 사령관이 되면서 두 직책을 겸직한 전통이 현재까지 이어지고 있다. 정보와 작전에서 핵심적인 두 기관의 수장을 겸직하는 것에 대해서는 폴 나카소네(Paul M. Nakasone)[11] 사령관이 2022년 상원 군사위원회에서 다음과 같이 증언하였다.[12] 그는 '사이버사령부와 NSA의 연계가 사이버, 정보, 작전 모든 분야에서 국가를 위한 중요한 결과를 달성하는데 필수적이며, 이중상하명령관계는 계획, 자원할당, 위험 완화, 노력의 통합을 향상시키고 속도와 민첩성 및 임무 효율성을 유지하면서 작전할 수 있으므로 적의 정교함, 공격성, 작전 범위가 증가함에 따른 적의 전략적 과제를 해결하는데 매우 중요하다.'고 말했다.

USCYBERCOM은 2010년 5월 21일 창설과 동시에 '기본운용능력(IOC : Initial Operating Capability)'을 확보한 것으로 평가되었다. 2018년 2월 15일에는 "사이버공간에서 더 효과적으로 작전하기 위해 필요한 기본구성원칙은 무엇인가?"를 주제로 국방대학교에서 제1회 사이버공간 전략 심포지엄[13]을 개최하여 최종적으로 사이버공간 작전에 직면한 과제를 점검·보완하였으며, 2018년 5월 4일 '완전작전능력(FOC: Full Operational Capability)'을 달성[14]하였고 '통합전투사령부'[15]로 승격되었다.

통합전투사령부는 국방장관 직속으로 예하에 육·해·공·해병·특수전 구성군사령부를 가지는 합동군으로 최상위 군령권 부대이며 사령관에는 대장이 보임된다. 미군의 핵심인 11개의 통합전투사령부는 지역별로 7개(아프리카, 중부, 유럽, 북부, 인도-태평양, 남부, 우주), 기능별로 4개(특수전, 전략, 수송, 사이버)의 사령부가 편제되어 있으며 사이버사령부는 기능별 구분에 속한다. 통합전투사령부는 외부의 지원 없이 국가가 국방부를 통해 명령한 임무를 수행할 수 있는 능력을 갖추고 있다.

2.4. 미 사이버사령부의 편성[16]

USCYBERCOM의 완전작전능력을 갖춘 사이버임무팀(Cyber Mission Force)은 2018년 총 133개이며 현역, 주(洲) 방위군, 예비군을 포함한 6,200여 명으로 구성되어 있다.[17]

133개의 사이버 임무 부대는 USCYBERCOM의 행동부대이며, 국가의 이익을 수호하기 위해 사이버공간 작전을 지휘하고 동기화 및 조정하는 임무를 수행한다. USCYBERCOM 예하에 4개 분야로 구비 된 사이버 임무 부대는 각자의 특정 임무를 통해 이를 지원한다.

이들 조직의 역할을 구체적으로 살펴보면 첫째, 13개의 국가임무팀은 사이버 공격으로부터 미국과 그 이익을 보호하는 것으로, 적의 활동을 식별하고 공격을 차단하며 적군을 물리치기 위한 기동을 통해 국가를 방어한다. 둘째, 68개의 사이버보호팀은 빠르게 진화하는 위협기술에 대한 국방부 네트워크 및 시스템을 방어하는 것으로, 국방부(DoD) 정보망을 방어하고 우선순위 임무를 보호하며 전투를 위한 사이버 부대를 준비한다. 셋째, 27개의 전투임무팀은 작전계획 및 비상 작전을 지원하는 통합 사이버공간 효과를 생성하여 전투사령부를 지원하는 것으로, 전투사령관의 우선순위와 임무를 지원하기 위해 군사 사이버공간 작전을 수행한다. 넷째, 25개의 지원팀은 국가 임무 및 전투임무팀에 분석 및 계획지원을 제공하는 것이다.

전투사령관은 국방장관의 지시에 따라 전투사령부에 배치 및 지원을 위한 사이버 작전능력을 제공한다.[18] 이에 따라

11) 2018년부터 사이버사령관과 NSA 국장을 겸직하고 있다.

12) Paul M. Nakasone, Commander, United States Cyber Command, posture statement before the Committee on Armed Services, U.S. Senate, 2022.https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf(검색일: 2022.12.20.)

13) USCYBERCOM, 2018 Cyberspace Strategy Symposium Proceedings, 2018.

