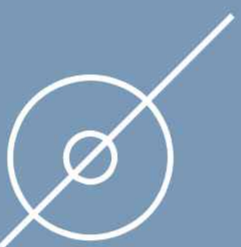
사이버 전쟁



2023

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 3호
발간일: 2023년 12월 27일

이중구 (국방연구원)

〈요 약〉

사이버전이 전쟁의 일부로 이해되는 시대가 시작되고 있다. 사이버 작전은 사이버 첩보, 사이버 방해, 사이버 성능저하 등의 작전유형별로 자세히 이해될 필요가 있다. 사이버 공격수단으로도 웹사이트 변조, 디도스 공격, 침범, 침투 등으로 구분될 수 있다.

하지만, 사이버전이 계속 발전하고 있는만큼, 사이버전에 대한 기술적 이해 이상으로, 사이버전의 이해를 둘러싼 쟁점들을 파악하는 것이 중요하다. 이는 사이버전의 발전방향을 가늠할 기준점들이 되어줄 것이기 때문이다. 이러한 쟁점으로는 우선 전술적인 차원에서 사이버전이 재래식 군사력에 부수적인 것인지 아니면 독립적인 것인지를 들 수 있으며, 그보다 한 단계 높은 차원에서 사이버전이 승리나 강압에 결정적일 수 있는지 등이 있을 수 있을 것이다. 그리고 궁극적으로 사이버전이 국제적 세력관계의 변화에 있어 약자에게 유리한 무기인지, 강자에게 유리한 무기라고 보아야 할지도 사이버전쟁의 이해를 둘러싼 쟁점에 속한다.

러시아-에스토니아 갈등, 러시아-그루지아 전쟁, 미국발로 추정되는 대이란 스턱스넷 사례 등 우크라이나 전쟁 이전의 사이버전 사례들과 우크라이나 전쟁 사례를 살펴볼 때, 사이버전쟁에 대한 쟁점들에서 근본적인 변환은 아직 도래하지 않은 것으로 보인다. 아직, 사이버전은 재래식 공격과 연계되기보다는 사회적 혼란을 야기하는 저강도 공세의 수단으로 주로 활용되고 있고, 사이버전은 결정적인 승리와 강압의 수단으로서 효과를 분명히 보여주지 못하고 있다. 약자의 무기라는 이미지와 다르게 약소국에 대한 강대국의 강압에 주로 활용되고 있다.

그럼에도 불구하고, 우크라이나 전쟁은 “썬더 런” 작전 등 보다 위력적인 사이버전의 도래를 예고하기도 했다. 이에 향후 미중경쟁의 전개 및 인공지능의 기술적 발전을 바탕으로 사이버전이 전쟁영역에서 보다 중심적인 위치를 차지해갈지 계속 주목할 필요가 있다고 하겠다.

Ⅰ. 머리말

오늘날 사이버공격은 전쟁에서나 볼 수 있었던 무력공격의 한 양상으로 이해되고 있다. 미 합참은 사이버전을 “사이버 수단만을 혹은 그 일부를 사용하여 수행되는 무장 분쟁”이라고 규정했고(US Joint Chiefs of Staff, 2010), 2011년에 미국은 이미 사이버공격은 전쟁행위라고 규정했다. 사이버공격을 억지하기 위해 재래식 무기로 대응할 수도 있다는 경고가 필요하다고 본 결과이다. 사이버공격의 피해가 광범위할 수 있다는 점은 널리 이해되고 있다. 디지털 사회의 도래와 사이버기술의 발전으로 우리는 인터넷이 끊긴 상태에서는 몇시간도 견디지 못할 정도로 사이버공간은 중요해졌다. 사이버범죄의 증가와 더불어, 적대세력의 사이버공격으로 국가 핵심인프라가 마비되는 ‘사이버 진주만 공습(Cyber Pearl Harbor)’과 같은 것도 등장할 수 있다는 우려도 공개적으로 제기되어 왔다. 한국의 경우에도, 2009년 7월에 북한이 대규모 디도스 공격으로 한국을 공격한 이래 사이버 공격에 대한 국가안보 차원의 대응이 강조되어 왔다. 곧 이어 사이버사령부도 창설되었다.

오늘날 우리의 눈앞에서 이루어지고 있는 사이버전 양상을 이해하기 위해서 사이버전에 대한 다양한 시각을 이해할 필요가 있다. 사이버전이 등장했다고 해서 사이버수단에 의해서만 전쟁이 이루어지고 있는 것은 아니다. 우크라이나 전쟁에서 보듯이, 사이버전이 러시아에 의해 수행되었지만 그것이 전쟁의 전통적인 모습인 지상전과 시가전을 불필요하게 만들고 대체한 것은 아니었다. 사이버 공격에 의한 피해는 광범위하고 분명 심각한 것이지만, 물리적 공격과 달리 피해가 일시성을 가지며 짧은 시간 내에 복원될 수도 있다는 속성을 갖는다. 이 때문에, 사이버전이 국가간의 세력균형을 변화시키고 한 나라의 요구를 상대국에 강압하는 효과를 얻기 위해서는 다른 수단과 결합되어야 한다는 지적이 존재한다. 동시에 사이버전은 재래식 전쟁보다도 더 자주 등장하고 있다. 오늘날 국가간에는 회색지대 분쟁이 자주 발생하고 있기 때문이다. 거짓정보 조작과 개입에 대한 관심도 유럽국가를 중심으로 증대되고 있다. 언젠가는 사이버전만으로 전쟁이 수행될지도 모른다. 이처럼, 변화하는 현실을 생산적으로 이해하기 위해서는 사이버전을 바라보는 다양한 시각을 참고할 필요가 있다. 시대가 변화함에 따라 우리 스스로의 견해를 검증하고 현실에 맞는 해석을 제시해가야 하기 때문이다.

본론을 시작하기에 앞서, 이 글에서 분석할 대상은, 사이버전쟁(Cyber war)보다는 사이버전(Cyber Warfare)임을 밝힌다. 이는 사이버공간에서만 이루어지는 전쟁이 아니라 다른 전쟁영역(지상, 해상, 공중 및 우주)과 연결되어 있는 영역으로서 사이버공간에서 이루어지는 공격과 방어를 분석하기 위한 것이다.

Ⅱ. 사이버작전의 유형과 수단

사이버전쟁을 이해하기 위해서는 우선 기본적인 작전의 유형이나 공격수단의 분류를 이해할 필요도 있다. 스테판 월트(Walt 2010)는 사이버전은 사이버전투(cyber-warfare)라는 하나의 이름으로 이해하기보다는 적의 능력을 약화시키기 위한 네트워크 침투, 사이버범죄, 사이버 첩보행위 등 보다 구체적이고 세부적인 개념들을 통해서 살펴볼 필요가 있다고 강조했었다. 그 이후 우크라이나 전쟁과 같은 구체적인 사이버전 사례를 분석하는 과정에서, 사이버작전의 주요한 유형으로 사이버 첩보(cyber espionage), 사이버 방해(cyber disruption), 사이버 성능저하(cyber

degrade)의 구분이 자리를 잡아가는 것으로 보인다(Valeriano and Maness 2014). 각각의 의미를 설명하면, 사이버 첩보는 상대방을 혼동시키거나 협상지형을 변화시키기 위해 정보를 탈취하는 것을 의미하며, 여기에는 정보탈취, 시스템 침투, 암호 수집, 데이터 조작 등의 방법이 동원된다. 다음으로 사이버 방해는 저비용/저이득의 사이버작전 형태로서 적대국을 조사하고 확전위험을 알게 하려는 의도에서 이루어진다. 사이버 방해에는 일반적으로 간단한 디도스 공격이나 웹사이트 변조 또는 다른 기본적인 사이버 작전수단들이 사용된다. 작전 유형 중에서 마지막으로는 사이버 성능저하를 꼽을 수 있는데, 이는 적대세력의 네트워크, 운영사업자 및 시스템을 파괴(sabotage)하는 것으로서 가장 강압적인 유형의 선택지라고 할 수 있다.

