KIPS Trans. Comp. and Comm. Sys.
Vol.11, No.10 pp.353~362
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2022.11.10.353

A Study on Korea's Countermeasures Through the Analysis of Cyberattack Cases in the Russia-Ukraine War

Hyungdong Lee† · Joonhee Yoon†† · Doeggyu Lee†† · Yongtae Shin†††

ABSTRACT

The Russian-Ukraine war is accompanied by a military armed conflict and cyberattacks are in progress. As Russia designated Korea as an unfriendly country, there is an urgent need to prepare countermeasures as the risk of cyberattacks on Korea has also increased. Accordingly, impact of 19 cyberattack cases were analyzed by their type, and characteristics and implications were derived by examining them from five perspectives, including resource mobilization and technological progress. Through this, a total of seven measures were suggested as countermeasures for the Korean government, including strengthening multilateral cooperation with value-sharing countries, securing cyberattack capabilities and strengthening defense systems, and preparing plans to connect with foreign security companies. The results of this study can be used to establish the Korean government's cybersecurity policy.

Keywords : Russia-Ukraine War, Cyberattack, Countermeasures, IT Army, Hacktivists

러시아-우크라이나 전쟁에서의 사이버공격 사례 분석을 통한 한국의 대응 방안에 관한 연구

이 형 동† · 윤 준 희†† · 이 덕 규†† · 신 용 태†††

요 약

러시아-우크라이나 전쟁이 군사적 무력 충돌과 함께 사이버공격이 진행되고 있다. 이번 전쟁과 관련하여 러시아가 한국을 비우호 국가로 지정함에 따라 한국에 대한 사이버공격의 위협성도 고조된 만큼 대응 방안 마련이 시급한 상황이다. 이에 따라 이번 전쟁에서 나타난 사이버공격 사례(19건)를 유형별로 영향을 분석하고, 자원 동원, 기술 진보 등 5가지 관점에서 고찰하여 특징과 시사점을 도출하였다. 이를 통해 한국 정부의 대응 방안으로, 가치공유 국가와의 다자협력 강화, 사이버공격 역량확보와 방어체계 강화, 해외 보안업체와의 연계 방안 마련 등 총 7가지를 제시하였다. 연구 결과는 한국 정부의 사이버안보 정책 수립에 활용될 수 있을 것이다.

키워드 : 러시아-우크라이나 전쟁, 사이버공격, 대응 방안, IT군대, 헥티비스트

1. 서 론

러시아-우크라이나 전쟁은 러시아가 2022년 2월 24일 우크라이나 영토를 침공하면서 시작되었다. 이번 전쟁은 군사적 무력 충돌 외에도 경제 제재, 사이버공격, 심리전 등 여러 형태의 하이브리드전 양상으로 진행되고 있다[1]. 특히 러시아는 2008년 조지아 및 2014년 우크라이나의 크림반도를 대상으로 한 무력 침공에서 전쟁 개시 전부터 감행했던 사이버공격을 이번 전쟁에서도 활용하고 있다.

이러한 전쟁 상황과 관련하여 미국 바이든 대통령은 2022년 3월 21일 러시아의 사이버공격을 경고하며, 민간 파트너들의 즉각적인 사이버보안 강화를 촉구하였다[2]. 한국도 러시아가 비우호국가로 지정함에 따라 사이버공격의 대상이 될 가능성이 있다. 따라서 이번 전쟁에서 나타난 사이버공격의 사례를 분석하여 한국의 대응 방안을 마련하는 것이 시급한 상황이다.

한편, 국제전기통신연합(ITU)이 2021년 발표한 국제사이버보안지수(Global Cybersecurity Index 2020)에 따르면 우크라이나와 한국은 각각 78위와 4위를 차지하여 사이버보안 역량에서 상당한 차이를 보여주고 있다[3]. 그러나 양국이 각각 러시아와 북한으로부터 지속적인 사이버공격을 받았다는 공통점도 가지고 있다. 우크라이나는 러시아의 '사이버 놀이터(Cyber Playground)'라고 불릴 정도로 2014년 이후 러시아로부터 많은 사이버공격을 받았으며, 2015년과 2016년에는 전력시설까지 공격을 받아 동부지역 및 수도 키예프가 일시 정전되는 피해를 겪었다[4]. 한국도 2009년 7·7 DDoS

† 준 회 원 : 숭실대학교 IT정책경영학과 박사과정
†† 비 회 원 : 숭실대학교 IT정책경영학과 박사과정
††† 종신회원 : 숭실대학교 컴퓨터학부 교수
Manuscript Received : June 14, 2022
Accepted : July 19, 2022
* Corresponding Author : Yongtae Shin(shin@ssu.ac.kr)

공격, 2013년 3·20 및 6·25 사이버테러, 2016년 정부 주요 인사 스마트폰 해킹 등 북한의 지속적인 사이버공격에 시달리고 있다[5]. 따라서 이번 전쟁에서 나타난 러시아의 사이버공격과 이에 대한 우크라이나의 대응 실태를 살펴보는 것은 유사시 북한의 사이버공격 양상을 예측하고 한국의 대응 방안을 마련하는 데 많은 시사점을 제공해 줄 것이다.

이전에도 사이버전에 대한 많은 선행연구가 있었지만, 사이버전의 개념이나 공격과 방어 기술[6]에 관하여 진행되었으며, 북한을 포함한 각국의 역량이나 실태 분석[7, 8]에 머물렀고, 정작 실제 물리적 전쟁과 연결된 사이버공격의 사례에 관한 연구는 이루어지지 않았다. 오현철은 러시아의 2014년 크림반도 합병 과정에서 등장한 하이브리드 전쟁과 관련하여 연구하였으나 사이버 무기의 종류와 국제법적 적법성에 관한 내용에 중점을 두었다[9].