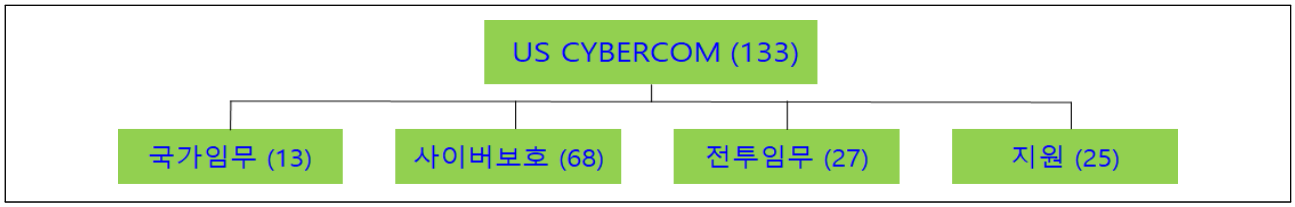
14) U.S. Department of Defense, "Cyber Mission Force Achieves Full Operational Capability," News release, 2018.3.17, 이는 국가 사이버부대가 사이버공간에서 국가를 방어할 수 있도록 완전히 훈련되고 장비되도록 보장하려는 군 서비스의 약속이다.

15) 미국에만 있는 편제개념이다. 국방장관 직속의 최고위급 부대로 통합사령관 지휘하에 군 본연의 전략, 전술 운용이 이루어진다.

16) G. Alexander Crowther, *National Defense and the Cyber Domain, in 2018 Index of U.S. Military Strength, ed. Dakota L. Wood,* Washington: The Heritage Foundation, 2017.https://www.heritage.org/sites/default/files/2017-10/2018_IndexOfUSMilitaryStrength-2.pdf.(검색일: 2022.12.15.)

17) 사이버 기술은 군이 가장 우위를 점한 분야가 아니므로 세계적으로 산·학·연·군·관·민이 통합된 사이버군을 창설하는 것이 기본이다. 〈이용석, "독일 연방 사이버군 창설 계획과 한국군 적용 방향". 『국방정책연구』 제133호, 2017.〉

18) U.S. Department of Defense, Joint Chiefs of Staff, 『Cyberspace Operations』, p. ix.



〈그림 2-1〉 2018년 이후 USCYBERCOM 조직도

출처: G. Alexander Crowther, 2017을 근거로 저자가 작성

USCYBERCOM은 4개 군이 사이버 임무 부대를 지원한다. 육군 사이버사령부(ARCYBER)는 사이버 임무 부대에 41개 팀을 지원한다. 해군 사이버사령부(FLTCYBER)는 40개 팀을 지원한다. 공군 사이버사령부(AFCYBER)는 39개 팀을 지원한다. 해병대 사이버사령부(MARFORCYBER)는 13개 팀을 지원한다.

합동 전략 및 교리 외에도 각 군은 사이버 문제를 처리하기 위한 자체 교리를 가지고 있다. 지상군의 사이버 방어는 해군 및 공군처럼 플랫폼을 보호하는 것과는 다르다. 육군은 지상 부대를 보호해야 하고, 해군은 전 세계 해상에서 운용되는 함선 그룹을 보호해야 하며, 공군은 개별 비행체를 보호해야 한다. 동시에 각 군은 자체 인프라를 보호하기 위해 공격 및 방어를 의미하는 전체 스펙트럼 사이버 작전을 수행한다. 사이버 훈련 및 교육에 대한 사이버연구와 역량 개발도 필수적으로 수행해야 한다.

그래서 폴 나카소네(Paul M. Nakasone) 사이버사령관이 제시하는 USCYBERCOM의 가장 중요한 목표[19]는 JCWA(Joint Cyber Warfighting Architecture: 합동 사이버전 아키텍처)를 통해 연결된 광범위한 파트너십과 세계적 수준의 인재를 확보하여 국가를 방어하기 위해 옵션을 제공하며 작전을 수행할 준비가 되어 있고 능력이 있는 사령부를 구축하는 것이다.

2.5. 미 사이버사령부의 주요 임무

폴 나카소네(Paul M. Nakasone) 사령관이 2022년 4월에 제117차 상원 군사위원회에서 밝힌 USCYBERCOM의 임무[20]는 '국내 관계기관과 협력[21]하여 국가 이익을 수호하고 발전시키기 위한 글로벌 사이버 작전, 활동 및 임무를 계획하고 실행하는 것'이다.

