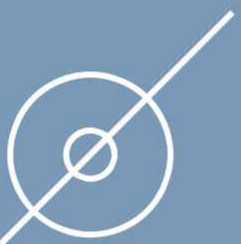
우크라이나 전쟁과 사이버전:



러시아의 사이버 공격 및 NATO의 우크라이나 지원

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 25호
발간일: 2024년 8월 25일

신범식 (서울대학교)
양정윤 (국가보안기술연구소)

Ⅰ. 머리말

2022년 2월 24일 러시아의 우크라이나 침공 이후 우크라이나 전쟁은 2년 이상 지속되며 장기전화 되고 있다. 러시아-우크라이나전은 제2차 세계대전과 컴퓨터와 인공위성, 인터넷으로 촉발된 제3차 산업혁명, 사이버-물리시스템의 융합으로 가속화된 4차 산업혁명 이후 유럽지역에서 발발한 대규모 전쟁이라는 측면에서 전쟁에서의 사이버 전력 활용에 전 세계의 이목을 집중시키고 있다. 러시아-우크라이나 전쟁의 사이버전 양상과 전쟁을 지원하는 타국의 역할은 현대전에 새로이 등장한 공간인 사이버가 전쟁에 미치는 영향에 대한 귀중한 통찰력을 제공한다. 우크라이나 전쟁의 시작에 대한 다양한 의견들이 있지만, 실제 공격은 2022년 2월 23일에 감행된 사이버공격으로부터 시작되었다는 분석이 나왔다.[1)]

2007년 에스토니아 공격, 2007년 러시아-조지아 분쟁 중 사이버공격, 2014년 크리미아 병합 시 샌드웜(Sandworm)과 같은 APT 공격과 2015년 우크라이나 전력망을 타겟으로 한 블랙에너지(BlackEnergy) 공격, 2017년 우크라이나 기업 및 글로벌 물류체계에 영향을 미친 낫페트야(Notpetya) 공격 등 러시아는 최소 15년 이상 공격적 사이버기술을 개발, 사용해왔으며 세계적으로 최고 수준의 사이버공격 역량을 보유한 것으로 알려져 왔다. 러시아는 서방의 해저케이블 및 산업제어시스템(ICS)을 포함한 중요 인프라에 대한 사이버공격 역량 또한 갖추고 있는 것으로 평가된다. 러시아의 우크라이나에 대한 사이버공격이 전쟁 초반 통신, 금융, 교통, 에너지 등 우크라이나의 주요기반시설을 광범위하게 마비시킬 정도의 위력은 아니었으나, 전쟁이 개시된 이래 지속적으로 사이버공간을 활용한 정보전, 심리전, 하이브리드전 등 공격적인 사이버(offensive cyber) 역량을 다면적으로 수행하고 있는 것으로 알려져 있다.[2)] 이에 대응해 우크라이나도 러시아의 사이버공격을 적극적으로 방어하고 있는데, 물리전과 동일하게 미국과 북대서양조약기구(NATO)를 위시한 서방 국가들의 적극적인 지원을 통해 러시아의 사이버공격에 대응하고 있는 것으로 알려져 있다.

---

1) Microsoft, “Defending Ukraine: Early Lessons from the Cyber War,” (June 22, 2022), at https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (검색일: 2023. 04. 15).

2) Julia Voo, Irfan Hemani, Daniel Cassidy, “National Cyber Power Index 2022,” Havard Kennedy School Belfer Center (September 2022), at https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (검색일: 2023. 12. 15).

NATO의 확장에 대한 조지 캐넌(George Kennan)의 경고[3]와 미어샤이머(Mearsheimer)의 책임론에도 불구하고[4] NATO의 동진(東進)은 진행되었으며, 전쟁 발발의 직접적인 원인이 되었다. 러시아는 전쟁 종결을 위한 협상 의제로 우크라이나의 비무장화, 탈나치화, 중립화와 함께 NATO 가입 금지 등을 주장하고 있고 NATO 회원국은 우크라이나를 정치적·경제적으로 적극 지원하고 있다. 공세적 현실주의에서 주장하는, 오히려 NATO가 더 빨리 확장하였다면 NATO조약 제5조의 적용에 따라 2014년 크림반도가 병합되지 않았을 것이고 2022년 우크라이나전은 발발하지 않았을 것이라는 반사실적 시나리오는 현재의 답보적 상황에 해결책을 제시하지 않는다.[5] NATO는 분쟁을 확대하지 않으면서 상대적으로 가시성이 낮은 사이버영역에서 우크라이나를 적극적으로 지원하고 있으며, 최선의 지원을 통해 전쟁의 더 나은 결과를 도출하려는 현 상황에서 사이버영역에서 러시아-우크라이나 전쟁의 NATO의 영향에 대한 고찰은 시의적절하다고 판단된다.

우크라이나전과 관련된 연구는 국내외적으로 다수 진행되고 있으며, 우크라이나 전쟁의 사이버전에 관한 연구도 다수 존재한다. 기존 연구들에서는 러시아가 수행하는 사이버전 기술과 전술, 위협 양상, 사이버가 재래식 전력에 미치는 함의 등에 주목하고 있다. 러시아의 초기 사이버전과 관련하여, 마커스 윌렛(Marcus Willett)은 러시아의 사이버전 진행 양상을 분석하며, 사이버공간에 적용되는 국제법의 불확실성으로 인하여 사이버분쟁이 사이버공간을 넘어 러시아와 NATO 간 분쟁으로 확대되는 것에 대한 위험성을 지적한다.[6] 국내 연구에서 송태은은 우크라이나전을 통해 전면전에서 사이버 전력의 역할을 분석하고 있으며,[7] 부형욱은 우크라이나전의 사이버전 전개 양상과 이를 통한 한미일 사이버안보 협력에 관한 함의를 고찰한다.[8] 이용석, 정경두는 러시아의 우크라이나 전쟁 전후 사이버 활동과 우크라이나에 대한 타국의 지원에 주목한다.[9] 문용득·박동휘는 하이브리드 전쟁의 시각에서 우크라이나전의 사이버전 진행 양상을 분석한다.[10]

이 연구에서는 우크라이나 전쟁과 관련하여 러시아의 사이버공격에 대항하는 우크라이나에 대해 사이버 전쟁 수행과정에서 NATO가 어떠한 지원을 실행하고 있으며 그 영향과 함의를 살펴보고자 한다. 구체적으로 우크라이나전에서 진행 중인 사이버-물리전력이 결합되어 투사되는 하이브리드전의 전장 환경에서 우크라이나를 지원하는 NATO의 사이버 전술의 실행, 대응, 효과와 한계를 살펴볼 것이다.

---

3) Thomas Hodgson, Kennan, "Revisited: NATO Expansion into the Former USSR in Retrospect," Foreign Affairs Review (April 4, 2022) at https://www.foreignaffairsreview.com/home/kennan-revisited-nato-expansion-into-the-former-ussr-in-retrospect (검색일: 2023. 12. 25.).

4) John J. Mearsheimer, "Why the Ukraine Crisis Is the West's Fault," Foreign Affairs 93-5 (September/October 2014), pp. 77-84, 85-89, at https://www.foreignaffairs.com/articles/russia-fsu/2014-08-18/why-ukraine-crisis-west-s-fault (검색일: 2023. 12. 04).

5) Harald Edinger, "Offensive ideas: structural realism, classical realism and Putin's war on Ukraine," International Affairs 98-6 (November 2022), pp. 1873-1893, https://doi.org/10.1093/ia/iiac217.

6) Marcus Willett, "The Cyber Dimension of the Russia-Ukraine War," Survival 64-5(September 2022), pp. 7-26, https://doi.org/10.1080/00396338.2022.2126193.

7) 송태은, "현대 전면전에서의 사이버전의 역할과 전개양상: 2022년 러시아-우크라이나 전쟁 사례," 『국방연구』 제65권 3호 (2022), pp. 215-236.

8) 부형욱, "우크라이나 전쟁에서의 사이버전과 한·미·일 사이버안보 협력의 향배," 『국가전략』 제30권 1호(2024), pp. 83-108.

9) 이용석·정경두, "러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점," 『국방정책연구』 제137권(2022), pp. 39-79.

10) 문용득·박동휘, "러시아의 사이버전 전략: 러시아-우크라이나 전쟁초기 전역을 중심으로," 『민족연구』 제80권 (2022), pp. 10-34.

Ⅱ. 우크라이나 전쟁과 러시아의 사이버공격

1. 러시아의 우크라이나에 대한 사이버 확전(擴戰)

2022년 2월 24일 탱크, 전투기, 순항미사일을 동원한 러시아의 "우크라이나에 대한 특수군사작전"(Специальная военная операция на Украине)이 실행되기 하루 전날인 2월 23일, 러시아는 파괴형 소프트웨어인 '폭스블레이드(Foxblade)'를 통해 우크라이나 전역의 19개 정부 및 주요기반시설을 공격하여 정부 및 주요기반시설 데이터 삭제를 시도한 사실이 드러났다. 러시아는 최소 2021년 3월부터 우크라이나 에너지 및 통신 네트워크에 대한 정찰 및 사이버공격을 위한 사전작업을 수행해 온 것으로 추측된다.[11] 우크라이나전에서 사이버전의 효과와 재래식 전력과 비교한 공격의 영향에 대해서 다양한 의견이 존재하나 일정 정도 이상의 효과를 발휘하였다는 것이 일반론이다.[12] 러시아는 지상군 투입 전 비아셋(Viasat) 위성시스템을 교란하고 독일의 5,800개의 풍력 터빈 마비를 포함하여 유럽 전역에 30,000개 이상의 인터넷 연결을 일시적으로 중단시켰으며, 우크라이나의 군사정보 소프트웨어인 Delta에 침투를 시도하였다. SpaceX 경영진은 우크라이나에서 스타링크(Starlink) 네트워크가 수차례 러시아의 사이버공격을 받았다고 발표하였다. 우크라이나 전쟁 발발 이후 주요 기반시설 표적에 대한 러시아의 공격이 증가하였으며, 물류공급업체에 대한 랜섬웨어 위협이 증대하였고, 사이버수단을 활용하여 지속적인 정보수집 활동이 러시아에 의해 수행되고 있는 것으로 알려지고 있다.

