# 중국 사이버 공격 양상 변화와 사이버 안보에의 함의

2024

한국사이버안보학회
KACS

**한국사이버안보학회 워킹페이퍼 21호**
**발간일: 2024년 8월 24일**

**김상규 (경기연구원)**

# Ⅰ. 서론

중국은 러시아, 북한과 더불어 가장 많은 사이버 공격을 시행하는 국가로 알려져 있다. 특히 경제력에 기초해 과학기술 역량을 고도화하며 양자통신과 같은 최첨단 기술을 우주와 사이버 공간에 투사해 국내외 정보 수집과 통제, 공격과 방어 등 다양한 형태의 행위를 시현하고 있다. 하지만 중국 정부는 이러한 사실을 서방 국가의 술책이라며 강하게 부정하고 반발한다. 오히려 "중국 정부 부처가 거의 매일 대규모 사이버 공격을 받고 있으며, 그중 대부분은 미국으로부터 온 것이라며 사이버 공격의 가장 큰 피해자는 중국"이라고 주장한다. (中国外交部, 2023/07/14) 또한, "중국에 대한 사이버 공격은 인도 해킹그룹에 의해서도 발생하고 있다."라며 인도를 세계 정보기관이 간과할 수 없는 위협적인 국가이자 중국 사이버 안보에 심각한 영향을 주는 국가로 평가하고 사이버 보안 시스템 구축을 가속해야 한다고 주장하고 있다. (新华网, 2021/11/20) 물론 그 기저에는 인도가 서구 지정학적 사고와 개념을 가지고 미국과 협력하고 있다는 인식이 깔려있다.

중국의 주장은 일견 "사이버 공격에는 국적이 없다. 특정 국가에 사이버 공격의 책임을 돌린다면, 거기에는 의도가 있는 것"이라는 점과 "서방 국가는 더욱 정교하고 전략적인 방식으로 사이버 작전을 수행하는 경향이 있기에 서방 국가의 사이버 작전에서 잡음이 더 적은 경우가 많다."라는 것과도 맥을 같이한다. (BBC, 2023/06/23) 사실 사이버 공격의 주체가 중국이라는 명확하고 객관적인 증거를 확보하기도 어려울뿐더러 설령 확인하더라도 우회하는 방식으로 이루어진 경우가 많아 중국의 사이버 공격이 어떤 형태로 이루어지고 있는지, 어떤 방식으로 진화하는지 그 양상을 정확히 확인하기란 쉽지 않다. 물론 관련 기술을 활용해 추적한 결과를 분석하면 사이버 공격의 주체와 내용을 어느 정도는 확인할 수 있지만, 개별 국가의 주장이 서로 다르고, 근거 역시 제각각이기에 상호 간 인식의 차만 더욱 커질 뿐이다.

이처럼 사이버 공격에 대한 개별 국가의 인식차가 존재하지만 사이버 공간에서 중국발 사이버 공격 행위는 이미 다양한 방식과 경로를 통해 확인할 수 있다. 심지어 공개적으로 공격 주체와 목적을 드러내기도 한다. 2023년 1월 22일, 중국 해킹 조직 '샤오치잉(曉騎營, Cyber Security Team)'은 한국의 교육 관련 사이트 70여 곳을 해킹했다. 곧이어 1월 24일, 텔레그램에 공개 성명을 올려 자신들이 한국 기관의 홈페이지를 공격했다고 밝혔다. 이들은 "중국 정부를 위해 일하지 않는 자유 그룹"이라며 "한국을 훈련장으로 삼아 각 멤버가 한국 공격에 참여하겠다."라고 천명하기도 했다. (연합뉴스, 2023/01/25)

그렇다면 중국이 시행하는 사이버 공격의 주요 주체와 대상, 방법은 무엇일까? 상술한 것처럼

공격 대상이 자신을 드러내는 경우를 제외하고 공격 주체를 정확하게 특정하거나 사전에 예상하기는 힘들다. 하지만, 사이버 공격이 어디에서, 누가 시작했는지, 어떤 목적과 방식으로 시행했는지 추적하고 추론할 수 있는 기술적 범위 안에는 있다. 이 때문에 선진 기술력을 가진 국가와 후발 주자로 추격하는 국가, 블랙 해커와 화이트 해커 사이에 창과 방패의 자웅을 겨루는 수단으로써 사이버 공방전이 벌어지기도 한다. 미국은 동맹국과의 규합을 통해 민주주의 가치, 규범을 강조하며 중국을 압박하고 있어 미·중 양국을 위시해 사이버 공간을 둘러싼 진영 간 대립이 무시로 일어난다. 국제사회의 현실 공간에서만큼 사이버 공간에서도 국가 간 갈등 상황이 치열하게 이루어진다는 점에서 미·중 양국이 벌이는 행위의 의도와 목적을 정확하게 파악하는 것은 상당히 중요한 국제정치학적 함의가 있다. 이에 본 논문은 유관 정부와 단체, 언론에서 공개한 여러 가지 해킹 관련 보고서와 사례 등 드러난 사실에 근거해 중국의 사이버 공격의 내용과 형태 등이 어떻게 변화하고 있는지 그 특징과 양상을 분석하고 사이버 안보 차원에서 어떤 시사점이 있는지 고찰해 보고자 한다.