USCYBERCOM은 공격 및 방어작전에서 국방부 네트워크 모니터링과 주요기반시설 방어를 지원하기 위해 첫째, 국방부 중요 인프라와 DODIN(Department of Defense Information Network: 국방부 정보망)의 보안, 운영, 방어 지시 및 국방부의 임무보증을 제공한다. 둘째, 미국과 미국의 국익에 대한 전략적 위협 억지와 격퇴를 지원한다. 셋째, 사이버공간에서 사이버공간을 통한 전투지휘관의 목표달성을 지원한다.

USCYBERCOM 임무의 핵심은 '전진 방어(Defence Forward)'개념이다. 전진 방어란 합동군 임무를 위협할 수 있는 적의 사이버 활동에 대항하여 민감한 국방 정보유출을 방지하기 위해 민간부문 특히 동맹국과 협력하고, 네트워크 손상 전에 네트워크 내에서 초기 단계에 적의 공격을 방해하기 위해 노력하며, 동맹국의 사이버 부대와 협력하기 위한 팀을 해외에 물리적으로 배치하는 것을 말한다.

한편 사이버 공격자들은 경제를 표적으로 삼고 있다. DIB(Defense Industrial Base) 회사는 사이버공간의 최전선에 있으며 악의적인 사이버 행위자들의 표적이 되고 있다. USCYBERCOM은 자발적인 정보 공유를 통해 민간 산업과의 관계를 심화해가고 있다. 미국에서 국가 중요기반시설과 시스

19) Paul M. Nakasone, Commander, United States Cyber Command, posture statement before the Committee on Armed Services, U.S. Senate, 2022.4.5.

20) General Paul M. Nakasone, Commander, 2022.4.5.

21) Paul M. Nakasone 사이버사령관은 기관 간 파트너십을 매우 중요시한다. 특히 'FBI(Federal Bureau of Investigation)와 국토안보부의 사이버보안 및 기반시설 보안국(CISA)과의 협력은 공조하면 훨씬 더 강하다는 것을 보여주었다. 실제로 어떤 기관도 단독으로 국가를 방어할 수 없다. USCYBERCOM은 위협 행위자에게 비용을 부과하고 국내외 파트너에게 악성 활동을 완화하고 대응할 수 있는 정보를 제공하여 각자의 권한에 따라 행동할 수 있도록 모범 사례와 전문 지식을 연방 정부 및 주(洲) 전역의 국내 파트너들과 협력 한다.'고 강조하고 있다.

템은 대부분 민간 소유이기 때문에 이러한 관계는 상업 시스템의 보안 외에도 국가 운영을 직접적으로 향상시키고 있다.

Ⅲ. 최근 미 사이버사령부의 주요 활동 사례

3.1. 러시아-우크라이나 전쟁

러시아-우크라이나 전쟁에서 러시아군의 사이버 공격은 우크라이나군을 지원하는 미국 위성통신 회사인 'Viasat'을 표적으로 하여 데이터를 지우도록 설계된 멀웨어[22]를 사용하였다. 러시아군은 악성 프로그램의 범위를 제한하지 않았고, 결국 다른 지상 위성 부품에 영향을 주었다. 이에 따라 우크라이나 외곽에서 수십만 명의 전력 및 인터넷[23] 연결이 끊어지게 되었다. 또 흑해 연안에 위치한 우크라이나의 주요 항구 도시인 오데사의 시의회에 대한 사이버 공격은 남쪽에서 공격하는 러시아군에 대한 우크라이나의 대응을 방해하기 위해 순항 미사일 공격과 동시에 발생하였다. 또 우크라이나의 많은 기간시설, 정부, 병원을 포함한 민간 네트워크에 대한 사이버 공격도 병행[24]되었다.

이에 따라 USCYBERCOM은 2021년 10월부터 러시아군이 우크라이나 국경과 벨라루스에 배치되기 시작함과 동시에 국가적인 대응을 시작하여, 구조적 위협에 대한 정보를 제공하고 미 정부와 산업계에 중요한 인프라 부문에서 보안을 강화하도록 경고하였다. 또 '전진 방어' 개념에 따라 우크라이나에 공격팀을 배치하여 DODIN에 대한 복원력을 강화하였으며 사이버 범죄 기업에 대한 대응 노력을 가속화하였다. 그 결과 2022년 2월 24일 러시아가 우크라이나를 침공하자 '전진 사냥 훈련(Hunt Forward Operations)'을 시행하여[25] 우크라이나와 NATO 동맹국 및 우크라이나의 회복력을 강화하기 위해 그들의 네트워크에 있는 잠재적 위협을 식별하여 해결하고 완화시켰다. USCYBERCOM은 우크라이나에 원격분석지원을 지속 제공하고 임무 파트너를 직접 지원하기 위해 우크라이나 외부의 중요 네트워크에 맞춰 네트워크 방어 활동을 수행하고 있다.