이에 따라 본 논문에서는 러시아-우크라이나 전쟁에서 나타난 사이버공격 사례로부터 새로운 특징을 분석하여 한국에게 주는 함의를 도출하고 대응 방안을 제안하고자 한다. 다만, 현재 러시아-우크라이나 전쟁이 진행 중이고 양국이 사이버공격의 피해 상황을 비공개 또는 부인하고 있어서 정확한 사례를 파악하는 데 어려움이 있다. 이러한 자료 수집의 한계를 감안하여 본 논문에서는 서방 언론이나 글로벌 보안업체에서 발표한 사이버공격 사례를 중심으로 분석하기로 한다.

본 논문은 제2장에서 사이버전의 개념과 특성을 파악하고, 과거 무력 전쟁에서 구사한 러시아의 사이버공격 사례와 특성을 살펴본다. 제3장에서 러시아-우크라이나 전쟁에서의 사이버공격 사례와 특징을 고찰하고자 한다. 마지막으로 제4장과 제5장에서는 제3장의 내용을 바탕으로 한국에게 주는 함의와 대응 방안을 정책적으로 제안한다.

2. 사이버전과 사이버공격의 개념

2.1 사이버전의 개념과 사이버공격의 관계

사이버전(Cyber warfare)이라는 용어는 시기나 상황에 따라 다양하게 정의되고 있다. 국내에서는 국방기술진흥연구소가 제공하는 국방과학기술용어사전에서 사이버전을 “컴퓨터 네트워크를 통하여 디지털화된 정보가 유통되는 가상적인 공간에서 다양한 사이버공격 수단을 사용하여 적의 정보 체계를 교란·거부·통제·파괴하는 등의 공격과 이를 방어하는 활동”으로 정의하고 있다[10].

또한 사이버전은 분류기준에 따라서 다양하게 나눌 수 있다. 박호균은 사이버공격과 사이버 방어로 나누었으며[11], 김진광은 공격적 사이버전, 방어적 사이버전, 사이버전 지원으로 확대하였다[12]. 류창하는 사이버전을 작전 수행 방법에 따라 사이버공격, 방어, 심리전으로 분류하였다[13]. 모두 사이버공격이 사이버전의 핵심을 차지한다고 할 수 있다. 따라서 이번 전쟁의 사이버공격의 사례를 분석하면 대략적인 사이버전 양상도 파악이 가능할 것이다.

2.2 사이버공격의 정의와 유형

사이버공격은 복합적인 개념이 포함되어 있다.「국가사이버안전관리규정」은 “해킹 · 컴퓨터바이러스 · 논리폭탄 · 메일폭탄 · 서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입 · 교란 · 마비 · 파괴하거나 정보를 절취 · 훼손하는 일체의 공격행위를 말한다.”라고 정의하고 있다[14].

한편, 사이버공격의 유형을 적용기술, 수행목적 등에 따라 구분할 수 있다. 이 연구에서는 물리 전쟁과 사이버공격의 의도 분석을 위해 정보 절취와 변조, 시스템 무력화, 국가기반시설 마비/파괴로 구분하여 수행목적의 관점에서 고찰하고자 한다.

또한 사이버공격은 크게 인원을 대상으로 사회 공학적 기법을 활용하는 방법과 시스템을 대상으로 취약점을 활용하는 방법으로 이루어진다. 여기에 사용되는 공격 기술은 단독 또는 복합적으로 활용되며, 대표적인 공격 기술을 Table 1로 정리하였다.

2.3 과거 러시아의 사이버공격 사례 및 특징

러시아가 무력 전쟁이나 유사한 분쟁에서 사용하였던 사이버공격 3건을 선정하여 그 특성을 분석하였다.

Table 1. Main Types of Cyberattack Techniques

Techniques	Contents
Phishing	Technology that deceives the other party into a harmful action with a forged email or message. Spear Phishing, Credential Stuffing. etc.
Malware	Software developed to interfere with the normal functioning of mobile phones, PCs, servers, networks, etc. Worm,Viruses, Trojans, Wiper, Ransomware, etc.
Denial of Service	Technology that interferes with the access of others by sending a large amount of traffic to a website that the server cannot handle. Including distributed denial of service.
SQL Injection	Using vulnerabilities such as websites, sending malicious query language(SQL) to control the database without permission.
Man-in-the-Middle	A hacker intervenes in the communication between the client and the server and intercepts all information such as the user's ID and password. ARP and DNS Spofing, Session Hijacking, etc.
Zero Day	When a vulnerability exists because a defect in software or hardware is not fixed, an attacker exploits it.

첫 번째는 에스토니아의 정부 시스템을 대규모 마비시킨 사례이다. 2007년 4월 에스토니아 정부가 수도 탈린에 있던 소련군 동상을 외곽으로 옮기면서 러시아계 주민들의 극심한 시위로 서로 충돌하였다. 러시아는 이에 대한 보복으로 약 3주에 걸쳐 서비스거부(DoS)와 분산서비스거부(DDoS) 공격을 감행하였다. 이에 따라 에스토니아는 대통령궁, 정부, 의회, 은행, 언론사 등 주요 국가기관들의 홈페이지와 전산망이 마비되어 극심한 사회적 혼란을 겪게 되었다[15]. 이 사건은 러시아가 무력 공격을 사용하지 않고 에스토니아에 정치적, 외교적으로 영향을 미친 사례라고 할 수 있다.

두 번째는 사이버공격을 활용한 조지아와의 하이브리드 전쟁(Hybrid War)이다. 2008년 8월 조지아 남오세티야의 독립 갈등으로 러시아가 조지아에 지상군을 투입하였다. 러시아는 무력 침공 이전부터 DDoS, 홈페이지 화면 변조(Deface) 등 다양한 사이버공격을 시작하여 조지아의 국방부·외교부 등의 전산망을 마비시키는 최초의 하이브리드 전쟁을 감행하였다. 조지아는 전쟁 지휘도 서방국의 원조도 요청할 수 없게 되어 5일 만에 패전하였다[13]. 러시아가 물리적 공격을 동반한 사이버공격으로 군사적, 정치적, 외교적 효과를 거두었다고 할 수 있다.