하버드대의 DCID 2.0[13]은 2021년 11월부터 2022년 5월까지를 분석대상기간으로 설정하여 2022년 전쟁 초기 러시아의 사이버 작전을 분석할 시 러시아 사이버공격 빈도는 75% 증가하였다고 발표하였는데, 우크라이나 침공 초기 사이버 중단사고가 57.4%를 차지하였고 첩보행위가 21.3%로 그 뒤를 이었다. 러시아 사이버공격의 59.6%가 민간·비국가행위자를 표적으로 하였으며, 31.9%가 국가·공공기관을 목표로 하였다. 정부군을 공격한 것은 8.5%에 불과하였으며 이러한 수치는 2000년부터 2020년까지의 러시아 사이버공격과 유사한 경향성을 가진 것으로 나타난다. 전쟁 후 군을 목표로 한 사이버공격이 크게 증가하지 않았다는 점이 일반의 예상과 다르게 보이나, 사이버 군사작전에 한계가 있다는 측면이 반증된다. 분석에 따르면 성공적으로 조정된 공격을 수행하기 위해서는 정교한 계획과 정보지원이 모두 필요하나 두 가지 조건을 만족할 수 없었기 때문에 사이버공격의 효과가 과대 평가되었으며, 사이버 수단이 간첩과 범죄에는 유용하게 활용되나 무력충돌의 상황에서는 결정적인 역할을 하지 못한다는 평가도 존재한다.[14]

전쟁 기간을 세 단계로 구분하여 △ 〈1단계〉 2022년 1월~3월 말: 러시아의 우크라이나 최초

11) Marcus Willett (2022), p. 11.
12) Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endownment (December 16, 2022), at https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657 (검색일: 2023.12.16).
13) Harvard Dataverse, "Dyadic Cyber Incident Dataset v 2.0," (Septemver 19, 2022), at https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV) (검색일: 2023. 12. 02).
14) James Andrew Lewis, "Cyber War and Ukraine," CSIS White Papers (June 16, 2022), at https://www.csis.org/analysis/cyber-war-and-ukraine (검색일: 2023.12.15).

침공기, △ 〈2단계〉 2022년 3월 말~2022년 9월: 러시아의 돈바스 집중을 위한 키이우 진격 철회기, △ 〈3단계〉 2022년 9월~2023년 3월: 우크라이나 동부 및 남부에서 우크라이나의 반격과 러시아의 대응기로 구분하여 러시아의 사이버공격을 분석할 시, 〈1단계〉에서는 데이터 삭제와 같은 파괴적인 공격이 수행되었으며, 〈2단계〉에서는 우크라이나 지원을 약화시키기 위한 피싱메일을 활용한 공격 등이 다수 수행되었으며, 〈3단계〉에서는 군수품 공급망 교란 등 군사작전과 병행한 사이버 영향력 작전이 강화되었다.[15)]

전쟁에서 러시아가 투사하는 물리전과 병행된 사이버공격은 위협적인 무력사용의 방편으로 활용되고 있으며, 전쟁 교착상태의 지속 및 서방 제재가 장기화되면서 러시아의 경제적 부담이 증가될 경우 러시아는 NATO에 대한 사이버공격, 산업제어시스템(Industrial Control System, ICS) 및 주요기반시설 사이버공격 등으로 전쟁의 소강상태 국면을 돌파하려는 출구를 찾을 수 있을 것으로 보인다. 사이버전은 효과의 가시성이 물리전보다 낮으므로, 확실한 공격 효과 또는 공격 성공을 필요로 하는 전장에서는 보완재적인 역할을 할 것이다. 개전 이후 러시아는 대규모 전투와 미사일 공격, 강제이주와 납치, 핵무기 사용 위협 등 재래식 전쟁을 이어가고 있으며, 사이버 전력 사용이 전쟁에 실질적인 영향을 끼치지 않았다는 분석에도 불구하고[16)] 사이버작전은 무력투사와 병행한 하이브리드 공격 및 첩보수집, 영향력 작전과 같은 정보전과 심리전 측면에서 정치적 도구로 유용성이 높으므로 제한적인 강압책으로서 지속 활용될 것으로 평가된다.[17)]

2. 러시아의 NATO 회원국에 대한 사이버공격

러시아는 우크라이나전 관련 서방 제재 및 지원에 대응하고 이에 대한 보복으로 NATO 국가에 대한 사이버공격을 수행하는 것이 나타난다. 러시아가 수행하는 사이버공격은 전 세계를 대상으로 하고 있으나 공격의 63%가 NATO 회원국과 관련되어 있음이 나타난다. 우크라이나를 지지하는 국가들의 연합이 우크라이나 방어를 위해 결집함에 따라 러시아에서 사이버 작전을 실행하는 정보총국(GRU), 연방보안국(FSB), 해외정보국(SVR)으로 대표되는 러시아 정보기관 및 민간·군사 정보기관(Russian civilian and military Intelligence Service, RIS)의 우크라이나 외부 동맹국 정부를 대상으로 한 네트워크 침투 및 간첩 활동이 증가한 것으로 조사된다. Microsoft는 러시아가 우크라이나 외 128개 기관을 대상으로 네트워크 침입을 시도한 것을 탐지하였으며, 최우선 공격대상국은 미국임을 밝혔다.[18)]

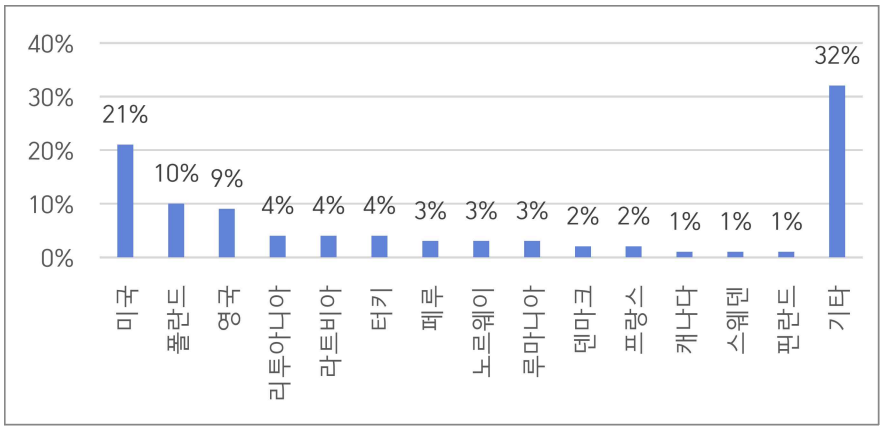
15) Microsoft, “A year of Russian Hybrid warfare in Ukraine,” (March 15, 2023), at https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (검색일: 2023.10.16).

16) Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, Jose M. Macias, “Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures,” Center for Strategic and International Studies (July 13, 2023), at https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war (검색일: 2023.12.15).

17) Grace B. Mueller et al (2023).

18) Microsoft, “An overview of Russia’s cyberattack activity in Ukraine,” Special Report: Ukraine (April 27, 2022), at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (검색일: 2023.12.12).

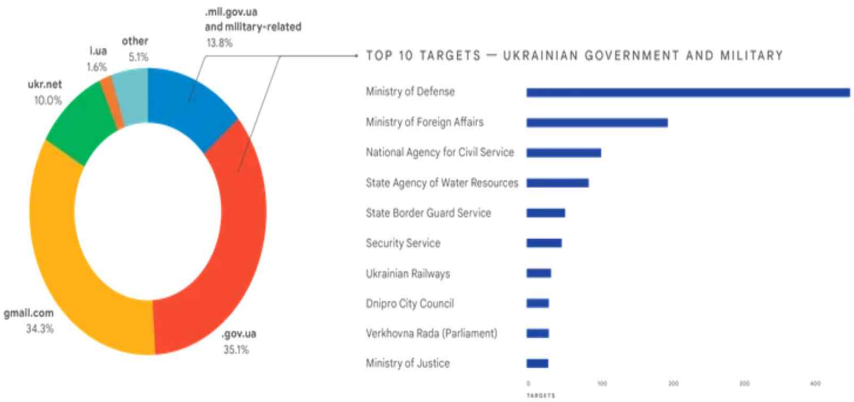
[그림 2] 러시아의 우크라이나 外 사이버공격 대상국(2022.2-2023.3)



※출처: Microsoft(2023.3)

마이크로소프트 위협인텔리전스센터(Microsoft Threat Intelligence Center, MSTIC)의 분석에 따르면 러시아 사이버 스파이 활동은 미국에 가장 많이 집중되어 있으며, 우크라이나를 제외한 미국을 표적으로 한 공격은 전 세계 대상 공격 총계의 12%를 차지한다. 이외 우크라이나의 군수와 인적 지원 조율을 담당하는 폴란드에 대한 침투가 8%였으며, 발트 3국에 해당하는 라트비아와 리투아니아에 대한 공격도 우크라이나를 제외한 지역의 전체 사이버공격 활동 중 14%를 차지하였다. 러시아는 덴마크, 노르웨이, 핀란드, 스웨덴도 사이버 침투의 표적으로 삼았으며, 이들에 대한 공격은 전체 관찰된 공격의 약 16%를 차지하는 것으로 분석된다.

[그림 3] 러시아의 우크라이나 사이버공격 DNS



※출처: Shane Huntley(Google)(2023)

전쟁 전후의 사이버공격을 분석할 시, 러시아의 우크라이나 대상 사이버공격은 전쟁 전인 2020년과 비교하였을 때 전쟁 발발 이후 250% 증가하였으며, NATO 국가에 대한 공격은 전쟁 후 300% 이상 증가한 것으로 분석되었다.[19] [그림 2]에 따르면 2021-2022년 간 러시아는

19) Shane Huntley, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape," Google Threat Analysis Group (February 16, 2023), at https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the

'gov.ua'와 'mil.gov.ua' 도메인을 가진 150개 이상의 기관에 대한 사이버공격을 수행한 것이 나타난다. 러시아의 군사정보기관은 정보수집, 네트워크 파괴, 러시아에 유리한 네러티브 형성을 위해 사이버공간을 적극적으로 활용하고 있으며 러시아 정부기관과 러시아 정부의 지원을 받는 친러시아 공격자들, 애국주의적 해커 등은 우크라이나와 NATO 기관, 군사시설, 주요기반시설 등 전방위적 표적을 대상으로 지속적으로 사이버공격을 수행할 것으로 예측된다.[20]

전쟁이 장기화되고 서방의 적극적 지원이 이루어짐에 따라 러시아가 우크라이나를 지원하는 국가의 에너지, 운송, 오수처리 시스템, 산업제어시스템과 같은 주요기반시설을 목표로 하는 공격이 지속될 것으로 판단된다. 러시아는 전쟁 초기 실행한 우크라이나 군 지휘통제 통신서비스를 제공하는 미국 인터넷 회사 비아사트(Viasat)에 대한 사이버공격[21]과 유사한 공격을 지속할 것이다. Viasat 공격으로 인해 독일에서 풍력 터빈이 오작동하고 유럽 내 인터넷 연결이 일시적으로 중단되어 수천 개 기관에 장애가 발생한 것과 같이[22] 러시아의 우크라이나 공격으로 인한 영향으로부터 서방국가도 자유로울 수 없다.