3.2. 연합 헌트 포워드(Hunt Forward) 훈련[26]

USCYBERCOM의 사이버 국가 임무 부대는 전진 방어개념을 구현하기 위해 우방국 정부 초청으로 주요 국방시스템과 외무부의 네트워크에서 악의적인 사이버 활동을 추적하는 사이버 작전을 훈련하였다.[27]

헌트 포워드 훈련의 목표는 양국을 위협하는 악의적인 사이버 활동을 관찰, 식별하고 통찰력을 사용하여 국토 방어력을 강화하며 사이버 위협에 대한 중요 네트워크의 탄력성을 높이는 것이다.

헌트 포워드 훈련은 정보 중심의 방어적인 사이버 작전이다. 2022년 5월 현재 사이버 국가 임무 부대는 에스토니아, 리투아니아, 몬테네그로, 북마케도니아, 우크라이나를 포함한 16개국에서 전 세계적으로 28회의 헌트 포워드 훈련(HFO)을 수행·훈련하였다.

22) 데이터 삭제형 사이버 공격무기체계인 'HermeticWiper'를 지칭한다. 이 멀웨어는 운영 체제가 코드 서명을 통해 소프트웨어 초기검사를 하므로 안티바이러스 보호 기능을 우회하도록 설계되었다. 따라서 미국은 이 멀웨어가 인증서 확인 및 사이버 방호체계를 우회할 수 있었다는 이유로 국가 후원 APT행위자가 사용하는 프로그램이라고 밝혔다. 〈이용석·정경두, "러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점". 『국방정책연구』 제137호, 2022.〉

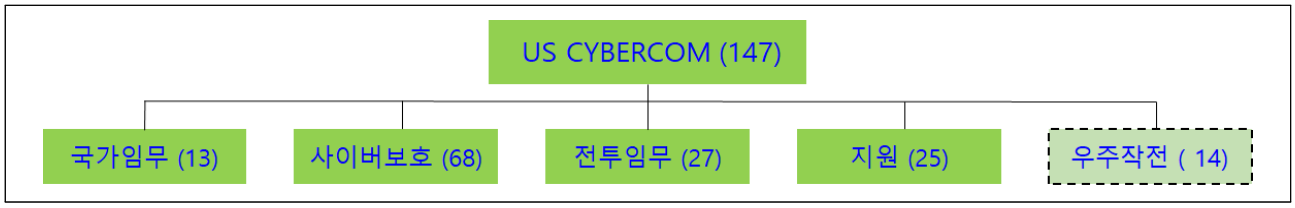
23) Stavros Atlamazoglou, Cyberattacks Quietly Launched by Russia Before Its Invasion of Ukraine May Have Been More Damaging than Intended, 「Business Insider」, 2022.5.18. https://www.businessinsider.com/russian-cyberattacks-on-ukraine-may-have-gotten-out-of-hand-2022-5(검색일: 2022.12.14.)

24) Yurii Shchyhol, Vladimir Putin's Ukraine Invasion Is the World's First Full-Scale Cyberwar, 「Atlantic Council Ukraine Alert」, 2022.6.15. https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/(검색일: 2022.11.20.)

25) "Before the Invasion: Hunt Forward Operations in Ukraine", 「U.S. Cyber Command News release」, 2022.11.28. https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/(검색일: 2022.11.30.)

26) "U.S. Conducts First Hunt Forward Operation in Lithuania," 「U.S. Cyber Command, Cyber News release」, 2022.5.4. https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/(검색일: 2022.11.30.)

27) 사이버 국가 임무 부대(CNMF) 사령관인 육군 소장 Joe Hartman은 "헌트 포워드 작전은 사이버가 얼마나 팀 활동인지를 보여주는 좋은 예이며 우리는 함께 활동해야 한다."라면서, "이러한 임무를 통해 우리는 이 악의적인 행위자들이 중요한 정부 네트워크를 공격하는 방법을 더 광범위하게 볼 수 있다."라고 말했다.