세 번째는 우크라이나의 사회기반시설까지 마비시킨 사례이다. 2014년 러시아가 우크라이나의 크림반도를 합병하는 과정에서 무력 침공하기 직전에 DDoS 공격을 시작하여 우크라이나의 통신 네트워크와 정부 웹사이트를 마비시켰다. 또한 러시아에 기반을 둔 해커들은 우크라이나 중서부에 대규모 정전을 유발하는 등 사회기반시설까지 사이버공격을 감행하였다[16]. 이러한 사이버공격은 물리적 전쟁을 유리하게 이끄는 데 크게 기여하였다.

3. 러시아-우크라이나 전쟁에서 나타난 사이버공격 사례 및 특징

현재 러시아-우크라이나 전쟁이 진행 중이고, 양국은 사이버공격이나 피해 상황을 구체적으로 공개하지 않고 있어서 공식 사례를 수집하는 데 어려움이 있었다. 이에 따라 본 연구에서는 각국 언론이나 보안업체가 제공하는 자료를 통해 사이버공격 사례를 수집하였다. 이들 사례를 유형별로 분류하고, 공격 대상과 영향을 고찰하여 사이버공격의 특징을 도출하고자 한다.

3.1 러시아(친러시아 포함)의 사이버공격 사례

1) 홈페이지 마비시키는 DDoS 공격

우크라이나의 은행이나 국방부 등 주요 웹사이트를 대상으로 한 러시아의 DDoS 공격은 여러 번 있었다. 그중 대표적인 것은 2022년 2월 러시아 군사 정보기관인 총정찰국(GRU)이 실행한 사례[17]와 2022년 3월 '다나봇(DanaBot)'을 활용한 사례이다[18].

2) 정부 기관의 홈페이지 화면을 변조하는 디페이스(Deface) 공격

2022년 1월 벨라루스 국방부 소속으로 추정되는 해킹조직인 '고스트라이터(Ghostwriter)'에 의해 우크라이나 정부의 웹사이트 70개 이상이 사이버공격을 받아 웹사이트가 훼손되었다. 해커들은 러시아 군대가 국경을 넘어 우크라이나로 진입하기 전에 "두려워하고 최악의 상황을 예상하라"라는 메시지를 웹사이트에 게시하는 화면 변조 공격을 했다[19].

3) 군인 및 정부 관료 대상 다양한 피싱 공격

러시아가 구사한 피싱 기법도 다양하게 발견되었다. 첫째, 벨라루스 해킹조직인 고스트라이터가 러시아의 무력 침공 다음 날 폴란드 군인 및 우크라이나 정부와 군인을 대상으로 첨부파일에 악성코드가 포함된 피싱 메일로 공격하였다[20]. 둘째, 2022년 3월에 러시아와 연관된 해킹조직인 가마레돈(Gamaredon)이 우크라이나를 대상으로 피싱 이메일을 유포하였다[21]. 셋째, 2022년 2월 하순부터 러시아 해킹조직인 APT28이 우크라이나의 미디어업체(UKRNet) 사용자를 대상으로 계정, 비밀번호 등 신원인증 데이터를 탈취하려고 크리덴셜 피싱(credential phishing) 공격을 하였다[22]. 넷째, 2022년 4월 초 '브라우저 인 더 브라우저(BitB, Browser in the Browser)'라는 새로운 피싱 공격이 우크라이나와 유럽지역에서 발견되었다. 우크라이나의 침해대응팀(CERT)과 보안업체(Mandiant) 등은 벨라루스 고스트라이터 그룹의 소행이라고 경고하였다[23].

4) 시스템 파괴하는 와이퍼(Wiper) 공격

컴퓨터나 네트워크 시스템의 데이터를 삭제하여 기능을 마비시키는 와이퍼 악성코드가 우크라이나에서 다양하게 발견되었다. 첫 번째는 '위스퍼 게이트(WhisperGate)'로 2022년 1월 우크라이나의 외무부를 포함한 70여 개의 정부 웹사이트를 중단시켰다[24]. 두 번째는 '허메틱 와이퍼(HermeticWiper)'인데, 러시아가 우크라이나를 침공하기 전날 우크라이나에 유포되어, 데이터를 훼손하고 시스템을 불능화하였다. 이것은 발트해 연안 국가의 시스템에도 영향을 미쳤을 수 있다[22]. 세 번째는 전쟁 발생 당일 유포된 '아이작 와이퍼(IsaacWiper)'이다. 이는 허메틱 와이퍼로 파괴되지 않은 우크라이나 시스템에서 발견되었으며, 먼저 침투해 있었던 것으로 추정된다[25]. 네 번째는 2022년 3월 발견된 '캐디 와이퍼(CaddyWiper)'이다. 이는 허메틱이나 아이작 와이퍼와 유사점이 없는 새로운 종류이다[26]. 다섯 번째는 2022년 3월 중순 발견된 더블 제로(DoubleZero)라는 새로운 변종 와이퍼이다[27].

5) 사회기반시설 마비 위한 사이버공격

우크라이나의 사회기반시설을 마비시키기 위한 사이버공격도 다수 발견되었다. 첫째는 국제 위성 인터넷(Viasat) 서비스를 마비시킨 공격이다. 전쟁 개시 당일에 위성 인터넷 제공업체인 Viasat의 일부 네트워크가 러시아 총정찰국(GRU)의 소행으로 추정되는 사이버공격을 받아서 우크라이나에서 통신 장애가 며칠 동안 발생하였다. 그 피해는 유럽 전역의 모뎀과 독일 에너지 회사(Enercon)가 운영하는 풍력 터빈에도 영향을 미친 것으로 알려졌다[28]. 둘째는 2022년 3월 말 우크라이나의 통신회사(Ukrtelecom)에 대한 사이버공격이다. 이 공격으로 전쟁 이전보다 인터넷서비스 능력이 13%까지 떨어졌으나, 15시간 이내 복구된 것으로 알려졌다[29]. 셋째는 우크라이나의 전력망에 대한 사이버공격 시도이다. 4월 우크라이나 보안기관(CERT-UA)과 보안업체(ESET)가 우크라이나의 고압변전소를 공격하려는 'Industroyer2' 악성코드를 사전 발견하였다. 이것은 2016년 우크라이나 키이우의 정전에 사용되었던 'Industroyer'의 새로운 버전이며, 러시아 해킹조직의 소행으로 알려졌다[30].

