http://dx.doi.org/10.35431/MINJOK.80.2

러시아의 사이버전 전략
: 러시아 – 우크라이나 전쟁초기 전역을 중심으로

문 용 득
제1저자, 육군3사관학교
(321yd@naver.com)

박 동 휘
교신저자, 육군3사관학교
(cyberwar@kakao.com)

국문요약

2022년 2월 24일 오랫동안 민족적인 갈등을 겪어왔던 러시아와 우크라이나 간 대규모 전면전이 발발하였다. 러시아의 우크라이나 침공은 러시아의 차세대 전쟁 전략에 따라 물리적 공간뿐만 아니라 사이버 공간에서도 함께 진행되었다. 러시아는 사이버전을 통해 상대국 군대와 국민의 저항의지를 말살하고자 했다. 이는 냉전의 종식 이후 러시아가 추구해온 다양한 방식의 전쟁 수단을 결합시켜 수행하는 하이브리드 전쟁의 전형이다. 본 연구는 러시아의 하이브리드 전쟁 전략 개념, 즉 차세대 전쟁의 핵심 수단으로서 사이버전을 분석하고 이를 실제 사례에서 확인해보고자 했다. 실제로 러시아는 이러한 전략 개념에 따라 전면 공격을 전후로 사이버 공격, 데이터 탈취, 허위조작사실 유포와 같은 사이버 심리전 등의 방법을 통해 상대국의 저항의지를 말살하여 전략적 승리를 추구하고 있다. 이번 연구의 범위가 전쟁 초기로 제한적이지만, 러시아의 하이브리드 전쟁과 사이버전에 관한 심도 있는 논의의 시작점이 되길 바란다.

주제어 : 러시아, 우크라이나, 사이버전, 하이브리드 전쟁, 차세대 전쟁

I. 서 론

우크라이나의 수도 키이우(Kyiv) 시간으로 2022년 2월 24일 05시경 러시아의 대통령 블라디미르 푸틴(Vladimir Putin)은 미리 녹화된 영상을 통해 '특별 군사작전(special military operation)'을 하달하며 우크라이나 침공을 공식적으로 발표했다. 그는 우크라이나의 '탈나치화'와 '중립화'를 전쟁 명분으로 내세우며, 러시아의 서쪽 국경과 맞닿아 있는 우크라이나 동부의 돈바스(Donbass) 지역에 대한 제한적 성격의 전쟁을 수행하겠다고 했다.[1] 하지만 러시아군은 동쪽의 돈바스 방면만이 아니라 2014년 러시아가 불법적으로 합병한 남쪽의 크림 반도와 친(親)러시아 국가인 벨라루스와의 북쪽 국경 쪽에서도 동시에 전면적인 침공을 해왔다. 오랫동안 민족적인 갈등을 겪어왔던 두 국가 간에 대규모 전면전이 시작된 것이다.

그런데 러시아의 우크라이나 침공은 단순히 눈에 보이는 물리적 공간에서만 이루어진 것이 아니었다. 전쟁은 러시아의 군사전문가들이 발전시켜온 차세대 전쟁(new-generation war) 전략에 따라 사이버 공간에서도 함께 진행되었다. 심지어 러시아는 자신들의 차세대 전쟁에 관한 군사교리를 충실히 따라 전쟁 이전 사이버전(cyber warfare)을 기반으로 한 정보전(information warfare)을 수행하여 적의 군대와 국민의 저항의지를 말살하고자 했다. 여기서 러시아의 차세대 전쟁은 서방 군사전문가들 사이에서 통용되고 있는 다양한 방식의 전쟁 수단을 결합시켜 수행하는 하이브리드 전쟁(hybrid war)이다. 러시아의 정보전은 텔레비전과 웹사이트, 그리고 소셜 미디어 등 다양한 온라인 수단을 통해 심리전이자 선전전을 수행해 상대국가의 전쟁 의지를 꺾으려는 것을 말한다(Thornton 2015, 42-43). 최근 이러한 정보전이 주로 온라인을 통해 이루어지기 때문에 여기서는 이를 서구에서 통용되고 있는 사이버전과 동일한 개념으로 하여 분석하고자 한다.[2]

본 연구의 학문적 중요성은 기존 연구 측면에서 다음과 같이 분석해 볼 수 있다. 러시아 사이버전에 관한 해외 연구는 크게 두 부류로 나뉜다. 그 첫 번째는 러시아를 배후로 하는 사이버전 사례에만 집중하는 경향이다(Blank 2008; Herzog 2011; Kozlowskin 2014). 두 번째는 서구식 개념인 하이브리드 전쟁을 러시아 측면에서 설명은 하나 사이버전을 하이브리드 전쟁의 한 수단으로 간략히 서술하는 경향이다(Hoffman 2007; Rácz

1) 출처: https://www.rt.com/russia/550408-speical-operation-putin-donbass/amp/ (검색일: 2022. 04. 07.).

2) 본 연구에서 러시아의 정보전 용어는 혼란을 방지하기 위해 서구의 사이버전이라는 용어로 통일되어 사용할 것이다. 다만, Ⅱ장 이론적 검토 부분에서는 러시아에서 사용되는 원어 그대로인 정보전으로 표기하고자 한다.

2015; Giles 2016). 국내의 연구 경향 역시도 이와 크게 다르지 않다. 송승종(2017)은 러시아의 하이브리드 전쟁을 이론적으로 자세히 분석하고 있지만, 그 역시도 하나의 예 정도로 사이버전을 언급하는 수준이었다. 송태은(2021)의 경우 하이브리드 전쟁의 위협 수단으로 사이버 심리전을 면밀히 분석했으나, 이 역시도 러시아의 전략 중심이 아닌 미국과 유럽의 대응에 주목한 바 있다. 즉 지금까지 국내·외 연구의 중점은 러시아의 하이브리드 전쟁에서의 한 수단으로서 사이버전을 간단히 언급하거나 러시아의 사례에 집중하기보다는 전체적인 조망 측면에서 사이버전을 바라본 점이 크다. 따라서 본 연구는 이러한 한계점을 극복하기 위해 러시아의 하이브리드 전쟁 전략 개념하에서 사이버전을 분석하고 이를 실제 사례에서 확인해보고자 한다.

이에 본 글은 러시아가 최근 적극적으로 활용하고 있는 차세대 전쟁의 개념과 그 핵심 수단인 사이버전이 실제 전쟁에서 어떻게 활용되고 있는지를 러시아-우크라이나 전쟁을 통해 고찰해보고자 한다. 보다 구체적으로 러시아의 우크라이나 침공 간 양측 간의 사이버전이 어떻게 수행되고 있는지에 대한 답을 하고자 한다. 이를 위해서 이 글은 서구의 하이브리드 전쟁 개념을 기초로하여 러시아의 차세대 전쟁 개념과 사이버전 전략을 설명할 것이다. 이후 최근 발생한 러시아의 우크라이나 침공 사례를 통해 러시아의 사이버전 전략이 실제로 어떻게 적용되고 있는가를 확인하여 교훈을 도출하고자 한다.

글의 구성은 다음과 같다. 먼저 II장은 러시아의 사이버전을 이론적으로 검토한다. 구체적으로 서구의 하이브리드 전쟁 개념과 이의 러시아적인 적용인 차세대 전쟁을 설명한다. 이어서 차세대 전쟁 전략 개념 하에서 러시아 사이버전의 특성과 목표, 그리고 전쟁 초기 작전 간의 실제 적용된 방법에 대해 이론적으로 고찰한다. III장은 러시아의 사이버전 개념이 실제 전쟁에서 어떻게 적용되었는가를 구체적으로 보여줄 것이다. 러시아는 물리적 전쟁에 앞서 사이버 수단을 사용하여 적의 전의를 말살시키려 했다. 심지어 전쟁이 임박한 순간의 사이버전은 전통적인 물리적 전쟁에서의 공격준비사격과 유사했다. 또한 전쟁 중에도 러시아의 사이버전은 치열하게 전개되고 있어 그 위험성이 있다고 하겠다. 마지막 장에서는 사이버전을 중심으로 한 러시아의 차세대 전쟁이 갖고 있는 군사적 의미와 한국에 주는 함의를 간략히 정리할 것이다.