아울러, 사이버 공격수단은 웹사이트 변조, 디도스 공격, 침범(intrusion), 침투(infiltration) 등의 구분으로 나누어져 왔다(Valeriano and Maness 2013, 353-355). 우선, 웹사이트 변조 혹은 반달리즘(Vandalism)은 해커들이 구조화된 쿼리 언어(SQL: Structured Query Language) 주입 혹은 사이트간 스크립팅(cross-site scripting)을 통해서 피해사이트를 변조하거나 파괴하는 것을 의미한다. 이러한 공격은 물리적 피해를 입히지는 않지만, 사회적 혼란을 야기하거나 정부에 대한 국민들의 믿음을 약화시키는 데에는 효과가 있다. 두 번째로, 디도스 공격은 북한의 사이버공격으로 우리에게도 익히 잘 알려져 있는 것이다. 디도스 공격은 특정한 사이트나 서버 혹은 라우터에 감당할 수 없는 데이터요청을 보내고, 해당 사이트나 서버가 기능할 수 없게 한다. 이러한 공격에는 봇넷이나 좀비 PC가 많이 사용된다. 다음으로, 침범은 트로이목마와 트랩도어(trapdoor)[1] 혹은 백도어(backdoor)를 포함하는 것으로 보다 높은 수준의 사이버 공격수단이다. 한번 침범이 되면, 프로그램에 들어 있던 트랩도어나 트로이목마를 통해 외부자의 접속이 계속 허용된다. 이러한 공격은 보안 네트워크에서 민감한 정보를 탈취하는 데 많이 사용된다. 네 번째로, 침투는 전쟁행위로 간주될 수 있는 사이버공격에 해당하는 것으로서, 침범의 경우에 비해 보다 정교한 공격이며, 목표 네트워크를 공격하는 데에도 논리폭탄, 바이러스, 웜, 패킷 침입자(packet sniffer), 키스트로크 로깅(keystroke logging)[2] 등 5가지 방식에 의한 공격을 통칭한다.

다만, 사이버 전쟁의 이해는 이러한 단순한 사실을 이해하는 수준을 넘어 사이버전이라는 새로운 현상이 인류활동의 무시하지 못할 부분인 전쟁이라는 영역에 어떠한 변화를 불러일으킬 것인가에 대한 전문가들의 논쟁이나 사회적 시각, 담론을 이해하는 데까지 나아갈 필요가 있다. 사이버전은 기술의 발전에 따라서 새로운 양상을 끊임없이 보이게 될 것이고, 새로운 양상이 등장하면 그것을 분석하기 위해서 새로운 유형과 용어가 만들어지게 될 것이기 때문이다. 따라서 정치학 또는 국제정치학적인 관점에서는 사이버전에 대해서 어떠한 질문들이 존재하는지에 대해 관심을 기울이는 것이 보다 지속적인 가치가 있는 작업일 것으로 생각된다. 이러한 관점에서, 사이버전의 전체 전쟁에 대한 결정성, 재래식 전쟁과 사이버전의 관계, 국가간의 세력관계에 사이버전의 등장이 미치는 의미에 대해서 전개되어 온 학계의 논의를 소개한다. 물론, 국가와 사회의 디지털화가 나날이 심화되고 있기 때문에, 이후에 논의될 문제에 대한 답들도 고정되어 있는 것이기는 어렵다.

Ⅲ. 사이버전 이해의 쟁점

1) 트랩도어는 사이버공격의 주체가 별도로 조작하지 않아도 미리 입력되어 있는 날짜부터 자동한다.
2) 키보드에 입력한 사항을 모두 키스트로크에 기록하여 사용자의 정보를 빼내는 사이버 공격방식이다.

1. 재래식 전쟁과 관계

이어서는 사이버전은 전체 전쟁의 승패에 대해서 독립적으로 영향을 미치기보다 다른 전장과 결합되어야 의미있는 영향을 미칠 수 있다는 논의들이 존재한다. 이러한 논의는 사이버공간의 공방균형(offence-defence balance)는 재래식 전쟁에 미치는 영향을 통해서 군사적 안정성 혹은 불안정성에 의미있는 요소가 된다는 견해들과도 연결될 수 있다.

1) 부속성/비독립성

사이버전이 기존의 전쟁이나 충돌양식과 구별되는 특징은 사이버공격에 의한 피해가 일시적이고, 상대국의 행동에 영향을 미치기 한 위협으로 활용되더라도 상대국의 굴복이나 타협을 유도하는 효과를 거두기 어렵다는 데 있다(Gartzke 2013, 57-60). 그런데 이점 때문에 사이버전은 재래식 전쟁이나 재래식 위협과 결합되어야 국제정치의 수단이 될 수 있다는 특성을 갖게 된다고 논의된다. 사이버공격의 준비와 실행에 투입되는 비용은 막대할 수 있지만, 대부분의 사이버공격에 의한 피해는 일종의 '소프트 킬(soft kill)'로서 금방 복구될 것이다. 이 때문에, 사이버전이 정치적으로 의미있는 군사행동으로서 목적을 달성하려면, 사이버전 행위는 재래식 전쟁에 기여하는 것이 되어야 한다. 그래야 장기적인 국가간의 세력균형에 영향을 줄 수 있다는 것이다. 뿐만아니라 위협으로 기능하기 위해서도 재래식 위협과 결합되어야 할 필요가 있다. 표적국가가 사이버공격을 막기도 어렵지만, 그것이 실행되어도 표적국가가 굴복하게 할 만큼 큰 피해를 주지 못하기 때문이다. 사이버전이 전쟁 혹은 분쟁의 맥락에서 의미있는 요소가 되기 위해서는 그것이 재래식 전쟁 영역의 능력 및 행동들과 결합된 것이어야 하는 이유이다.

참고로, 사이버전은 종래의 재래식 전쟁과 결합되어야 한다는 위 내용의 연장선에서 볼 때, 사이버전 영역의 공방균형은 재래식 전쟁에 영향을 미친다. 특기한 것은 사이버전 영역에서 공격자가 유리한가, 방어자가 유리한가를 따보았을 때, 그 결과가 재래식 전쟁의 균형에 대해서 정반대의 영향을 준다는 것이다. 사이버공간의 군사활동에 대한 기여가 디지털화된 지휘통제체계를 통해 재래식 군사력 세계의 공격우위를 확대시키는 것이라면, 사이버공간에서 방어가 유리하다는 의미는 첨단지휘통제체계를 갖춘 공격자의 우위가 보다 공고하다는 의미가 된다. 실제로 2022년 이후 우크라이나 전쟁에서는, 민간영역의 혁신, 국제적 조율, 국가들의 사이버전 교리의 정비로 사이버 영역은 방어우위 전장으로서의 면모를 보여주었다(Mueller 2023, 9-10). 이는 우크라이나 전쟁 전반에 대해서도 주는 함의가 있을 것이다.[3] 덧붙여, 역으로 사이버 공간이 공격이 보다 유리한 곳이라면, 오히려 지상분쟁은 안정화될 수 있다(Gartzke 2013, 66-68). 사이버 수단으로 침공국가의 사이버지휘통제능력이 쉽게 공격될 수 있기 때문에, 방어자가 보다 유리한 구조하에서 전쟁이 전개될 수 있기 때문이다.