3.2. 우크라이나(친우크라이나 포함)의 사이버공격 사례

1) 주요 기관 사이트 마비 공격

러시아에 대한 DDoS 공격은 여러 번 실행되었다. 먼저, 어나니머스 그룹은 러시아 크렘린궁과 국방부 사이트 등을 마비시켰다[31]. 또한 우크라이나 정부가 SNS로 전 세계에서 모집한 'IT군대(IT Army of Ukraine)'는 러시아의 정부 및 은행 웹사이트들을 마비시켰다[32].

2) 러시아 국영 TV 해킹 및 방송 변조

이번 전쟁 개시 다음 날 국제 핵티비스트인 어나니머스(Anonymous) 그룹은 러시아 정부에 대해 "사이버 전쟁"을 선포하였다. 이후 러시아 스트리밍 서비스인 Wink와 Ivi, 라이브 TV 채널 Russia 24 등을 해킹하여 전쟁의 참상을 알리고 전쟁을 반대하는 영상을 송출하였다[33].

3) 시스템 침투 및 자료 절취·공개

4월 초에는 어나니머스 그룹이 러시아 군인 12만 여명의 이름, 생년월일, 소속 부대를 포함한 개인 데이터를 공개하면서 "우크라이나 침공에 참여하는 모든 군인은 전범 재판에 회부되어야 한다"고 주장하였다[34]. 또한 러시아의 오일·가스 업체(Aerogas), 에너지 업체(Petrovsky Fort) 등에서 빼돌린 400GB의 이메일을 고발 전문 사이트인 디도시크렛(DDoSecrets)에 공개하였다[35].

4) 러시아 시스템 선별 파괴 와이퍼 공격

2022년 3월 등장한 '루랜섬(RURansom) 와이퍼'는 친우크라이나 핵티비스트가 사용한 것이며, 코드 내에 벵골어로 "러시아를 해칠 목적으로 개발했다"는 메모가 포함되어 있었다. 또한 러시아 IP의 시스템에서만 악성코드가 실행되도록 설계되어 있었다[36].

5) 데이터 파괴 프로테스트웨어(protestware) 공격

2022년 3월 오픈소스(node-ipc)의 개발자가 러시아에 항의하기 위해 자신이 개발한 라이브러리에 악성코드를 삽입하여 올려놓았다. 이 악성코드는 시스템의 IP주소가 러시아나 벨라루스인 경우 모든 파일을 '하트' 캐릭터로 덮어쓰도록 하였다. 그런데 일반 개발자가 이 라이브러리를 활용하여 응용프로그램을 개발할 경우 연쇄적인 피해가 발생할 수 있었다. 이에 프로테스트웨어 개발자는 악성기능이 있다는 설명을 붙인 버전으로 수정하여 일반개발자가 그 악성 기능의 활용 여부를 선택하도록 하였다[37].

6) 벨라루스 기반시설인 철도 시스템 공격

벨라루스의 반정부 핵티비스트 그룹인 사이버 파르티잔(Cyber Partisans)은 2022년 1월 러시아 군대가 벨라루스에 배치되는 것을 방해하기 위해 벨라루스 철도의 데이터베이스를 암호화한 것으로 알려졌다. 또한 2월에도 벨라루스에서 우크라이나로 이동하는 러시아군의 이동을 늦추기 위해 기차 통제시스템과 웹사이트를 사이버 공격하여 승차권 구매와 열차 운행에 차질을 주었다[38].

지금까지 살펴본 사이버공격 사례(19건)를 유형별로 분석하여 정리하면 Table 2와 같다.

3.3 양국 사이버공격의 특징 및 함의

여기서는 Table 2를 참고하여 양국의 사이버공격을 조직·기술 자원 동원, 기술의 진보, 대상, 목적, 효과 등 측면으로 고찰하여 특징과 시사점을 도출하고자 한다. 특히 러시아의 경우에는 제2장에서 분석한 사례와도 비교하여 변화 양상을 살펴보려고 한다.

1) 러시아 사이버공격의 특징과 함의

첫째, 공격자원 동원 측면에서 과거에 대비하여 훨씬 많은 기술과 조직을 활용한 총력전을 펼치고 있는 것으로 보인다. 기술적으로, 와이퍼의 변종이 최소 5개 이상이고, 피싱도 BitB 등 여러 종류가 등장하였다. 이렇게 다양한 변종이 출현했다는 것은 여러 조직을 동원했다는 것을 시사해 준다. 또한, 동일 시스템에서 2개 이상의 변종 악성코드가 동시 출현했다는 것은 조직간 사전 조율이나 지휘통제 체계가 미흡한 것이라고 볼 수 있다.

둘째, 공격기술의 진보 측면에서 러시아는 획기적인 진전이 없는 정체 상태라고 할 수 있다. 물론 새로운 피싱, 다양한

Table 2. Classification by Type of Cyber Attacks in Both Countries

	Type	Target	Impact
Russia	Interrupting access (DDoS)	Websites of banks and Ministry of National Defense	Temporary access failure
	Information tampering	70 websites of government agencies	Creating a sense of fear by tampering with the website
	Information theft (3 cases)	Bureaucrats, Soldiers	Providing a base for information leakage and penetration
		Media company users, Soldiers	Leakage of identity authentication data
	Systems destruction (5 cases)	Computer networks of the Ministry of Foreign Affairs and the Cabinet	Wiper wipes data and paralyzes the system
	Infrastructure destruction (3 cases)	Satellite network, Wired internet	Recovery after some internet paralysis
		Control system of high voltage substation	Detect malware in advance, no damage
Ukraine	Interrupting access	Government websites such as the Ministry of National Defense	Temporary access failure
	Information tampering	Government websites such as the Ministry of National Defense	Informing Russian citizens of the facts and encouraging anti-war
	Information theft and disclosure	Military and state-owned enterprises	Disclosure of personal data of soldiers and confidential information of enterprises
	Systems destruction (2 cases)	Russian and Belarusian computer networks	Supply chain security threats. No specific damage confirmed
	Infrastructure destruction	Belarusian Railway system	Stop trains and disrupt the deployment of Russian troops

변종 등 일부 진전은 있었지만, 사이버공격의 전략이나 기술, 기법 등에서 현재까지 혁신적인 모습을 보여주지 못하고 있다. 러시아가 2014년 이후 우크라이나에서 지속 활용해왔던 기술과 특별한 차이가 없다면 학습효과로 인해 사이버공격의 효과에도 한계가 존재할 것이다.