# Ⅱ. 중국의 사이버 전략과 공격 양태 분석

## 1. 사이버 공격의 정의와 형태

사이버 공격은 일반적으로 디지털 네트워크를 통해 정보시스템, 인프라, 컴퓨터 네트워크, 개인의 디지털 기기 등을 대상으로 데이터의 변조, 손상, 삭제, 절도 또는 시스템의 중단을 목적으로 진행하는 것을 말한다. 사이버 공격은 넓게 2가지 유형으로 분류될 수 있는데, 하나는 대상 컴퓨터를 비활성화하거나 오프라인으로 만드는 공격이고 다른 하나는 대상 컴퓨터의 데이터에 접근해 관리자 권한을 얻는 것이 목표인 공격 유형이다. (Josh Fruhlinger, 2020/03/03) 이러한 공격은 대부분 무단으로 액세스하여 시스템을 악용하기에 금전적, 정치적, 개인적, 사회적 손해가 발생할 수 있다. 즉, 사이버 공격은 경제적 이득을 위한 자금 탈취, 민감한 데이터 도난, 판매 행위, 개인 보복의 목적, 정치적, 사회적으로 메시지를 전달하기 위한 핵티비즘(Hacktivism) 공격으로 특정 이슈나 원칙을 대중에 알리기 위해 사용되고 있다. 사이버 공간에서의 충돌 범위는 폭력 및 범죄 활동에서 첩보 활동 및 사보타주까지 모든 행위를 포괄한다. 이 범주의 폭력적인 극단에 있는 사이버 공격은 핵심 기간 시설 경제, 재산 및 시민의 복지를 위협할 수 있다.(이상현 외 역, 사이버 안보, 2023, 129)

한편, 사이버 무기체계는 사이버 공간에서 다양한 목표를 달성하기 위한 사이버 공격 및 방어 기술들을 통합한 체계인데, 이는 다시 소프트웨어 및 하드웨어 무기체계로 구분한다. 소프트웨어 무기체계는 다양한 사이버 공격기법뿐만 아니라 공격자의 전략, 인프라, 자원, 지식 등의 개념을 포함한다. 사이버 공격기법은 소프트웨어 무기체계 내에서 사용되는 도구 또는 기술로, 이러한 기법을 효과적으로 전개하기 위한 전체적 구조와 전략을 의미한다. (유도진, 2023) 구체적으로 보면 악성 소프트웨어인 악성코드, 웜, 트로이 목마와 다른 악성 소프트웨어를 개발 및 배포하여 타깃 시스템에 침투하고 제어하는 데 사용한다. 최근에는 소프트웨어 개발자들이 깃허브(GitHub) 등 소스 코드 개발 공유사이트를 많이 이용하는 점을 노려 그 안에 악성코드를 삽입하거나 소스 코드를 탈취하는 공격을 하고 로그 j 등 유명 오픈 소스의 심각한 취약점을 악용, 라이브러리에 악성코드를 삽입하는 방식을 활용한다. (과학기술정보통신부, 2023)

이는 중요한 데이터나 시스템을 파괴하거나 변조하는 목적으로 사용할 수 있으며, 대상 시스템의 기능과 사이버 공간의 무력화를 통해 사용 불가능하게 만드는 공격을 수행한다. 특히 기술적인 발전을 이루면서 군사적 차원에서 충돌을 불러일으키는 데 활용이 가능하며 온라인 사이버 전투 플랫폼을 통해 사이버 공격 기술을 관리하고 조정할 수 있다.

**<표 1> 사이버 공격의 주요 유형과 내용**

| 유형 | 내용 |
|---|---|
| **악성코드(Malware)** | 악성 소프트웨어(malicious software)의 줄임말<br>'단일 컴퓨터, 서버 또는 컴퓨터 네트워크에 손상을 입히기 위해 고안된' 모든 종류의 소프트웨어<br>신뢰할 수 있는 전자 메일 첨부 파일 또는 프로그램(예: 암호화된 문서 또는 파일 폴더)으로 가장하여 바이러스를 악용하고 해커가 컴퓨터 네트워크에 침입할 수 있음<br>웜(Worms), 바이러스(viruses), 트로이목마(trojans), 스파이웨어(Spyware) 등 다양한 종류의 악성코드로, 복제하고 확산하는 방법에 따라 서로 구별 |
| **피싱(Phishing)** | 사기성 이메일, 문자 메시지, 전화 통화 또는 웹사이트를 사용하여 사람들을 속여 민감한 데이터를 공유하거나 멀웨어를 다운로드 해 범죄에 노출되도록 하는 행위 |
| **랜섬웨어(Ransomware)** | 피해자의 파일을 암호화하는 악성코드의 일종<br>사용자는 암호화 해독 키를 얻기 위해 비용을 지불하도록 요구 |
| **서비스 거부 공격 (DDoS)** | 특정 서버(컴퓨터)나 네트워크 장비를 대상으로 많은 데이터를 발생시켜 일부 온라인 서비스가 제대로 작동하지 않도록 시도하는 무작위 입력 공격 방법 |
| **중간자 공격 (Man in the middle)** | 공격자가 사용자와 그들이 접근하려고 하는 웹서비스 사이에 은밀하게 끼어드는 방법<br>일단 사용자가 로그인하면, 공격자는 뱅킹 비밀번호를 포함해 사용자가 전송하는 모든 정보를 수집할 수 있음 |
| **SQL 주입 공격** | 공격자가 취약점을 이용해 피해자의 데이터베이스를 제어할 수 있는 수단<br>SQL 명령을 사용자 입력 필드에 주입하여 데이터베이스에서 특정 명령을 실행하는 방식으로 작동 |
| **XSS (교차 사이트 스크립팅)** | 공격자가 악의적인 스크립트를 신뢰할 수 있는 웹사이트에 삽입하여 사용자의 브라우저에서 실행되도록 만드는 것 |
| **제로데이 익스플로잇 (Zero-day exploits)** | 컴퓨터 소프트웨어, 하드웨어 또는 펌웨어의 알려지지 않았거나 해결되지 않은 보안 결함을 활용하는 사이버 공격 벡터 또는 기법 |

자료: IT world, MS, IBM 등

소프트웨어 무기체계와 사이버 공격기법은 상호 연관되어 있으나 그 개념에는 차이가 있다.