2) 차별성/독립성

다른 한편, 사이버전은 재래식 전쟁의 승리와 별개로 여론조작과 혼란 유발이라는 또다른 전쟁에서 중심적인 기능을 하고 있다는 지적도 있다(Rid 2020; Mueller 2023). 우크라이나에 대한 지지를 약화하는 데에는 사이버전이 중점적으로 이루어지고 있다는 것이다. 그러한 사이버전

3) 우크라이나전쟁은 공격자에게 유리한 전쟁일 수도 있다.

양상은 '네러티브전(Narrative War)'이라는 이름으로 주목받고 있다. 이러한 사이버전의 효과에 대한 관심은 코소보전쟁에서부터 디도스 공격과 이메일 등 국제여론전이 처음으로 등장한 코소보 전쟁으로까지 거슬러 올라갈 수 있고, 그 이후의 전쟁들에서도 전쟁수행의지 약화를 위한 사이버전은 수행되어 왔었다. 대규모 사이버 공격이 이루어진 사례가 아니더라도, 국제분쟁이 발생할 때마다 관련국에서는 SNS를 이용한 사이버전이 치열하게 전개된다. 가짜뉴스 등에 의한 여론조작전이 극심해짐에 따라, 우크라이나 전쟁 발발 이후 유럽국가들을 중심으로 FIMI(Foreign Information Manipulation and Interference) 문제에 대한 관심이 증가해왔다.

덧붙여, 사이버 첩보행위는 전쟁이 아닌 시기에도 활발 전개된다. 우크라이나 전쟁 이전인 2000년부터 2020년까지 러시아의 우크라이나에 대한 사이버공격의 46.4%가 사이버 첩보일만큼 사이버첩보는 지배적인 사이버 공격의 양상이었다(Valeriano 2023). 역설적으로, 잠재적인 적대세력에 대한 사이버 첩보능력 확대가 오히려 국가들의 군사적 행위를 감소시킬 수 가능성이 있다는 주장도 있다(Gartzke 2013, 70-71). 사이버수단은 잠재적인 적에 대한 첨보능력을 강화시켜주는 효과가 있기 때문에, 국가들의 비밀유지를 더욱더 어렵게 하고 있다. 위키리크스 사건은 이를 실증해주었다. 그 결과로 국가들은 기습공격에 필요한 기밀유지가 보다 어려워지고 있다는 점을 인식하고 있다. 이로부터 이론적으로는 그로 인해 군사적 공격의 유인은 줄어들고 협상을 택할 가능성도 커질 수 있다는 함의도 이끌어낼 수 있다.

2. 승리와 강압의 효과

사이버전 가운데에는 목표국가의 핵심인프라를 파괴하거나 마비시킬 수 있는 유형의 공격도 존재한다. 2007년 에스토니아의 통신 및 전력 인프라에 대한 친러세력의 공격에서 처음으로 현실화되었다. 이후 사이버전쟁은 임박하고 실제적인 위협으로 다루어져갔다(Lynn III 2010). 오늘날 현실 정책결정자들도 기습적인 사이버 공격으로 인한 대규모 혼란을 우려하고 있다. 그러한 논의의 결과로 사이버영역은 지상, 공중, 해상, 우주와 더불어 주요 전장의 하나로 이해되기 시작했고, 사이버영역을 동등한 전장의 하나로 보아야 한다는 시각은 다영역작전 개념에서 보듯이 구체적인 군사정책으로도 투영되었다. 그럼에도 불구하고, 사이버전의 실제 효과를 검토할 때, 사이버공격은 전쟁의 승패나 국가간 분쟁의 진로에 영향을 줄만한 결정적인 영향을 갖지 못한다는 견해와, 아직 안 드러났을 뿐 결정적인 사이버 공격의 위험은 존재하고 있다는 견해는 교차하고 있다.

1) 부족한 결정력

우선, 사이버공격은 자체로서 전쟁수단이 되기는 어렵다는 주장이 등장해왔다(Gartzke 2013). 사이버전의 개념이 정책화되기 시작하여 주요국가들이 사이버안보전략을 제시하기 시작했던 배경에서, 사이버전이 야기할 수 있는 국가적 피해에 대한 이해가 과장되어 있다는 지적에서 2010년대 초에 이러한 주장이 제기되었던 것이다. 전쟁은 상대방의 영토를 지배하기 위한 점령, 혹은 일방의 의지를 타방에게 강요하기 위한 강압을 위해서 수행되는 것이다. 그런데 첫째 문제인 점령을 위해서는 지상군의 역할이 핵심적인 것이고 사이버공격으로 달성할 수 있는 것이 거의 없을 수도 있다. 이러한 의견은 2022년 우크라이나 전쟁에 대한 여러 전문가들의 분석에도

나타났었다. 이들은 우크라이나 전쟁에서 러시아는 '썬더 런' 전략을 통한 사이버공격으로 우크라이나에게 막대한 피해를 줄 것이라고 예상했지만, 실제 사이버전은 그만한 피해를 우크라이나에게 주지 못했다고 이야기한다(Mueller 2023, 7-9). 다음으로, 강압을 위해서 사이버공격이 의미가 있다고 하기에도 사이버 공격이 남기는 피해가 일시적이고 짧은 시간 내에 복구가능한 것에 해당한다는 점에서 사이버 공격은 강압을 달성할 수 있는 수단이 되기도 어려울 수 있다. 냉전기에 보여진 다양한 사례에서와 같이, 위협이 효과적이기 위해서는 상대방에게 장기적이고 지속적인 피해를 입힐 것이라는 내용을 갖고 있어야 하지만, 사이버 공격의 위협은 단기회복이 가능한 위협을 입히겠다고 하는 것에 해당한다는 것이다. 따라서 사이버 공격은 강압에 필요한 위협을 제공해주기 어렵다. 오히려 사이버 공격 위협은 해당국에게는 사이버공격에 대해 경각심을 갖게 하고 오히려 위협국가에 대해 더욱 적대감을 갖게 한다.

이처럼 사이버공격이 전쟁이나 국가분쟁 해결에 결정적인 수단이 될 수 있느냐에 대해 회의적인 이들은 냉전기에 미국과 소련이 핵능력이 있다는 사실만으로 핵전쟁이 일어나지 않았다는 데 주목한다. 국가의 행동을 예측하는 데에는 특정한 행위자 정치적 목적을 이루는 데 도움이 되느냐는 질문이 중요하다는 관점에서는, 사이버전 행위가 기존의 물리전을 대체하기는 어렵다는 주장이 힘을 받는다.