한편, 본 연구의 한계점 두 가지는 다음과 같다. 첫 번째는 본 연구가 분석의 대상으로 삼은 러시아-우크라이나 전쟁은 본 글이 집필되고 있는 시점에도 여전히 진행 중에 있다는 사실이다. 그래서 본 연구의 분석 기간은 전쟁과 직접적 연관성이 있는 1월 13일 사이버전 시기부터 초기 작전 기간(2022. 2. 24 ~ 3. 31)[3]으로 한정할 것이다. 두 번째는 본

3) 러시아 국방부는 3월 25일 경 자신들이 세운 초기 목표를 어느 정도 달성했다고 발표하며 1단계 작전의 종료를 알렸고, 동시에 앞으로 우크라이나 동부 지역의 해방에 집중하겠다고 했다. 따라서, 본 연구는 전쟁과 직결된다고 여겨지는 첫 대규모 사이버전이 발생한 1월 중순부터

연구가 서구의 시각에 치운친 점이다. 본 연구는 방법론 측면에서 문헌연구에 기초하고 있고, 서구와 러시아 양측의 사료를 발굴하고 이를 면밀히 검토 및 분석함이 중요하다. 그러나 아직 양측의 모든 자료가 공개되어 있지 않았을 뿐만 아니라 신뢰할만한 러시아 측의 자료 접근 제한과 필자들의 언어적 한계점 때문에 서구적 사료와 시각으로 치우치는 문제가 발생할 수밖에 없었다. 그럼에도 서구와 국내의 다양한 자료들, 그리고 일부 접근할 수 있는 친(親)러시아 성향 언론의 영문 웹사이트의 기사들을 중립적으로 비교 분석하여 한쪽의 시각에 치우치지 않도록 노력했음을 알린다.

Ⅱ. 러시아 사이버전의 이론적 검토

1. 러시아의 하이브리드 전쟁 개념

냉전의 종식 이후 1994년 체첸전쟁, 9/11 테러와 이라크 전쟁, 아프간 전쟁, 2006년 이스라엘-레바논 전쟁, 2014년 우크라이나 사태 등을 계기로 서방국가에서는 전통적인 군사 강대국에 대항하는 비대칭적 위협에 초점을 맞추는 이론적 연구가 본격적으로 진행되었다. 비대칭적 전략이 구사되었던 것은 냉전의 종식 이후에 나타난 새로운 현상이 아니라는 공감대가 있기도 하지만(송승종 2017, 65), 이러한 위협은 2000년대부터 본격적으로 세계 안보환경의 성격과 국제분쟁 양상을 본질적으로 변화시키는 데에 일조하고 있다고 평가되기 때문에 특별히 주목받고 있다(송태은 2021, 70).

2014년 초 러시아가 우크라이나 크림 반도를 합병하고, 러시아와 국경을 맞대고 있는 동부 돈바스 지역의 분리ㆍ독립에 개입하는 과정에서 활용한 전투방식은 북대서양조약기구(NATO, 이하 나토) 동맹국들에게 특별한 도전으로 인식되었다. 선전포고를 앞세우지 않고 전시와 평시의 구분이 모호한 상황에서 벌어지는 일련의 전쟁 양상에 대해 나토는 침략국의 소행을 명확히 규정해야 가동할 수 있는 집단안보 매커니즘의 허점을 드러냈다. 2014년 나토는 회원국에 대한 사이버 공격에 대해 나토의 설립 취지의 핵심인 헌장 5조 '집단방위 원칙'을 적용할 수 있다고 천명했으나, 나토 회원국을 대상으로 특정국가의 지원을 받는 비국가 행위자의 사이버 공격이 지속되고 있음에도 불구하고 나토는 아직까지 군사적 대응이나 보복을 실시한 적이 없다(박동휘 2019, 320). 우크라이나 사태에 대해 적절한 군사적 대응을 취하지 못한 나토는 러시아의 행위를 가리켜 우크라이나를 겨냥한

앞서 설명한 러시아의 1단계 작전 종료 시까지를 연구 기간으로 삼고자 한다.

하이브리드 전쟁으로 규정하고, 이를 "고도로 통합된 구상 속에서 노골적 및 은밀한(overt and covert) 군사, 준군사 및 민간 수단(civilian measures)들이 광범위하게 운용되는 현상"으로 정의했다(송승종 2016, 127). 나토 방위대학(NATO Defence College)의 라이징거(Reisinger)는 2014년 러시아의 우크라이나 침공을 하이브리드전으로 간주하며, 군사와 비군사, 재래식 전력과 비정규 전력, 사이버전과 정보전과 같은 새롭지 않지만 모든 종류의 요소를 포함하는 전쟁 양상이 상대국에 대해 놀라운 효과를 달성하고 모호성을 창조하면서 그들이 적절한 대응을 하는 것을 매우 어렵게 만들었다고 강조하였다(Reisinger & Goltz 2014).

이와 같은 전쟁 현상을 규정하는 용어는 하이브리드 전쟁, '모호전(abmiguous warfare)', '비선형 전쟁(unlinear war)', 차세대 전쟁 등으로 다양하게 불리고 있다(Hoffman 2007; Galeotti 2014; Connell and Evans 2015). 러시아 입장에서는 서방측 시각을 반영하는 하이브리드 전쟁이라는 용어보다는 자체적으로 차세대 전쟁 개념을 일반적으로 사용하고 있다. 서방과 러시아 각각에서 모두 용어의 개념이 정규전과 비정규전, 재래전과 비재래전, 전투원과 비전투원의 경계가 흐릿해지고, 테러 또는 범죄행위를 포함한 비군사적 요소의 중요성을 강조한다는 측면에서 공통점을 갖고 있다(송승종 2017, 68).

한편, 러시아 군사사상가들은 전쟁의 본질에서 일어나는 변화와 새로운 전쟁 형태의 출현에 대해 깊이 있게 연구해왔다. 러시아의 시각에서 소련의 붕괴 이후 러시아가 가장 취약했던 1990년대에 서방은 나토의 군사력을 통해 유고슬라비아를 강제 분할했고, 2000년대에 들어서 코소보 독립과 이라크, 아프가니스탄에서 강제적 정권교체를 추진했다. 러시아는 미국에 의한 강제적 정권교체의 패턴이 대부분 새로운 방식이라고 평가한다. 군사작전 수행 결정, 인종청소 예방이나 대량살상무기 압수 같은 적당한 명분 발견, 마지막으로 정권교체를 위한 군사작전 순서로 이루어지는 정권교체 과정에서 중요한 것은 노골적 군사침공 대신 선전매체, 인터넷과 소셜미디어, 비정부단체와 같은 비군사적 활동으로부터 시작한다는 것이다(송승종 2017, 69).

새로운 전쟁과 무기체계를 연구해 온 러시아 장군 마흐무트 가레예프(Makhmut Gareev)는 『If War Comes Tomorrow』라는 책을 통해 러시아의 군사전략 및 전술 개념이 서방의 안보위협으로부터 대응하기 위해 충분히 발전되고 있음을 설명했다(Gareev 1998). 그는 미래전에서는 정보전이 결정적인 역할을 하게 된다고 보았다. 기술발전으로 정보전의 방법과 수단이 이전보다 훨씬 더 정교해지고, 컴퓨터와 통신매체는 보다 빠른 정보 수집, 대응, 명령, 통제가 가능하도록 만들었으며, 적의 컴퓨터와 통신매체를 파괴하기 위한 광범위한 전자전도 활용될 것으로 보았다(김경순 2018, 69). 그는 새로운 정보전 방식이 직접적인 무력 공격 대신 분명히 드러나지 않고 잠재되어 있으며, 선언되지 않은

전쟁으로 바뀔 수 있다는 것을 강조했다(Rácz 2016, 35).

2014년 크림 반도에서 러시아의 군사작전을 지휘한 바 있으며 현재 러시아 연방 총참모장인 발레리 게라시모프(Valery Gerasimov)는 그의 유명한 논문인 「The Value of Science is in the Foresight」를 발표하며 미래 전쟁에 있어 새로운 형태의 전쟁 개념을 크게 발전시킨 바 있다. 그는 '아랍의 봄'을 계기로 전쟁의 규칙이 변화하였다고 설명하였다(Gerasimov 2016, 24). 전쟁에 있어 정치적、전략적 목적 달성을 위한 비군사적 수단의 역할이 증가하였고, 많은 경우 이들은 효과면에서 재래식 무기의 위력을 능가한다는 것이다. 현대전에서는 은폐되고 비대칭적이며 간접적인 방법과 수단의 중요성이 물리적 현실 공간뿐만 아니라 정보 공간에서도 중요하며, 심리전과 정보전이 강조되고 민간요소도 중점적으로 활용된다.

서방의 많은 전문가들은 게라시모프의 논문을 통해 러시아가 취한 우크라이나 공세에 대한 개념적 근거를 발견했으며, 이를 게라시모프 독트린이라고 불렀다(Fridman 2019, 106). 군사적 개념 측면에서 게라시모프는 차세대 전쟁을 "정치, 경제, 정보, 인도주의, 기타 비군사적 수단들의 광범위한 사용... 지역 주민들 사이의 내란과 은폐된 무장세력들에 의해 보충된다"고 묘사했다(Galeotti 2014, 2).