러시아는 NATO 회원국의 외교부를 비롯한 정부기관을 우선 공격 대상으로 삼고 있으며, 기타 싱크탱크, 인도주의적 지원단체, IT 기업, 에너지 등 주요 인프라 공급업체도 공격 대상으로 한다. 러시아 해커들은 전쟁 관련 정보수집을 위해 키이우에 있는 20개 대사관을 표적으로 사이버공격을 수행한 바 있으며, 우크라이나 사이버방어에 허브 역할을 수행해 온 키이우 주재 미국 대사관 이메일 계정 침입을 시도 한 것으로 드러났다.[23] 분석에 따르면 전쟁이 시작된 이래 러시아의 사이버공격 성공률은 29% 정도 인 것으로 집계되었으며, 침입에 성공한 공격 중 25%는 침투 대상의 데이터 유출을 목표한 것으로 확인되었다.[24]

-cyber-threat-landscape/ (검색일: 2023.12.24).

20) Daryna Antoniuk, "War brought big spikes in cyberattacks on Ukraine, NATO allies, Google says," Recorded Future News (February 16, 2023), at https://therecord.media/ukraine-cyberattacks-russia-google-tag-mandiant (검색일: 2023.12.13).

21) UK NCSC, "Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion," (May 10, 2022), at https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion (검색일: 2024. 03. 16).

22) Jonathan Greig, "NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation," Recorded Future News (August 11, 2023), at https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions (검색일: 2023. 10. 12).

23) Sean Lyngaas, "Russian hackers targeted NATO forces and diplomats to aid Ukraine war effort," CNN (December 7, 2023), at https://edition.cnn.com/2023/12/07/politics/russian-hackers-nato-forces-diplomats/index.html (검색일: 2023.12.24).

24) Sean Lyngaas (2023).

[표 1] 러시아 APT 그룹의 사이버공격 유형, 대상별 분류

공격그룹 / 공격유형	FROZENBARENTS Alliances	FROZEN-LAKE Alliances	COLDRIVER Alliance	FROZEN-VISTA Aliases	PUSHCHA Aliases	SUMMIT Aliases
	Sandworm Voodoo Bear IRIDIUM	APT28 SOFACY Fancy Bear STORONTIUM Sednit	GOSSAMER BEAR Callisto Group SEABORGIUM TA446	UNC2589	UNC1151	Turla Team Snake Uroburos VENOMOUS BEAR UNC4210
첩보	○	○	○	○	○	○
정보 작전	○	○	○	○		○
파괴	○				○	
공격대상	우크라이나 NATO국가 조지아 한국 중동 중앙아시아	우크라이나 NATO국가 유럽 남미 중동 중앙아시아	우크라이나 NATO국가	우크라이나 NATO국가	우크라이나 NATO국가 러시아	우크라이나 NATO국가 호주 남미 중동 중앙아시아
공격목표	정부 군 에너지 금융 중공업 첨단기술·통신 교육기관 미디어 NGO 물류·철도	정부 군 에너지 금융 중공업 첨단기술·통신 교육기관 미디어 NGO 물류·철도	정부 군 에너지 교육기관 미디어 NGO 물류·철도	정부 군 에너지 금융 중공업 첨단기술·통신 교육기관 물류·철도	정부 군 교육기관 미디어 NGO	정부 군 교육기관 미디어 NGO

※출처: Shane Huntley(Google)(2023)

또한 러시아는 우크라이나에 대한 서방의 지원을 약화시키기 위해 적극적으로 허위정보를 생성, 유포하고 있다. 사이버수단을 통한 영향력 작전의 목표는 우크라이나에 대한 서방의 신뢰를 약화시키는 것이다. 러시아가 사이버 및 재래식 전력 통합을 위해 고군분투하나 우크라이나의 높은 사이버 방위력으로 사이버 교착상태에 빠져 있으며, 이에 따라 공격 대상을 미국으로 선회함과 동시에 서방의 우크라이나 지원을 감소시키기 위한 영향력 작전에 주력하고 있는 것으로 분석된다.[25] MS는 러시아가 우크라이나 외 40개 이상 국가의 100개 이상 기관의 네트워크에 침입하였다고 발표하였으며, 이러한 활동에는 허위정보를 생성, 유포하는 APM(Advanced Persistant Manipulator)팀의 공격이 포함되는 것으로 알려져 있다. 러시아는 허위정보를 통해 전쟁에 대한 러시아인, 우크라이나인, 서방국가의 인식을 변화시키려고 하며, 이를 위해 가짜 소셜미디어 계정을 생성하여, 조작된 허위정보를 타겟팅 된 사용자를 대상으로 봇을 통해 유포하는

25) Grace B. Mueller et al (2023).

것으로 알려진다.[26] 이러한 활동은 남반구 국가에서도 효과적으로 작용하여 러시아를 서구 신제국주의의 희생자로 만들고, 푸틴을 노령의 독재자가 아닌 21세기의 체게바라로 이미지화하고 있으며, 생성형 AI를 적극적으로 활용하여 딥페이크 기술이 적용된 허위정보 컨텐츠를 활용한 소셜미디어 공세를 통해 전쟁에 대한 서방의 냉소주의를 확산시키고 있다. 러시아는 사이버수단을 통해 분쟁을 확대하고 사회를 양극화하며 전쟁에 대한 미국의 개입 여론을 약화시키기 위해 영향력 작전에 주력한다.

Ⅲ. NATO의 우크라이나전 사이버 지원

1. NATO의 사이버 방위 정책 기조

사이버 방위에 대한 NATO의 목표는 △NATO의 네트워크 및 회원국 보호, △회원국의 회복력(resilience) 강화 지원, △NATO 회원국 간 정치적 협력 및 공동행동(집단행동)을 위한 플랫폼 제공이다. 사이버공격에 대한 NATO의 방어역량 강화의 필요성은 2002년 프라하에서 열린 정상회담에서 연합국 지도자들에 의해 최초로 인정되었으며, 이후 사이버는 NATO 정상회담 의제에서 주요 쟁점이 되었다.

2008년, 러시아와 조지아 간의 갈등은 NATO에 사이버공격이 재래식 전쟁의 주요 구성 요소가 될 가능성이 있음을 인식하게 해주었으며, NATO는 2008년 최초의 〈NATO 사이버 방어 정책〉을 채택하였다. 2011년, NATO 국방장관은 빠르게 진화하는 위협 및 기술환경에서 동맹 전체의 사이버 방어에 대한 조정된 노력에 대한 비전을 제시한 사이버 방어에 관한 두 번째 NATO 정책을 승인하였으며, 2012년 사이버안보가 NATO의 국방계획에 포함되었다. 2014년 NATO 정상회담에서 회원국은 새로운 사이버 방어 정책에 대해 지지를 표명하였으며, 이 정책에서 회원국에 대한 사이버공격은 NATO의 핵심 임무인 〈NATO조약(The North Atlantic Treaty, 1949)〉 제5조가 발동될 수 있는 집단방위의 일부로 인정되었다. 또한 회원국들은 또한 기존 국제법이 사이버공간에 적용됨을 인정하였다.

2016년 NATO는 NATO의 방위에 관한 임무 조항을 재확인하고 사이버공간을 NATO의 작전영역으로 인정하였다. 〈NATO 전략적 개념(2022)〉은 국가의 개방성, 상호연결성, 디지털환경을 악용하여 다자간 규범과 제도를 훼손하는 위협이 증가하고 있음을 지적하였으며 NATO가 사이버 및 우주공간에서 치열한 경쟁이 진행 중이며, 새로운 파괴적 기술이 글로벌 경쟁의 핵심 영역으로 부상하였음에 대한 인식을 나타내고 NATO의 3대 핵심임무로 ①억지 및 방어, ②위기예방 및 관리, ③안보협력을 명시하였다.[27] 2023년 NATO 회원국은 〈사이버방위서약(2016)〉을 강화하고 주요기반시설을 포함한 회원국 사이버방어를 최우선 과제로 NATO의 사이버안보 목표를 강화할 것임을 선언하였다. 또한 교육, 훈련을 포함한 NATO의 사이버 역량 강화를 위한 활동을 지속하였다.

NATO는 억지력과 방어태세를 강화하여 잠재적인 적의 공격 가능성을 차단할 것이며, 핵과 재

26) Stanford Internet Observatory, “Evidence of Russia-Linked Influence Operations in Africa,” (October, 2019), at https://cyber.fsi.stanford.edu/io/news/prigozhin-africa (검색일: 2024. 02. 24).

27) NATO, “2022 NATO Strategic Concept,” (June 29, 2022), at https://www.nato.int/cps/en/natohq/topics_210907.htm#:~:text=The%202022%20Strategic%20Concept%20describes,and%20management%3B%20and%20cooperative%20security (검색일: 2023. 04. 15).

래식 공격에 대한 방어태세 강화는 사이버 및 우주 역량을 통해 보강될 것임을 명시하였다. 또한 NATO는 자체 디지털 전환을 촉진하여 정보화시대에 적합한 NATO의 지휘체제를 갖출 것이며, 효과적 억지 및 방어를 위해 우주, 사이버 능력을 강화할 것이고 가용한 모든 수단을 통해 위협의 예방, 탐지, 대응이 가능하도록 우주, 사이버 역량을 향상시킬 것임을 선언했다. NATO 회원국은 NATO의 방어 임무를 재확인하고 집단적 대응에 대한 고려를 포함하여 항시 전방위의 사이버 위협을 적극적으로 억제, 방어 및 대응하기 위해 모든 역량을 동원할 것임을 서약하였으며, 또한 이러한 대응에 있어 지속적이고 정치적, 외교적, 군사적 도구를 포함한 전체 NATO의 가용한 수단을 활용할 것임을 확인한 바 있다. 동맹국들은 또한 앞서 언급한 것과 같이 중대하고 악의적인 사이버 활동에 대해 NATO 조약 제5조가 발동가능한 무력 공격으로도 간주 될 수 있음을 인식한 바 있다. 신흥기술 관련, NATO는 DIANA(Defence Innovation Accelerator for the North Atlantic) 창설과 NATO AI 전략개발을 포함하여 신흥기술을 계획 및 운영에 통합하기 위해 노력하고 있는 것으로 알려져 있다.