2) 파괴적 결정성

한편, 러시아가 우크라이나 전쟁에서 우크라이나의 사이버방어만이 아니라 국제적인 사이버보안체계 앞에서 인상적인 사이버 공격을 보여주지 못했더라도, 러시아를 포함해 사이버강국들이 치명적인 사이버공격을 준비하고 실행할 가능성은 여전하다는 의견들이 있다(Mueller 2023, 10-11). 우크라이나전쟁에서도 개전 초기 러시아는 우크라이나의 지휘통제를 방해하기 위해 사이버공격을 가했다. 우크라이나 전쟁 중인 2023년에도 러시아는 우크라이나의 군사정보 및 표적 융합 소프트웨어인 델타를 공격하고 있다. 뿐만아니라, 러시아는 우크라이나를 지지하는 나라들에 말웨어 배포하고 있는 것으로 알려져 있다. 이러한 관찰에 이어서 특히 주목해볼만한 치명적인 사이버 무기의 등장 가능성은 러시아도 이미 정교한 사이버 공격도구를 개발하고 있는 것으로 보인다는 여러 분석들에서 찾아진다. 그것은 스턱스넷과 유사하게 산업용 제어 프로그램을 공격할 것으로 추정되고 있다. 그러한 무기의 개발은 표적국가의 핵심인프라를 사보타주하기 위한 러시아의 SOPKVO 혹은 SODCIT (Strategic Operation for the Destruction on Critically Important Targets) 개념에 따른 것이기도 하다. SODCIT는 상대국이 군사행동을 지속할 수 없을 정도로 타격을 주는 것을 목표로 하는 것으로 알려져 있다(Kofman et al. 2021. 68). 아직 러시아가 이러한 사이버 공격수단을 쓰지 않는 이유는 사이버 방어가 강하거나 러시아의 공격력이 약해가 아니라 러시아와 같은 나라들이 향후의 필요를 위해 그것들을 아껴두기 때문이라는 해석도 있다. 우크라이나의 핵심인프라를 파괴하는 데 사이버무기를 쓰기보다 순항미사일을 대신 사용하고 있다는 것이다. 이러한 견해에 따르면 사이버공격은 전쟁승패에 결정적인 역할을 할 가능성을 여전히 지니고 있으며, 그러한 역할은 증명될 때를 기다리고 있을 뿐이다.

1. 국제 세력관계에 대한 영향

아울러, 사이버전은 약자의 무기로 이해되기도 하지만, 오히려 재래식 우위를 가진 강대국에게

진정한 효과를 가지는 수단이라는 이견도 있다. 아래에서는 이러한 논의의 흐름을 살펴보도록 한다.

1) 약소국의 무기

사이버전에 있어서는 초강대국이 오히려 취약하고 비대칭적인 사이버 공격으로 약소국이나 민간집단들이 큰 이익을 볼 수 있게 되었다는 주장이 제기되어 왔다. 사이버전의 개념이 대중화되고 확산되던 2000년대 초부터 이러한 주장은 나타났다(Adams 2001). 탈냉전 이후에는 일반적 군사력으로는 미국에 도전할 수 없는 상황이 만들어졌기 때문에, 일부 적대적인 국가들은 사이버전을 통한 비대칭전을 추구하게 되었다는 진단이었다. 그리고 군사혁명과 더불어 미국의 군사력이 더더욱 디지털 정보기술에 기초하게 되었기 때문에, 미국에 대한 사이버전의 효과는 더욱 확대되었다. 뿐만아니라 사이버공격은 공공영역만이 아니라 사이버보안이 취약한 민간영역에 대해서까지 가해질 수 있다. 이른 시기부터 가장 극단적으로 이러한 우려를 현실적으로 만들어준 것은, 1997년에 실시된 적합한 수신기(Eligible Receiver)라는 훈련이었는데, 이 훈련에서 35명의 해커들은 미국 여러 도시의 전력망에 침투, 911 시스템을 손쉽게 해킹했다. 유사시 북한의 해커도 미국에 사이버 혼란을 야기할 수 있다는 우려를 간접적으로 증명했다.

실제로 2009년 이후 북한이 한국에 대한 사이버전을 본격화하면서, 국내에서도 사이버전은 북한의 비대칭 무기로서 이해되어 왔다. 한국에서도, 2010년대 초반~중반에 이르러 국방연구 분야에서도 북한이 핵과 사이버공격 등 한미동맹과 다른 작전방식으로 한미동맹의 취약점을 이용하고 한미동맹의 강점을 약화시키는 비대칭 전략을 추구한다는 시각은 널리 받아들여지게 되었다(노훈 2013). 그런데 비대칭전의 개념 자체는 이 전략을 구하는 국가가 정면승부로는 승리를 기대하기 어려운 작은 나라라는 것을 전제한다. 비대칭전이라는 개념 자체가 약소국이 강대국에 대처하는 전쟁의 경우에 적용되는 것이기 때문이다. 물론 북한은 핵무기라는 폭력수단을 지니고 있기 때문에, 일방적인 약자라고 보기는 어려울 수 있다. 핵과 사이버가 결합되어 있고 사이버 공격이 핵위협 증대를 시사하는 것일 수 있기 때문에 사이버전이 우리에게 위협이 되는 것이다.

2) 강대국의 무기

반면, 사이버전은 재래식 능력이 우세한 국가에게 강점을 확대시켜주는 수단이 된다고 보는 시각도 있다. 현대전의 시작인 제2차 세계대전 시기 독일의 전격전에서 보듯이, 독일공군의 스투가 전투기 폭격도 독일이 재래식 군사력 상 우세할 때나 군사적, 전략적 효과가 있었고, 재래식 우위를 상실한 이후에는 스투카 폭격으로 얻고자 한 테러효과는 소모적인 것이 되었다(Gartzke 2013). 사이버전도 이와 유사하게 독립적으로는 그로부터 얻을 수 있는 테러효과나 전략적인 효과를 기대하기 어려울 수 있다는 논리에서, 결국 사이버전 외의 지해공 및 우주 전장에서 우세를 가질 수 있는 국가에게나 사이버전이 강압외교나 전쟁수행의 수단이 될 수 있다.

이러한 관점에서는, 강대국 혹은 군사강국이 약소국을 공격할 때에나 사이버전이 매력적인 수단이 된다. 사이버공격이 물리적인 공격에 앞서 공격기회를 만드는 데 도움이 될 때, 사이버전은 국가간의 세력관계를 변화시키는 데 기여할 수 있다. 강압을 위해 상대국에 영향력을 행사하려는 때도 동일하게 재래식 위협이 뒷받침되지 않으면, 사이버 공격은 상대국의 적의만 강화시키는 결과를 낳는다. 아울러, 사이버무기는 보안시스템의 취약성이 방치된 일정한 시기 동안만[4] 공격능

력이 있다는 점에서 결국 '부패성' 무기이므로, 군사적 강압이나 억제에 모두 쓰이기 어려운 속성도 있다.

Ⅳ. 사이버전의 사례

앞에서 사이버전에 관련된 기본적인 개념과 사이버전이라는 현상을 이해하는 데 관련된 쟁점을 살펴본 바탕에서, 이 장에서는 주요한 사이버전 사례를 제시한다. 현재까지 사이버전의 발전 과정과 앞으로의 발전 전망을 정을 생각해보기 위해서이다.

1. 우크라이나 전쟁 이전 사례

1) 에스토니아에 대한 사이버공격 사례

에스토니아 정부는 2007년 4월에 수도인 탈린 중심에 있던 소련군 청동동상의 이전을 추진했고, 이에 러시아계 주민들은 반대시위를 진행했다. 이러한 배경에서 러시아는 에스토니아의 대통령궁, 의회, 언론사, 은행 등 주요 기관의 홈페이지와 전산망을 봇넷을 통한 디도스 공격으로 마비시켰다(Pamment at el 2019). 디도스 공격으로 평상시보다 수백배의 트래픽이 발생하면서, 이들 웹사이트만이 아니라 에스토니아 전체의 네트워크가 정상 기능하지 못했다. 이 사이버 공격에 노출된 웹사이트와 네트워크를 복구하는 데 보름 가량이 필요했다. 그로 인해 수천만불의 경제적 피해도 발생한 것으로 집계되었다. 에스토니아는 2005년에 이미 온라인 투표를 도입하는 등 디지털화가 상당히 진전된 나라였기 때문에, 사이버 공격으로 인한 피해도 더욱 컸다. 디도스 공격에 동원된 봇넷의 IP를 분석한 결과에 따라, 나토는 러시아를 배후로 지목했다. 그러나 구체적인 제재는 이루어지지 못했고, NATO는 사이버방위센터(CCDCOE)를 창설하며 사이버방어태세 강화를 택했다.