게라시모프 독트린은 2000년대 후반부터 러시아 군부의 관점을 형성하는데 중요한 역할을 한 러시아 고위 장교 세르게이 체키노프와 세르게이 보그다노프에 의해 더욱 자세히 설명된다. 그들은 정치, 경제, 기술, 생태, 정보 수단을 병행해 적의 군사적 우위를 무력화하려는 비대칭 행동의 중요성을 강조한다. 또한 무력 대결을 앞두고 또 무력 대결을 벌이는 동안 비군사적 방법을 대량으로 사용할 필요성에 대해 매우 노골적으로 강조한다(Chekinov and Bogdanov 2013). 그들에 따르면 현대전쟁은 육、해、공 3차원 공간을 넘어서 정보의 4차원으로 확대되며, 따라서 정보기술을 비롯한 네트워크 체계에서 상대적 정보 우위가 미래전의 성공을 보장한다. 실제 공격에 앞서 집중적인 선전활동과 적의 지휘통제통신 능력을 무력화하기 위한 전자전을 지속적으로 사용함으로써 대상국에 대한 정보 우위를 확보할 필요가 있다고 강조한다. 차세대 전쟁의 주전장은 사이버 공간이 될 것이며, 차세대 전쟁은 적군과 국민의 사기를 꺾어 저항의지를 말살하기 위한 심리전과 정보전이 주를 이룰 것으로 전망한다(송승종 2017, 75).

체키노프와 보그다노프는 차세대 전쟁의 전개 과정을 개전 이전부터 종전 기간까지 단계별로 자세히 기술하였다(Chekinov and Bogdanov 2013, 19-22). 개전 단계에서는 수개월에 걸쳐 적국 주민의 단결을 와해시키고, 적군의 사기를 약화시키기 위해 외교·경제·이념·심리·정보적 수단을 통한 대대적인 선전선동 활동이 전개된다. 군사적 단계가 시작되기 직전에 군부대, 핵심 정부시설 및 주요 인프라를 파악하기 위한 정보수집 활동과

뒤이어 적의 정부 및 군의 무력화를 겨냥한 본격적인 전자전 활동이 실시될 것이다. 이를 후속하여 장거리 포병뿐 아니라 정밀유도 미사일, 드론 및 여타 자동화 무기가 포함된 대대적인 군사공격이 진행된다. 체키노프와 바그다노프가 이론적으로 기술한 차세대 전쟁의 모습은 2014년 우크라이나 사태에서 러시아가 보여 준 군사작전과 매우 흡사하며(송승종 2017, 76), 2022년 진행 중인 우크라이나와의 전쟁에서도 개전 이전 단계부터 사이버 수단을 비롯한 비군사적 성격을 매우 중요시 여기는 양상을 보이고 있다.

2. 하이브드리 전쟁의 핵심 수단으로서 사이버전

하이브리드 전쟁에 대한 학술적 개념화에 큰 기여를 한 프랑크 호프만(Frank G. Hoffman) 역시 사이버전에 관해 언급했다(2007, 28). 전통적 군사작전을 비롯하여 전술적 효과를 극대화하기 이해 기존의 첩보활동(intelligence operations), 정보작전(information operations), 정보전(information warfare)이 사이버 공간에서 본격적으로 사용되고 있음을 의미한다(송태은 2021, 76). 한편, 러시아는 사이버 공간이라는 용어 대신 미디어, TV, 컴퓨터와 인간의 마음을 포함하여 이를 정보 공간(information space)이라고 부른다(Ajir and Vailliant 2018, 72). 러시아 정부 문서인 '정보 공간에서 러시아 연방군의 활동에 관한 개념적 견해(Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space)'(2011, 5)에 따르면, 구체적으로 정보전이란 정보시스템, 프로세스, 자원을 훼손함으로써 정보 공간에서 국가와 대치하는 것으로 정의된다. 이것은 러시아가 상대국의 국민들을 세뇌시켜 사회와 국가를 불안정하게 만들어 정치, 경제, 사회 시스템을 파괴하는 데 매우 중요한 역할을 한다. 정보 공간은 국가 선전 목표를 가능하게 하는 새로운 기술적 수단인 것이다. 2014년 우크라이나에 대해 러시아가 수행한 정보전의 핵심 요소 중의 하나는 러시아의 목표와 목적을 숨기면서 대중에게 공포를 심어주고 러시아의 목표가 제한적이며 궁극적으로 대중 스스로 받아들이도록 설득을 강요한 것이다(Snegovaya 2015, 7).

러시아가 말하는 정보전은 하이브리드 전쟁의 한 수단으로서 공격수단과 행위 주체자의 모호성을 추구한다. 하이브리드 위협은 국가 행위자 외에도 다양한 행위자 차원에서 실행될 수 있고, 국가 활동과 전혀 관계가 없을 수도 있다. 하이브리드 전쟁의 모호한 전술은 비가시적인 영역인 디지털 커뮤니케이션 공간에서 사용될 경우 공격 주체의 모호성을 극대화시켜 공격 대상의 적대행위가 강화되는 상황을 선제적으로 차단하는 전술로 사용될 수 있다(송태은 2021, 77). 정보전은 2014년 크림 반도에서 러시아 군사작전의

성공에 중심에 있었다. 전술적 차원에서 전자전(electric warfare, EW)과 사이버 공격은 우크라이나 당국의 대응 능력을 무력화시켰고, 보다 광범위한 미디어 활용은 진실과 거짓의 경계를 모호하게 만들어 대중들이 러시아 측의 시각을 수용하게 하였다. 그리고 이러한 러시아의 정보전은 서구적 개념인 사이버전으로 치환될 수 있다. 사이버전 역시도 디도스 공격(DDoS Attack, 분산서비스 거부 공격) 같은 단순 사이버 공격부터 해킹과 악성 코드 유포, 그리고 상대방의 전투 의지를 말살하는 사이버 심리전까지도 포함하는 개념이기 때문이다.

사이버전의 목표는 대상 국가의 핵심 인프라 시스템과 대중, 그리고 앞서 설명한 크림반도와 같은 위기 조장이다. 21세기 디지털 정보통신기술의 발전과 인터넷과 네트워크의 전방위적인 연결로 인해 국가 인프라 시스템 네트워크에 대한 러시아발 사이버 공격이 빈번하게 나타나고 있다. 그리고 악성 코드 감염이나 해킹을 통한 민감한 정보의 유출과 허위조작정보의 유포 등 사이버전이 하이브리드 위협의 주요 수단으로 사용되고 있다. 사이버전은 앞서 언급한 모호성으로 인해 상대국의 정책결정을 지연시킴과 동시에 사이버 공격을 통해 국가 시스템을 마비시키고, 여론 교란이나 사회적 혼란을 유발함으로써 정치적 우위를 점하는 전략에 매우 효과적인 수단이다. 결국 전쟁 목적 달성의 마지막 결정적인 국면에서만 군사행동이 필요하므로 목적 달성에 드는 비용 대비 효과가 크다고 볼 수 있다(김경순 2018). 나아가 초연결 사회의 연결성은 사이버전 파괴력을 최대화시킬 수 있는 취약점으로 인식되고 있으며, 시간과 장소의 구애 없이 공격주체가 언제든지 선제적으로 취할 수 있는 사이버 공격은 상시적 위기를 유발할 수 있다(송태은 2021, 80). 특히 러시아는 미국을 비롯한 서방과 정면대결을 할 수 없다는 인식으로 인해 비대칭적 대응을 지속적으로 강구하였다. 이에 따라 러시아의 정보전, 서구적 개념으로 사이버전은 러시아에게 비대칭 우위를 달성할 수 있는 수단으로 간주되었고, 무엇보다 재래식 군사력을 보완하는 데 비용을 절감할 수 있는 매우 유용한 수단이었다. 더불어 초연결 사회로 칭해지는 정보 기술의 출현과 급속한 발전은 러시아인들의 성공적인 작전활동을 보강시켜 주었다(Ajir and Vailliant 2018, 74). 사이버 공간은 비교적 적은 비용과 희생으로 상대국을 불안정하게 만들고 지리적으로 멀리 떨어진 지역에서 군사작전을 전개하는 데 매우 효과적인 플랫폼을 제공한다(박동휘 2022, 26-31).

또한 사이버전은 악성코드를 활용하여 네트워크 인프라 및 하드웨어와 소프트웨어에 대한 훼손을 가하는 기술정보 차원과 온라인 공간을 통해 여론을 교란시키는 사이버 심리전의 방법으로 수행된다. 러시아는 소련의 붕괴와 아랍의 봄, 색깔혁명에서 대중에게 끼친 정보의 위협적인 영향력을 인식했기 때문에 정보를 심리적 차원에서도 위협적으로 인식한다(신범식·윤민우 2020, 170).

냉전의 종식 이후 러시아는 대외 전쟁 시 하이브리드 전쟁이라고 하는 러시아식 차세대 전쟁 전략을 적극 적용하고 있다. 그리고 2008년 러시아-조지아 전쟁부터 이러한 러시아의 차세대 전쟁 전략의 큰 축을 담당하는 것은 그들이 정보전이라 부르는 사이버전이라 할 수 있다. 그들은 전쟁 시작 이후만이 아니라 전쟁 이전부터 이러한 전략 개념에 따라 정보통신기술을 적극 활용하여 상대국의 국민과 군대의 저항의지를 말살하여 신속한 승리를 추구하고 있다. 러시아의 구체적인 사이버전 방법은 사이버 공격을 통한 공공 웹사이트, 군과 정부의 주요 지휘 시스템의 마비부터 악성 코드와 해킹을 통한 주요 데이터 유출, 그리고 사이버 심리전으로 볼 수 있는 온라인 소셜 미디어 등의 매체를 통한 허위조작정보의 유통 등으로 요약할 수 있다.