셋째, 공격대상 측면에서 살펴보면 목표를 개인과 홈페이지에서 사회기반시설까지 우크라이나 지역 내 전방위로 확대하고 있다. 이것은 이전의 크림반도 합병에서 나타난 공격 대상과 크게 다르지 않으며, 물리적 군사작전을 위한 여건 조성에 중점을 둔 것으로 판단된다. 한편, 지역적으로는 우크라이나를 넘어 유럽으로 확대되고 있다. 러시아는 다국적 기업이 운영하는 위성통신망을 공격하여 유럽의 일부 위성 인터넷까지 마비시켰다. 또한 폴란드 정부와 군대를 직접 겨냥하고 있으며, 발트해 연안 국가와 유럽지역에도 의도 또는 비의도적인 피해가 미쳤다. 이러한 러시아의 사이버공격 양상은 나토와의 사이버전으로 확산할 위험성을 안고 있음에도 불구하고 미국 및 유럽연합의 우크라이나 지원에 대한 불만의 표시일 수도 있다.

넷째, 공격목적 측면에서 정보활동과 시스템 파괴를 병행하고 있는 것으로 보인다. 러시아는 우크라이나 및 폴란드 정부와 군인을 대상으로 대규모 피싱 공격을 한 것은 정보 수집을 위한 것으로 볼 수 있다. 또한 와이퍼가 최소 5종 이상이 발견된 것을 감안하면 우크라이나의 주요 시스템에 대한 파괴에도 집중하는 것을 알 수 있다.

다섯째, 공격의 효과 측면에서는 러시아의 공세 강도를 감안하면 실제 효과는 저조한 것으로 보인다. 그 원인은 먼저, 러시아의 기술과 수법이 상대의 방어역량을 압도할 만큼 높은 수준이 아니었다는 점이다. 또 하나는 우크라이나 정부에 대한 서방국가와 민간 보안회사의 협력이다. 특히 MS사, ESET사 등 민간업체들은 전쟁 초기부터 러시아의 사이버공격을 탐지하고 우크라이나를 지원해 왔다[39]. 마지막으로 2014년 이후 우크라이나가 러시아의 사이버공격에 대비하여 자체 보안시스템을 강화한 결과라고 할 수 있다. 특히 이 과정에서 미국의 지원이 있었으며, 미국 사이버사령부는 2021년 가을부터 '헌트 팀(Hunt Team)'을 파견하는 등 우크라이나에 대한 기술지원을 지속하고 있다[40].

2) 우크라이나의 사이버공격 특징과 함의

이번 전쟁에서 우크라이나는 전 세계에서 모집한 해커 용병 또는 핵티비스트의 사이버공격에 의존하였다. 이러한 상황에서도 새롭고 다양한 사이버공격으로 상당한 효과를 얻은 것으로 확인되었다.

첫째, 공격자원의 동원 측면에서 국제 핵티비스트의 자율적인 사이버공격에 의존하였다. 우크라이나는 부족한 인력자원 확보를 위해 SNS로 전 세계에서 '사이버 의용군(Cyber Volunteer Army)'을 모집·활용하면서 사이버전의 새로운 패러다임을 보여주고 있다. 이렇게 모집한 IT 군대는 우크라이나의 수적 열세를 만회하고, 사이버공격뿐 아니라 러시아의 허위정보를 차단하면서 러시아 국민들에게 전쟁의 실상을 전파하는 임무도 수행하는 것으로 알려졌다. 여기에 어나니머스 그룹, 벨라루스 반정부 해킹조직, 오픈소스 개발자 등도 함께 참여하고 있다. 그러나 이들 사이버공격의 상당한 성과에도 불구하고, 전략적이고 체계적이지 못하여 우크라이나의 군사 작전과의 연계성과 효과성에서 한계를 드러냈다.

둘째, 공격 기술의 진보 측면에서는 DDoS, 피싱, 와이퍼 등 기존 기법 외에도 새로운 기술이 등장하였다. 이번에 발견된 프로테스트웨어(Protestware)는 러시아 소재의 시스템만 선별하여 공격하도록 통제하는 기법도 적용되어 있다. 그러나 러시아 소재의 국제기구나 의료기관 등으로 의도하지 않게 피해가 확산할 수 있으며, 오픈소스 생태계의 신뢰성을 훼손하고 글로벌 정보통신(ICT) 공급망 보안 문제를 악화시키는 부작용이 발생하였다.

셋째, 공격대상의 측면에서 우크라이나도 러시아에 못지않게 다양하다. 러시아의 크렘린궁과 국방부 웹사이트, 국영 기업, 방송·언론사 등은 물론 러시아와 벨라루스의 철도 시스템까지 폭넓게 사이버공격이 진행되었다. 그러나 핵티비스트들의 자발적인 사이버공격에 의존하고 있어서 공격대상의 선정이 체계적이고 전략적이지 못한 한계가 있었다.

넷째, 공격의 목적과 효과 측면에서 정규조직 못지않은 의용군의 역량을 보여주고 있다. 핵티비스트들은 TV 방송 화면 변조, 군인 신상정보의 절취 및 공개, 군 수송 철도 시스템 마비 등으로 전쟁의 실상을 러시아인에게 알리고, 러시아군의 전쟁 수행을 방해하는 데 중점을 두고 있음을 알 수 있다. 특히, 러시아의 TV 방송 화면을 변조하여 전쟁의 참상을 알리거나 벨라루스의 기차 시스템을 마비시켜 러시아군의 이동을 늦추는 등의 공격 효과는 국가 배후 해킹조직에 못지않은 실력과 성과라고 할 수 있다.