2) 그루지아전쟁 시 사이버공격

러시아는 2008년에도 사이버공격을 수행했다(White 2018). 조지아로부터 독립을 요구하는 남오세티아가 조지아를 침공하자, 러시아가 남오세티아를 보호하기 위해 개입했다. 그 결과 그루지아 전쟁이 발생했다. 그루지아 전쟁 당시 러시아와 그루지아군 간의 실제 군사적 충돌은 일주일 내에 마무리되었다. 러시아의 개입 직후 러시아 국영통신사 웹사이트가 몇시간 가량 마비되었는데, 이에 러시아의 사이버 반격이 개시되었다. 그루지아의 대통령실, 국회, 국영은행 등 45개 사이트가 마비되었고, 이때 친러시아측의 디도스 공격은 평균 2시간 15분, 길게는 6시간 지속된 것으로 알려져 있다. 그루지아 인터넷 네트워크의 35%가 정상적으로 기능하지 못했다. 러시아의 조지아에 대한 디도스 공격과 웹사이트 조작 공격은 러시아군의 재래식 군사작전과 동기화되어 진행되었다. 이 시기의 사이버전은 군사적 승리에 결정적인 기여한 수준의 결과는 낫지 못했지만, 이를 계기로 러시아군은 심리조직이나 정보전 수단으로 사이버전을 주목하게 된 것으로 알려진다.

---

4) 이는 해당 취약성을 해결한 보안조치가 이루어질 때까지의 기간을 의미함.

3) 이란에 대한 스턱스넷 사이버공격 사례

이는 2010년 이란에 대해 이루어진 사이버 공격 사례이다. 스턱스넷 악성코드는 산업용 장비 제어에 많이 쓰이는 독일제 스카다(SCADA) 소프트웨어를 공격하도록 제작되었다. 스턱스넷 코드는 USB로 전파되도록 설계되었다. 2007년 11월부터 스턱스넷 공격이 개시된되었다는 보도도 존재한다(Finkle 2013). 이란 핵시설 내의 우라늄가스 원심분리기의 스카다 제어 프로그램을 공격하기 위한 악성코드로 추정된다. 스턱스넷에 감염된 컴퓨터의 상당수가 이란에 있다는 점으로 미루어보아도, 스턱스넷의 공격대상이 이란 시설임을 짐작할 수 있다. 이란 핵시설 내의 원심분리기 상당수가, 약 수백대 가량이 스턱스넷 공격으로 고장난 것으로 생각되고 있다. 미국과 이란이 이 공격의 배후라는 의혹이 제기되었다.

4) 우크라이나에 대한 사이버공격 사례(2014~2015)

러시아는 우크라이나 침공 이전에도 우크라이나에 대한 사이버 공격을 감행해왔기에, 러시아의 침공가능성이 불거지면서 우크라이나에 대한 사이버 공격 우려도 확대되었다. 친러시아 해커집단들은 러시아의 크림반도 합병 이후에 열린 우크라이나 대선(2014. 5. 25) 직전에 선거관리위원회의 컴퓨터를 해킹하여 악성코드를 통한 결과조작을 시도한 바 있으며, 1년여 뒤인 2015년 12월에는 우크라이나 서부의 전력회사들에 대한 해킹에 - 우크라이나 대선 시와 달리 - 성공했다. 이러한 전력(前歷)으로 러시아는 사이버 공격에 매우 능한 국가로 여겨져왔다. 그리고 게라시모프 독트린으로 알려진 최근 러시아의 군사교리 상 러시아군은 상대방의 저항의지를 약하게 하고 정치적 분열과 사회적 혼란을 조장하기 위해 사이버 공격을 적극적으로 활용할 것으로 전망되어 왔다.[5] 이점에서, 우크라이나 침공이 개시되었을 때, 우크라이나 전쟁은 본격적인 사이버 전쟁의 첫 사례를 보여줄 것으로서 주목을 받았다(Miller 2022).

2. 우크라이나 전쟁(2022~2023)[6]

우크라이나에 대한 사이버 공격은 러시아의 침공과 함께 시작된 것이 아니라, 그에 앞선 시점에서, 2022년 들어 나타나기 시작했다.[7] 2018년 7월의 우크라이나 정수시설에 대한 해킹 이후 3년여 만에 재개된 우크라이나에 대한 적대적 사이버 공격은 2022년 1월 13일의 멀웨어(Malware) 공격이었다. 우크라이나 정부 및 비영리 단체, IT 기업들에 침투한 멀웨어는 감염된 장치들의 미작동을 초래하는 기능을 지녔었다.[8] 1월 14~15일에도 이루어진 우크라이나에 대한

5) 게라시모프 독트린은 전쟁과 평화상태를 명확하게 구분하기 어려운 현대전의 특성 상 비군사적 수단의 역할이 더욱 큰 역할을 하게 되었다는 진단에 바탕하여, 러시아군이 군사적 능력만이 아니라 비군사적 능력을 광범위하게 구축해야 한다는 점을 강조한다. 이에 따라서 게라시모프는 개전 초기 및 긴장고조 단계에서 비군사적 조치에 보다 무게를 두어야 한다고 보았다(김경순 2018, 70-72, 85).

6) 본 소절의 내용은 필자의 워킹페이퍼(이중구 2022)를 수정, 보완하여 작성하였다.

7) 사이버 공격은 공격자를 특정하는 데 수개월 이상의 시간이 소요되므로, 우크라이나에 대한 적대적 사이버 공격들이 곧 러시아에 의해 이루어진 것이라고 현 시점에서 단정하기는 어렵다. 그럼에도 불구하고, 우크라이나에 대한 적대적인 사이버 공격은 러시아의 이익에 부합하는 것이라는 점에서 그것이 러시아를 지지하는 세력에 의해 이루어진 것이라고 보는 데에는 무리가 없을 것이다. 따라서 이 글에서는 러시아의 사이버 공격을 이해하기 위해 우크라이나에 대한 적대적인 사이버 공격을 논의의 대상으로 삼는다.

8) 이 글에서 소개되는 우크라이나에 대한 적대적인 사이버 공격 사례는 다음을 참조하였다. “UKRAINE: Timeline of

사이버 공격은 우크라이나의 내각, 에너지부, 체육부, 농업부, 보훈부, 환경부 등 정부 웹사이트를 훼손하는 것이었다.[9] 이어 한달 뒤인 2월 15일부터 16일 사이에는 우크라이나의 여러 웹사이트를 광범위하게 공격하는 사이버 공격이 발생했는데, 그 배후는 러시아로 추정되었다. 미국의 백악관도 이 사이버 공격의 배후로 러시아군 정보기관인 총정찰국(GRU)를 지목했기 때문에, 이러한 주장에 무게가 더해졌다(이상우 2022). 2월 15~16일 디도스(DDOS) 공격은 우크라이나에 대한 사이버 공격 중 최대규모의 것이었다. 아울러, 2월 15일에는 우크라이나의 현금인출기가 작동하지 않는다는 잘못된 정보가 은행고객들에게 유포되는 스팸공격이 발생하기도 했다.

