국가전략연구위원회 이슈브리핑 13호 (발간일: 2023.11.14.)

우크라이나 전쟁과 사이버전: 러시아와 나토(NATO) 관계의 맥락과 함의[1)]

신범식 (서울대학교)

Ⅰ. 서론

2022년 2월 24일 러시아의 우크라이나 침공 이후 우크라이나 전쟁은 20개월째 접어들며 장기전화 되고 있다. 우크라이나 전쟁의 시작에 대한 다양한 의견들이 있지만, 실제 공격은 2022년 2월 23일에 감행된 사이버공격으로부터 시작되었다는 분석이 나왔으며,[2)] 세계적으로 최고 수준의 사이버공격 역량을 보유한 것으로 알려진 러시아는 전쟁이 개시된 이래 사이버공간을 활용한 정보전, 심리전, 하이브리드전을 다면적으로 계속해 수행하고 있는 것으로 알려지고 있다.[3)] 물론 우크라이나도 러시아의 사이버공격을 적극적으로 방어하고 있는데, 물리전과 동일하게 미국과 NATO를 위시한 서방 국가들의 적극적인 지원을 통해 러시아의 사이버 공격에 대응하고 있는 것으로 알려져 있다. 이글에서는 우크라이나 전쟁과 관련하여 이 전쟁이 가진 사이버 측면의 공격과 방어는 어떤 양상으로 수행되고 있으며, 특히 러시아의 사이버 공격에 대항하는 우크라이나의 사이버 전쟁 수행과 관련해 NATO가 어떤 지원을 하고 있는지를 살펴보려 한다.

---

1) 이 글은 2023년 10월 25일 제5차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.

2) Microsoft, "Defending Ukraine: Early Lessons from the Cyber War(2022.06.22.)" (https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/)

3) Julia Voo, Irfan Hemani, Daniel Cassidy, "National Cyber Power Index 2022" Havard Kennedy School Belfer Center. (2022. 9) (https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf)

Ⅱ. 우크라이나 전쟁과 러시아의 사이버공격

1. 러시아의 우크라이나에 대한 사이버 공격

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 주요 기반시설을 공격하여 정부 및 주요기반시설 데이터 삭제를 시도한 사실이 드러났다. 러시아의 우크라이나 대상 사이버공격은 전쟁 전인 2020년과 비교하였을 때 250% 증가하였으며, NATO 국가에 대한 공격은 300% 이상 증가한 것으로 분석되었다.[4] [그림 1]에 따르면 2021-2022년 간 러시아는 gov.ua와 mil.gov.ua 도메인에 대한 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 등의 사이버공격은 우크라이나와 NATO의 기관, 군사시설, 주요 기반시설 등 전방위적 표적을 대상으로 지속적으로 수행될 것으로 예측된다.[5]

[그림 1] 러시아의 우크라이나 사이버공격 DNS

※출처: Google(2023)

4) Google, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape" Google Threat Analysis Group(2023. 2. 16)

5) Daryna Antoniuk, War brought big spikes in cyberattacks on Ukraine, NATO allies, Google says, (2023.2.16.) (https://therecord.media/ukraine-cyberattacks-russia-google-tag-mandiant)

전쟁에서 러시아가 투사하는 물리전과 병행된 사이버수단은 위협적인 공격수단으로 활용되고, 전쟁의 교착상태가 지속 및 서방 제재가 장기화되면서 러시아 경제의 부담이 증가될 경우 러시아는 NATO에 대한 사이버공격, ICS, 주요 기반 시설 사이버공격 등으로 전쟁의 소강상태의 국면을 돌파하려는 출구를 찾을 수도 있을 것으로 보인다.

2. 러시아의 NATO 회원국에 대한 사이버공격

러시아는 우크라이나전 관련 서방 제재 및 지원에 대한 보복으로 NATO 국가에 대한 사이버공격을 수행하고 있다. 러시아의 사이버공격은 전 세계를 대상으로 하며, 사이버공격의 63%는 NATO 회원국과 관련되어 있음이 나타났다. 우크라이나를 지지하는 국가 연합이 우크라이나 방어를 위해 결집함에 따라 사이버 작전을 실행하는 GRU, FSB, SVR로 대표되는 러시아 정보기관의 우크라이나 외부 동맹국 정부를 대상으로 한 네트워크 침투 및 간첩 활동이 증가하였다. Microsoft는 러시아가 우크라이나 외 128개 기관에 대한 네트워크 침입을 시도한 것을 탐지하였으며, 최우선 공격대상국은 미국임을 밝혔다.[6] MSTIC의 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 침해도 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 거의 16%를 차지하는 것으로 분석되었다.