지금까지 살펴본 양국의 사이버공격 특징을 자원 동원, 기술 진보, 대상, 목적, 효과 등 5가지로 분석 구분하여 정리하면 Table 3과 같다.

4. 양국 사이버공격 사례의 시사점과 대응 방안

본 장에서는 제3장에서 도출한 양국의 사이버공격 특징을 고찰하여 한국에게 주는 시사점과 대응 방안을 제시하고자 한다.

첫째, 가치공유 국가와의 다자간 협력을 강화하여야 한다. 이번 전쟁에서 러시아의 막강한 사이버공격에도 불구하고 우크라이나가 선전하고 있는 것은 미국 등 서방 국가들의 물밑 지원이 크게 작용한 것을 알 수 있었다. 한국도 유사시 사이버공격에 대응할 수 있는 정보와 기술을 지원받기 위해서는 우방국과의 협력이 중요하다. 이를 위해 자유롭고 안전한 인터넷 환경의 가치를 공유하는 다른 국가들과 양자 및 다자협력을 확대해 나갈 필요가 있다.

두 번째, 유사시에 대비하여 물리 작전과 연계 가능한 사이버공격 역량을 확보하여야 한다. 이번 전쟁을 포함한 조지아, 크림반도 등 러시아의 무력 침공에는 사이버공격을 사전 동원하는 하이브리드 전쟁 형태가 반복되고 있다. 북한도 러시아의 전술을 따라 할 가능성이 농후하다. 특히 북한이 세계

Table 3. Characteristics of Cyber Attacks in Both Countries

	Russia	Ukraine
Resource mobilization	Mobilize the army, criminal gangs, Belarus, etc.	Voluntary mercenaries at home and abroad (Hectivists)
Technological progress	Using advanced technologies such as wipers and control system malware, but no breakthrough	Combination of existing technologies such as phishing and wipers with new technologies such as protestware
Attack target	Attacks from all directions, including soldiers, government agencies, and infrastructure	Attacks focused on military, government agencies, state broadcasters and infrastructure
Attack purpose	Gathering and distorting information, paralyzing and destroying systems	Disclosure and dissemination of information, system paralysis and destruction
Attack effect	Low contrast effect on offensive strength	Some success

상위권의 사이버공격 역량을 보유한 것으로 평가되고 있는 상황에서 무력 전쟁과 사이버공격을 병행할 경우 한국에게 상당한 위협이 될 것이다. 이에 적극적으로 대응하기 위해서는 한국도 사이버공격 역량을 확보할 필요가 있다. 이를 위해는 물리 작전과 사이버공격을 효과적으로 연계할 수 있는 전술 개발이 필요하다. 또한 사이버공격은 기술에 따라 정밀 타격이 곤란하고, 비의도적으로 민간 및 의료 시설 등으로 피해가 확산할 수 있다. 전시 국제법에 맞게 공격 기술이나 기법별로 대상 목표와 전술을 개발하는 것도 중요한 과제이다.

세 번째, 신종 위협에 대응한 사이버보안 체계를 강화하여야 한다. 이번 전쟁에서 우크라이나가 러시아의 막강한 사이버공격에도 선전하고 있는 주된 이유는 튼튼한 방어 역량이라 할 수 있다. 2014년 이후 러시아의 지속적인 사이버공격이 오히려 우크라이나의 방어역량을 강화하는 데 기여한 것이다. 물리 전쟁이 발생하더라도 사이버공격을 담당하는 인력과 기술은 크게 달라지지 않기 때문에, 평소의 방어역량이 전시에도 효과를 발휘할 수 있다. 한국도 북한으로부터 평시 많은 사이버공격을 받아온 만큼, 이 경험을 토대로 변종 위협에도 대응할 수 있는 방어역량을 강화할 필요가 있다.

네 번째, 정보통신 공급망의 보안 생태계를 강화하여야 한다. 이번 전쟁에서 새롭게 등장한 프로테스트웨어는 정보통신 공급망의 안전성을 심각하게 위협하는 행위이다. 특히 최근 소프트웨어나 IT시스템을 개발하는 과정에서 오픈소스 활용을 확대하는 추세임을 감안할 때 보안대책이 시급한 상황이다. 이에 따라 정부 기관이 ICT 제품을 도입할 경우, 미국의 경우처럼 납품업체가 소프트웨어 구성내역(Software Bill of Material, SBOM)을 의무 제출하도록 현행 보안적합성 검증 제도를 보완할 필요가 있다.

다섯 번째, 유사시에 대비하여 국내외 사이버 인력의 활용 방안과 해외 보안업체와의 협력체계를 마련하여야 한다. 이번 우크라이나의 IT 군대 사례를 참고로 유사시 국내외 인력을 '사이버 의용군'으로 확보하는 방안을 강구할 필요가 있다. 이를 위해서 평소 국내의 사이버 인력을 유사시 예비병력으로 관리해야 한다. 또한 국내외 사이버 의용군 모집을 위한 외국인 신원확인 체계를 마련하고, 국제법에서 요구하는 교전권 확보방안 등을 준비해야 한다. 그 외에도 평상시 해외의 사이버보안 업체와 협력 관계를 강화해 둘 필요가 있다.

여섯 번째, 전쟁 수행에 대한 명분 확보하고 국가 이미지를 관리하여야 한다. 이번 전쟁에서 우크라이나는 자발적인 사이버 의용군을 30만 명 이상 확보할 수 있었다. 이것은 '러시아는 국제법 위반 침략자이고 우크라이나는 피해자라'는 이미지가 국제 사회에 널리 형성되었기 때문이다. 따라서 평소 국가 이미지를 강화하고, 유사시 참전의 불가피성과 정당성을 대외에 지속 발신하여 도덕적 우위를 확보하는 정책이 필요하다.