〈그림 4-1〉 2023년 이후 USCYBERCOM 조직도

출처: James Di Pane, 2022.을 근거로 저자가 작성

3.3. 미국 내 주요 해킹 사건에 대한 대응

USCYBERCOM의 '사이버 국가 임무 부대(CNMF)'는 2020년 6월 SolarWinds 공급망 침해손상 사건으로 시작하여 2021년에 연달아 발생한 Ransomware 사건(5월 Colonial Pipeline, 6월 JBS, 7월 Kaseya) 등에서 민간 회사에 영향을 미치는 주요 사이버보안 문제를 처리했다. 이러한 사이버 공격은 정치적 목적이 결부된 국가급 사이버 침해집단의 랜섬웨어 공격으로 사회기반시설을 공격대상으로 삼았기에 명백히 군사안보 차원에서 다루어졌다.

CNMF의 주요 활동은 미국 시스템 및 네트워크에 대한 첫 번째 방어선인 국토 안보 및 법 집행 파트너에게 관련 정보를 제공하는 것이었다. 이를 통해 사이버 국가 임무 부대는 법 집행 기관 간, 산업 및 외국 파트너와 긴밀한 협력 관계를 통해 랜섬웨어와 싸우기 위해 수많은 조치를 하여 국가의 중요 인프라를 공격하는 랜섬웨어 그룹의 운영을 방해하고 완화 시켰다.

사이버 국가 임무 부대와 NSA는 거의 실시간으로 주요 정보를 전달하여, 랜섬웨어 공격자를 대상으로 하는 범정부적 조치를 가능하게 했다. 이러한 노력의 핵심은 부서, 기타 전투사령부 및 DIB 회사가 열악한 사이버 환경에서도 운영할 수 있도록 준비하면서 시스템과 플랫폼의 회복 탄력성을 구축하는 것이다.

Ⅵ. 미 사이버사령부의 미래 발전 방향

4.1. 미 사이버사령부 내 우주작전팀 추가

USCYBERCOM은 2023년부터 2027년까지 5년 동안 기존의 133개 팀에서 '우주작전팀' 14개를 추가하여 총 147개 팀을 확보할 계획이다.

도널드 트럼프 대통령은 2019년 12월 20일 미 공군 우주사령부를 미 우주군(U.S. Space Force)으로 지정하는 국방수권법에 서명하여 공군 우주사령부를 공군으로부터 독립시켜 육군, 해군, 공군, 해병대, 해안경비대에 이어 6번째 독립 군종으로 창설(약 16,000명 규모)하였다. 우주군이란 지상으로부터 100㎞ 이상의 고도에서 우주 공간을 활용한 다양한 군사 활동과 작전을 수행할 수 있는 군대를 의미한다.

미 우주군은 모체인 미 공군 및 NASA와 밀접한 협력 관계를 유지한다. 우주군의 임무는 우주 공간에서 국가 이익을 보장하고 우주로부터의 위협을 저지하며 우주 공간의 자유로운 이용을 확보하기 위해 창설되었다.

이에 USCYBERCOM에 신설되는 '우주작전팀'은 우주작전에서 우주사령부를 포함한 전투지휘관을 지원하고 사이버 영향력의 확대에 대응하고자 한다.[28]

4.2. 주한 미 우주군 (SPACEFOR-KOR) 신설 및 역할

미 우주군은 2022년 12월 14일 고도화된 북한의 미사일 능력에 대응하기 위하여 우리나라에 '주한 미 우주군(SPACEFOR-KOR)'을 신설하였다. 주한 미 우주군 부대는 미국이 본토 밖에 창설한 세 번째 우주군 부대로서 역내 미사일 경보 및 GPS, 위성통신 관련 임무를 수행할 예정이다.[29] 주한 미 우주군은 합동 연합작전, 우주전투 통합 능

28) U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), *United States Department of Defense Fiscal Year 2023 Budget Request: Defense Budget Overview*, April 2022.

29) 김선재, "중국의 우주굴기와 미·중·러 간 신(新)우주경쟁", 『국회도서관』 통권 제54호, 2023.