사이버 공격기법은 사이버 공간에서 시스템, 네트워크, 데이터에 대한 공격이나 침투를 실행하는 데 사용되는 특정한 방법이나 기술로서, 워너크라이(WannaCry), 낫페트야(NotPetya), 배드래빗(Bad Rabbit) 등의 랜섬웨어, SQL 주입, 제로데이(Zero-day) 공격, 지능형 지속 공격(APT: Advanced Persistent Threat), 분산 서비스 거부(DDoS:Distributed Denial of Service) 등이 해당한다. 이러한 기법들은 사이버 공격을 수행하는 동안 취약점을 이용하거나 시스템 조작에 사용한다. (유도진, 2023) 소프트웨어 무기체계는 국제적 해킹그룹의 주요 공격수단으로 사용하며, 주요 방식은 하드웨어 무기체계를 이루는 컴퓨터 시스템, 네트워크 인프라, 통신 장비 등 물리적인 하드웨어를 공격하거나 하드웨어 침입을 통해 타깃 시스템 파괴와 제어를 통해 전투 상황에서 상대방의 하드웨어를 무력화하는 데 활용한다. 이처럼 사이버 무기체계는 공격과 방어의 목적으로 사용할 수 있으며, 군사적 충돌, 국가 간 갈등, 정보 수집, 경제 스파이 등 영역을 넘나들며 사이버 공간에서 국가 간 경쟁과 안보의 위협을 증대시키고 있다. 중국 역시 이 같은 공격 방식을 활용하고 사이버 전략에 기초해 사이버 공간에서의 영향력을 확장하고 있다.

앞서 서술한 샤오치잉은 한국 내 기관 2천여 개 웹사이트를 대상으로 사이버 공격을 예고하고 개인정보 유출 등 피해를 준 다음, 해킹포럼 등을 통해 공개한 바 있다. 공격에 성공한 후 획득한 관련 정보를 공개하는 것은 피해 기관과 기업에 추가적 부담과 더불어 자신들의 공격이 사회적으로 영향력을 행사한다는 이미지를 심어주기 위한, 즉, 사이버 공격을 통해 경제적 이익, 정치적 목적, 사회적 영향력의 확보 의도가 있는 것이다. 일반적으로 해킹의 대상은 주로 소규모 기관과 기업, 학회 등을 표적으로 선택하는데 그 이유는 중소기업 등 소규모 조직의 경우 보안에 대한 경각심이 부족하고 취약해 공격 성공 확률이 높기 때문이다. (유도진, 2023) 주로 사용하는 공격 방식은 SQL 주입(Injection)과 공개 정보를 활용하는 취약점 공략이다. 실제로 2018년부터 2023년 상반기까지 공격 유형별 통계를 살펴보면, 취약한 인증과 세션 관리, 부적절한 권한 검증 취약점 유형이 상위로 올라간 사실을 알 수 있다.

**〈표 2〉 2018년~2023년 상반기 공격 유형별 통계**

| 번호 | 공격 유형 | 포상건수 |
|---|---|---|
| 1 | 크로스 사이트 스크립트(XSS) | 374건 |
| 2 | 오버플로우 | 332건 |
| 3 | 명령어 삽입(Command Injection) | 175건 |
| 4 | 파일 다운로드 및 실행 | 165건 |
| 5 | 부적절한 권한 검증 | 68건 |
| 6 | SQL Injection | 63건 |
| 7 | 취약한 인증 및 세션 관리 | 52건 |
| 8 | 임의 파일 실행 | 38건 |
| 9 | URL Redirection | 31건 |
| 10 | 파일 업로드 | 26건 |

| 번호 | 공격 유형 | 포상건수 |
|---|---|---|
| 1 | SQL Injection | 196건 |
| 2 | 취약한 인증 및 세션 관리 | 100건 |
| 3 | 부적절한 권한 검증 | 100건 |
| 4 | 명령어 삽입(Command Injection) | 99건 |
| 5 | 크로스 사이트 스크립트(XSS) | 78건 |
| 6 | 파일 다운로드 및 실행 | 69건 |
| 7 | 오버플로우 | 65건 |
| 8 | 파일 업로드 | 35건 |
| 9 | 파라미터변조 | 31건 |
| 10 | 임의 파일 실행 | 30건 |

자료: 2023 상반기 사이버 위협 동향 보고서 (KISA 한국인터넷진흥원)

일례로, 2018년 중국인으로 추정되는 해커가 러시아·이탈리아 삼성전자 서비스 센터를 해킹한 후 국내 삼성전자 본사에 접근하려는 시도를 발견하였고, LG전자 미국 앨라배마 지사, LG생활건

강 베트남 지사 등 국내 기업의 해외 지사를 대상으로 한 사이버 공격 때문에 내부 정보가 유출하는 사건이 지속해서 발생했는데, 이는 상대적으로 공격이 쉬운 해외 지사를 통해 국내 본사에 접근, 추가 내부 기술을 유출하려는 시도로 분석할 수 있다. (최원석 외, 2022, 189) 사이버 공격은 전통적인 공격 수법에 그치지 않고 다중 인증(MFA: Multi-Factor Authentication) 우회, TOAD 등과 같은 복잡한 사이버 공격 기법으로 진화하고 있다. 특히, 중국과 러시아의 공격 그룹이 기업의 소프트웨어 공급망을 표적화하는 사례가 늘어나고 있다. 기업 공급망은 다양한 SW 제품, 개발업체, 수요자 등 구성요소가 많고, IT 자산, 개발 환경, 인력, 계약관리 등 관계가 복잡하여 공격 탐지와 조치가 어렵고 파급력이 매우 큰 특징을 가지고 있기 때문이다. (과학기술정보통신부, 2023, 11)

## 2. 중국의 시기별 사이버 전략

중국은 경제, 군사 문제, 정치, 기술 분야에 걸쳐 정보력의 우위를 개발하기 위해, 그리고 적의 작전상 효율을 약화하기 위해 사이버 첩보 활동과 지식 재산 탈취에 노력을 집중해 왔다. 정보 수집에 대한 이러한 집중은 중국의 선제 타격 및 정보전 전략과 일치한다. (이상현 외 역, 사이버 안보, 2023, 129) 중국은 정보 통신의 가장 기초적인 분야에서조차 기술적인 측면이나 시스템 구축 차원에서 상당히 낙후되어 1978년 전 세계의 전화 보급률이 11%인데 반해 중국은 0.38%에 지나지 않았다. (吴基传, 申江婴, 2008, 26). 이와 달리 1960년대 말, 미국은 이미 군사적인 목적에 근거해 인터넷을 개발하여 이를 상용화하고 전 세계 인터넷 시스템 구축을 계획하고 있었다. (허재철 외, 2019, 204) 이 같은 상황에서 기술력을 강화하기 위한 정책을 수립하고 제도를 정비하는 것만이 중국의 지도자가 할 수 있는 최고의 선택이었을 것이다. 덩샤오핑은 “중국의 경제가 발전하고, 현대화하기 위해서는 교통, 통신 분야부터 시작해야 한다”라고 강조하며 관련 조직을 정비해 나가기 시작했다. (허재철 외, 2019, 205)