일곱 번째, 범국가적으로 사이버 공방과 복구 훈련을 강화할 필요가 있다. 심각한 사고나 유사시에 대비하여 민관군 합동의 범국가적 사이버 공격과 방어 그리고 복구 훈련을 주기적으로 시행할 필요가 있다. 이를 위해 현재 기관별로 운영 중인 자체 훈련을 유사 기관과의 합동 훈련으로 확대하여야 한다. 또한 미국의 사이버 스톰(CYBER STORM), NATO의 락쉴드(Locked Shield) 등 다양한 국제 훈련에 참가하여 기술과 경험을 쌓고, 우방국과의 네트워크를 형성해 나가야 한다.

5. 결 론

본 연구는 러시아-우크라이나 전쟁에서 나타난 사이버공격 사례(19건)를 고찰하고 특징을 분석하여 한국에게 주는 함의와 대응 방안을 제시하였다.

러시아는 대규모 기술·인적 자원을 총동원하여 공포감 조성부터 사회 기반시설까지 마비를 시도하고, 우크라이나를 넘어 유럽으로 사이버공격을 확대하는 한편, 광범위한 사이버 정보활동도 전개하였다. 그러나 2014년도 크림반도 합병 시 사용했던 사이버공격 전략과 기법에서 획기적인 진전을 보여주지 못했으며, 그 효과도 기대만큼 크지 않았다.

우크라이나는 SNS를 이용하여 의용군을 모집하는 등 사이버전의 새로운 패러다임을 바꾸면서 국제 핵티비스트의 자율적 사이버공격에 의존하였다. 그럼에도 불구하고 정규조직 못지않은 기량으로 상당한 효과를 거두었다.

이러한 러시아와 우크라이나의 사이버공격 특징과 시사점으로부터 가치공유 국가와의 다자협력 강화, 유사시 대비한 사이버공격 역량 확보 및 방어 체계 강화, 공급망 보안 생태계 구축, 국내외 사이버 인력 활용 및 해외 보안업체와의 연계 방안 마련, 국가 이미지 관리, 사이버 공방 훈련 등을 한국 정부의 대응 방안으로 제시하였다.

본 논문은 물리 전쟁에서의 사이버공격 사례를 자원 동원, 공격의 기술 진보, 대상, 목적, 효과 등 관점에서 분석하였다는 점이 기존 논문과 차별성을 가진다. 실용적으로는 한국 정부의 사이버안보 정책을 수립하는 데 활용될 수 있을 것이다. 다만, 본 연구에 활용한 사이버공격 사례는 이번 전쟁의 일부분이고, 대부분 구체적인 기술적 특성이나 피해 규모가 공개되지 않아 분석의 깊이에 한계가 있었다.

References

[1] Y. J. Kim, "Russia's hybrid warfare, Ukraine faces another cyberattack," The Kyunghyang Shinmun, 2022.2.24. [Internet], https://www.khan.co.kr/world/europe-russia/article/202202241638001.

[2] Biden, "Before Business Roundtable's CEO Quarterly Meeting," The White House, [Internet], https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/21/remarks-by-president-biden-before-business-roundtables-ceo-quarterly-meeting/.

[3] International Telecommunication Union, "Global Cybersecurity Index 2020," pp.25-26, 2021.

[4] Mathew J. Schwartz, "Cyber Activity Surges as Russia Masses on Ukraine's Border," BankInfoSecurity, [Internet], https://www.bankinfosecurity.com/cyber-activity-surges-as-russia-masses-on-ukraines-bider-a-18201.

[5] Y. D. Jung and G. S. Jeong, "A study on countermeasures against North Korea's Cyber Attack," *Journal of Convergence Security*, Vol.16, No.6, pp.43-50, 2016.

[6] D. I. Seo and H. S. Cho, "Security technology status and prospect for cyber warfare," *Korea Institute of Information Security and Cryptology*, Vol.21, No.6, pp.42-48, 2011.

[7] C. S. Park and Y.S. Park, "A study on the improvement of capability assessment and the plan for enhancing cyber warfare capability of Korea," *Journal of the Korea Institute of Information and Communication Engineering*, Vol.19, No.5, pp.1251-1258, 2015.

[8] Y. S. Lee, "A study on enhancing cyber security capabilities -Focusing on cyber weapon system development-," Ph.D. dissertation, Korea University, 2018.

[9] H. C. Oh, "The emergence of hybrid warfare and the legality of cyber weapons under international law," *The Journal of Peace Studies*, Vol.21, No.1, pp.35-57, 2020.

[10] "Cyber Warfare," Defense Science and Technology Glossary, [Internet], https://terms.naver.com/entry.naver?docId=2757573&cid=50307&categoryId=50307.

[11] H. K. Park, "Types and information security technology on cyber warfare," *The Journal of the Korea Contents Association*, Vol.11, No.4, pp.41-44, 2013.

[12] J. G. Kim, "North Korea's cyber attack threat analysis research(Based on the type of attack technology)," *Proceedings of the Korean Society of Computer Information Conference*, Vol.28, No.2, pp.107-110, 2020.

[13] C. H. Ryou, "A study on the classification and history of cyber warfare by generation," *Military Research and Development*, Vol.14, No.2, pp.59-92, 2020.

[14] "National Cyber Safety Management Regulations," [Internet], https://www.law.go.kr/LSW/admRulLsInfoP.do? admRulSeq=2000000100482.

[15] K. N. Seong, "The world's first cyber warfare and cyber security law," Boannews [Internet], http://m.boannews.com/html/detail.html?idx=53325.

[16] "Serious damage to Ukraine's electricity shortage due to continuous cyberattacks," ScienceON [Internet], https://scienceon.kisti.re.kr/srch/selectPORSrchTrend.do?cn=GTB2016001113&dbt=AGT.

[17] NCSC, "UK assesses Russian involvement in cyber attacks on Ukraine," GOV.UK [Internet], https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine.