력, 통합억제를 가능케 하는 즉각적 전투태세 향상 등 한미 연합전력의 대응 능력을 향상시킬 것으로 보인다.[30]

USCYBERCOM은 주한 미 우주군 신설을 위해 2023년에 '사이버공간 활동'에 대한 예산 112억 달러를 포함하였다.[31] 이는 사이버공간에 대한 104억 달러가 포함된 2022회계연도의 국방부 예산 요구액보다 8억 달러가 증가 된 금액이며[32], 2021회계연도 예산 약 100억 달러보다는 12억 달러가 증가한 것이다.[33][34]

미국의 주한 미 우주군을 통한 한반도 우주 전투 역량 강화 이유는 미국의 전략 경쟁 상대인 중국[35]과 미 본토를 겨냥해 핵미사일 위협 능력을 계속 키우고 있는 북한을 염두에 두고 있다는 지적이 있다.[36] 미 국가정보국(DNI)이 매년 발행하는 '연례위협분석보고서' 2023년 판[37]에 의하면 미국에 위협을 주는 국가를 중국·러시아·북한·이란으로 특정하고, 이 국가들의 사이버 역량을 구체적으로 분석하였다. 이 중 북한은 대량살상무기(WMD) 프로그램과 같은 정권의 우선순위에 자금을 지원하기 위해 점점 더 사이버 절도 및 금지되지 않은 상품 수출을 포함한 불법 활동에 관여할 것이라고 평가하였다. 북한은 정교하고 민첩한 사이버 스파이 행위와 사이버 범죄, 사이버 공격에 특화되어 있으며 은밀성과 과감한 행동력으로 기습적인 사이버 공격에 최적화되어 있고, 북한의 능력은 미국의 인프라와 비즈니스 네트워크를 중단시킬 수 있는 전문성을 보유하고 있다고 지적하였다.

북한은 사이버 범죄[38] 외에도 여러 국가의 미디어, 학계, 방산 회사와 정부를 포함한 다양한 조직을 대상으로 사이버 스파이 활동을 수행하였다. 이는 북한의 군사 및 WMD 프로그램을 고도화하기 위해 관련된 기술 정보를 얻기 위한 활동으로 평가된다.

2022년에 발행된 '연례위협분석보고서'[39]에 따르면 랜섬웨어 공격의 수, 규모, 정교함의 측면에서 전 세계적 중요 서비스의 중단을 초래할 가능성이 증가하고 있으며 다국적 사이버 범죄는 송금 사기, 사이버인질, 강탈 등으로 사업 모델을 다각화하고 있다고 규정하였다. 특히 무관해 보이는 분야의 융복합이 새로운 기술 환경을 조성하고 있으며, AI·로봇공학·자동화·스마트 소재 및 제조 등에서 구 체계와 사회적 역학 관계를 교란하고 개인·사회·정부의 관리 방법을 조정하고 있다고 역설하였다.

이처럼 미국은 과학기술 발전에 따른 새로운 국가위협에 대응하기 위하여 사이버 역량 강화와 더불어 우주감시체계의 선도적인 부대창설과 전력 증강 등을 통해 위기를 준비하고 있다.

V. 결론

본 연구는 미국의 사이버 영역을 책임지는 USCYBERCOM의 임무, 역할, 최근 주요 활동 그리고 발전 방향 등을 살펴보았다. USCYBERCOM은 통합전투사령부로서 133개 사이버 임무 팀으로 구성되었고 우주작전팀 14개를 추가할 계획이다. 사이버 임무 팀은 국가임무팀(13), 사이버보호팀(68), 전투임무팀(27), 지원팀(25)으로, 국가임무팀은 적의 활동을 식별 및 공격을 차단하는 등 국가를 방어한다. 사이버보호팀은 국방부 네트워크와 시스템을 방어하며, 전투임무팀은 전투사령부를 지원하고, 지원팀은 국가임무팀과 전투임무팀을 지원한다. USCYBERCOM은 임무 수행을 위해 적의 사이버 활동에 대항하여 물리적으로 해외에 배치하는 전진 방어 개

30) 송태은, "연합 사이버 전력의 역할과 한·미 사이버 안보협력의 과제", 『정책연구시리즈』 제12호, 국립외교원, 2022.

31) U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), 2022.

32) U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), *United States Department of Defense Fiscal Year 2022 Budget Request: Defense Budget Overview*, May 2021.

33) Nakasone, Posture Statement Before Senate Armed Services Committee, March 25, 2021.

34) 사이버사령부의 예산 항목은 총 27개로 구성돼 있다.

35) 1960년대 미국과 소련의 '우주경쟁(Space Race)'이 최근에는 중국의 '우주굴기'라 불리는 우주개발 정책과 함께 신(新)우주경쟁으로 확장되고 있다.

36) 김상진·황수빈, "美, 주한미군에도 '우주군' 창설... 北핵시설 타격도 높일 것", 『중앙일보』, 2022.12.14..

37) Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community,* Feb, 2023.