이후 장쩌민 시기부터 현 시진핑 시기까지 중국은 기술, 조직과 법, 제도의 수립 등 단계별, 시기별로 역량을 분석하고 그에 맞는 목표를 세워 장기적이고 안정적인 정책을 진행하고 있다. 우선, 장쩌민 집권 시기인 1990년대 초부터 2000년대 초까지는 인터넷 후발 주자로서 선진국의 정보화 발전을 따라잡기 위해 국가정보센터 등 관련 조직을 구성하고 기술 발전을 위한 연구와 지원 시스템을 만드는 등 정보 인프라 구축 환경을 조성하는 데 중점을 둔 전략을 시행했다. 이 시기는 냉전 해체 이후 화해와 협력이라는 새로운 국제질서가 도래하면서 과거의 냉전 질서 속에서의 안보 갈등의 군비경쟁이 아닌 경제교류와 기술협력, 그리고 국민복지 향상과 경제발전을 먼저 추구하는 저위정치(low politics) 시대와 맞물려 있었기에 사이버 공간의 안전보다는 경제발전과 인터넷 활성화에 주된 목표를 두고 있을 수밖에 없었다. (김승채, 1999, 46)

2000년대 초반부터 2010년대 초반까지인 후진타오 집권 시기는 중국이 경제적 발전에 기초해 대외적으로 국제사회의 ‘책임 대국’으로 역할을 자처하며 영향력을 확대하던 때였다. 하지만 대내적으로는 빈부격차 증가와 부패 만연, 경제개발의 부작용이 두드러지면서 사회적 불만과 혼란이 가중되고 있었다. 이와 관련한 정보는 인터넷 보급과 모바일 사용자의 급증에 따라 빠르게 확대 재생산하였고 중국 내부 정치의 불안정성을 배태하는 원인으로 작용하였다. 따라서 중국 정부는 사회적 불안정성을 약화하고 외부로부터 유입되는 정보를 차단하기 위한 방어적 전략 사고를 통해 정보화 조직을 개편하고 사이버 공간의 질서를 수립하기 위한 정책 등 질적 성장에 주력했다.

시진핑 집권 이후 사이버 공간에 대한 장악력 확대를 위한 조직 구성, 기술 발전, 통제, 방어와 위협 능력 강화 등 다방면에 걸쳐 대내외적 국가 이익 실현을 위한 전략을 공격적으로 가동하게 된다. 특히 이 시기는 중국이 사이버 공간에 대한 제도 마련과 전략 수립이 두드려졌다. 2015년 「국가안전법(国家安全法)」, 2016년 「국가사이버공간안전전략(国家网络空间安全战略)」, 2017년 「네트워크안전법(网络安全法)」, 2021년 「데이터안전법(数据安全法)」 등 중국이 사이버 공간을 국가안보 영역으로 편입시키고, 네트워크의 구축과 운용을 넘어 데이터 안보에 대한 의무와 책임을 규정한 데이터 3법은 물론 「반독점법(反垄断法)」과 「개인정보보호법」을 제정함으로써 사이버 공간에 대한 '의법치국(依法治国)'의 대내외적 통제력 강화 전략을 수립했다.

그중에서도 2016년 12월 27일, 중국이 최초로 수립한 '국가사이버공간안전전략'은 중국의 사이버 공간에 관한 인식과 목표를 살펴볼 수 있는 바로미터이다. 중국은 해당 전략을 통해 사이버 공간을 어떻게 평가하고 있는지, 어떤 원칙을 가지고 전략 임무를 이루고자 하는지 명확히 제시하고 있다. 사이버 주권의 중요성을 강조하면서 국가안전 유지, 정보 기반시설 보호, 사이버 문화 건설, 사이버 범죄와 테러 예방, 사이버 거버넌스 체제 개선, 사이버 안전 기초 마련, 사이버 방어력 향상, 그리고 사이버 국제협력 강화 등 9개의 전략목표를 제시하였으며, 그중에서도 해킹으로 인한 국가 분열이나 반란 선동 기도, 국가기밀 누설 등의 행위를 중대 불법행위로 간주하고 이를 막기 위해 군사적인 수단까지 동원하겠다고 천명했다. (김상배, 2019, 84) 이어 2017년 3월 발표한 「사이버공간국제협력전략(网络空间国际合作战略)」을 보면, 중국은 주권 수호와 안보, 국제 규범 체제의 확립, 공평한 인터넷 관리 추진, 인민의 합법적 권익 보장, 디지털 경제 협력 추진, 온라인 문화교류 플랫폼 구축 등을 언급하고 있다. (채재병 외, 2020, 10)

중국이 추구하는 사이버 전략의 핵심은 중국의 주권 수호와 안전 보장, 국제 규범 체제 확립, 디지털 경제권 장악과 기술 우위를 위한 중국의 핵심 이익 수호와 실현이 기저에 깔려있다. 특히 시진핑 시기는 사이버 문제를 외교적 관점에서 접근하고 사이버 안보를 미·중 관계를 비롯한 국제사회의 중요한 대외적 의제로 설정하고 그에 따른 전략을 공격적으로 시행하는 중이다. 따라서 중국의 사이버 전략은 경제적, 기술적 자신감에 기초해 국제사회에서 공세적 발언과 행동 강화로 이루어진다. 이는 중국의 사이버 공격 형태와 방식, 의도가 직간접적으로 결부되어 나타난 것이며 이를 통해 중국이 향후 행보를 추론할 수 있는 근거로 활용할 수 있다는 것을 의미한다.