6) Microsoft, "An overview of Russia's cyberattack activity in Ukraine" Special Report: Ukraine(2022. 4. 27) (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd)

[그림 2] 러시아 APT 그룹의 사이버공격 유형, 대상별 분류

※출처: Google(2023)

러시아는 외교부를 비롯한 NATO 회원국 정부를 우선 공격 대상으로 삼았으며, 기타 공격 대상으로 싱크탱크, 인도주의적 지원단체, IT 기업, 에너지 등 주요 인프라 공급업체도 포함되었다. 분석에 따르면 전쟁이 시작된 이래 목표 대상에 대한 러시아의 공격 성공률은 29%로 나타났으며, 침입에 성공한 공격 중 25%는 침투 대상의 데이터 유출을 목표한 것으로 확인되었다.[7)]

Ⅲ. NATO의 우크라이나전 사이버 지원

1. NATO의 사이버 방위 정책 기조

7) Ibid.

사이버 방위에 대한 NATO의 목표는 △ NATO의 네트워크 및 회원국 보호, △ 회원국의 회복력 강화 지원, △NATO 회원국 간 정치적 협력 및 공동행동(집단적 행동)을 위한 플랫폼 제공이다. 사이버공격에 대한 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 사이버안보는 NATO의 국방계획에 포함되었다. 2014년 NATO 정상회담에서 회원국은 새로운 사이버 방어 정책에 대해 지지를 표명하였으며, 이 정책에서 회원국에 대한 사이버공격은 NATO의 핵심 임무인 <나토조약(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, ②위기 예방 및 관리, ③안보협력을 명시하였다.[8] 2023년 NATO 회원국은 <사이버 방위서약(2016)>을 강화하고 주요 기반시설을 포함한 국가 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 재래식 공격에 대한 방어태세 강화는 사이버 및 우주 역량을 통해 보강될 것임을 명시한다. 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 선언한다. NATO 회원국은 NATO의 방어 임무를 재확인하고 집단적 대응을 고려하는 것을 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 포함하는 전체 NATO의 가용한 수단을 활용할 것임을 확인한 바 있다. 동맹국들은 또한 중대하고 악의적인 사이버 활동에 대해 NATO 조약 제5조가 발동 가능한 무력

8) 2022 NATO Strategic Concept (https://www.nato.int/cps/en/natohq/topics_210907.htm#:~:text=The%202022%20Strategic%20Concept%20describes,and%20management%3B%20and%20cooperative%20security, 2022. 6).

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 전략문서를 통해 러시아와의 협력 의지를 나타내거나(1991),[9] 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 강압적이며 증가하고 있다고 평가된다.[10] 러시아의 NATO 대상 사이버공격에 관한 고려사항으로, 러시아가 사이버 공격을 통하여 NATO에 어떠한 압력을 가할것인가와 함께 NATO가 이에 대응하여 집단적 자위권을 발동할 것인가,[11] 기존 국제법의 적용에 관한 문제들이 수반된다. 즉, NATO를 대상으로 한 사이버공격이 무력 공격의 임계값을 충족시키게 될 것인지에 관한 사항이 관건이 될 것이다.

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. 또한 사이버 작전은 규모와 효과의 고려에 따라 유엔헌장과 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 사이버 공격에 적용되는 레드라인과 전쟁과 평화, 법과 규범에 관한 기존 사례가 부재한 사이버 공격의 특성상, 전장이 사이버공간으로 확대되는 상황은 러시아와 NATO 모두 유의해야 하는 부분임이 분명하다. 국제법적으로 러시아가 NATO 회원국을 겨냥하여 사이버 작전을 수행하는 것은 피해국의 국가주권을 침해하는

9) Ibid.

10) 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.

11) <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 해석되고 있다.

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 사이버 공격에 대한 NATO의 대응은 하나 이상의 회원국에 의해 수행된다. 또한 사이버 공격의 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 사이버 공격을 집단적 자위권 발동 요건으로 인정하고 있다는 사실은 NATO 회원국에 대한 러시아가 우크라이나전과 연계한 사이버 공격을 수행할 시 확전의 위험이 존재함을 의미한다. 또한 전쟁의 긴장고조 동학에도 주목해야 할 필요성이 존재하는데, NATO가 우크라이나를 지원하는 현재 러시아는 국제법 하에서 이에 대한 대응이 가능하기 때문이다.