2. NATO의 대러시아 사이버 대응에 관한 인식

기존 NATO는 러시아와의 관계에 대하여 NATO는 전략문서에서 러시아와의 협력 의지를 피력하거나(1991),[28] 러시아와의 전략적 파트너십(2010)을 표명하기도 하였으나, 러시아의 우크라이나 침공 이후에는 러시아를 NATO의 가장 중대하고 직접적인 위협으로 인식하게 되었다. 러시아에 대한 NATO의 위협인식은 <NATO 전략적 개념(2022)>에서 비교적 명확히 나타나는데, 전략에서 러시아가 회원국의 안보와 유럽-대서양 지역의 평화, 안정에 가장 중대하고 직접적인 위협이며 러시아가 사이버 및 하이브리드 수단을 통해 국제질서를 훼손하고 있음을 명시한다.

NATO 회원국에 대한 러시아의 사이버위협은 복잡하고 파괴적이며 강압적으로 증가하고 있다고 평가된다.[29] 러시아의 NATO 대상 사이버공격에 관한 고려사항으로, 러시아가 사이버공격을 통하여 NATO에 어떠한 압력을 가할 것인가와 함께 NATO가 이에 대응하여 집단적 자위권을 발동할 것인가[30]와 같은 기존 국제법 적용에 관한 문제들이 수반된다. 즉, NATO를 대상으로 한 사이버공격이 무력 공격의 임계값을 충족시키게 될 것인지에 관한 사항이 관건이 될 것이다. 2024년 3월 미국 정보공동체(Intelligence Community, IC)[31]가 발간한 연례위협평가(Annual Threat)[32]는 러시아가 미국 및 NATO와 직접적인 군사적 대립을 원하지 않으며, 타국에 대한

28) NATO (2022).

29) NATO, “Cyber defence,” at https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=NATO's%20policy%20on%20cyber%20defence&text=Allies%20reaffirmed%20NATO's%20defensive%20mandate%20and%20committed%20to%20employing%20the,including%20by%20considering%20collective%20responses (검색일: 2024. 02. 24).

30) <NATO 조약> 5조의 집단적 자위권은 전시상황을 염두한 조항으로, 최근 우크라이나 전쟁과 관련하여 사이버작전의 영향이 무력 공격 수준의 임계값을 넘으며 결과의 심각성이 확인될 때 집단적 자위권이 발동될 수 있는 것으로 해석됨.

31) 미국의 외교정책 및 국가안보 이익을 위한 정보활동을 수행하는 미 연방정부 정보기관 및 하위조직으로, 1981년 행정명령(EO) 12333에 의해 설립되어 1992년 정보조직법(Intelligence Organization Act)로 조직의 근거가 성문화되었으며 국가정보국장(DNI)가 수장이 되는 국가정보국장실(ODNI)가 감독하며 DNI는 대통령에 직속으로 보고함. 현재 국가안보국(NSA), 중앙정보국(CIA), 국토안보부(DHS), 연방수사국(FBI) 등 17개 기관이 포함됨(참조: DNI 홈페이지 at https://www.dni.gov) (검색일: 2024. 02. 24).

32) US ODNI, “Annual Threat Assessment of the U.S. Intelligence Community,” at https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community (검색일: 2024. 03. 20).

군사적 충돌 임계점 이하의 비대칭 공격 활동을 지속적으로 수행할 것으로 판단하고 있다

관련하여 러시아가 NATO 회원국에 미치는 '유해한 영향'과 '규모', '효과'에 대한 검토가 필요하다. 우선 '유해한 영향'은 개방적 정의로 러시아의 사이버 작전이 NATO 회원국에 물리적 침해나 영토주권의 불법적 침해를 발생할 시, 사이버공격이 국가기능의 손실이나 데이터 조작 또는 변경을 야기할 시, 국가가 심각한 손실 및 영국적 주권 침해를 받을 시 유해한 영향을 미친 것으로 판단된다.[33] 또한 사이버 작전은 규모와 효과에 대한 고려에 따라 유엔헌장 제2조 4항과 국제관습법을 위반하는 불법적 무력사용을 구성한다는 입장을 취하고 있다.

러시아와 NATO 회원국은 직접적인 군사 충돌을 피하기 위해 계속 노력할 것으로 관측되나, 기존 군사 분쟁과 달리 공세적인 사이버공격에 적용되는 레드라인과 전쟁과 평화, 법과 규범에 관한 기존 사례가 부재한 사이버공격의 특성상, 전장이 사이버공간으로 확대되는 상황은 러시아와 NATO 모두 유의해야 하는 부분임이 분명하다. 국제법적으로 러시아가 NATO 회원국을 겨냥하여 사이버 작전을 수행하는 것은 피해국의 국가주권을 침해하는 행위임이 명백함에도 불구하고 러시아의 사이버 작전에 대한 NATO의 대응 옵션 또한 명확하지 않은 상황이다. 2014년 NATO는 사이버 방어를 집단 방어의 핵심 임무로 설정한 바 있으나 NATO는 회원국이 제공하는 장비와 인력에 의존하기 때문에, 러시아의 사이버공격에 대한 NATO의 대응은 하나 이상의 회원국에 의해 수행된다. 또한 사이버공격의 귀속 문제, 공격의 부인 등의 문제가 존재한다.

개별적 자위권 또는 〈NATO 조약〉 상의 집단적 자위권이 무력 공격이 발생한 경우에만 발동될 수 있기 때문에 극단적인 상황을 제외하고는 사이버 개입에 따라 발동될 가능성이 낮은 것으로 판단된다. 그럼에도 불구하고 〈NATO 조약〉에 따라 집단적 자위권이 합법적이며 NATO가 사이버공격을 집단적 자위권 발동 요건으로 인정하고 있다는 사실은 NATO 회원국에 대한 러시아가 우크라이나전과 연계한 사이버공격을 수행할 시 확전의 위험이 존재함을 의미한다. 또한 전쟁의 '긴장고조의 동학'(escalation dynamics)에도 주목해야 할 필요성이 존재하는데, NATO가 우크라이나를 지원하는 현재 러시아는 국제법 하에서 이에 대한 대응이 가능하기 때문이다.

3. NATO의 우크라이나 사이버안보 지원

NATO의 우크라이나 사이버안보 지원에 있어, 주지해야 하는 사실은 NATO가 전쟁 당사국이 아니고, 우크라이나 또한 NATO 회원국이 아니라는 것이다. 전쟁에서의 NATO의 우크라이나 지원은 재정적 지원, 인도주의적 지원, 군사적 지원으로 구분할 수 있으며 기타 정치적 지원도 있고[34] 개별 동맹국의 양자적 군사 지원이 주를 이룬다. 러시아의 침공 직후 웹사이트 공격과 서비스 거부 공격, 광범위한 정보전과 선전전이 확산되었으나 NATO를 위시한 서방국가 및 민간기업의 악성코드 탐지 및 즉각적 패치와 같은 적극적 지원에 따라 러시아의 사이버공격이 전체적인 혼란을 야기하지 않았다고 평가된다.

침공 이전부터 NATO 회원국가는 우크라이나의 사이버역량과 회복탄력성 강화를 위해 상당한 투자를 지속해 왔었다. 우크라이나는 NATO의 우크라이나 신뢰기금(NATO Trust Fund Ukraine)중 사이버방위 기금을 통해 기술역량을 강화해왔으며, 평화와 안보를 위한 과학 프로그램(Science for Peace and Security (SPS) Programme of Cooperation, SPS)을 통해

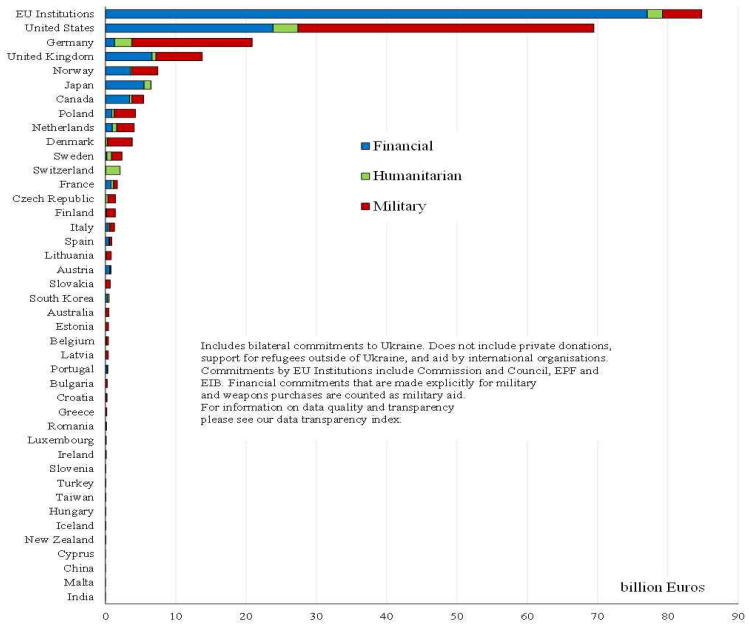
33) Jeppe T Jacobsen, "Cyber offense in NATO: challenges and opportunities Get access Arrow," International Affairs 97-3 (May 2021), pp. 703-720, https://doi.org/10.1093/ia/iiab010.

34) KIEL Institute for the World Economy, "Ukraine Support Tracker Data," at https://www.ifw-kiel.de/publications/ukraine-support-tracker-data-20758/ (검색일: 2023.03.10.).

2014-2017년에만 220만 유로와 사이버보안 사고 조사에 관한 사고관리센터(Incident Management Centre, IMC)의 지원을 받았다. 또한 국방자원에 대한 사이버공격 대응 방법을 포함한 사이버 방위 훈련을 받아왔다.[35] 미국 사이버사령부(U.S. Cyber Command)는 우크라이나에 방어적 사이버작전 수행 전문 인력을 배치하여 공격 탐지 및 취약점 식별활동을 수행하였으며, 원격으로 정보 분석 및 자문을 지원했다. 영국 정보통신본부(GCHQ)는 전쟁 발발 후 美 연방수사국(FBI)과 공동으로 공격조사 및 기술자문을 수행하였으며 美 국제개발처(USAID)는 기술전문가 파견 및 필수 서비스제공업체, 정부관료 및 주요기반시설 운영자에 6,750건 이상의 비상통신을 제공하였다.[36]

전쟁에서 NATO는 사이버 방위 분야의 역량 강화와 회복탄력성 구축을 목적으로 한 우크라이나에 대한 지원을 계속하고 있다. 우크라이나의 긴급 사이버 지원 필요성에 따라 지원 규모가 증가하였으며, 이러한 지원은 장비, S/W, 기타 관련 지원이었고, 전쟁 개시 후 1년 6개월 간 약 1,070만 EURO 규모의 지원이 이루어진 것으로 추산된다.