## 3. 중국의 사이버 공격 주요 주체

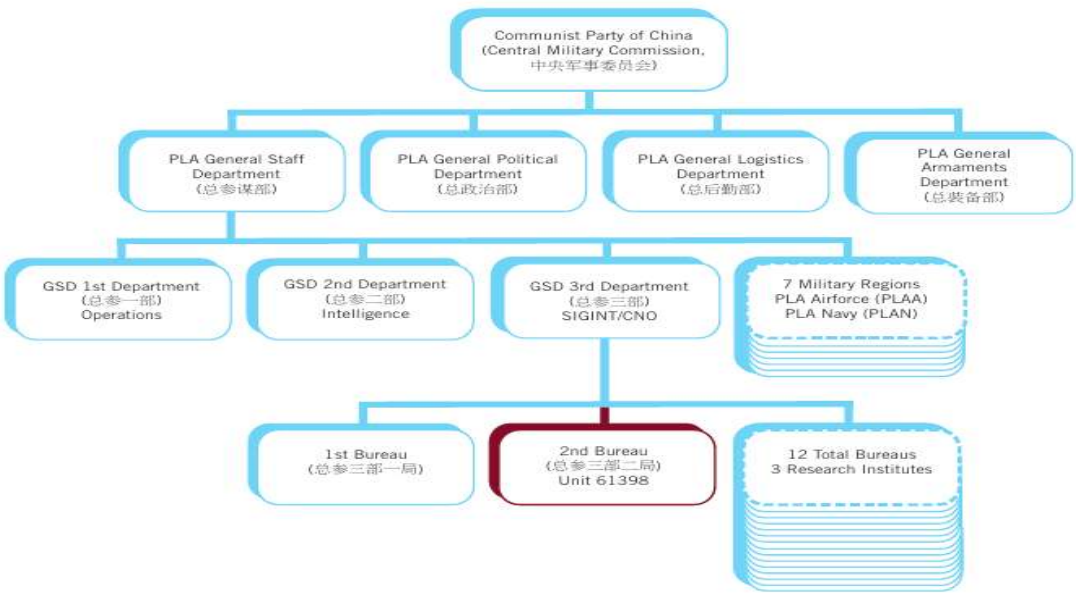
중국 사이버 공격의 주요 주체와 해킹 조직은 구체적인 특성이나 규모, 임무 등을 정확하게 확인하기는 사실상 어렵다. 하지만 기본적인 방첩 업무를 수행하는 국가기관을 비롯해 국내외 정보기관이 해킹 결과를 분석하거나 사이버 공격 행위에 대한 선전 포고 등을 통해 드러난 사실을 토대로 일정 정도는 확인할 수 있다. 중국에서 사이버 공격은 물론 첩보 활동을 수행하는 조직 중 하나는 중국 인민해방군 (PLA, People's Liberation Army)이다. 해당 조직은 국가 차원에서 정보 수집, 군사 기밀 획득, 정치적 영향력 확장, 경제적 이익 추구 등 다양한 목적에 기반해 사이버 공격을 수행한다. 사이버 공격을 통해 중요 정보와 기술을 탈취하고, 미국을 비롯한 기타 국가와의 군사 및 경제적 경쟁에서 이득을 취하려는데 주안점을 두고 있다. 중국 국가안전부 (MSS: Ministry of State Security) 역시 정보 수집과 사이버 활동을 주도하는 주체 중 하나이다. 이외에 중국 정부나 군사 기관과 직접 연관되지 않은 독립적인 해커 그룹들도 많이 존재한다. 이들 해커 그룹은 자체적인 활동, 해킹 업무 계약에 따른 특정 임무의 수행, 금전적 이득을

얻기 위한 목적에 기초하고 있다.

중국이 주로 행하는 해킹의 방식은 지능형 지속 위협(APT)인데 이 같은 방식은 특정한 피싱 공격을 통해 전자 우편 주소로 악성코드를 발송하고 대상 기기를 감염시킨 이후 수 시간 내에 관련 조직 전체의 기능을 마비시킬 수 있다. APT 그룹은 목표 기관에 대한 정교한 표적 공격을 수행하고 지속해서 침투하는데 이는 다양한 벡터를 결합하여 공격 효과를 높일 수 있다. 다중 벡터 공격은 소셜 엔지니어링, 제로데이 취약점 활용, DDoS 공격, 악성코드 배포 등 공격 형태를 조합하는 방식으로 나타난다. 특히 APT 1 또는 Comment Crew라 불리는 그룹은 PLA Unit 61398의 일부로 활동 시기는 2006년부터라고 알려져 있다. 이는 중국이 인터넷 및 사이버 과학기술 분야에서 급속한 성장이 시작하는 시기와 맞물려 있으며, 중국이 군사교리를 재정의하면서 정보시스템 보호나 파괴가 인민 해방군(PLA:People's Liberation Army)의 '전쟁 방법'이 될 것이라 명시한 것과 관련이 있다. (IISS, 2021, 90) 주로 에너지, IT, 통신, 항공 우주, 국방 분야를 공격 대상으로 삼으며 기업 정보, 지적 재산, 정치 정보와 관련한 중요 데이터를 탈취하고 수집한다.

주요 공격 방식은 표적형 피싱(spear-phishing)과 악성코드를 배포하거나 자체적으로 개발한 프로그램을 사용하여 정보를 수집하기만 해킹의 흔적은 남기지 않는다. 공격 대상은 주로 영어권 국가들이며 미국이 가장 많은 공격을 당했다고 알려져 있다. (Mandiant 2021, 22) 이외에도 메뉴 패스팀으로도 불리는 APT 10 역시 2006년부터 관리형 IT서비스 제공업체를 활용해 미국, 유럽과 일본 등 전 세계의 항공 우주 및 통신 기업과 건설과 엔지니어링 기업, 정부 기관을 노리고 공격 활동을 벌였다. 실제로 미국 법무부는 미국, 브라질, 프랑스를 비롯한 12개국에서 안보 기밀, 영업비밀, 지식재산권 등을 유출하기 위해 해킹을 저지른 혐의로 APT 10 소속 중국인 해커 2명이 기소했는데, 이들은 IBM, HP 등 민간 기업들을 비롯하여 미국의 해군과 항공우주국(NASA) 제트추진연구소, 미국 에너지부 등의 정부 기관 전산망을 공격했다. (문화일보, 2018/12/21)