3. NATO의 우크라이나 사이버안보 지원

우크라이나 전쟁에서 NATO의 사이버지원의 목적은 NATO의 사이버 관련 동맹의 안정성을 강화하고 적대적 사이버 작전으로 인한 국제체제 불안정에 대항하고자 하는 것에 있다.[12] 사이버방위 측면에서 NATO는 사이버 관련 교육・훈련, 사이버방위서약 등 공동 독트린과 전략을 통해 동맹의 안정성을 강화하는데 기여한다. 전쟁 관련 NATO는 우크라이나 지원은 △ 사이버공격 대응 지원, △ 허위정보 대응 지원, △ 교육, 훈련 지원, △ 민간 지원으로 구분할 수 있다.

12) 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.

[표 1] 우크라이나 사이버 방어를 위한 국제 지원 활동

구분	활동내용	정보활동	민간활동
네트워크 방어_배치	• (우크라이나/인접국 대상) • 사이버 인력 파견	• 미 사이버사(hunt forward)(전쟁전 긴장고조시) • EU 긴급 사이버대응팀(Cyber Rapid Response Teams) 작동	-
네트워크 방어_원거리	• 원격 사이버 보안 지원	• UK의 민간부문 사이버 보안 서비스 예산 지원 • USAID의 민간부문에 대한 예산 지원	• BitDefender, Cisco, Cloudflare, ESET, Google, Microsoft, and Sophos • 우크라이나국민 대상 무료 추가 보안 기원
위협정보	• 공격지표 등 기밀/독점 데이터 공유 • 적의 전술, 기술 및 절차, 전략 평가	• FBI, CISA 등 US 기관의 우크라이나와 정보 공유	• 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	• 기여국에서 하드웨어 업그레이드 제공	• Cloudfare 암호키재배치 • 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 국영기업에 무료로 이전 허용

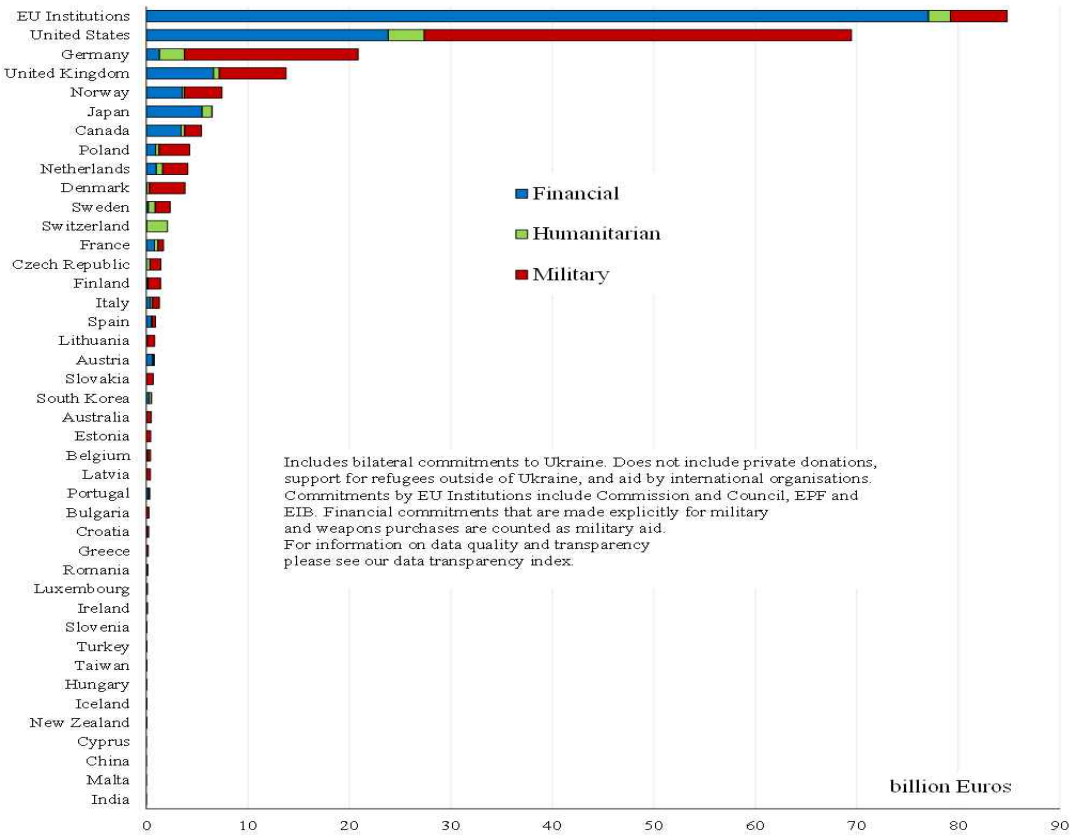
* 출처: Nick Beecroft(2022)[13]

NATO의 우크라이나 사이버안보 지원에 있어, 주지해야 하는 사실은 NATO는 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 있으며,[14] 개별 동맹국의 양자적 군사 지원이 주를 이룬다. 전쟁에서 NATO는

13) Nick Beecroft, Evaluating the International Support to Ukrainian Cyber Defense, Cargegie Endowment for International Peace(2022.11.3.)(https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322)

사이버방위 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, 현재까지 1070만 EURO 규모의 지원이 이루어진 것으로 추산된다.