또한, 러시아군의 군사작전 개시 직전에도 우크라이나에 대한 사이버 공격이 발생했다. 푸틴 대통령이 작전승인을 내리기 직전인 2월 23일에 러시아발로 추정되는 디도스 공격으로 우크라이나 정부의 웹사이트 대부분에 대한 접속장애가 발생했다. 비록 대부분의 접속장애는 2시간 내에 해소되었지만 말이다. 같은 날, 데이터 삭제를 초래하는 멀웨어인 'HermeticWiper'에 의한 우크라이나 여러 기관에 대한 사이버 공격도 동시에 발생했다. 공격 당일에 약 6주 전부터 유포된 멀웨어를 활성화하는 방식으로 이루어진 것으로 추정된다.

우크라이나에 대한 적대적 사이버 공격이 가장 왕성했던 시기는 러시아의 침공 당일과 그 바로 다음날이었다. 침공 당일인 2월 24일에는 4건의 사이버 공격이 발생했고, 다음날인 2월 25일에는 3건이 이루어졌다. 그 이후에도 2월 27일과 4일 후인 2월 28일에 각각 1건의 사이버 공격이 탐지되었다. 구체적으로, 러시아의 침공 당일인 2월 24일에는 키예프 포스트(The Kyiv Post) 등 언론사 웹사이트가 디도스 공격을 받은 것은 물론, 그와 동시에 우크라이나의 정부 네트워크도 멀웨어(IsaacWiper) 공격을 받았고, 같은 날 우크라이나 난민 사태에 관여하는 다른 유럽국가들의 정부 직원들 역시 멀웨어 유포를 위한 피싱공격에도 노출되었다. 뿐만아니라, 유럽지역에 인터넷 서비스를 제공하는 통신위성 'KA-SAT'도 2월 24일 사이버 공격을 받아, 우크라이나만이 아니라 다른 유럽지역 및 중동지역의 통신서비스가 부분적으로 중단되었다. 다음날인, 2월 25일에도 각종 사이버 공격이 다양한 분야에서 진행되었다. 우크라이나의 국경통제소에 대해 데이터 삭제 공격이 이루어져 루마니아로의 난민 입국이 지연되기도 했고, 우크라이나의 여러 대학 웹사이트도 사이보 공격을 받았으며, 페이스북, 트위터, 인스타그램, 유투브, 텔레그램, 오드노클라스니키(Odnoklassniki), VK 등에서 가짜 인물 계정을 통한 허위정보 확산 시도도 탐지되었다(Meta 2022). 그 이후에도 2월 말까지 우크라이나에 적대적인 사이버 공격은 이어졌다. 2월 27일에는 우크라이나의 유명인사들의 개인계정을 도용하여 허위정보 게시하려는 해킹 사건들이 탐지되었으며, 2월 28일에는 우크라이나의 금융, 농업, 에너지 분야의 디지털 인프라에 걸쳐, 'HermeticWiper' 멀웨어 공격이 시도되었다. 이 디지털 인프라들의 개인정보와 공공데이터를 절취하기 위한 것이었다.

우크라이나와 러시아 간의 대화가 논의되기 시작한 3월 초에도, 우크라이나에 대한 사이버 공격은 낮은 빈도이지만 지속되었다. 3월 4일에는 자선단체, NGO 및 기타 원조기관에 대한 멀웨어 공격이 아마존에 의해 감지되었고(Amazon Staff 2022), 3월 5일에는 우크라이나의 일반 시민들에 대한 피싱공격이, 3월 9일에는 이동통신업체(Triolan社)에 대한 디도스 공격이 발생했다. 해당 업체의 서비스가 12시간 가량 중단되었다(Moss 2922). 가장 최근의 것으로는 3월 14일에 발생한, 우크라이나에서 'CaddyWiper'라는 새로운 데이터 삭제 멀웨어에 의한 사이버 공격이 있다. 이어 3월 16일 우크라이나 24 방송국 홈페이지가 해킹되어 젤렌스키의 투항 보도와

Cyberattacks on critical infrastructure and civilian objects," 출처: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/ (검색일: 2022년 3월 15일).

9) 이는 벨로루시와 연계된 APT 해킹그룹의 소행으로 여겨졌다.

같은 거짓보도가 이루어졌으며, 3월 28일에는 우크르텔레콤(Ukrtelecom)과 워드프레스에 15시간 동안의 대규모 디도스 공격이 가해졌다(Moss 2022). 그 이후에는 러시아의 강력한 사이버 공세는 두드러지지 않았다. 러시아의 사이버 공격은 우크라이나 시민 및 정부관계자의 개인식별정보 탈취와 공공데이터 유출을 위한 말웨어 공격을 위주로 한 양상을 보였던 것이다. 2022년 후반에 들어서도 러시아의 우크라이나에 대한 사이버 공격은 저비용, 저효과의 사이버 방해 작전 위주로 이루어지는 양상을 계속 보였다(송태은 2022).

Ⅴ. 사이버전 이해의 쟁점으로 본 사이버전 사례의 함의

1. 우크라이나 전쟁 이전 사례

일반적으로, 우크라이나 이전에 이루어진 미국과 러시아 등 주요국들의 사이버 작전에 대한 평가는 사이버전은 전술 차원에서도 저강도의 정보작전을 위주로 했으며 사회적 혼란을 조성하는 데 주된 목적이 있었고, 작전 차원에서도 강압외교 수단으로 결정적 역할은 보이지 못했다는 것이었다. 의외로 사이버전은 강대국에게 유리한 무기로 작용해왔다. 아래에서는 우크라이나 이전 사이버전 사례들이 주는 함의를 사이버전과 재래식 전쟁과의 관계, 사이버전이 가질 수 있는 승리와 강압의 효과, 강대국/약소국의 사이버전 활용 이점 등의 범주에서 살펴보고자 한다.

우선, 우크라이나 전쟁 사이버작전은 재래식 군사력 위협과 결합되기보다는, 평시 회색지대 분쟁에서 독립적으로 혼란조성을 위해 전개되었고, 무력충돌 사태에서도 여론전 및 심리전을 위해 주로 활용되었다. 러시아의 대우크라이나 사이버공격 사례에 있어, 사이버 공격은 상대국에게 실질적인 피해를 주는 성능저하(degrade)보다는 정보작전을 지원하는 수단으로서 적극적으로 활용되어왔다. 파괴보다는 상대국의 취약점을 찾기 위한 사이버 정탐(cyber espionage)과 저비용 공격으로 낮은 수준의 피해를 가하는 방해(disruption)을 위주로 하여, 러시아의 사이버 공격이 이루어져왔다는 것이다. 뮬러(Mueller 2023, 6) 등은 2000~2020년 사이에 이루어진 러시아의 우크라이나에 대한 사이버 작전을 분석한 결과, 전체의 29%만이 성능저하를 위한 공격이었다고 지적했다. 물론, 사이버 작전은 재래식 전쟁과 동시에 이루어졌을 때에는 혼란 조성을 통해 승리를 지원하는 기능을 맡았다. 이러한 특성은 그루지아 전쟁에서 보여졌었다.[10)]

다음으로, 우크라이나 전쟁 이전 사례에서 사이버 작전은 강압에 뚜렷한 효과를 보여주지는 못했다. 사이버 공격으로 인한 피해의 수준이 매우 높지는 않기 때문에, 사이버 공격만으로 분쟁의 원인이 된 정치적 쟁점에 대한 상대국의 양보나 굴복이 이끌어내진 경우는 거의 없었다. 전술한 2010년대 중반 우크라이나와 에스토니아의 사례에서 모두 해당국들은 러시아의 사이버작전만으로 러시아와 타협을 선택하지 않았다.