**〈그림 1〉 61398 부대 지휘 계통**




자료: Mandiant 2021

APT 20은 중국 정부의 정책인 '중국제조 2025'나 '일대일로'와 같은 국가 대전략의 성공적인 수행을 위해 필요한 산업 기밀 해킹을 통해 정보를 수집하는 데 주요 방식은 오픈 소스인 제이보스(JBoss)의 취약한 특정 버전으로 운영하는 네트워크에 침입하거나 스피어 피싱 메일, 휴대용 미디어 장비의 감염, 소프트웨어 공급망 공격 등의 행태를 보인다. 중국 해커 그룹 Barium(APT 41, Winnti)은 중국 정부와 연계된 곳으로 주로 산업 스파이 활동 및 금융 범죄에 관여한 것으로 알려져 있다. 주요 공격 수단과 방법은 스피어 피싱, 제로데이 취약점, 무선 툴을 사용하며 주로 게임 회사, 기술 기업, 통신 업체, 정부 기관 등을 대상으로 산업 스파이 활동과 금융 이익 추구를 병행한다.

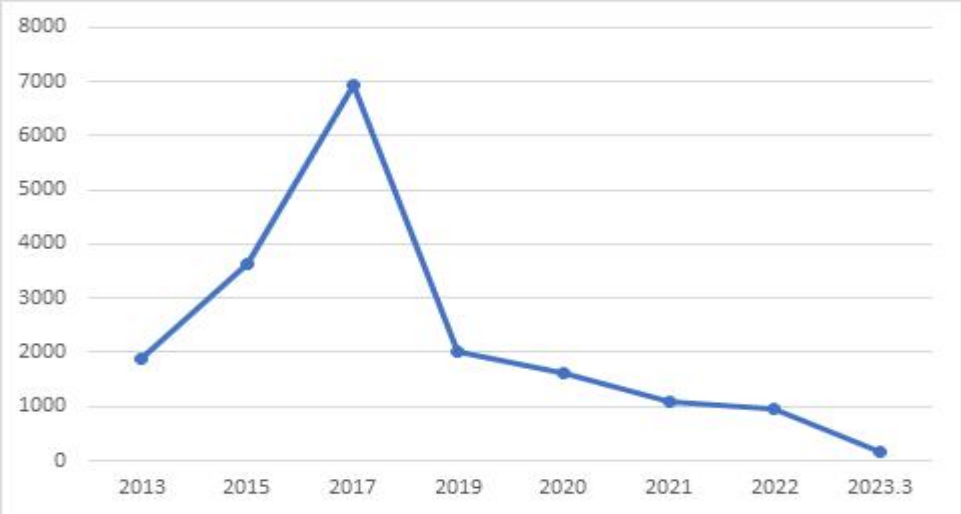
'틱'(Tick)은 주로 한국과 일본의 방위와 관련한 기밀 정보를 탈취할 목적으로 임무를 수행하는 해커집단이다. 주요 공격 방식은 표적형 공격(TTP)을 사용하여 스피어피싱 이메일을 전송하고, 악성코드를 이용해 시스템 방비가 허술한 대상에 바이러스를 침투시키는 방법을 활용한다. 2016~2017년 우주항공연구개발기구(JAXA)를 비롯한 연구기관과 대학, 방위·항공기업 등 약 200곳의 정보 탈취를 시도했는데, 일본 경찰은 틱이 중국군 61419부대의 지시를 받으며 2018년 이후 미국과 유럽을 대상으로 활발한 활동으로 벌이는 조직으로 판단했다. 또한, 무스탕 판다(Mustang Panda), 딥 판다(Deep Panda) 같은 조직은 중국 정부의 전략적 목표에 맞춰 미국, 아시아뿐 아니라 러시아 조직을 비롯한 유럽 단체들까지 다양한 분야와 주요 기업을 대상으로 지적 재산 및 민감 데이터 탈취를 하는데, 딥 판다는 정부, 군대, 공공시설, 금융 기관을 대상으로 하는 별도의 국가 후원 사이버 스파이 그룹으로 로그 4j 취약점[1]을 악용해 공격하고, 공격 지속성을 유지하기 위해 맞춤형 백도어(Back Door)를 배포하는 형태로 활동한다. (ZDNET, 2023/04/21)

## 4. 중국의 사이버 공격 방식과 목표

중국의 사이버 공격 주체나 기술적인 것 이외에 내용적인 차원에서 분석해 보면 그 형태가 어느 정도 분류가 가능하다. 초기에는 기술적인 차원에서 여러 가지 방법을 시도했다면, 기술 축적을 이루고 난 후 자국에 유리한 국면을 조성하기 위한 좀 더 적극적인 공격 형태로 전환했다. 특히 중국의 사이버 공격은 미국의 동맹을 비롯한 우호 관계를 맺는 국가, 그리고 중국에 부정적 태도를 보이는 국가를 대상으로 공격이 이루어진 사례가 많이 나타난다. 구체적인 사례를 보면, 한국의 경우 외교부에 대한 중국발 사이버 공격은 2013년에 1,890건이었지만, 국내 사드 배치가 언급되던 2015년 3,649건으로 급증했고, 사드 배치가 완료된 2017년에는 6,941건을 기록했다. (KBS, 2023/05/20) 하지만 관련 이슈가 없어진 이후에는 중국발 해킹 시도가 급격히 줄어들었다. (그림 2)

1) 원격 코드 실행 취약점으로, 공격자가 이를 악용하면 사실상 피해자의 컴퓨터를 원격으로 제어할 수 있게 되는 것은 물론 시스템에서 임의의 코드를 실행하여 시스템을 탈취할 수도 있다.