[그림 3] 국가 및 분야별 우크라이나 지원액(단위: €)



※출처: KIEL Institute(2023)

EU와 우크라이나에 대하여 ENISA와 우크라이나 National Cybersecurity Coordination Centre 간 Working Arrangement 체결을 위해 노력 중이다. EU는 2022년 10월 최초로 국가 행위자의 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.[15]

14) KIEL Institute for the World Economy. "Ukraine Support Tracker Data" (https://www.ifw-kiel.de/publications/ukraine-support-tracker-data-20758/) (2023.10.10. 검색)

15) NATO의 2022 전략 개념(2022)과 EU 사이버보안전략(2020)은 국방 및 안보분야에서 더 긴밀한

IV. NATO의 우크라이나에 대한 사이버 지원의 영향

1. 우크라이나전의 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 2014년 이래 러시아로부터 많은 사이버공격을 받아왔으며, 2015년과 2016년 러시아의 대대적 사이버공격으로 전략시설의 마비까지 발생한 피해를 겪었다. 이러한 우크라이나의 선전(善戰)은 전쟁 10년 전부터 준비한 러시아의 사이버공격을 통해 학습한 결과로 우크라이나의 방위역량 강화와 NATO의 지원에 기반한 것이었다.

러시아-우크라이나 전쟁에 대한 평가로 '현대전이 일반 인식보다 현대적이지 않음'에 대한 평가가 존재한다.[16] 그러나 전쟁에서 물리적 공격에 앞선 사이버공격, 드론 등 다양한 수단에 사용되는 사이버공격 무기의 영향력을 과소평가할 수 없다. 러시아의 사이버공격과 사이버 작전은 주요 기반시설 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 전술 작전이 활용되는 전쟁으로, 전쟁을 통해 사이버공격 및 사이버안보 역량이 진화되는 모습을 보인다. 러시아는 전쟁 전후 파괴적 맬웨어 중 하나인 사이버 '와이퍼' 공격으로 정부 시스템을 공격하고, 주요 기반시설 등에 대한 전면적 공격을 감행하였으며,[17] 우크라이나 전쟁에서 개전 초기 러시아는 우크라이나 정부 데이터 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.[18] 전쟁을 통해 사이버 작전이 제한적으로 유효함을 나타냄에도 불구하고, 사이버 작전에 대항하기 위한 노력이 충분하였다고 판단된다.

EU-NATO 파트너십의 필요성을 명시하고 있음(CTI, 모범사례 공유, 교육-연구 협력)

16) 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' Michaels, Daniel. Wall Street Journal (Online); New York, N.Y.. 04 July 2022.

17) 우크라이나 CERT(CERT UA)와 이셋연구소(ESET Research)는 샌드웜(Sandworm)이 ICS에 사용되는 특정 통신 프로토콜을 이용해 망 운영을 제어하고 공격하기 위해 설계된 맬웨이인 Industroyer2를 우크라이나 전력망을 타겟으로 하였으며, 이를 조기에 포착·방어하였음을 발표함.

18) Tim Stevens, Joe Burton, "NATO and strategic competition in cyberspace"(2023.6.6.) (https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html)

2. NATO 국가에 대한 영향

한 분석에 따르면 지난 한 해 동안 탐지된 러시아 공격의 90%가 NATO 회원국을 대상으로 했으며 이러한 공격의 48%는 회원국에 기반을 둔 IT회사를 대상으로 했음이 나타났다.[19] 세계 최고의 군사동맹인 NATO의 안보태세는 국제안정에 지대한 영향을 끼치며 NATO가 사이버공간을 작전영역으로 지정하며 소위 군사화한 것은 러시아, 중국에 큰 영향을 끼친 것이 사실이다.