38) 북한 해커는 암호화폐 강탈과 금전적 동기가 있는 사이버 작전을 다양화하고, 고급 사회공학기술을 지속 활용함으로써 사이버 범죄의 글로벌 추세에 적응하고 있다고 평가되었다. 그 증거로 2022년 싱가포르에서 블록체인 기술회사로부터 6억 2,500만 달러를 훔쳤다고 알려져 있다.

39) Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community,* Feb, 2022.

념을 도입하였고 이를 러시아-우크라이나 전쟁에 적용한 바 있으며, 미국 내 주요 해킹 사건 등 주요 사이버보안 문제를 처리하였다. 최근 USCYBERCOM은 우주작전에서 전투지휘관을 지원하고자 우주작전팀을 추가할 계획이다.

사이버 무기체계는 실전에서 가장 용이하게 사용할 수 있는 공격용 무기체계라고 할 수 있으며, 사이버공간은 적들이 우리나라 민간조직과 정부 기관 사이의 사이버 격차와 접촉점을 이용하려고 하는 역동적이고 상호 연결된 영역이다. 적들은 다양한 사이버 수단을 이용하여 시스템을 침해하고, 의도를 왜곡하며 잘못된 정보를 유포한다. 이러한 행동은 보안을 훼손시켜 국민의 안전을 침해하고 지적 재산과 개인 정보를 도용하는 동시에 기관의 정당성을 훼손함으로써 국가 이익을 위협한다. 적들은 경쟁, 위기 및 분쟁에서 사용할 수 있는 정교한 사이버 공격 능력을 보여주므로 사이버 임무를 담당하는 부대는 이러한 국가적인 도전에 대처할 준비가 완벽히 되어 있어야 한다.

대한민국 헌법은 제5조제2항에 '국군은 국가의 안전보장과 국토방위의 신성한 의무를 수행함을 사명으로 한다.'라고 규정하고 있다. 우리는 이것을 국가가 국방에 부여한 '헌법적 소명'이라고 한다. 헌법적 소명이란 명시적인 과업으로 국방에 종사하는 모든 사람과 조직은 이 명령에 부응해야 한다. 이 명령에 부응하기 위하여 국방조직은 국민의 생명과 재산이 존재하는 새로운 영역인 사이버공간에 대한 안전보장과 방위도 물리적 공간과 동일하게 완수할 수 있어야 한다. 이것은 전 세계가 공통적으로 처한 상황일 것이다.

앞서 살펴본 바와 같이 미국도 미 사이버사령부의 국가임무팀은 선거에 개입하려는 적성국가의 공작과 민간영역을 침해하려는 해킹 집단에 대응하는 임무를 수행한다. 또 새롭게 식별된 우주작전 영역에 대한 능동적 대응을 위해 우주작전팀을 신설하고 있다. 미국 사이버사령부가 이처럼 국익을 위하여 끊임없이 발전하고 있는 것은 우리에게 시사하는 바가 크다. 이는 우리나라가 북한이라는 사이버강국과 적으로 대치하고 있으며 이들은 호시탐탐 사이버공간에서 우리의 국익을 침해할 태세를 갖추고 있기 때문이다. 워싱턴에 본부를 둔 싱크 탱크인 '신미국안보센터(Center for a New American Security)'가 주최한 웨비나에서 앤 뉴버거(Anne Neuberger) 사이버 및 신흥 기술 국가 안보 부보좌관(DNSA)은 "북한은 사이버 자금으로 미사일 프로그램 자금의 최대 3분의 1을 사용하는 것으로 추정한다"고 하면서, '중요한 문제(major issue)'라고 말했다.[40]

이에 우리나라가 명실상부한 사이버 강국이 되기 위해서는 불특정 사이버공격자들의 공격에 대하여 철저한 대비 태세를 갖추는 방호력을 가져야 하며 사이버 선진국과의 긴밀한 협력 관계를 구축해야 할 필요가 있다. 최근 우리나라는 2022년 5월 나토 사이버방위센터(Cooperative Cyber Defence Centre of Excellence, CCDCOE)에 아시아 국가 중 최초로 비나토회원국으로 가입하여 오스트리아, 스웨덴, 핀란드, 스위스와 함께 5개 기여국이 되었다. 또한 우리나라 사이버작전사령부는 2022년 8월 18일 미 사이버사령부와 양해각서(MOU)를 체결하고, 10월 버지니아에서 열리는 미국 주도의 다국적 사이버 군사훈련인 사이버 플래그(Cyber Flag)에 최초로 참가했다.[41]

우리나라는 북한의 사이버공격 및 탄도미사일 도발 등에 대응하기 위해 사이버공간에서의 국방력 강화를 위한 국제협력과 함께 미국의 사이버 역량 강화와 우주감시체계[42]를 주목하여야 할 것이다. 그리고 이를 위해 앞서 살펴본 미 사이버사령부의 역할, 그리고 최근 우주작전팀 추가 등을 주의 깊게 살펴야 할 것이다.