Ⅲ. 러시아의 對우크라이나 사이버전의 실제

1. 러시아의 우크라이나 침공

2022년 러시아의 우크라이나 침공은 근본적으로 우크라이나와 러시아 간의 오랜 민족적 갈등과 경제적, 그리고 안보적 이해관계에 기반하고 있다(Elsherbiny 2022).[4] 무엇보다 2004년 초반 발생한 오렌지 혁명으로 우크라이나 내부의 친서방과 친러시아 국민들 간의 분열이 극명하게 대외적으로 노출되었다(Kuzio 2010). 그리고 2014년 유로마이단 사건으로 인해 양측 간의 내부적인 정치적 대립만이 아니라 러시아의 무력 개입이 발생했다. 러시아의 구체적인 무력 개입은 2014년 러시아의 불법적인 크림 반도 합병이고, 이어진 돈바스 내 친러 분리주의자에 대한 군사적 지원이었다(Grant 2015; Robinson 2016). 이러한 상황 속에서 볼로디미르 젤렌스키(Volodymyr Zelensky) 우크라이나 대통령이 2019년 5월 취임 이후 보여 온 EU와 나토 가입 시도 등의 적극적인 친서방 정책은 러시아를 크게 자극하기 시작했다.[5]

우크라이나를 침공하기 위한 러시아의 직접적 움직임은 2021년 봄부터 시작하였다. 그들은 우크라이나와의 국경 지역으로 군사력을 이동시켰다. 4월에 러시아 군대는 병력 10만 명 이상과 40척 이상의 전함을 크림 반도 지역으로 보내 대규모 군사훈련을 실시했

4) 2022년 러시아의 우크라이나 침공의 원인과 관련된 근본적 원인에 관해서는 다음의 글들을 참고할 것. Sebastian(2022), Mankoff(2022), Parihar(2022).

5) 출처: https://www.ft.com/content/4c942a46-8791-11e9-a028-86cea8523dc2 (검색일: 2022. 05. 13.).

다.[6] 이는 단순히 우크라이나 내에서 주도권을 쥐고 있는 친서방 세력에 대한 경고성 훈련만은 아니었다. 통상의 경우와 달리 훈련에 참가한 병력과 장비 상당수가 훈련 종료 후에도 러시아로 복귀하지 않았던 것이다. 이에 더하여 2021년 11월 1일 우크라이나 국경 주변으로 군사력을 증강하고 있는 러시아의 모습이 또다시 서방의 위성첩보자산에 의해 식별되었다.[7]

러시아의 침공 위협이 가시화하는 것 아니냐는 관측 속에 미국 등 서방은 러시아의 군사적 행동 중지 촉구 메시지를 계속적으로 내놓기 시작했다. 대표적으로 2021년 12월 7일 미국의 조 바이든(Joe Biden) 대통령은 우크라이나를 상대로 러시아가 전쟁을 일으킬 시 경제 제재를 포함한 강력한 수단을 통해 그에 상응하는 댓가를 물릴 것이라 경고했다(박동휘 2022, 129). 이러한 군사적 움직임의 이유는 2021년 12월 17일 푸틴의 공식적 요구를 통해 명확히 드러났다. 그는 우크라이나의 나토 가입 반대, 서방과 나토의 우크라이나를 포함한 동유럽 내에서의 군사활동 중지, 구소련 국가의 나토 가입 금지, 러시아에 대한 법적인 안전보장 등을 요구한 것이다.[8]

러시아는 미국을 비롯한 서방 측의 경고에도 불구하고 오히려 더 긴장감을 높였다. 푸틴은 2022년 1월 친(親)러시아 국가인 벨라루스와의 연합훈련을 실시하기 위해 우크라이나의 북쪽 국경으로 약 30만 명에 달하는 병력을 이동시켰다.[9] 러시아와 우크라이나 사이의 군사적 긴장은 고조되었다. 러시아는 2월 10일 벨라루스와 대규모 연합훈련인 '얼라이드 리졸브 2022(Allied Resolve 2022)'에 돌입한 데 이어 돈바스 내의 도네츠크 인민공화국과 루한스크 인민공화국을 독립국으로 인정한다고 발표했다.[10] 결국 러시아는 2022년 2월 24일 05시(키이우 현지시간)를 기점으로 돈바스 지역에서의 특별군사작전 뿐만 아니라 남부의 크림 반도, 북부의 벨라루스 방면에서 동시에 총공세를 단행했다.

한편, 젤렌스키 우크라이나 대통령은 푸틴이 침공을 발표한 날 마찬가지로 계엄령을 선포하고 결사항전의 의지를 드러냈으며, 우크라이나인들은 러시아의 공격에 쉽게 굴하지

---

6) 출처: https://www.reuters.com/world/europe/russian-defence-minister-oversees-large-scale-military-drills-crimea-ria-2021-04-22/ (검색일: 2022. 05. 13.).

7) 출처: https://www.politico.com/news/2021/11/01/satellite-russia-ukraine-military-518337 (검색일: 2022. 05. 10.).

8) 출처: https://www.theguardian.com/world/2021/dec/17/russia-issues-list-demands-tensions-europe-ukraine-nato (검색일: 2022. 05. 17.).

9) 출처: https://www.theguardian.com/world/2022/jan/17/russia-moves-troops-to-belarus-for-joint-exercises-near-ukraine-border (검색일: 2022. 05. 17.).

10) 출처: https://apnews.com/article/russia-ukraine-europe-russia-vladimir-putin-moscow-bcd0c04a2aa146e76b7e757f482f27bb (검색일: 2022. 05. 19.).

않았다. 러시아군이 속전속결로 우크라이나 수도 키이우를 점령할 것이라는 예측과는 달리 전쟁은 장기화하는 양상으로 전개되고 있다.

2. 물리적 전쟁 개시 이전의 사이버전

현대적 개념으로서 러시아의 하이브리드 전쟁은 체첸 전쟁을 기원으로 한다. 하이브리드 전쟁이라는 용어를 처음 사용했다고 알려져 있는 윌리엄 J. 네메스(William J. Nemeth 2002)의 미 해군대학 석사학위 논문은 체첸 전쟁을 분석한 것이었다. 그러나 사이버 수단이 결합된 형태로서 본격적인 러시아의 하이브리드 전쟁 시작은 2008년 러시아-조지아 전쟁(the 2008 Russo-Georgian War, 2008.08.07.-12.)이었다. 러시아는 전쟁 시작과 동시에 사이버 수단을 통해 조지아의 전략적 시설을 무력화시켰고, 이들을 외부 세계와 단절시켰다.[11] 러시아는 육군, 해군, 공군의 재래식 전력과 사이버 수단을 결합해 단 5일 만에 조지아의 항복을 받아내는데 성공한 것이다. 러시아는 이후 2014년 크림 반도의 불법적 합병 당시에도 우크라이나에 대한 일련의 사이버 공격을 통해 하이브리드 전략을 선보인 바 있다(Rácz 2015, 81-82). 요약하면 러시아는 과거 자신들의 영향력 아래 있던 주변 국가들 중 친서방 정책을 펼치는 이들에 대해 하이브리드 전쟁 전략을 사용하고 있다. 더욱이 사이버 수단은 러시아의 하이브리드 전쟁 전략에서 그 역할과 비중이 계속 커지고 있다.

이러한 하이브리드 전략 개념에 따라 러시아는 2014년의 크림 반도를 합병 이후부터 사이버 공격을 통해 친서방 정책을 펼치려는 우크라이나를 괴롭혀 왔다. 우크라이나는 2015년 12월과 2016년 12월 두 번에 걸쳐 러시아를 배후로 하는 해커 세력으로부터 전력망에 대한 대규모 사이버 공격을 받은 바 있다(Park and Walstrom 2017). 유로마이단 사건 이후 우크라이나 대통령이 된 친서방 성향의 페트로 포로센코(Petro Poroshenko)는 2016년 12월의 사이버 공격 발생 직후 지난 두 달간 자국 내 전력시설에 대하여 6,500여 회의 해킹 시도가 있다고 밝힌 바 있다(박동휘 2022, 123).

우크라이나는 러시아를 배후로 하는 사이버 공격으로부터의 피해를 막기 위해 오랫동안 많은 준비를 해왔다. 우크라이나는 자체적으로 사이버 안보를 위한 다양한 노력을 실시해왔다. 이에 더하여 미국을 비롯한 서방 국가들은 2015년 전력망에 대한 대규모 사이버 공격을 기점으로 하여 우크라이나의 사이버 방어태세를 위해 수천만 달러를 투자했다.[12]

---

11) 출처: https://kookbang.dema.mil.kr/newsWeb/m/20210208/1/BBSMSTR_000000100135/view.do (검색일: 2022. 05. 13.).