[그림 4] 국가 및 분야별 우크라이나 지원액(단위: €)



※출처: C. Trebesch et al.(2023).

EU와 우크라이나에 대하여 EU 사이버보안청(ENISA)와 우크라이나 국가사이버안보조정센터(NCCC), 우크라이나 특수 통신 및 정보보호 국가서비스국(Administration of the State Service of Special Communications and Information Protection of Ukraine, SSSCIP) 간 협약이 체결되었으며 EU의 우크라이나에 대한 사이버 지원을 공식화하였다(2023. 11). 협약을 통해 EU는 우크라이나의 사이버 복원력 강화를 위한 사이버 인식 및 역량 구축, 입법 부문에서

35) Natalia Spinu, "Ukraine Cybersecurity Governance Assessmen,t" DCAF(Geneva Centre for Security Sector Governance) (November 2020), at https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf (검색일: 2024. 02. 24).

36) Marcus Willett (2022), p. 15.

모범사례 공유, 사이버안보 위협 환경에 대한 공동의 상황인식 향상을 위한 체계적 정보공유를 강화하게 된다. EU는 2022년 10월 최초로 국가행위자의 사이버공격에 대한 합동 점검을 실행하였는데, EU와 NATO 간 긴밀한 협력 관계임을 고려하였을 때 NATO의 우크라이나 사이버 지원이 유럽 차원에서 광범위하게 일어나고 있음을 알 수 있다.[37)]

사이버방위 측면에서 NATO는 사이버 관련 교육·훈련, 사이버방위서약 등 공동 독트린과 전략을 통해 동맹의 안정성 강화에 기여하는데, 우크라이나 전쟁에서 NATO의 사이버지원의 목적은 NATO의 사이버 관련 동맹의 안정성을 강화하고 적대적 사이버 작전으로 인한 국제체제 불안정에 대항하고자 하는 것에 있다.[38)] 전쟁 관련 NATO는 우크라이나 지원은 △사이버공격 대응 지원, △허위조작정보 대응 지원, △사이버안보 교육·훈련 지원, △민간의 사이버방위 지원으로 구분할 수 있다.

1) 사이버공격 대응 지원

러시아는 우크라이나에 대해 파괴적 맬웨어와 같은 고도의 전방위적 공격을 실행하고 있으며, 전쟁이 장기화됨에 따라 재래식공격과 함께 하이브리드 방식의 사이버공격을 실행하는 것으로 분석된다. NATO 사이버보안센터(NCSC)는 중앙 집중식 24/7 사이버방어 지원을 제공하여 NATO의 자체 네트워크를 보호한다. NATO는 정보공유 및 모범사례 공유를 촉진하고 개별국가의 전문성을 발전시키기 위한 합동 사이버 방어훈련을 실시함으로써 동맹국이 국가 사이버 방어를 강화할 수 있도록 지원한다. 개별 동맹국은 자발적으로 NATO의 지원을 받아 다른 동맹국이 국가 사이버방어 능력을 개발하도록 지원하는 체계를 갖춘다. NATO 사이버 신속 대응팀은 북대서양 평의회의 요청과 승인이 있을 시 동맹국을 지원하기 위해 항시 대비체계를 갖추고 있다.

NATO는 모든 회원국의 국가 사이버 방어 담당 기관과의 연락을 포함하여 상황 인식을 높이고 정보 교환을 촉진하는 여러 가지 실용적인 도구를 보유하며 이를 회원국의 우크라이나 사이버 지원에 활용하는 것으로 알려져 있다. NATO는 사이버 사고를 예방하고 회복력(resilience) 및 대응 역량을 개선을 목적으로 우크라이나에 사이버 방어 정보 및 지원을 제공하고 정보공유 관련 조치를 실행한다. NATO의 사이버공격 정보 침 침해 지표의 신속 공유를 목적으로 구축된 맬웨어 정보공유 플랫폼(MISP)을 통해 NATO 기관 및 회원국의 전반적인 방어 태세를 강화하고 우크라이나에 정보지원을 제공한다.[39)]

37) NATO의 2022 전략 개념(2022 NATO Strategic Concept)과 EU 사이버보안전략(EU's Cybersecurity Strategy for the Digital Decade, 2020)은 위협정보 및 모범사례 공유, 교육·연구 협력 등 국방 및 안보분야에서 더욱 긴밀한 EU-NATO 파트너십의 필요성을 명시하고 있음.

38) NATO, "Cyber defence," at https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=NATO's%20policy%20on%20cyber%20defence&text=Allies%20reaffirmed%20NATO's%20defensive%20mandate%20and%20committed%20to%20employing%20the,including%20by%20considering%20collective%20responses (검색일: 2024. 02. 24).

39) NATO, "Sharing malware information to defeat cyber attacks," (December 29, 2013), at https://www.nato.int/cps/en/natolive/news_105485.html (검색일: 2024. 02. 12).

[표 2] 우크라이나 사이버 방어를 위한 국제 지원 활동

구분	활동내용	정보활동	민간활동
네트워크 방어(배치)	(우크라이나/인접국 대상) 사이버 인력 파견	미 사이버사 hunt forward 작전(긴장고조시) EU 긴급 사이버대응팀(Cyber Rapid Response Teams) 작동	-
네트워크 방어(원격)	원격 사이버 보안 지원	英 민간부문 사이버 보안 서비스 예산 지원 USAID의 민간부문에 대한 예산 지원	BitDefender, Cisco, Cloudflare, ESET, Google, Microsoft, and Sophos 우크라이나국민 대상 무료 보안 지원
위협정보	공격지표 등 기밀/독점 데이터 공유 적의 전술, 기술 및 절차, 전략 평가	FBI, CISA 등 US 기관, 우크라이나와 정보공유	긴급정보공유 메커니즘 구축
역량강화	교육, 기관강화 및 정책조정	CISA와 합동교육실시협약 NATO CCDCOE의 파트너로 우크라이나 가입	AWS(Amazon Web Services) 우크라이나 국민 대상 클라우드 훈련
기술 지원	취약성 및 공격 영향 완화를 위한 하드웨어 및 기술적 지원 제공	하드웨어 업그레이드 제공	Cloudfare 암호키 재배치 SpaceX Starlink 위성통신 군, 민간 사용 제공
클라우드 지원 회복탄력성	우크라이나 외부에 위치한 민간 ISP 운영 상용 클라우드에 데이터 이전 지원	-	공공-민간 부문 데이터 AWS 이전 Google Cloud 특정 기관체 credits 제공 MS, 정부기관 및 국영기업 대상 무료 클라우드 이전 허용

* 출처: Nick Beecroft(2022)[40]

40) Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense," Carnegie Endowment for International Peace (November 3, 2022), at https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub

2) 허위조작정보 대응 지원

사이버공격 대응 지원과 동시에 전쟁의 장기화에 따라 주요 이슈로 부상하는 러시아發 허위정보에 대응하여 NATO는 우크라이나 정부와 공조하여 허위정보에 대한 적극적 대응을 지속하고 있다. 특히 러시아는 대형언어모델(LLM), 인공지능(AI), 머신러닝(ML) 기술을 활용한 해킹코드 생성과 더불어 허위정보를 유포하고 딥페이크(deepfake) 기술을 허위정보 생성에 활용하고 있다. 러시아의 사이버 영향력 작전의 대상은 러시아 국민, 우크라이나 국민, 서방국, 제3국을 대상으로 실행되는 것으로 분석된다.[41] 러시아는 자국민을 대상으로는 러시아는 전쟁에 대한 책임이 우크라이나군에 있는 것으로 묘사함으로써 러시아 내 전쟁지지 여론 조성을 목표로 허위정보를 유포하고, 우크라이나 국민에 대해서는 러시아의 공격을 견딜 수 있는 국가의 의지와 능력에 대한 신뢰를 훼손하고 항전의지를 약화시키려는 목적으로 영향력 작전을 전개하는 것으로 알려져 있다. 미국을 위시한 서방국에 대해서는 영향력 작전을 통해 서방국가들의 통합을 약화·와해시키고 러시아의 군사 전쟁 범죄에 대한 비판여론을 억제시키고자 한다. 제3국에 대해서는 러시아가 UN 등 국제활동을 통해 지원하는 비동맹 국가들을 대상으로 민주주의 및 서방국에 대한 비판여론을 조성하고 식량부족, 유가상승 등 우크라이나 전에 의한 부정적 파급효과에 대한 비난을 서방국으로 향하게 하는 영향력 작전을 실행한다. 러시아는 APM(Advanced Persistent Manipulator) 팀을 통해 공개 인터넷 영역에 허위정보 및 거짓정보를 사전에 공개·배치·유포하고 정부지원 인플루언서, 블로그, 채널, SNS, 인터넷 공격 도구를 통해 허위조작정보를 확대·유포하는 것으로 알려져 있다.

사이버 침투와 허위정보를 통해 NATO 회원국 간 동맹 내 분열을 발생시키기 위한 러시아의 적대적 노력에 대항하여, NATO는 이를 NATO 회원국에 대한 직접적인 안보 도전으로 인식하고 있으며 국제체제와 사이버공간의 안정성 강화를 기치로 이러한 러시아의 활동에 대항하고 있다. NATO는 허위정보에 대항한 팩트체크(fact check)를 재유포하거나, 정보 수요자에 대한 인식제고 활동을 적극적으로 수행하고 있다. NATO는 2017년 '유럽 하이브리드 위협 대응센터(European Centre of Excellence for Countering Hybrid Threats. Hybrid CoE)'를 설립하였는데, Hybrid CoE에 허위조작정보 유포를 통한 사이버 심리전도 하이브리드 위협에 포함시켜 다루고 있다. EU 집행위원회는 '유럽의 보호: 하이브리드 위협 대응 진척 사항'[42]의 22개 실행계획에 허위조작정보에 대응하여 신속하게 사실을 전달하고 대중의 경각심을 높이는 전략커뮤니케이션(strategic communication) 강화를 포함한 바 있다.[43]

-88322 (검색일: 2023. 06. 15).

41) Microsoft (2022).

42) European Commission, "A Europe that protects: good progress on tackling hybrid threats," (May 29, 2019), at https://www.bing.com/search?q=A+Europe+that+protects%3A+good+progress+on+tackling+hybrid+threats&cvid=0c62d5c178d84e81a555e59b6e88430c&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzMyMmowajSoAgCwAgA&FORM=ANAB01&PC=LGTS (검색일: 2024. 02. 18).

43) 송태은, "하이브리드 위협에 대한 최근 유럽의 대응,"『IFANS 주요국제문제분석』2020-31호 (2020년 10월 21일), pp. 1-32, https://www.ifans.go.kr/knda/ifans/kor/pblct/PblctView.do (검색일: 2024. 02. 18).