끝으로, 사이버전은 우크라이나 전쟁 이전에도 강대국이 유리함을 가지는 수단으로서의 면모를 보였다. 러시아는 위에서 언급한 내용 중 에스토니아, 그루지아, 우크라이나 사례에서 약소국들에 대해 사이버전 수단을 활용했다. 미국 역시 스턱스 사례에서 비확산을 위해 이란의 우라늄농축장비의 고장 혹은 파괴를 모색한 바 있다.

2. 우크라이나 전쟁 사례

10) 덧붙여, 미국의 사이버 공격 사례는 많지 않지만 스턱스넷과 같이 성능저하를 모색하는 면모를 보여왔다.

기존의 평가를 배경으로, 우크라이나전쟁은 러시아와 같은 국가의 실제 사이버전략이 실행된 사례로서, 사이버전의 미래를 보여줄 것이라는 관점에서 주목을 받았왔다.[11] 따라서 우크라이나 전쟁의 사이버 공격 양상에 대한 평가는 사이버 전쟁의 미래를 이해하는 데 중요한 참고가 될 수밖에 없다.

먼저, 사이버 공격이 재래식 작전과 결합되는 양상이 우크라이나 전쟁에서 보여지기는 했지만, 아직 그러한 결합이 사이버작전의 주된 유형이 되지는 못했다고 할 수 있다. 즉, 우크라이나 전쟁에서 사이버전과 재래식 작전이 부분적으로 연계기는 했지만, 우크라이나 전쟁에서 러시아의 사이버 공격이 다영역 전투의 일환으로 수행되는 모습은 뚜렷하지 않았다. 우크라이나 개전 이후 6개월 간 이루어진 러시아의 사이버 공격을 분석했을 때 그 중 15%만이 다영역 전투와 관련되어 있었다는 분석이 존재한다(Valeriano 2023). 이에 더해 마이크로소프트는 다영역 작전의 일부로 보이는 조율된 사이버 작전은 6~7건밖에 파악하지 못했다는 보고서를 공개했다(Smith 2022). 이점에서, 우크라이나 전쟁에서 사이버전의 양상은 과거와 확연한 차이점을 보이지는 않았다. 결국, 기존 사이버전 사례에서 보여진 모습의 연장선에서, 전쟁 중에도 사이버수단들은 상대국 내부의 정치적인 분열과 사회적인 혼란을 야기하는 데 주되게 동원되어 갈 것으로 보인다(Mueller et al. 2023). 사이버 무기는 본격적인 전쟁 이전 상태에서 이루어지는 정치전에 분야에 효과적인 무기라는 점은 입증되어 왔고, 이러한 역할은 전쟁 중에 확대되었다. 뮬러 등은 우크라이나 전쟁 이전과 이후를 비교하면서, 우크라이나 전쟁 이전에는 러시아의 사이버 작전에서 사이버 정탐이 가장 큰 비중(46.4%)을 차지했다면, 우크라이나 전쟁 중에는 사이버 방해가 가장 큰 비중을 차지하는 작전의 자리(58%)를 차지하게 되었다고 지적했다.

또한, 우크라이나 전쟁에서도 사이버전으로 인한 충분한 강압효과는 덜 증명되었다. 앞서 일부 사이버전 전문가들은 전쟁 초기 러시아의 사이버전쟁은 소위 러시아의 “썬더 런(Thunder run)” 전략에 의한 것으로서, 사회혼란과 내부 혼선, 우크라이나 전쟁의 장기화를 막을 것으로 예측했었다. 그러나 사이버 공격은 우크라이나의 타협이나 양보를 가져올 만큼 심각한 피해를 주지 못했다는 것이 우크라이나 전쟁이 시작된지 1년 반이 지난 지금의 중론이다. 물론에 이에 대해서 일종의 소수의견이지만 반론도 존재한다. 침공 초기 러시아의 사이버전은 수시간 동안 우크라이나 정부와 군대의 중요 네트워크와 인터넷 서비스를 마비시켰으므로, 러시아의 사이버 공격은 우크라이나에 엄청난 군사적 손실을 초래하는 데 성공했다고 보아야 한다는 주장이다(Cattler and Black 2022). 또한 피해가 적은 이유로는 앞서 수년간 러시아의 사이버 공격에 노출되었던 우크라이나군의 사이버 방어 노력이 꼽히기도 한다. 우크라이나 침공 이후 우크라이나 지도자의 호소로 20만명의 IT부대가 조직되어 우크라이나 전쟁 개전 이후 우크라이나의 사이버 방어 노력이 크게 확대되었다. 뿐만아니라, 아마존과 페이스북과 같은 해외기업도 러시아의 사이버 공격에 대한 방어 노력을 공동으로 전개했다(Miller 2022).

끝으로, 사이버 작전은 강대국에게 유리한 무기로서 성격을 우크라이나 전쟁에서도 보여주었다. 우크라이나는 사이버 공격에 대해 기본적으로 방어자의 입장에 있었으며, 러시아가 재래식 공격의 성공확률을 높이고 우크라이나 혼란을 조성하기 위해 사이버 공격을 가했다. 재래식 군사

11) 기존 전문가들의 주요 관심사를 참고할 때, 전문가들이 관심을 가진 가설 혹은 이슈는 우크라이나 전쟁에서 사이버공격 빈도가 기존의 사례에서보다 증가할 것인지, 사이버공격의 피해에서 심각도가 증가할 것인지, 사이버 정찰이나 교란을 넘어서서 파괴적인 공격 양상을 주로 보여줄 것인지, 사이버공격이 상대국에 대한 제한적인 강압능력도 보여줄 수 있을지, 사이버 공격의 대상이 기존의 사례에서는 주로 민간대상이었다면 그 공격대상이 군사목표에 집중될 것인지, 다영역 작전의 증거가 증가할 것인지, 사이버 기반 정보작전도 증가되는 모습을 보일 것인지 등이었다(Valeriano and Maness 2012).

력 우위를 가진 러시아는 우크라이나 침공 직전에 우크라이나 정부 및 언론기관 웹사이트를 대거 공격하고 허위정보를 유포함으로써 재래식 군사활동이 야기할 공포와 혼란을 극대화하고자 했던 것이다.

Ⅵ. 맺음말

이글에서는 사이버전은 아직 발전 중인 과정에서 그를 둘러싼 여러 쟁점 속에서 파악하는 접근방식이 필요하다는 점을 강조했다. 사이버전에 대한 기술적인 분석은 사이버정찰, 방해, 성능저하 등 작전유형에 따라서 전쟁 기간 중 혹은 분쟁 기간 중 이루어진 사이버전의 특성을 분석하는 데 중점을 두고 있다. 이에 대비해서, 국제정치학적 관점에서 사이버전에 대한 관심은 그것이 결정적인 파괴수단으로 발전해갈지, 다영역전쟁의 한 영역으로서 혹은 국제여론전의 주된 영역으로서 발전해갈지, 약소국에게 유리한 무기인지 혹은 강대국에게 보다 결정적으로 활용될 수 있는 무기인지 등과 같은 전략적 쟁점에 놓여 있다. 궁극적으로 어떠한 방향으로 사이버전이 발전해갈지가 국방 사이버 정책의 방향에 심대한 영향을 주는 문제이기 때문이다.