12) 출처: https://www.politico.com/news/2022/02/19/despite-years-of-preparation-ukraines-el

EU는 러시아의 우크라이나 침공 위협이 고조되던 2021년 12월 향후 3년 간 3,100만 유로를 우크라이나의 사이버 안보 분야 등에 지원하기로 결정하기도 했다.[13] 즉, 우크라이나는 그간 러시아가 적대적 행위를 위해 즐겨 사용해온 하이브리드 전쟁 전략에 대한 이해와 과거의 경험을 바탕으로 사이버 안보를 위한 막대한 예산을 투입하며 만일의 사태에 대비해 왔던 것이다.

하지만 러시아는 우크라이나의 대비에도 불구하고 2022년 러시아-우크라이나 전쟁 초기 전역에서 적극적으로 사이버전을 수행했다. 특히나 이는 체키노프와 보그다노프가 주장한 러시아 정보전의 전개 과정과 목적에 부합했다. 두 군사사상가는 개전에 앞서 수개월에 걸쳐 적국 주민의 단결을 와해시키고, 적군의 사기를 약화시키기 위해여 다양한 수단을 사용할 것을 주장한 바 있다(Rácz 2015, 38). 적의 군대와 국민의 저항의지 말살을 목표료 하는 러시아의 다양한 수단들 중 단연 돋보이는 것은 사이버전이었던 것이다.

계속된 러시아의 사이버 공격 시도 중 의미 있는 사건은 2022년 1월 14일에 일어났다. 그날 대규모 디도스 공격이 발생해 약 70여 개의 우크라이나 정부기관 웹사이트가 서비스를 제공할 수 없는 상태가 되었다.[14] 우크라이나 정부는 외교부, 내무부, 에너지부, 교육부, 농업부 등과 공공 서비스를 담당하는 여러 주요 웹사이트가 공격을 받았다고 밝혔다.[15] 이에 덧붙여 우크라이나 측은 공격 이후 수시간 내에 대부분의 웹사이트를 정상화 시켰다고 발표했다.

서비스 불능에 대한 우크라이나 정부의 빠른 대처가 있었음에도 1월 14일의 공격은 우크라이나 사회를 혼란으로 빠뜨렸다. 러시아와 연계되었다고 의심되는 세력에 의한 디도스 공격에는 데이터 탈취 시도와 디페이스먼트(defacement)라는 위·변조 공격이 함께 했다. 어떠한 데이터의 외부 유출도 없었다는 우크라이나 정부 측의 공식적 발표와 달리 위·변조 공격을 받은 웹사이트는 다른 말을 하고 있었다. 정상적인 웹사이트 화면이 공격자가 게시한 다른 사진과 글들로 도배되는 위·변조 공격을 받은 우크라이나 외교부 웹사이트 등은 우크라이나 국민들을 위협하는 글과 사진으로 도배되었다. 게시된 사진 파일에는 우크라이나 지도와 국기에 대한 모독을 넘어 우크라이나어, 러시아어, 그리고

---

ectric-grid-still-far-from-ready-for-russian-hackers-0001037 (검색일: 2022. 05. 19.).

13) 출처: https://www.politico.com/news/2022/02/19/despite-years-of-preparation-ukraines-electric-grid-still-far-from-ready-for-russian-hackers-0001037 (검색일: 2022. 05. 19.).

14) 출처: https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers (검색일: 2022. 05. 20.).

15) 출처: https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/ (검색일: 2022. 05. 20.).

폴란드어로 아래와 같이 쓰여 있었다.

> "우크라이나인이여! 너희의 모든 개인 데이터가 인터넷상에 업로드 되었다. 컴퓨터에 있는 모든 데이터는 파괴되었고, 그것들을 복구하는 것은 불가능하다. 너희들과 관련된 모든 정보가 세상에 공개되었다. 두려워하고 최악을 기대하라. 이것이 너희들의 과거이자 현재, 그리고 미래다."[16]

위·변조 공격에 의한 사이버전이 사이버 심리전 공격으로 확장되는 순간이었다. 특히, 이는 전쟁 시작 이전 적의 국민에게 공포감을 조성한다는 목표를 가진 러시아의 차세대 전쟁 전략에서 강조하는 사이버전이었다. 2021년 12월부터 러시아의 전쟁 위협이 한층 고조되던 상황에서 러시아를 배후로 하는 세력이 "두려워하고 최악을 기대하라"라는 문구를 남겼다는 것은 마치 전쟁을 암시하는 것이었고, 전쟁을 원하지 않는 우크리아나 시민들에게 심리적으로 영향을 줄 수밖에 없는 상황이 만들어진 것이다.

우크라이나 외교부 대변인은 사회적 혼란을 잠재우기 위해 즉각 트위터를 통해 IT 전문가들이 이미 복구를 시작했고, 사이버 수사팀이 수사에 들어갔음을 알렸다.[17] 우크라이나 국가안보국방회의 부의장인 세르히 데미듀크(Serhiy Demedyuk)는 로이터와의 인터뷰에서 이번 위·변조 공격의 배후로 UNC1151을 지목했다.[18] UNC1151은 이전부터 벨라루스 정부를 이롭게 하는 해킹 사건에 자주 등장해온 벨라루스 정보기관과 밀접한 관계에 있는 해커 집단이었다.[19] 글로벌 사이버보안 기업 맨디언트(Mandiant)가 2021년 11월 16일 발표한 자료에 따르면, 이 해커 집단은 그동안 우크라이나를 비롯한 동유럽 국가들과 벨라루스의 야권 세력 등을 대상으로 사이버 공격을 진행해왔던 것에 반해 러시아와 벨라루스 정부를 공격하지는 않았었다. 이러한 점에 비춰볼 때, 벨라루스 정보기관과 연계된 UNC1151로 추정되는 세력의 사이버 공격은 러시아를 배후로 한 공격일 가능성이 매우 높은 상황이었다. 우크라이나 정부만이 아니라 EU도 사이버 공격 직후 러시아의 배후설을 내놓았다. EU의 외교안보정책 고위대표를 맡고 있는 조셉 보렐(Josep Borrell)은 누구 소행인지 명확한 증거는 없지

16) 출처: https://www.npr.org/2022/01/14/1073001754/ukraine-cyber-attack-government-websites-russia (검색일: 2022. 05. 23.).
17) 출처: https://www.npr.org/2022/01/14/1073001754/ukraine-cyber-attack-government-websites-russia (검색일: 2022. 05. 23.).
18) 출처: https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/ (검색일: 2022. 05. 25.).
19) 출처: https://www.mandiant.com/resources/unc1151-linked-to-belarus-government (검색일: 2022. 05. 25.).

만 우리는 그 공격의 배후로 의심할만한 국가는 상상할 수 있다는 모호한 말로 러시아의 사이버 공격을 강력히 비난한 것이다.[20]

러시아는 우크라이나에 대한 1월 14일의 대규모 사이버 공격과 자신들의 연관성을 부인하는 한편 또다시 유사한 형태의 사이버 공격을 이어가며 군사적 긴장감과 우크라이나 시민들의 저항의지를 꺾고자 했다. 그것은 2월 15일 다시 한번 우크라이나를 대상으로 한 대규모 디도스 공격이었다. 이번 공격은 전쟁이 임박했음을 조금 더 암시하듯 정부기관 웹사이트만이 아니라 군의 핵심 웹사이트 공격에 집중했다. 우크라이나에서 가장 큰 두 개의 국영은행과 함께 우크라이나 국방부와 육군 군부 웹사이트가 다운된 것이다.[21] 우크라이나 정부는 이번에도 공격의 배후로 러시아를 지목했고, 미국 국가안보회의와 영국 정부도 이에 가세해 러시아의 군사정보국(GRU, Glavnoye Razvedyvatelnoye Upravlenie)을 공격자라며 비난을 했다.[22] 공격의 배후 분석 근거는 해당 공격 기간 동안 러시아 군사정보국이 보유한 IT 인프라와 이번 공격의 대상이 된 기관들을 중심으로 우크라이나에 속한 IP 주소 및 도메인 간에 발생한 엄청나게 많은 양의 데이터 통신 행위였다(박동휘 2022, 146).