3) 사이버안보 교육, 훈련 지원

NATO는 연례 사이버 연합 훈련과 같은 정기훈련을 실시하고 위기관리 훈련(Crisis Management, Exercise, CMX)을 포함한 동맹 훈련의 전체 범위에 사이버 방어 요소와 고려사항을 통합하는 것을 목표로 훈련을 수행한다. NATO는 에스토니아 탈린에 있는 NATO 사이버 방위 협력센터(CCDCOE)는 인정된 전문 지식을 위한 사이버 방위 허브이며 사이버 방위 교육, 자문, 교훈 및 연구 개발 활동을 수행하고 있으며 NATO Cyber Range를 포함하여 교육 및 훈련 능력을 강화하고 있다.

포르투갈의 NATO 통신 및 정보(NCI) 아카데미는 NATO 통신 및 정보 시스템의 운영 및 유지 관리와 관련하여 동맹국(및 비 NATO) 국가의 인력을 대상으로 사이버 방어 훈련 및 교육을 제공한다. NATO 학교는 동맹국의 운영, 전략, 정책, 교리 및 절차를 지원하기 위해 사이버 방어 관련 교육 및 훈련을 실시하고 있으며, 이탈리아의 NATO 국방 대학은 사이버 방위를 포함하여 정치-군사 문제에 대한 전략적 사고를 육성한다. 이러한 교육 자원을 기반으로 러시아의 공격에 대항한 우크라이나 군, 정부, 민간을 대상으로 교육, 훈련을 제공한다.

4) 민간의 사이버방위 지원

우크라이나 전쟁은 사이버보안에 대한 비국가행위자(Starlink, MS, Mandiant 등)의 영향력과 민군협력의 중요성을 보여주었다. 전쟁 초기 우크라이나 데이터 센터에 대한 와이퍼 공격의 영향을 우크라이나가 선제적으로 디지털 인프라를 AWS(Amazon Web Service)의 지원으로 퍼블릭 클라우드에 분산시킴으로서 피할 수 있었으며 사이버보안 기업인 Cloudflare는 Project Galileo 서비스를 통해 우크라이나 전역의 인권, 시민사회, 언론과 같은 민주주의 증진을 위한 부문을 보호하였고, Google의 Project Shield는 사이버 침입으로부터 우크라이나를 방어하였다.

Mandiant는 우크라이나 엔지니어에 대한 기술 지원을 수행하였으며, 러시아 사이버 침략에 직면한 플랫폼과 가용성 유지를 위한 MS등의 이니셔티브가 실행되었다. MS는 우크라이나 전쟁 초기 러시아와 NATO 회원국간 경쟁을 피할 수 있었던 것에 MS의 역할이 컸으며, MS가 우크라이나의 MS 제품에 대한 러시아 맬웨어를 무력화하였음을 주장한다. 또한 신속한 공공-민간 파트너십 덕분으로 NATO와 러시아 간 직접적 대결을 피할 수 있었다고 강조한다. Starlink의 일론 머스크(Elon Must) 또한 우크라이나에 위성 인터넷 액세스 제공하여 인터넷 연결 안정성을 지원하였다. NATO 또한 세 차원의 사이버 방어 수준(정치, 군사, 기술)을 더욱 통합하여 평시, 위기 및 분쟁을 통해 항시 민군협력을 보장하고 민간부문과의 참여를 적절하게 보장할 것임을 확인하였는데, 전시 우크라이나 방어에서도 이를 적극적으로 활용하는 것으로 나타난다.

민간 사이버역량 구축을 목표로 NATO 회원국은 2023년 12월 우크라이나와 다수의 NATO 회원국의 참여[44]하에 탈린 매커니즘이 출범하였는데, 이를 통해 우크라이나가 사이버공간에서 기본적 자위권을 유지하고 사이버 복원력 향상을 위한 민간 사이버 역량 구축을 촉진할 것을 선언하였다.[45]

---

44) 참여국: 캐나다, 덴마크, 프랑스, 독일, 네덜란드, 폴란스, 스웨덴, 우크라이나, 영국, 미국(참조: Девять стран НАТО и Швеция подписали пакт о защите киберпространства Украины(December 20, 2023), at https://ukraina.ru/20231220/1052280907.html?ysclid=lry0q4j7ep76567031 (검색일: 2024. 01. 12)).

45) U.S. Department of State, “Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine” (December 20, 2023), at https://state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/

Ⅳ. NATO의 우크라이나에 대한 사이버 지원의 영향

1. 우크라이나전쟁에 대한 영향

NATO의 사이버 지원이 우크라이나 전쟁에 어떤 영향을 미쳤을까? 전쟁 전후 러시아가 대대적으로 실행한 사이버공격으로 전쟁에서 승기를 잡고 전쟁을 속전속결로 끝내려는 러시아의 전략은 우크라이나의 사이버 방어역량과 NATO의 적극적 사이버 지원으로 실패하였다. 우크라이나는 소위 러시아의 사이버 놀이터(cyber playground)라고 불릴 정도로 러시아로부터 많은 사이버공격을 받아왔으며, 2015년과 2016년 러시아의 대대적 사이버공격으로 전략시설의 마비까지 발생한 피해를 겪었다. DCID(Dyadic Cyber Incident and Campaign Data)에 따르면 2000년에서 2020년간 우크라이나 사이버공격의 93% 러시아에 의한 것이었고, 공격에 대한 자국 및 서방의 지원에 따른 방어력 강화, 모범사례 축적, 학습효과에 따른 회복력(resilience) 강화에 따라 전쟁에서의 사이버 전력 효과가 제한적이었다는 평가가 존재한다[46]. 이와 같이 우크라이나의 선전은 전쟁 10년 전부터 준비한 러시아의 사이버공격을 통해 학습한 결과로 우크라이나의 방위역량 강화와 NATO의 지원에 기반한 것이었다.

우크라이나는 자체적으로 지난 7년간 신기술 개발을 통해 국방력을 강화하고 민간의 적극적인 참여하여 자국의 사이버방위력 강화를 이루었으며 여기에는 美 국토안보부(DHS)와 EU, NATO의 적극적 지원이 있었다. 우크라이나는 2023년 5월 NATO CCDCOE에 가입하여, NATO의 사이버 정책, 전략, 방어 및 교육 훈련에 더욱 적극적으로 참여하게 되었다. 우크라이나는 2021년부터 NATO CCDCOE에 가입을 추진해왔으며, 러시아 침공의 영향으로 가입이 성료되었다.[47]

러시아-우크라이나 전쟁에 대한 평가로 '현대전이 일반 인식보다 현대적이지 않음'에 대한 평가가 존재한다.[48] 그러나 전쟁에서 물리적 공격에 앞선 사이버공격, 드론 등 다양한 수단에 사용되는 사이버공격 무기의 영향력을 과소평가할 수 없다. 러시아의 사이버공격과 사이버 작전은 주요기반시설 파괴, 정부 데이터 삭제, 우크라이나와 전 세계의 개인을 대상으로 한 파괴적인 스파이활동 및 공격 수행과 같은 여러 목적으로 활용할 수 있는 공격이 시도되었다. 우크라이나전은 육안으로 확인할 수 있는 진화된 공세적 사이버 기술 및 전술작전이 활용되는 전쟁으로, 전쟁을 통해 사이버공격 및 사이버안보 역량이 진화되는 모습을 보인다. 러시아는 전쟁 전후 파괴적 맬웨어 중 하나인 사이버 '와이퍼' 공격으로 정부 시스템을 공격하고, 주요기반시설 등에 대한 전면적 공격을 감행하였으며,[49] 우크라이나 전쟁에서 개전 초기 러시아는 우크라이나 정부 데이터

(검색일: 2024. 02. 24).

46) Grace B. Mueller et al (2023).

47) NATO CCDCOE, "The NATO CCDCOE welcomes new members Iceland, Ireland, Japan and Ukraine, " (May 17, 2023), at https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-reland-japan-and-ukraine/ (검색일: 2024. 02. 24).

48) Daniel Michaels, "Lessons of Russia's War in Ukraine: You Can't Hide and Weapons Stockpiles Are Essential; U.S., its allies study Europe's biggest conflict in decades; 'You can't cyber your way across a river'," Wall Street Journal(Online) (July 1, 2022), at https://www.wsj.com/articles/lessons-of-russias-war-in-ukraine-you-cant-hide-and-weapons-stockpiles-are-essential-11656927182 (검색일: 2024. 02. 24).

49) 우크라이나 CERT(CERT UA)와 이셋연구소(ESET Research)는 샌드웜(Sandworm)이 ICS에 사용되는 특정 통신

센터에 물리적 공격을 가하였다.

러시아-우크라이나전에서의 사이버는 작전영역으로 포함됨이 나타난다. 전쟁에서 러시아는 우크라이나군, 정부, 민간 등을 목표로 선제적 사이버공격을 실행하여 전략적 우위를 얻고자 하였으나 이를 달성하지 못함이 드러났으며, 러시아-우크라이나전에서의 사이버 전력의 활용은 사이버 수단의 전쟁에서 유용한가에 대한 시험대가 되었다는 판단은 적절해 보인다.[50] 전쟁을 통해 사이버 작전이 제한적으로 유효함을 나타냄에도 불구하고, 사이버 작전에 대항하기 위한 노력이 충분하였다고 판단된다.

2. NATO에 대한 영향

우크리이나전에서 전개되는 사이버전에 관한 분석에 따르면 2022년 한 해 동안 탐지된 러시아 공격의 90%가 NATO 회원국을 대상으로 했으며 이러한 공격의 48%는 회원국에 기반을 둔 IT 기업을 대상으로 했음이 나타났다.[51] 세계 최고의 군사동맹인 NATO의 안보태세는 국제안정에 지대한 영향을 끼치며 NATO가 사이버공간을 작전영역으로 지정하며 소위 군사화한 것은 러시아, 중국에 큰 영향을 끼친 것이 사실이다.