사이버공격에 따른 우크라이나전의 확대는 NATO 및 러시아가 모두 가장 우려하는 상황이다. 즉 러시아 공격 영향이 지리적 경계를 넘어 NATO 회원국에 미칠 경우 NATO조약 제5조의 집단방위체제가 가동될 것을 우려하고 있으며 이는 러시아와 미국을 위시한 EU, 서방 모두 경계하는 상황이다. 이에 따라 NATO는 NATO 장 5조에 따른 집단 사이버 방어 및 공격 가능성에 대한 정책적 대안을 마련해 둘 것을 촉구하는 주장이 제기되고 있다.[20] NATO는 사이버공간에 대한 교전규칙이 없으며 국가들의 행동을 통일할 대응 지침이 부족한 상황에서 NATO가 촉발요인(trigger)과 한계선(redline)을 식별하고 이에 대한 합의(consensus)가 필요한 상황이다. 2022년에는 우크라이나 내 통신을 차단하기 위해 Vissat 위성 네트워크에 대한 러시아의 사이버공격으로 독일 풍차 발전 및 배전이 중단되는 사건이 발생하게 되는데, 이는 우크라이나에 대한 사이버공격이 NATO 회원국으로 전이된 사례이다.

우크라이나 전쟁에서 NATO 역할이 커짐에 따라 전쟁의 게임체인저가 될 집단방위에 관한 5조의 발동 조건에 대한 논란이 지속될 것이다. NATO는 사이버공간이 유엔 헌장, 국제 인도법 및 국제 인권법을 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.

러시아의 우크라이나 外 타국 대상 사이버공격에 대하여, 우크라이나 방어를 위한 서방국의 지원이 활발해짐에 따라 러시아는 정보기관을 중심으로 우크라이나 外 타국을 대상으로 한 사이버공격 활동을 증가한 양상을 보인다. 또한 우크라이나에 대한 서방의 전쟁 대응 전략 및 첩보 수집을 목적으로 타국의 정부 기관들을 대상으로 한 사이버 스파이 활동을 활발하게 전개한다.[21] 전쟁이 시작된 이후 우크라이나 제외, 42개국에 분포된 128개 타겟에 대한 러시아 네트워크 침입 및 사이버 스파이 시도가 탐지되었다. 국가별로 살펴볼 때, 러시

19) Cristina Vanberghen. "Ukraine marks a turning point for cyberwarfare." (https://www.politico.eu/article/russia-ukraine-cyber-invasion-warfare-kremlin-nato/)(2022.12.28.)
20) Michael Klipstein, Tinatin Japaridze, Collective cyber defence and attack:NATO's Article 5 after the Ukraine conflict(2022. 5. 16)(https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/)
21) Microsoft(2023.6)

아의 사이버공격은 전 세계를 공격 대상으로 하며, 공격의 63%는 NATO 회원국과 연관됨. 러시아 사이버 스파이 활동은 우크라이나 다음으로 미국에 가장 많이 집중되었으며, 미국 대상 공격이 러시아 발 공격의 12%를 차지함. 다음으로는 덴마크, 노르웨이, 핀란드, 스웨덴이고, 이들에 대한 공격은 전체 공격의 16%를 차지한 것으로 분석된다.[22)]

Ⅴ. 맺음말

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 우크라이나가 NATO에 가입할 것이라는 예측도 있지만, 핵전력 사용 가능성을 포함한 러시아의 전략적 선택에 따른 전쟁의 향방 등에 관한 다양한 예측들도 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, 나토의 도움을 받은 우크라이나는 이에 대응하면서 러시아의 공격력을 약화시키기 위한 다양한 사이버 공격도 감행할 것으로 예측된다. 사이버 전쟁은 분쟁에 대한 해결책이 없는 상황에서 점점 더 중요한 무기가 될 것이며 이를 통제할 재래식 수단은 제한적이다.[23)] 하지만 한 가지 분명한 점은 우크라이나 전쟁에서 나타난 바와 같이 현재로 성큼 다가온 미래전에서 사이버전은 필수적인 요소로 확고히 자리잡게 되었다는 것이다.

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, 한국은 NATO 사이버방위센터에 정식으로 가입하여 합동훈련도 시작하게 되었다. 이같은 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 나토와 우크라이나 간의 사이버방위 분야에서의 협력은 물론이고

22) Ibid.
23) Cristina Vanberghen(2022).

러시아의 사이버 작전의 수행 과정과 그 성과 및 한계에 대한 면밀한 검토를 통해 한국의 사이버 방위체계를 고도화하려는 시사점들을 도출하려는 노력이 기울여야 할 것이다.

※ 이슈브리핑에 수록된 내용은 필자 개인의 의견이며, 한국사이버안보학회의 공식적인 입장이 아님을 알려드립니다.