여기에 더하여 전쟁 개전 이전에 갑자기 파괴형 악성 코드가 등장하기도 했다. 2022년 1월 14일 대규모 디도스 공격, 해킹, 그리고 위·변조 공격 바로 전날인 13일 우크라이나 정부와 기업 등의 전산망에서 파괴형 악성 코드가 발견된 것이었다. 이를 처음 발견한 해외 민간 글로벌 IT 보안기업인 마이크로소프트 위협 지능 센터(MSTIC, Microsoft Threat Intelligence Center)는 이 악성 코드가 우크라이나 정부와 기업, 비영리 단체, 그리고 IT 기관 웹사이트만을 공격하도록 설계되어 있음에 주목했다.[23] '위스퍼게이트 와이퍼(WhisperGate Wiper)'로 명명된 본 악성 코드는 금전을 요구하도록 설계된 랜섬웨어로 위장되어 있었지만 실제로는 공격 대상 시스템이 작동하지 못하도록 하는 기능만이 있는 독특한 구조를 지녔다. 보안전문가들은 이러한 위스퍼게이트와 같은 형태의 악성 코드를 특정 국가가 우크라이나 정부가 비상 상황 발생 시 적절한 대응 역할을 하지

---

20) 출처: https://news.sky.com/story/ukraine-reveals-website-attacks-were-cover-for-more-destructive-actions-12517808 (검색일: 2022. 05. 26.).

21) 출처: https://www.npr.org/2022/02/15/1080876311/ukraine-hack-denial-of-service-attack-defense.

22) 출처: https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine; https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine; https://www.computerweekly.com/news/252513645/UK-joins-US-in-pinning-Ukraine-DDoS-attacks-on-Russia (검색일: 2022. 05. 27.).

23) 출처: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (검색일: 2022. 05. 28.).

못하게 만드려는 악의적 의도를 숨기고 있다고 평가하기도 했다.[24] 즉, 파괴형 악성코드의 목적은 전쟁이라는 상황이 발생될 시 우크라이나 주요 시스템이 제기능을 하지 못하도록 하기 위한 사이버전 도구였던 것이다.

3. 전쟁의 시작과 러시아의 사이버전

하이브리드 전쟁 개념에 따라 사전에 사이버 공격을 시도했던 러시아는 2022년 2월 24일 우크라이나에 대한 전면적인 공격을 시작했다. 그들은 지상 병력의 투입에 앞서 우크라이나의 주요 목표물에 대한 미사일, 포병, 항공기를 통한 공격준비사격을 실시하여 주병력의 안전한 진격과 수월한 작전을 돕는 전통적인 방법을 사용했다. 그런데 러시아는 이러한 전통적인 군사교리에 따른 공격준비사격에 앞서 사이버 공격준비사격도 실시하는 치밀함을 보였다.

2월 23일 늦은 오후 시간 우크라이나를 대상으로 한 러시아의 집중적인 사이버 준비사격이 시작되었다. 그 공격은 디도스 공격과 악성 코드 공격으로 나눌 수 있다. 러시아의 대규모 디도스 공격은 순식간에 우크라이나의 정부기관과 군, 그리고 금융기관 웹사이트들을 불능 상태로 만들었다.[25] 이는 러시아의 사이버전 개념에 정확히 부합하는 것으로서 전쟁 시작과 동시에 우크라이나 정부와 군의 지휘체계를 무력화함과 동시에 은행 등 금융기관의 마비를 통해 사회적 혼란을 유도하기 위한 매우 계산적인 전략적 행위였다. 그 이유는 지상병력의 투입이 임박한 상황에서 전쟁을 지휘해야 할 우크라이나 정부와 군을 대상으로 한 공격이었기 때문이었다.

동시에 우크라이나의 국방과 항공을 담당하는 정부기관과 금융 및 IT기업의 컴퓨터와 시스템을 파괴할 목적으로 악성 코드 공격도 발견되었다.[26] ESET 연구소는 이 악성코드에 '헤르메틱 와이퍼(Hermetic Wiper)'라는 이름을 부여했다.[27] 기술적 분석에 따르면, 공격자는 악성 코드 유포 전에 공격대상으로 선정된 피해 네트워크를 방문한 기록이 있으며 이를 통해 이번 공격이 우크라이나라는 명확한 목표 대상을 설정하고 사전에 치밀하게 계획된 상태에서 이루어졌음을 알 수 있다. 2월 24일에는 일부 컴퓨터와 시스템의

---

24) 출처: https://blog.alyac.co.kr/4421.

25) 출처: https://apnews.com/article/russia-ukraine-technology-business-europe-russia-9e9f9e9b52eaf53cf9d8ade0588b661b (검색일: 2022. 06. 02.).

26) 출처: https://www.eset.com/sg/about/newsroom/press-releases1/products/hermeticwiper-new-data-wiping-malware-hits-ukraine/ (검색일: 2022. 06. 02.).

27) 출처: https://www.dailysecu.com/news/articleView.html?idxno=134662 (검색일: 2022. 06. 02.).

파괴가 제대로 수행되지 않아 이를 보완한 것으로 추정되는 또 다른 악성 코드인 '아이작 와이퍼(Isaac Wiper)'도 식별되었다.[28]

악성 코드의 기술적인 분석만으로는 공격자를 특정하기가 어려운 상황이지만 우크라이나와 러시아 간의 전면전이 임박한 상황에서 동일한 목적의 악성 코드가 우크라이나에서만 식별되었다는 사실은 특정 국가를 공격의 배후로 의심하기에 충분하다고 할 수 있다. 나아가 두 국가의 물리적 충돌이 계속된다면 이들 악성 코드를 통한 유사한 공격 패턴이 지속될 것으로 예상된다.

유럽의 팩트 체크 전문가들은 전쟁의 시작과 동시에 우크라이나와 관련된 허위 또는 가짜 뉴스가 엄청나게 늘었다는 보고를 내놓았다. 작년 말부터 본격적으로 러시아와 우크라이나 사이에 전쟁에 대한 긴장감이 돌기 시작했다. 그럼에도 불구하고, 2022년 1월부터 전쟁 바로 직전까지 우크라이나와 관련된 허위 정보나 가짜 뉴스가 온라인상에서 거의 발견되지 않았다.[29] 그런데 양적이나 질적으로 대수롭지 않았던 우크라이나에 관한 허위 정보와 가짜 뉴스는 2월 24일 러시아의 우크라이나 침공과 함께 질적으로나 위험성 측면에서 엄청나게 달라졌다. 전 세계인들이 전쟁에 주목하고 있는 상황에서 일부 사람들이 자극적인 글과 사진을 온라인에 게시하는 방법을 통해 많은 조회수를 거두거나 모금을 통해 돈을 벌고자한 경우가 있을 수도 있지만, 팩트 체크를 전문으로 하는 유럽 디지털 미디어 전망대(European Digital Media Observatory)는 이를 특정한 목적을 가진 러시아의 선전전으로 분석했다.[30] 그 이유는 전쟁 초기 전 세계인들이 많이 사용하는 트위터와 페이스북, 그리고 틱톡 등과 같은 소셜 미디어와 블로그 등에 게시된 정보와 사진들 중에 포함된 허위 정보와 가짜 뉴스의 상당수가 러시아의 정보전 전략에 부합했기 때문이었다.

유럽 디지털 미디어 전망대는 개전 이후 나온 300여 개의 허위 정보와 가짜 뉴스 관련 자료들을 분석해 두드러진 담론을 5가지로 정리했다.[31] 그것들은 '핵무기와 생화학무기가 등장하는 제3차 세계대전의 발발 예고'부터 '우크라이나 난민에 대한 혐오', '우크라이나 지도자와 군인에 대한 지나친 영웅주의', '영화 세트장에서 찍은 가짜 전쟁', '젤렌스키에 관한 허위 정보와 가짜 뉴스'까지였다. 이들 중 우크라이나인들에 대한 과장된 영웅주의를

---

28) 출처: https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/ (검색일: 2022. 06. 02.).

29) 출처: https://edmo.eu/2022/02/28/war-in-ukraine-the-fact-checked-disinformation-detected-in-the-eu/ (검색일: 2022. 06. 08.).

30) 출처: https://edmo.eu/2022/02/28/war-in-ukraine-the-fact-checked-disinformation-detected-in-the-eu/ (검색일: 2022. 06. 08.).

31) 출처: https://edmo.eu/2022/03/11/the-five-disinformation-narratives-about-the-war-in-ukraine/ (검색일: 2022. 06. 08.).

제외하고 나머지 모두는 러시아의 정보전 전략에 따른 전쟁 의지 말살과 관련이 깊었다. 구체적으로 이들 허위 정보는 가깝게는 우크라이나 군인과 시민들의 저항의지를 꺾는 것부터 국민들에게 공포감을 주어 자신들의 국가가 우크라이나 난민 수용을 반대하거나 우크라이나를 위하여 전쟁에 개입하지 못하도록 부정적 여론 조성을 위한 것까지 있었다.