러시아의 적극적 사이버 공세에도 불구하고 사이버공격에 따른 우크라이나전의 확대는 NATO 및 러시아가 가장 우려하는 상황이다. 즉 러시아의 공격 영향이 지리적 경계를 넘어 NATO 회원국에 미칠 경우 NATO 조약 제5조의 집단방위체제가 가동될 것을 우려하고 있으며 이는 러시아와 미국을 위시한 EU, 서방 모두가 경계하는 상황이다. 이에 따라 NATO가 NATO 조약 5조에 따른 집단 사이버 방어 및 공격 가능성에 대한 정책적 대안을 마련해 둘 것을 촉구하는 주장이 제기되고 있다.[52] 사이버공간에 대한 교전규칙은 부재하며 국가들의 행동을 통일시킬 수 있는 대응지침이 부족한 상황에서 NATO는 자구책으로 촉발요인(trigger)과 한계선(redline)을 식별하고 이에 대한 합의(consensus)를 강구해야 하는 상황이다. 앞서 언급한 2022년 우크라이나 내 통신을 차단하기 위해 Viasat 위성 네트워크에 대한 러시아의 사이버공격으로 독일 풍차 발전 및 배전이 중단되는 사건은 우크라이나에 대한 사이버공격이 NATO 회원국으로 전이된 대표적 사례이다.

유사한 맥락에서 NATO 국가의 공세적 사이버 대응 지원의 영향이 물리공간으로 확대되어 NATO가 전쟁의 당사자가 되는 상황은, 공세적 사이버 작전의 국제법적 인정 여부는 차치하더라도, NATO 회원국이 피하고자 하는 상황이다. 러시아 또한 2022년 3월까지 많은 사이버공격을 받은 것으로 알려져 있으며, 이러한 공격은 크렘린, 정부기관(Roskomnadzor 등), 국영뉴스 방송사(RT, TASS 등), RUTUBE 등을 대상으로 광범위하게 이루어진 것으로 알려져 있다. 2023년

프로토콜을 이용해 망 운영을 제어하고 공격하기 위해 설계된 맬웨이인 Industroyer2이 우크라이나 전력망을 타겟으로 하였으며, 이를 조기에 포착·방어하였음을 발표함.

50) Tim Stevens·Joe Burton, “NATO and strategic competition in cyberspace,” NATO (June 6, 2023) at https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html (검색일: 2023. 06. 15).

51) Cristina Vanberghen, “Ukraine marks a turning point for cyberwarfare,” Politico (December 28, 2022), at https://www.politico.eu/article/russia-ukraine-cyber-invasion-warfare-kremlin-nato/ (검색일: 2023. 11. 31).

52) Michael Klipstein·Tinatin Japaridze, “Collective cyber defence and attack:NATO’s Article 5 after the Ukraine conflict,” (May 16, 2022), at https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/ (검색일: 2023. 11. 05).

4월 FSB는 성명서를 통해 러시아연방의 주요기반시설에 대한 사이버공격이 5,000건 이상 발생한 것으로 집계되었으며[53], 미 국방부와 NATO가 우크라이나전 관련 러시아에 대한 대규모 사이버공격의 배후가 있다고 발표하고 서방을 규탄한 바 있다[54]. 이와 같이 우크라이나 지원 국가 및 민간 연합의 적극적 공세는 사이버분쟁의 확산 가능성을 증대시키고 보복 및 잘못된 귀속 등의 문제를 낳는다.

우크라이나 전쟁에서 NATO 역할이 커짐에 따라 전쟁의 게임체인저가 될 집단방위에 관한 5조의 발동 조건에 대한 논란이 지속될 것이다. NATO는 사이버공간이 유엔헌장, 국제인도법 및 국제인권법을 포함한 국제법에 따를 것임을 강조한다. NATO는 자유롭고 개방적이며 평화롭고 안전한 사이버공간을 지속적으로 촉진하고 국제법 존중을 보장하고 사이버공간에서 책임 있는 국가 행동의 자발적 규범을 지원함으로써 사이버공간의 안정성을 강화하고 분쟁의 위험을 줄이기 위한 노력을 촉진하고 있음을 밝힌다.

Ⅴ. 맺음말

러시아는 우크라이나 침공으로 인해 국내외적으로 막대한 손실을 받았으며, 2023년 발생한 PMSC(Private Military & Security Company) 바그너그룹 반란과 같이 엘리트 계층의 변화, 경제적 압박(에너지 부문 외국인 투자감소 등), 우크라이나 전쟁 부담 등에 직면하고 있으나, 여전히 회복력있고 유능한 서방의 경쟁자며 국방과 경제 발전을 위해 중국, 이란, 북한뿐 아니라 서방제재에 동참하지 않는 인도, 아세안, 중남미 등 글로벌 사우스 국가들과 관계를 강화하고 있다. 러시아는 우크라이나의 중요 영토 탈환 노력이 무뎌졌고, 자국이 전쟁의 승기를 잡았으며 이스라엘-하마스 전쟁을 통해 우크라이나에 미국과 서방의 지원이 제한적일 것이라 판단하고 있는 것으로 평가된다.[55] 우크라이나 전에서 초기 군사적 목표였던 우크라이나의 탈군사화, 탈나치화, 중립화는 실패하였고, 제2차 세계대전 이후 최대치의 군사적 손실이 초래되었으나, 2023년 후반부터 서방 군사지원의 불확실성으로부터 이익을 얻고 있는 현재, 2023년 유가상승으로 인한 이익을 보았으며 해상 석유 수출이 증가하고 있다. 러시아는 국익을 증진하고 미국과 동맹국 약화를 위해 에너지 활용, 악의적 영향력 작전, 사이버 작전 등을 광범위하게 수행하고 있다. 또한 핵무기를 현대화하고 핵무기 비축량을 유지하여 미국과 NATO에 대한 잠재적 군사적 충돌에 대한 억지력을 유지할 것이다. 생화학무기(CBW) 위협을 지속적으로 가하고 있으며[56], 비공개 화학 무기 프로그램을 보유한 것으로 판단되고 관련 기술을 연구·개발중이다.

이러한 상황에서 전선에서의 전투가 교착상태에 빠져 있고 신뢰성있는 협상의 타결 가능성이 모호한 현재 미국을 비롯한 NATO 국가들의 전쟁피로감에 따른 우크라이나의 군사적·경제적 원

53) ФСБ at http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439694%40fsbMessage.html (검색일: 2024. 01. 24).

54) ФСБ “ФСБ заявила, что за массированными кибератаками из Украины против РФ стоят Пентагон и НАТО,” (February 13, 2023), at https://tass.ru/proisshestviya/17515409?ysclid=lry0f90v7n446551626 (검색일: 2024. 01. 15).

55) US ODNI (2024).

56) US Department of State, “Imposing New Measures on Russia for its Full-Scale War and Use of Chemical Weapons Against Ukraine,” (May 1, 2024), at https://www.state.gov/imposing-new-measures-on-russia-for-its-full-scale-war-and-use-of-chemical-weapons-against-ukraine-2/#:~:text=The%20Department%20of%20State%20has,Chemical%20Weapons%20Convention%20(CWC) (검색일: 2024. 05. 10).

조 확보에 어려움이 존재하고 있다. 우크라이나 전쟁이 장기화 될 것이라는 예측이 지속되는 현재, 사이버를 포함한 모든 영역에서 미국과 NATO의 직접적이고 강력한 군사적 개입이 전쟁의 향방에 어떠한 영향을 미치게 될 것인지에 대한 영향성 타진이 필요하다. 전쟁이 촉발한 NATO의 확장과 전쟁 후 우크라이나의 NATO 가입 유무에 대한 가능성, 핵전력 사용 가능성을 포함한 러시아의 전략적 선택에 따른 전쟁의 향방 등에 관한 다양한 예측들이 존재한다. 전쟁 종결을 위해 우크라이나는 영토의 해방과 2014년 이전 국경의 회복을 주장하지만, 러시아는 우크라이나 정권 교체, 중립화, 그리고 점령지의 영토화를 주장한다. 전쟁의 결과에 따라 지역정치 구도는 완전히 다른 방향으로 전개될 것이라는 점에서 전망의 불확실성은 높기만 하다.

하지만 최종적 결론에 도달하기까지 긴 시간을 요할 것이며, 전쟁이 계속됨에 따라 러시아와 해커들은 반대 의견을 무마하고 우크라이나의 에너지, 운송 및 디지털 인프라를 무력화하기 위해 사이버 작전을 지속할 것이며, NATO의 도움을 받은 우크라이나는 이에 대응하면서 러시아의 공격력을 약화시키기 위한 다양한 사이버공격도 감행할 것으로 예측된다. 사이버공격이 전쟁에서 결정적인 역할보다는 전쟁을 지원하는 역할과 대규모 분쟁 발생 시 강압의 도구로 제한적인 역할을 수행한다는 평가도 존재하나,[57] 분쟁에 대한 해결책이 없는 상황에서 사이버도구는 점점 더 중요한 무기가 될 것이며 이를 통제할 비재래식, 재래식 수단은 제한적이다.[58] 하지만 한 가지 분명한 점은 우크라이나 전쟁에서 나타난 바와 같이 현재로 성큼 다가온 미래전에서 사이버전은 필수적인 요소로 확고히 자리잡게 되었다는 것이다.

또한 미국, NATO 등 우크라이나를 지원하는 서방은 사이버공간을 통해 국제 여론을 왜곡하여 전쟁에서 승기를 잡으려는 심리·정보전에 더욱 적극적으로 대응해야 한다. 악성코드에 대한 대응이 허위정보를 방어하는 것보다 수월하다는 평가가 주는 경각심을 상기하여, 국가안보적 관점에서 허위정보를 통한 영향력 작전에 대한 대응체계가 필요하다. 러시아는 서방동맹을 분열시키고 미국의 글로벌 지위를 약화시키고 국내 혼란을 야기하기 위하여 사이버 영향력 작전을 수행하고 있으며 생성형 AI 등 신기술을 활용한 영향력 작전을 증대하고 있는 것으로 평가된다[59]. 특히 2024년 미 대선의 결과가 우크라이나에 대한 서방의 지원에 결정적 역할을 할 것임을 인지하여 선거 대상 영향력 작전을 수행하고 있음이 공공연한 사실이며 이에 대한 유의가 필요하다.

더불어 우크라이나 전쟁에서 Microsoft, Cisco, Starlink가 나타내듯 공공부문이 가진 자원의 제약성을 극복하고 데이터의 폭넓은 활용을 통해 사이버전장에서 승기를 획득하기 위해 민간의 역할이 강조되고 민관파트너십을 최대한 활용하여야 할 필요성이 증가한다. 민간부문과의 협력과 우크라이나의 사이버 방어가 NATO와 NATO 회원국을 통해 가능하였다는 점에서 동맹국 및 파트너국과의 적극적인 협력을 통해 정보공유와 상호운용성을 증대하여 효과적 사이버 방어를 달성해야 함이 드러난다.