[18] ThreatLabz, "DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense," Zscaler [Internet], https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense?&web_view=true.

[19] Pavel Polityuk and Steve Holland, "Cyberattack hits Ukraine as U.S. warns Russia could be prepping for war," REUTERS [Internet], https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/.

[20] Michael Raggi and Zydeca Cass, "Asylum Ambuscade: State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement," proofpoint [Internet], https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails.

[21] Charlie Osborne, "Ukraine warns of InvisiMole attacks tied to state-sponsored Russian hackers," ZDNet [Internet], https://www.zdnet.com/article/ukraine-warns-of-invisimole-attacks-tied-to-state-sponsored-russian-hackers/?web_view=true.

[22] Shane Huntley, "An update on the threat landscape," Threat Analysis Group [Internet], https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

[23] Keyur Talati, "Browser-in-the Browser (BITB) – A New Born Phishing Methodology," WeSecureApp [Internet], https://wesecureapp.com/blog/browser-in-the-browser-bitb-a-new-born-phishing-methodology/.

[24] Mike Lennon, "Microsoft Uncovers Destructive Malware Used in Ukraine Cyberattacks," SECURITYWEEK [Internet], https://www.securityweek.com/microsoft-uncovers-destructive-malware-used-ukraine-cyberattacks

[25] ESET Research, "IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine," ESET(welivesecurity) [Internet], https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.

[26] Charlie Osborne, "CaddyWiper: More destructive wiper malware strikes Ukraine," ZDNet [Internet], https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/.

[27] "Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243)," CERT-UA [Internet], https://cert.gov.ua/article/38088.

[28] Viasat Corporate, "KA-SAT Network cyber attack overview," Viasat [Internet], https://www.viasat.com/ about/newsroom/blog/ka-sat-network-cyber-attack-overview/.

[29] Forbes.it, "Il provider ucraino Ukrtelecom colpito dal più grave attacco informatico dall'inizio dell'invasione russa," Forbes [Internet], https://forbes.it/2022/03/30/provider-internet-ucraino-ukrtelecom-colpito-attacco-informatico/.

[30] ESET Research, "Industroyer2: Industroyer reloaded," [Internet], https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

[31] Dan Milmo, "Anonymous: the hacker collective that has declared cyberwar on Russia," The Guardian [Internet], https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

[32] Sam Schechner, "Ukraine's 'IT Army' Has Hundreds of Thousands of Hackers, Kyiv Says," The Wall Street Journal [Internet], https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX.

[33] Stuti Mishra, "Anonymous hacks Russian state TV with Ukraine footage," INDEPENDENT [Internet], https://www.independent.co.uk/news/world/europe/anonymous-wink-ivi-russia-24-channel-1-moscow-24-b2029915.html.

[34] Andrew Stanton, "Anonymous Apparently Behind Doxing of 120K Russian Soldiers in Ukraine War," Newsweek [Internet], https://www.newsweek.com/anonymous-leaks-personal-data-120k-russian-soldiers-fighting-ukraine-1694555.

[35] Vilius Petkauskas, "Three Russian firms have over 400 GB worth of emails leaked," cybernews [Internet], https://cybernews.com/cyber-war/three-russian-firms-have-over-400-gb-worth-of-emails-leaked/.

[36] Jaromir Horejsi, and Cedric Pernet, "New RURansom Wiper Targets Russia," TREND MICRO [Internet], https://www.trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html.

[37] Lucian Constantin, "Developer sabotages own npm module prompting open-source supply chain security questions," CSO [Internet], https://www.csoonline.com/article/3654298/developer-sabotages-own-npm-module-prompting-open-source-supply-chain-security-questions.html.

[38] Peter Dickinson, "Cyber partisans target Russian army in Belarus amid Ukraine war fears," Atlantic Council [Internet], https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/.

[39] Joyce Hakmeh, and Esther Naylor, "How the tech community has rallied to Ukraine's cyber-defence," The Guardian [Internet], https://www.theguardian.com/commentisfree/2022/mar/07/tech-community-rallied-ukraine-cyber-defence-eu-nato.

[40] Gen. Paul M. Nakasone, "Posture statement of Gen. Paul M. Nakasone, commander, U.S. Cyber Command before the 117th Congress," U.S. Cyber Command [Internet], https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/.

이 형 동

https://orcid.org/0000-0001-6791-3144
e-mail : hdtiger77@gmail.com
1990년 서울시립대학교 전자공학과(학사)
2017년 건국대학교 정보보호학과(석사)
2021년 ~ 현 재 숭실대학교 IT정책경영학과 박사과정
2021년 ~ 현 재 국가안보전략연구원 수석연구위원
관심분야 : 정보보호, 사이버보안 정책, ICT공급망 보안, ML

윤 준 희

https://orcid.org/0000-0002-2954-3098
e-mail : jhmom21088@gmail.com
1995년 강원대학교 전자공학과(학사)
2019년 건국대학교 정보보호학과(석사)
2021년 ~ 현 재 숭실대학교 IT정책경영학과 박사과정
관심분야 : 사이버보안 정책, 사이버 위협정보 공유, IoT

이 덕 규

https://orcid.org/0000-0003-1323-3084
e-mail : leedg317@naver.com
1987년 계명대학교 전자계산학과(학사)
2016년 카톨릭대학교 의료경영학과(석사)
2021년 ~ 현 재 숭실대학교
IT정책경영학과 박사과정
1987년 ~ 현 재 건강보험심사평가원 실장
관심분야 : :보건의료 관련 IT정책 및 정보화분야

신 용 태

https://orcid.org/0000-0002-1199-1845
e-mail : shin@ssu.ac.kr
1985년 한양대학교 산업공학과(학사)
1990년 Univ. of Iowa, 컴퓨터학과(석사)
1994년 Univ. of Iowa, 컴퓨터학과(박사)
1995년 ~ 현 재 숭실대학교 컴퓨터학부 교수
관심분야 : 정보보호, 인터넷 프로토콜, IoT, 클라우드 컴퓨팅