우크라이나 전쟁서도 사이버전의 양상이 과거의 사례들과 확연하게 차이를 보이는 모습으로 나타났다고는 하기 어렵다. 개전 초기에는 우크라이나의 지휘통제체계를 마비시키고 혼란을 조성하기 위해 다수의 사이버공격이 동시다발적으로 이루어졌으나, 우크라이나도 오랜 갈등 뒤의 전쟁인만큼 러시아의 사이버공격에 무방비는 아니었다. 아울러, 다영역 전투로서 사이버전의 모습도 개전 초기를 제외하면 두드러지지 않는다. 특기한 것은 러시아는 강대국 입장에서 사이버전을 재래식 공격에 유리하게 활용하고자 했으나, 우크라이나의 사이버방어는 효과적이었던 것으로 평가되고 있다는 것이다. 이것은 사이버전장이 강대국에게 일방적으로 유리한 전장만은 아니라는 점을 뜻한다. 그럼에도 불구하고, 보다 대규모이고 악성의 사이버공격이 미래에 실행될 가능성이 있기 때문에, 사이버 공습에 대한 우려가 사라진 것은 아니다. 사이버 방어가 강화되었다고 해도, 강대국의 재래식 공세를 늦추는 데 약소국의 사이버방어 효과가 없다. 재래식 공격이나 물리적 파괴의 위협이 뒤이어 올 것이라고 예측되는 상황에서, 사이버공격은 기습으로 인한 혼란과 공포를 극대화하는 효과를 가질 것이다. 향후 군사충돌에서도 사이버 공격은 이러한 작전용도에서 자주 사용될 가능성이 크다.

특히, 중국의 군사작전이나 교리에서 사이버전은 중심적인 수단으로 발전해갈 것으로 전망된다. 소위 오늘날의 분쟁에서는 가장 먼저 시작되는 것도 사이버전이고 전반적인 군사태세에 결정적인 영향을 주는 것도, 사회적 전쟁수행의지를 약화시켜 전쟁을 끝내는 데 이용되는 수단도 사이버전이라고 이야기된다. 중국은 걸프전 이래 미국의 첨단군사력에 대항하기 위해 미국의 정보화된 지휘통제체계를 초기에 마비시키고 그 동안 군사적인 우위를 달성한다는 망전일체전 개념을 발전시켜왔다. 이는 오늘날 체계대항전쟁 개념으로 이어지고 있다. 체계대항전도 적대국의 정보 네트워크를 마비시킨 후에 장거리 타격으로 상대국의 군사력을 파괴한다는 망전일체전의 접근방식을 이어받고 있다. 하지만 중국의 기대와 달리 미국이 사이버방어에 성공할 경우 전쟁은 체계대항전의 구상대로 흘러가지 않을 것이다.

끝으로, 인공지능(Artificial Intelligence)의 등장이 사이버 영역의 속성을 어떻게 바꾸어갈지도 주목해야 할 것이다. 이러한 발전추세는 한반도 주변정세는 물론 남북관계에도 영향을 줄 것이기 때문에, 우리의 군사 및 외교정책 상에서도 사이버전의 발전추세는 중심적인 주제로 다루어져야

할 것이라고 생각된다.

〈참고문헌〉

Adams, James. 2001. "Virtual Defense." Foreign Affairs 80 (3): 98-112.

Amazon Staff, "Amazon's assistance in Ukraine," https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine (검색일: 2022년 3월 15일).

Cattler, David and Daniel Black, 2022. "The Myth of the Missing Cyberwar Russia's Hacking Succeeded in Ukraine?And Poses a Threat Elsewhere, Too." The Foreign Affaris, April 6. https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar

Finkle, Jim. 2013. "Researchers say Stuxnet was deployed against Iran in 2007." Reuter, February 27. https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226

Gartzke, Erick. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." International Security 38 (2): 41-73.

Kofman, Michael, Anya FinkDmitry, Gorenburg, Mary Chesnut, Jeffrey Edmonds and Julian Waller. 2021. Russian Military Strategy: Core Tenets and Operational Concepts. Arlington, VA: Center for Naval Analysis.

Lynn III, William J. 2010. "Defending a New Doman: Pentagon's Cyberstartegy." Foreign Affairs 89 (5): 97-108.

Maggie Miller, "Russian invasion of Ukraine could redefine cyber warfare," Politico, January 28. 출처: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051 (검색일: 2022년 3월 16일).

Meta, "Updates on Our Security Work in Ukraine (February 27, 2022)," 출처: https://about.fb.com/news/2022/02/security-updates-ukraine/ (검색일: 2022년 3월 15일).

Moss, Sebastian. 2022. "Ukraine: Ukrtelecom hit by 15 hour outage due to cyberattack: Largest outage in Ukraine since Russia's war began." Data Center Dynamics, March 29. https://www.datacenterdynamics.com/en/news/ukraine-ukrtelecom-hit-by-15-hour-outage-due-to-cyberattack/

Mueller, Grace B., Benjamin Jensen , Brandon Valeriano , Ryan C. Maness , and Jose M. Macias. 2023. "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures." CSIS, July 13. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#:~:text=Of%20the%2030%20recorded%20cyber,operations%20targeted%20government%20military%20targets.

Pamment, James et al. 2019. "Hybrid Threats: 2007 cyber attacks on Estonia." Nato Strategic Communications Center of Excellence, June 6.

https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86

Rid, Thomas. 2020. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Macmillan.

Sebastian Moss, "Ukraine's Ukrtelecom goes down nationwide for 40m, ISP Triolan outage caused by cyber attack: As Internet services continue to be targeted by Russian forces," March 10, 2022, https://www.datacenterdynamics.com/en/news/ukraine-ukrtelecom-goes-down-nationwide-for-40m-isp-triolan-outage-caused-cyber-attack/ (검색일: 2022년 3월 16일).

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

Valeriano, Brandon and Ryan C. Maness. 2014. "The Dynamic of Cyber Conflict between Rival Antagonists, 2001-11." Journal of Peace Research 51 (3): 346-360.

Valeriano, Brandon. 2023. "Where was Russia's 'Cyber Thunder Run' during Ukraine invasion? - Prof. Brandon Valeriano." Youtube, May 20. https://www.youtube.com/watch?v=GMpqh8qUzLw&ab_channel=MITSecurityStudiesProgram

Walt, Stephen. 2010. "Is the Cyber Threat Overblown?" The Foreign Policy, March 30. https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/

White, Sarah P. 2018. "Understanding Cyberwarfare: Lessons from the Russia-Georgia War." Modern War Institute, March 20. https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf

김경순, "러시아의 하이브리드전: 우크라이나사태를 중심으로,"『한국군사』4(2018), pp. 70-72, 85.

김경아, 2022년 2월 12일자.『파이낸셜 뉴스』, "러, 오는 16일 우크라이나 침공 검토?…외신들 '美, 첩보 입수.'"

노 훈. 2013. "북한 비대칭 전략과 우리의 대응개념."『국방정책연구』29(4): 83-112.

"UKRAINE: Timeline of Cyberattacks on critical infrastructure and civilian objects," 출처: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/ (검색일: 2022년 3월 15일).

송태은. 2022. "현대 전면전에서의 사이버전의 역할과 전개양상: 2022년 러시아-우크라이나 전쟁 사례."『국방연구』65(3): 215-236.

이상우,『아주경제』, 2022년 3월 14일자, "[Tech in Trend] ① 디지털 시대의 현대戰, 사이버공간으로 퍼진 국가분쟁."

이중구. 2022. "우크라이나 전쟁과 사이버전," 서울대학교 국제문제연구소 이슈브리핑 제174호,

3월 21일.
http://www.snuiis.re.kr/sub5/5_4.php?mode=view&number=1565&b_name=isu

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.