여기서 가장 주목할 것은 젤렌스키에 관한 허위 정보와 가짜 뉴스였다. 전쟁 개전에서 러시아의 푸틴은 우크라이나의 나치즘에 대한 철퇴를 전쟁의 이유 중 하나로 내놓았다.[32] 그런 측면에서 젤렌스키를 신나치주의자로 묘사한 가짜 뉴스는 러시아의 침공을 정당화하는 기재로 작동하기에 충분했다. 더욱이 전쟁 시작된지 얼마지나지 않은 시점에 젤렌스키가 자신의 안전을 위해 전쟁 초기에 우크라이나를 떠났다는 확인되지 않은 가짜 정보가 온라인상에 급속도로 퍼졌다. 특히, 러시아 국가 두마(하원) 의장인 뱌체슬라프 볼로딘(Vjačeslav Volodin)의 공식 텔레그램이 이러한 허위 뉴스의 출처이기도 했다.[33] 군통수권자인 젤렌스키 대통령이 떠났다는 것이 사실이라면, 전선에서 싸우는 우크라이나의 군인과 전쟁의 공포 속에 떨고 있는 국민들은 항전이 아닌 투항과 전쟁 포기를 선택할 수도 있을 만큼 파급력이 큰 허위 뉴스였다. 러시아 정부가 직접 개입했는지의 여부를 직접적으로 밝히기는 어렵지만, 어쨌든 이는 물리적 전쟁을 쉽게 끝낼 수 있는 파급력을 가진 가짜 뉴스이자 러시아의 전략과도 합치되는 것이었다.

대통령의 국외 탈출이라는 엄청난 허위 정보 전략에 대해 젤렌스키 대통령과 그 참모들은 역시도 온라인의 빠른 전파력을 통한 대응을 선택했다. 젤렌스키는 2월 25일을 시작으로 자신이 직접 등장하는 영상을 찍어 소셜 미디어와 언론을 통해 전 세계에 공개했다. 첫 번째 게시된 짧은 영상은 어두운 밤 자신의 참모, 그리고 총리 등과 함께 수도 키이우 대통령 집무실 앞 거리에서 자신의 전쟁 의지를 과시하고 전 세계에 도움을 호소하는 것이었다.[34] 한밤중으로 추정되는 시간에 찍은 영상에서 그들 뒤로 보이는 건물은 대통령 집무실(좌)과 의회 건물(우)이었다. 전쟁 초기 러시아가 키이우로 젤렌스키 암살을 위한 특수부대를 파견했다는 사실을 비춰 볼 때, 이는 대통령의 위치를 노출하는 매우 위험한 결정이었다.[35] 그러나 이러한 결정은 전쟁 초기 러시아가 배후로 추정되는 젤렌스키의 국외 탈출설이란 가짜 정보에 맞서 군과 국민들의 저항의지를 고취해야만 하는 어쩔

32) 출처: https://www.rt.com/russia/550408-speical-operation-putin-donbass/amp/ (검색일: 2022. 04. 07.).

33) 출처: https://voxukraine.org/en/fake-volodymyr-zelensky-fled-ukraine-after-russian-invasion/ (검색일: 2022. 06. 09.).

34) 출처: https://www.nytimes.com/2022/02/25/world/europe/zelensky-speech-video.html (검색일: 2022. 06. 10.).

35) 출처: https://www.thetimes.co.uk/article/spies-accused-of-betraying-putins-chechen-units-537fj6lnr (검색일: 2022. 06. 10.).

수 없는 선택지였다.

첫 번째 영상 이후부터는 단순히 가짜 뉴스에 대한 대응을 넘어 군과 국민의 결집을 위하여 자신이 함께 싸우고 있다는 영웅적 이미지를 부각시키는 형태의 젤렌스키 대통령 영상이 주기적으로 올라오기 시작했다.[36] 다음날인 2월 26일에는 젤렌스키 대통령은 낮 시간대에 의회 건물을 배경으로 찍은 영상이 온라인상에 올렸다. 그리고 3월 7일에는 집무실 내에서 찍은 영상까지 올라왔다.

러시아는 전쟁 개시 이전에 이어 물리적 전쟁 개시에 맞춰 집중적인 사이버전을 수행했다. 미사일과 지상군의 투입 불과 몇시간 전에 이루어진 러시아의 사이버전은 마치 군사교범에 나오는 공격준비사격과도 유사했다. 우크라이나 정부와 군, 그리고 주요 공공 웹사이트들을 대상으로 한 디도스 공격과 악성 코드 유포는 전쟁 지도부의 눈을 가리기 위한 명확한 목표를 갖고 있었다. 이러한 사이버 공격은 자연스럽게 국민과 군의 저항의지를 상실하게 만드는 효과도 갖고 있었다. 군사적 관점에서 물리적 마비와 심리적 마비를 동시에 추구한 것으로 해석하기에 충분한 상황이었다. 흥미로운 점은 마비의 수단이 사이버전이었다는 사실일 것이다. 여기에 더해 러시아는 가짜 뉴스와 허위 정보를 유포하여 전선에서 전투하는 군인과 포탄 소리에 공포를 느끼고 있을 국민들의 희망을 꺾고자 했다. 소셜 미디어와 블로그에는 젤렌스키 대통령이 국민들과 군인들을 버리고 국외로 망명했다는 소식이 유포되었다. 일부 언론은 확인되지 않은 사실을 보도하며 러시아의 사이버 심리전을 돕는 상황도 발생했다. 즉, 러시아의 우크라이나 침공 초기 상황에 대한 군사적 관점 분석을 통해 볼 때, 이번 전쟁에서 러시아는 자신들의 군사적 교리에 따라 사이버전을 중심으로 하여 차세대 전쟁을 수행했음이 분명하다.

Ⅳ. 결 론

2022년 2월 25일 러시아의 우크라이나 침공은 한순간에 전 세계의 이목을 집중시켰다. 이는 냉전의 종식 이후 큰 전쟁은 없으리라 생각했던 인류의 바람이 빗나간 사건이었기 때문이기도 했지만, 러시아의 전쟁 전략과 미래의 전쟁 모습을 전망하는데 있어 중요한 사례임이 틀림 없기 때문이기도 하다. 특히 이번 러시아의 우크라이나에 대한 전면적 침공은 전쟁 초기 국가가 승리라는 목표 아래 전쟁의 전체 국면을 위해 사이버 수단을 어떻게 활용하는지를 극명히 보여주고 있어 그 연구 가치가 높다.

---

36) 출처: https://voxukraine.org/en/fake-volodymyr-zelensky-fled-ukraine-after-russian-invasion/ (검색일: 2022. 06. 09.).

먼저, 러시아는 서구가 말하는 비선형 전략인 하이브리드 전쟁 전략을 차세대 전쟁이란 용어로 부르며 군사적 교리를 정교히 발전시켜왔다. 이러한 상황을 말해주듯이 미 해대원의 석사논문에서 처음 사용된 하이브리드 전쟁이란 용어 자체도 냉전 종식 직후 러시아와 체첸 간의 전쟁 사례를 분석하여 나온 바 있다. 더욱이 2008년 러시아-조지아 전쟁은 전통적인 물리적 수단과 사이버전이 결합된 첫 대규모 하이브리드 전쟁으로 평가받고 있다. 여기서 러시아는 군사교리적으로 사이버전을 정보전이라 부르고 있으며, 정보통신기술을 사용해 전쟁 이전부터 전쟁 단계에서까지 적의 국민과 군대의 저항의지를 말살시키는 것으로 정의하고 있다. 즉, 러시아는 디도스 공격과 같은 단순한 사이버 공격부터 해킹과 악성 코드 유포, 데이터 탈취, 그리고 소셜 미디어 등 온라인 가상 공간을 통해 가짜 뉴스와 허위조작사실 유포하는 등의 사이버전을 통해 전쟁의 전략적 승리를 추구하고 있다.

2022년 러시아-우크라이나 전쟁의 초기 전역은 이러한 러시아의 사이버전이 군사교리상으로 정확히 적용된 전형적 사례이다. 러시아의 군사사상가들이 주장한 것처럼 전쟁 이전에 적의 국민과 군인들이 싸우고자 하는 의지를 상실하도록 사이버전을 수행했다. 물리적 전쟁 시작 약 40일 전에 우크라이나의 주요 웹사이트들이 디도스 공격부터 해킹 공격에 노출되었다. 그리고 약 10일 전에 우크라이나 군대의 웹사이트도 러시아 추정 해커들의 공격 목표였다.

전쟁의 시작 역시도 사이버 공격준비사격과 함께 시작되었다. 러시아의 물리적 공격 수시간 전에 우크라이나의 주요 웹사이트 등이 사이버 공격을 받은 것이다. 이는 마치 제1·2차 세계대전 이후 발전된 공격준비사격이라는 전술과도 유사했다. 전 세계의 군대는 지상병력의 안전과 작전의 성공을 위해 미사일과 포병 사격으로 적의 주요 목표에 대한 제압 또는 전선에 있는 병력의 시야 확보를 어렵게 한 후 주력 부대를 적의 전선으로 진격시킨다. 그런데 이번 전쟁에서 러시아는 미사일과 포병 사격에 앞서 사이버 공격을 통한 공격준비사격을 먼저 하는 치밀함까지 보였던 것이다.