NATO는 한국을 포함하여, 호주, 일본 등 파트너국을 NATO 정상회의에 초대하여 아태지역 국가와의 협력을 확대하는 노력을 강화하고 있다. 한국 또한 미국, 일본과의 안보협력을 강화하고 있으며, NATO 정상회의에서 한국과 NATO 간 핵심가치를 공유하고 있음을 강조하면서 가치에 기반한 안보협력의 강화에 뜻을 모으고 있다. 한국과 NATO는 국제사이버훈련센터 설치 등과 관련하여 긴밀한 협력 의지를 피력하고 있으며, 2022년 5월 아시아국가로는 최초로 NATO 사이버방위센터(CCDCOE)에 가입하였고 락드 쉴즈(Locked Shields)등 국제 사이버보안 합동훈련에 참여하고 있다.

57) Grace B. Mueller et al (2023).
58) Cristina Vanberghen (2022).
59) ODNI (2024).

이와 같은 협력 체제를 구축하는 과정은 한국을 지구적 진영화의 과정과 깊이 연결시킬 가능성이 높지만, 한국은 이와 관련된 분쟁 연루의 문제에 대하여 보다 신중한 대응책을 마련해 둘 필요가 있다. 또한 우크라이나 전쟁이 수행되는 과정에서 NATO와 우크라이나 간의 사이버방위 분야에서의 협력은 물론이고 러시아의 사이버 작전의 수행 과정과 그 성과 및 한계에 대한 면밀한 검토를 통해 한국의 사이버 방위체계를 고도화하려는 시사점들을 도출하려는 노력을 기울여야 할 것이다.

〈참고문헌〉

1차 자료

European Commission, “A Europe that protects: good progress on tackling hybrid threats,” (May 29, 2019),at https://www.bing.com/search?q=A+Europe+that+protects%3A+good+progress+on+tackling+hybrid+threats&cvid=0c62d5c178d84e81a555e59b6e88430c&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzMyMmowajSoAgCwAgA&FORM=ANAB01&PC=LGTS (검색일: 2024. 02. 18).

European Commission, “EU’s Cybersecurity Strategy for the Digital Decade, 2020,” (December 16, 202), at https://digital-strategy.ec.europa.eu/en/library/eus-cubersecurity-strategy-digital-decade-0 (검색일: 2023. 04. 15).

NATO, “2022 NATO Strategic Concept,” (June 29, 2022), at https://www.nato.int/cps/en/natohq/topics_210907.htm#:~:text=The%202022%20Strategic%20Concept%20describes,and%20management%3B%20and%20cooperative%20security (검색일: 2023. 04. 15).

NATO CCDCOE, “The NATO CCDCOE welcomes new members Iceland, Ireland, Japan and Ukraine, ” (May 17, 2023), at https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-reland-japan-and-ukraine/ (검색일: 2024. 02. 24).

NATO, “Cyber defence,” at https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=NATO's%20policy%20on%20cyber%20defence&text=Allies%20reaffirmed%20NATO's%20defensive%20mandate%20and%20committed%20to%20employing%20the,including%20by%20considering%20collective%20responses (검색일: 2024. 02. 24).

NATO, “Sharing malware information to defeat cyber attacks,” (December 29, 2013), at https://www.nato.int/cps/en/natolive/news_105485.html (검색일: 2024. 02. 12).

Tim Stevens·Joe Burton, “NATO and strategic competition in cyberspace,” NATO (June 6, 2023) at https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html (검색일: 2023. 06. 15).

UK NCSC, “Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion,” (May 10, 2022), at https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion (검색일: 2024. 03. 16).

U.S. Department of State, “Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine” (December 20, 2023), at https://state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/ (검색일: 2024. 02. 24).

US Department of State, “Imposing New Measures on Russia for its Full-Scale War and Use of Chemical Weapons Against Ukraine,” (May 1, 2024), at https://www.state.gov/imposing-new-measures-on-russia-for-its-full-scale-war-and-use-of-chemical-weapons-against-ukraine-2/#:~:text=The%20Department%20of%20State%20has,Chemical%20Weapons%20Convention%20(CWC) (검색일: 2024. 05. 10).

US ODNI, “Annual Threat Assessment of the U.S. Intelligence Community,” at https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community (검색일: 2024. 03. 20).

Девять стран НАТО и Швеция подписали пакт о защите киберпространства Украины(December 20, 2023), at https://ukraina.ru/20231220/1052280907.html?ysclid=lry0q4j7ep76567031 (검색일: 2024. 01. 12).

ФСБ at http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439694%40fsbMessage.html (검색일: 2024. 01. 24).

ФСБ “ФСБ заявила, что за массированными кибератаками из Украины против РФ стоят Пентагон и НАТО,” (February 13, 2023), at https://tass.ru/proisshestviya/17515409?ysclid=lry0f90v7n446551626 (검색일: 2024. 01. 15).

논문

문용득·박동휘, “러시아의 사이버전 전략: 러시아-우크라이나 전쟁초기 전역을 중심으로,” 『민족연구』 제80권(2022).

부형욱, “우크라이나 전쟁에서의 사이버전과 한·미·일 사이버안보 협력의 향배,”『국가전략』 제30권 1호(2024).

송태은, “현대 전면전에서의 사이버전의 역할과 전개양상: 2022년 러시아-우크라이나 전쟁 사례,”『국방연구』 제65권 3호 (2022).

이용석·정경두, “러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점,”『국방정책연구』 제137권(2022).

Harald Edinger, “Offensive ideas: structural realism, classical realism and Putin’s war on Ukraine,” International Affairs 98-6 (November 2022), https://doi.org/10.1093/ia/iiac217.

Jeppe T Jacobsen, “Cyber offense in NATO: challenges and opportunities Get access Arrow,” International Affairs 97-3 (May 2021), https://doi.org/10.1093/ia/iiab010.

Marcus Willett, “The Cyber Dimension of the Russia-Ukraine War,” Survival 64-5(September 2022), https://doi.org/10.1080/00396338.2022.2126193.

보고서

송태은, “하이브리드 위협에 대한 최근 유럽의 대응,”『IFANS 주요국제문제분석』2020-31호 (2020년 10월 21일), https://www.ifans.go.kr/knda/ifans/kor/pblct/PblctView.do (검색일: 2024. 02. 18).

Cristina Vanberghen, “Ukraine marks a turning point for cyberwarfare,” Politico (December 28, 2022), at https://www.politico.eu/article/russia-ukraine-cyber-invasion-warfare-kremlin-nato/ (검색일: 2023. 11. 31).

Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, Jose M. Macias, “Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures,” Center for Strategic and International Studies (July 13, 2023), at https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war (검색일: 2023.12.15).

James Andrew Lewis, “Cyber War and Ukraine,” CSIS White Papers (June 16, 2022), at https://www.csis.org/analysis/cyber-war-and-ukraine (검색일: 2023.12.15).

Jon Bateman, “Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications,” Carnegie Endownment (December 16, 2022), at https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657 (검색일: 2023.12.16).

Julia Voo, Irfan Hemani, Daniel Cassidy, “National Cyber Power Index 2022,” Havard Kennedy School Belfer Center (September 2022), at https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (검색일: 2023. 12. 15).

Natalia Spinu, “Ukraine Cybersecurity Governance Assessmen,t” DCAF(Geneva Centre for Security Sector Governance) (November 2020), at https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf (검색일: 2024. 02. 24).

Nick Beecroft, “Evaluating the International Support to Ukrainian Cyber Defense,” Carnegie Endowment for International Peace (November 3, 2022), at https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (검색일: 2023. 06. 15).

Microsoft, “A year of Russian Hybrid warfare in Ukraine,” (March 15, 2023), at https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (검색일: 2023.10.16).

Microsoft, “An overview of Russia’s cyberattack activity in Ukraine,” Special Report: Ukraine (April 27, 2022), at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (검색일: 2023.12.12).

Microsoft, “Defending Ukraine: Early Lessons from the Cyber War,” (June 22, 2022), athttps://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (검색일: 2023. 04. 15).

Shane Huntley, “Fog of war: how the Ukraine conflict transformed the cyber threat landscape,” Google Threat Analysis Group (February 16, 2023), at https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/ (검색일: 2023.12.24.).

Stanford Internet Observatory, “Evidence of Russia-Linked Influence Operations in Africa,” (October, 2019), at https://cyber.fsi.stanford.edu/io/news/prigozhin-africa (검색일: 2024. 02. 24).

Thomas Hodgson, Kennan, “Revisited: NATO Expansion into the Former USSR in Retrospect,” Foreign Affairs Review (April 4, 2022) at https://www.foreignaffairsreview.com/home/kennan-revisited-nato-expansion-into-the-former-ussr-in-retrospect (검색일: 2023. 12. 25.).

뉴스기사·인터넷 자료

Daniel Michaels, “Lessons of Russia's War in Ukraine: You Can't Hide and Weapons Stockpiles Are Essential; U.S., its allies study Europe's biggest conflict in decades; 'You can't cyber your way across a river',” Wall Street Journal(Online) (July 1, 2022), at https://www.wsj.com/articles/lessons-of-russias-war-in-ukraine-you-cant-hide-and-weapons-stockpiles-are-essential-11656927182 (검색일: 2024. 02. 24).

Daryna Antoniuk, “War brought big spikes in cyberattacks on Ukraine, NATO allies, Google says,” Recorded Future News (February 16, 2023), at https://therecord.media/ukraine-cyberattacks-russia-google-tag-mandiant (검색일: 2023.12.13).

Harvard Dataverse, “Dyadic Cyber Incident Dataset v 2.0,” (Septemver 19, 2022), at https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV) (검색일: 2023. 12. 02).

John J. Mearsheimer, “Why the Ukraine Crisis Is the West’s Fault,” Foreign Affairs 93-5 (Septemver/October 2014), pp. 77-84, 85-89, at https://www.foreignaffairs.com/articles/russia-fsu/2014-08-18/why-ukraine-crisis-west-s-fault (검색일: 2023. 12. 04).

Jonathan Greig, “NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation,” Recorded Future News (August 11, 2023), at https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions (검색일: 2023. 10. 12).

KIEL Institute for the World Economy, “Ukraine Support Tracker Data,” at https://www.ifw-kiel.de/publications/ukraine-support-tracker-data-20758/ (검색일: 2023.03.10.).

Michael Klipstein·Tinatin Japaridze, “Collective cyber defence and attack:NATO’s Article

5 after the Ukraine conflict," (May 16, 2022), at https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/ (검색일: 2023. 11. 05).

Sean Lyngaas, "Russian hackers targeted NATO forces and diplomats to aid Ukraine war effort," CNN (December 7, 2023), at https://edition.cnn.com/2023/12/07/politics/russian-hackers-nato-forces-diplomats/index.html (검색일: 2023.12.24.).

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.