〈그림 2〉 중국발 한국 외교부 해킹 시도 수




자료: 외교부

또 다른 사례로는 2020년 호주의 스콧 모리슨 총리가 코로나19 바이러스의 중국 우한 기원설에 대한 조사를 공식적으로 제안하자 양국 관계가 급속도로 악화했는데, 양국이 무역 보복을 하는 과정에서 중국발 해킹 봇이 호주 정부의 인터넷 네트워크를 동시다발적으로 공격하는 사건이 발생했었다. 2020년 5월에는 중국과 인도가 국경에서 무력 충돌을 벌인 후, 중국 해커가 인도의 주요 기반 시설에 대해 4개월간 4만여 건 정도의 사이버 공격을 벌였고 전력 부하 관리 센터에 악성코드를 심어 정전 사태를 촉발하기도 했다. (NYT, 2021/02/28) 특히 양안 관계가 악화하면서 대만에 대한 중국의 사이버 공격이 무차별적으로 이루어졌다. 2023년 5월 30일, 대만 정보기관인 국가안전국(NSB)을 담당하는 국가안전회의(NSC)가 발표한 내용에 따르면, 대만은 매일 500만 회에 달하는 인터넷 공격을 받았으며 대부분 중국발 사이버 공격이었다. (연합뉴스, 2023/05/30)이에 대해 대만은 2024년 선거를 앞둔 상황에서 중국이 친중 정권 수립을 위해 대만 내부의 혼란을 도모하고 중국의 의도를 이식하고자 사이버 심리전을 벌이는 것으로 판단했다.

이외에도 중국 정부가 조직한 '912 특별 프로젝트팀'이 가짜 SNS 계정을 이용해 코로나19 발원지가 중국이라는 주장, 남중국해에서 중국의 군비 확장 위험성 경고, 인권 문제의 심각성 등 중국에 불리하거나 민감해하는 내용과 관련한 의사를 표명한 인사들에게 사이버 공격을 가한 사실이 밝혀졌다. 이는 미국 연방 검사가 중국 공안부 소속 요원 34명을 궐석 기소하면서 제출한 89페이지 분량의 고소장과 진술서에 관련 활동을 상세히 기술했는데 트위터·유튜브 등에 개설한 가짜 계정을 통해 중국 공산당과 정부를 옹호하는 메시지를 적극적으로 전파했는가 하면 이른바 '중국의 적'들을 겨냥해 강도 높게 공격했다는 것이다. (한국일보, 2023/04/26) 이렇듯 중국에 반하는 형태의 정보나 행위들이 나타나는 경우 민감하게 반응하며 사이버 공간에서 해킹과 공격을 적극적으로 시행하는 것을 보여준다.

**〈표 2〉 중국의 시기별 사이버 공격 양상과 주요 내용**

| 시기/ 내용 | 주요 주체 | 주요 목표 | 주요 방식과 내용 | |
|---|---|---|---|---|
| 1990년대 중반 | 해킹그룹 정부 연관성 미확인 | 정보 탈취, 도용, 경제적 목적 | 기본적 해킹 방식, 스파이웨어 | 초기 단계 사이버 공격으로부터 경험 축적 |
| 2000년대 초반 | | | 악성코드, 표적형 공격 | 기술 확보, 국가안보와 사이버 제도 수립 |
| 2010년대 초반 | PLA | 군사, 과학기술, 기업 대상 및 경제적 목적 포괄 | 고급 표적형 공격, APT 활동 | 사이버 전략 고도화, 사이버 부대 활동 확대 및 공격 강화, 기술 발전 주력 |
| 2010년대 중반 | MSS | 정부 기관과 인사, 다국적 기업 대상 해킹 | | |
| 2020년대 | 정부 기구, 해킹그룹 | 이념, 선전 활동, 내부 정치 관리 | 생성형 AI와 대규모 언어 모델 사용 등 고도화된 기술 접목<br>허위 정보 제작 및 유포 | 최첨단 기술 적용 사이버 공격과 방어 능력 다각화<br>소프트웨어 공급망 공격<br>사회 인프라 시설에 대한 악성코드 침투 공격 |

자료: 저자 작성

**〈표 3〉 NCPI 2022 사이버 역량 순위**

| Rank | 2022 |
|---|---|
| 1 | 미국 |
| 2 | 중국 |
| 3 | 러시아 |
| 4 | 영국 |
| 5 | 오스트리아 |
| 6 | 네덜란드 |
| 7 | 한국 |
| 8 | 베트남 |
| 9 | 프랑스 |
| 10 | 이란 |

자료: Belfer Center for Science and International Affairs Harvard Kennedy School, National Cyber Power Index 2022, 9

하버드벨퍼연구소(Belfer Center for Science and International Affairs)가 세계 30개 국가의 사이버 역량을 평가한 보고서인 국가 사이버 역량 지수(NCPI: National Cyber Power Index 2022)에 따르면 현재 중국의 사이버 역량은 미국에 이어 전 세계 2위를 차지하고 있다. 해당

지수는 감시, 방어, 정보 수집, 상업, 규범, 금융, 정보 통제, 파괴 등 8가지 항목으로 구성되어 있는데, 중국의 사이버 역량은 공격, 감시 60, 정보 제어, 상업 50, 금융 20, 방어, 규범 30점으로 평가 대상 국가 중 감시, 정보 통제, 공격과 정보 수집 관련 역량이 강력한 것을 확인할 수 있다. 중국의 행위와 역량을 종합해 미루어 볼 때, 중국이 자국 내에서 언론을 검열하고 통제하는 행태를 국제사회에서도 똑같이 적용하려는 의도가 기저에 깔려있음을 추론할 수 있다.

**<그림 3> 중국의 사이버 역량 지수**


자료: Belfer Center for Science and International Affairs Harvard Kennedy School, National Cyber Power Index 2022, 22

한편, 미국은 '2023 국방부 사이버 전략'을 발표했는데, 주요 내용은 중국의 사이버 위협 사례가 어떤 형태로 일어나고 있는지, 향후 어떤 방향성을 가지게 될 것인지 등에 관한 내용을 포함하고 있다. 즉, 미국 기업과 정부 기관 해킹, 기술 탈취를 위한 사이버 스파이 활동, 미국 내정 간섭 시도 등이 대규모로 진행하고 있고, 미국과 동맹을 상대로 악의적인 사이버 활동을 벌이는 행위가 광범위하게 만연되어 사이버 위협이라고 규정한 것이다. (DoD Cyber Strategy, 2023) 미국의 이 같은 위협 인식의 발로는 중국의 사이버 공격이 기술적인 차원에서 이전보다 더 고도화하고 전문화한 그룹들이 주도하며 확장성을 갖기 때문이다.