전쟁 중에도 러시아의 사이버전은 계속되었다. 본문에 설명은 되어 있지 않지만 데이터 탈취부터 상대의 지도부와 군의 네트워크 시스템을 마비시키기 위한 다양한 사이버전이 치열하게 벌어지는 것은 당연한 것이었다. 이러한 당연한 모습보다 더 큰 주목을 받은 사이버전의 형태는 소셜 미디어 등을 통해 소위 가짜 뉴스라고 하는 허위조작된 정보가 급속도로 대중에게 유통된 사실이었다. 저항의지를 말살하기 위한 다양한 허위정보가 유통되었고, 그 중에 가장 대표적인 것은 젤렌스키 대통령의 국외 탈출 뉴스였다. 그 가짜 뉴스가 가져올 파급효과가 엄청날 것으로 예상되었기에 젤렌스키 대통령 등 우크라이나 정부는 적극적으로 대처하여 위기를 넘기기도 했다. 이는 단순히 적의 시스템 무력화와

중요한 정보의 탈취를 넘어 상대의 전쟁 수행 의지 자체를 말살시키고자 하는 러시아의 사이버전 전략이 완벽히 적용된 것이었다.

본 연구는 서구에서 하이브리드 전쟁과 사이버전으로 불리고 있는 러시아의 차세대 전쟁과 정보전을 통해 2022년 러시아-우크라이나 전쟁의 초기 전역을 분석하였다. 전쟁이 아직 종료되지 않은 시점이긴 하지만, 이번 분석을 통해 러시아가 전쟁 이전부터 사이버전을 통해 하이브리드 전쟁 전략을 적용하여 적의 국민과 군대의 저항의지를 조기에 말살시켜 손쉬운 전쟁의 승리를 추구했었음을 알 수가 있었다. 그리고 이러한 분석을 통해 지금 이순간, 그리고 전쟁 이후에도 계속해서 하이브리드 전쟁 전략 개념에 기초하여 우크라이나에 대한 사이버전을 수행하리라 예상된다. 더욱이 이러한 하이브리드 전쟁 개념과 사이버전은 러시아만이 아니라 앞으로 모든 국가들이 적극적으로 군사교리상 적용할 것으로 예상되기에 우리 군도 이에 대한 대비를 철저히 해야할 것이다. 끝으로 이번 연구는 작성 시점의 문제로 인해 전쟁 초기까지로 범위가 제한적이라는 한계점을 갖고 있다. 그러나 본 논고가 앞으로 전쟁 종료 이후 러시아의 하이브리드 전쟁과 사이버전에 관한 심도 있는 논의의 시작점이 될 수 있길 바란다.

참고문헌

- 김경순. 2018. 러시아의 하이브리드전 - 우크라이나사태를 중심으로. 한국군사 4, 63-95.
- 박동휘. 2019. 국가의 적대적 사이버 공세 전략의 기원 - 볼셰비키 혁명 직후 영국의 러시아 내전 개입을 중심으로. 영국 연구 42, 317-352.
- _____. 2022. 사이버전의 모든 것. 플래닛미디어.
- 송승종. 2016. 하이브리드 전쟁과 북한에 대한 시사점: 우크라이나 사례를 중심으로. 국방 연구 59(4), 125-165.
- _____. 2017. 러시아 하이브리드 전쟁의 이론과 실재. 한국군사학논집 73(1), 63-94.
- 송태은. 2021. 디지털 시대 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술: 미국과 유럽의 대응을 중심으로. 세계지역연구논총 39(1), 69-105.
- 신범식·윤민우. 2020. 러시아 사이버안보 전략 실현의 제도와 정책. 국제정치논총 60(2), 167-209.
- Ajir, Media and Bethany Vailliant. 2018. Russian Information Warfare: Implications for Deterrence Theory. Strategic Studies Quarterly 12(3), 70-89.
- Blank, Stephen. 2008. Web War I: Is Europe's First Information War a New Kind of War?. Comparative Strategy 27(3), 227-247.
- Chekinov, S.G. and S.A. Bogdanov. 2013. The Nature and Content of a New-Generation War. Military Thought, 12-23.
- Galeotti, Mark. 2015. 'Hybrid War' and 'Little Green Men': How It Works and How It Doesn't. E-International Relations. 출처: https://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/ (검색일: 2022. 05. 30.).
- Gareev, M. Translated by Yakov Vladimirovich Fomenko. 1998. If War Comes Tomorrow? The Contours of Future Armed Conflict. Routledge.
- General Gerasimov's article is available in English from Mark Galeotti. 2014. 7. The 'Gerasimov Doctrine' and Russian Non-Linear War. In Moscow's Shadows (blog), 출처: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war (검색일: 2022. 06. 15.).

- Gerasimov, Valery. 2016. The Value of Science is in the Foresight. Military Review January-Febrary, 23-29.
- Grant, Thomas D. 2015. Annexation of Crimea. The American Journal of International Law 109(1), 68-95.
- Herzog, Stephen. 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security 4(2), 49-60.
- Hoffman, Frank G. 2007. Conflict in the 21st Century: the Rise of Hybrid Wars. Potomac Institute for Policy Studies.
- Kozlowski, Andrzej. 2014. Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. European Scientific Journal 3, 237-245.
- Kuzio, Taras. 2010. Nationalism, identity and civil society in Ukraine: Understanding the Orange Revolution. Communist and Post-Communist Studies 43(3), 285-296.
- Mankoff, Jeffrey. 2022. Russia's War in Ukraine Identity, History, and Conflict. Center for Strategic and International Studies.
- NATO. 2014. 7. Hybrid War: Hybrid Response. 출처: https://www.nato.int/docu/review/articles/2014/07/01/hybrid-war-hybrid-response/index.html (검색일: 2022. 06. 15.).
- Nemeth, W. J. 2002. Future War and Chechnya: a Case for Hybrid Warfare. Master Thesis, Monterey, California. Naval Postgraduate School.
- Parihar, S. 2022. Russia Ukraine War-the Current Scenario. Academic Journal of Digital Economics and Stability 16, 29-38.
- Park, D. and M. Walstrom. 2017. Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks. University of Washington, The Henry M. Jackson School of International Studies. JSIS News.
- Racz, Andras. 2015. Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. FILA Report No. 43.
- Reisinger, Heidi and Aleksandr Golts. 2014. Russian Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defence. research paper no. 105, NATO Defence College.

■ Robinson, Paul. 2016. Russia's role in the war in Donbass, and the threat to European security. European Politics and Society 17(4), 506-521.
■ Sebastian, N. 2022. Russia-Ukraine Conflict: Issues and Implications for Regional and Global Politics. From Illusion to Reality-The Nation 75, 762-773.
■ Snegovaya, Maria. 2015. Russia Report 1. Putin's Information Warfare In Ukraine: Soviet Origins of Russia's Hybrid Warfare. Institute for the Study of War(ISW). 출처: https://www.understandingwar.org/report/putins-information-warfare- ukraine-soviet-origins-russias-hybrid-warfare (검색일: 2022. 05. 30.).
■ Russian Federation. 2011. Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. NATO Cooperative Cyber Defence Center of Excellence(CCDCOE). 출처: https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf (검색일: 2022. 06. 15.).

■ 국방일보
■ AP News
■ CNN
■ Computerweekly
■ NPR
■ Politico
■ Reuters
■ Russian Today(RT News)
■ Sky News
■ The Financial Times
■ The Guardian
■ The New York Times
■ The Times
■ VoxUkraine

■ blog.alyac.co.kr

■ edmo.eu
■ eset.com
■ gov.uk
■ mandiant.com
■ microsoft.com
■ ncsc.gov.uk
■ welivesecurity.com

● 투고일: 2022.07.04. ● 심사일: 2022.07.28. ● 게재확정일: 2022.08.25.

| Abstract |

Russian Cyber Warfare Strategy during the Early Stage of Russia's Invasion of Ukraine

Moon Yongdeuk (First Author, Korea Army Academy at Yeongcheon)
Park Donghui (Corresponding Author, Korea Army Academy at Yeongcheon)

On February 24, 2022, an all-out war broke out between Russia and Ukraine, which have long experienced ethnic conflicts. Based on its new-generation war strategy, Russia wages its war on Ukraine not only in the physical domains but also in cyberspace. It tries to obliterate the will of Ukrainian people and military to resist against Russia by using cyber warfare. This is a typical hybrid war that Russia has pursued since the end of the Cold War. This study analyzes the concept of Russia's cyber warfare as a key means of new-generation war, and tries to verify the concepts in the real case. In fact, Russia pursues its strategic victory by obliterating the will of the Ukrainian resistance through variety methods such as cyber attacks, data theft, and cyber psychological warfare before and after an all-out war. Although the scope of this study is limited to the early stage, it is hoped that this study will serve as a starting point for an in-depth discussion on Russian cyber warfare.

〈Key words〉 Russia, Ukraine, Cyber warfare, Hybrid war, New-generation war