40) 『The Korea times』, "Ranking US official visits South Korea to discuss cyber security: NSC," 2022.7.29.

41) 송태은, "북한의 사이버 공격과 우리의 대응", 『IFANS FOCUS』 IF2022-28K, 2022.

42) 그간 우리나라의 우주영역인식은 한국천문연구원, 항공우주연구원, 공군의 세 개 기관 주도로 이루어져 왔다.〈배학영 외 2, "국방우주력 발전을 위한 해상기반 우주영역인식체계 활용방안 연구". 『한국방위산업학회지』 제29권 제1호, 2022.〉

참고문헌

1) 김상진·황수빈, “美, 주한미군에도 ‘우주군’ 창설… 北핵시설 타격도 높일 것”, 『중앙일보』, 2022.12.14..
2) 김선재, “중국의 우주굴기와 미·중·러 간 신(新)우주경쟁”, 『국회도서관』 통권 제54호, 2023.
3) 박동휘, 『사이버전의 모든 것』, 플래닛미디어, 2022.
4) 배학영·김주형·임종수, “국방우주력 발전을 위한 해상기반 우주영역인식체계 활용방안 연구”. 『한국방위산업학회지』 제29권 제1호, 2022.
5) 송태은, “북한의 사이버 공격과 우리의 대응”, 『IFANS FOCUS』 IF2022-28K, 2022.
6) 송태은, “연합 사이버 전력의 역할과 한·미 사이버 안보협력의 과제”, 『정책연구시리즈』 제12호, 국립외교원, 2022.
7) 이용석, “독일 연방 사이버군 창설 계획과 한국군 적용 방향”. 『국방정책연구』 제133호, 2017.
8) 이용석·정경두, “러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점”. 『국방정책연구』 제137호, 2022.
9) 장상국, “미래전을 대비하는 차기자주포의 화력 강화방안”. 『한국방위산업학회지』 제29권 제3호, 2022.
10) 장원준·송재필, “디지털 전환시대에 걸맞은 한국형 신속획득 프로세스 정립방안 연구”. 『한국방위산업학회지』 제29권 제3호, 2022.
11) G. Alexander Crowther, *National Defense and the Cyber Domain, in 2018 Index of U.S. Military Strength, ed. Dakota L. Wood,* Washington: The Heritage Foundation, 2017.
12) James Di Pane, *Cyber Warfare and U.S. Cyber Command in 2023 Index of U.S. Military Strength,* Washington: The Heritage Foundation,, 2022.
13) 『nbcnews』 “Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups”, 2023.2.2.
14) 『The Korea times』, “Ranking US official visits South Korea to discuss cyber security: NSC,” 2022.7.29.
15) Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community,* Feb, 2022
16) Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community,* Feb, 2023.
17) Paul M. Nakasone, Commander, United States Cyber Command, posture statement before the Committee on Armed Services, U.S. Senate, 2022.4.5.
18) Stavros Atlamazoglou, Cyberattacks Quietly Launched by Russia Before Its Invasion of Ukraine May Have Been More Damaging than Intended, 「Business Insider」, 2022.5.18.
19) 『The Korea times』, “Ranking US official visits South Korea to discuss cyber security: NSC,” 2022.7.29.
20) U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), *United States Department of Defense Fiscal Year 2023 Budget Request: Defense Budget Overview*, April 2022.
21) U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), *United States Department of Defense Fiscal Year 2022 Budget Request: Defense Budget Overview*, May 2021.
22) Yurii Shchyhol, Vladimir Putin’s Ukraine Invasion Is the World’s First Full-Scale Cyberwar, 「Atlantic Council Ukraine Alert」, 2022.6.15.
23) U.S. Cyber Command homepage https://www.cybercom.mil/About/History/(검색일: 2023.2.20.)
24) U.S. Cyber Command homepage https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/(검색일: 2022.11.30.)
25) U.S. Cyber Command homepage https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/(검색일: 2022.11.30.)
26) https://en.m.wikipedia.org/wiki/Eligible_Receiver_97 (검색일: 2023. 2.16)