중국은 자체 해킹 도구와 악성 소프트웨어를 개발하고 있는데, 이는 중국의 사이버 공격을 효과적으로 수행하는 데 유리하며 자국의 능력을 강화하고 외부 의존도를 줄이는데 유효하기 때문이다. 또한, 사회 공학적(Social Engineering) 차원에서 피싱 공격을 통해 개인과 기업의 정보를 획득하려 한다. 이러한 시도는 주로 악성 이메일을 통해 실행하는데 정보 수집과 사이버 스파이 활동의 주요한 방식으로 외국 기업과 정부 기관의 중요 정보와 경제, 군사, 기술을 탈취하는 데 그 목적이 있다. 실제로 2023년 6월, 중국 업체가 제조해 한국 기상청에 납품한 장비의 소프트웨어에서 악성코드가 발견됐었다. 한국 정부는 국내 통관 이전부터 악성코드가 설치되어 들어온 장비가 있음을 확인하였고, 국내 정부 기관과 지자체에 공급된 외산 장비에 대한 전수조사를 시행하였다. 또한 중국 배후의 해커조직(Storm-0558)은 MS사 이메일 소프트웨어(Outlook, Exchange Online)의 인증 취약점을 악용하여 미국 정부 기관 등 약 25개 기관의 시스템에 접근하였다. (국가정보보호백서, 2024, 12)

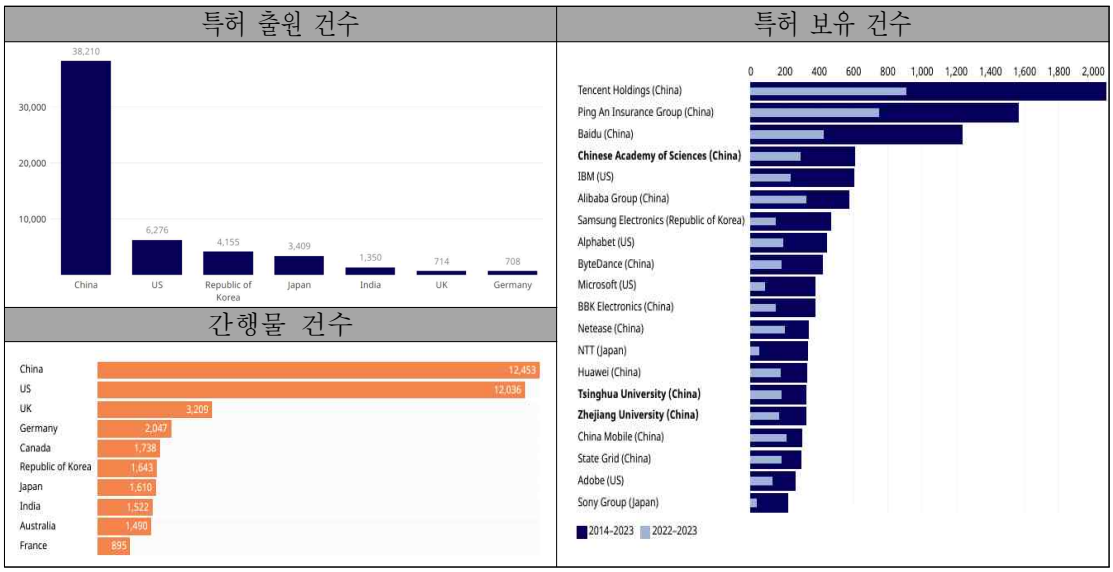
소프트웨어 공급망에서는 오픈 소스 및 상용 소프트웨어를 조합하여 사용하는 경우가 많다. 클라우드 컴퓨팅, 오픈 소스 생태계, 소프트웨어 배포 및 자동화 도구 등의 발전으로 인해 소프트웨어 개발과 배포가 더 빠르고 광범위하게 이루어진다. 따라서 한 번의 악성코드 공격으로 수십만 대, 수백만 대의 컴퓨터를 감염시킬 수 있다. 이런 이유로 보안과 관리가 더욱 어려워 사이버 공격에 취약한 것이다. 2017년 러시아가 벌인 악성코드 NotPetya(2017) 사건과 중국 해커 그룹 Barium[2]도 소프트웨어 공급망을 활용한 것으로 알려져 있다. 이들은 1단계 공격 시 향후 추가로 이용할 가능성이 있는 피해자에게 2단계 스파이웨어를 남겨두어 단순히 현재의 이익에만 치중하는 공격이 아닌 한 번의 성공적인 공격으로 장기적인 접근 권한을 확보하는 방식을 사용했다. 이렇게 되면 시스템의 무결성은 손상되고, 소프트웨어를 신뢰하는 기본 메커니즘은 더욱 약화한다.

이외에도 보안, 네트워킹, 가상화 소프트웨어, 라우터 표적화에서 조직의 네트워크 내외부로 공격자 트래픽을 중계하고 감추기 위해 제로데이 취약점을 악용한다. Mandiant Intelligence는 2021년과 2022년 중국이 제로데이(zero-day) 취약점을 공격했다고 분석했는데, 이는 보안, 네트워킹, 및 가상화 기술에 중점을 두고 목표 대상으로 삼은 것이다. 이렇게 해야 피해자 네트워크에 은밀하게 접근하고 유지할 수 있는 전술적 이점이 있다. 일부 탈취 공격에서는 탐지를 피하려고 로그 및 보안 제어 우회, 로그 삭제 및 수정, 시작 시 파일 시스템 확인 비활성화에 우선순위를 둔 맞춤형 멀웨어를 사용했다. (Mandiant, 2023/07/18)

가장 주의 깊게 살펴봐야 하는 것은 AI 기술을 활용한 자동화 방식의 사이버 공격 양상이 점차 확대할 수 있다는 점이다. 챗GPT뿐 아니라 '웜(Worm) GPT', '사기(Fruad) GPT' 등 피싱 공격을 수행하기 위해 개발된 AI 모델로 사이버 공격을 하고 있다는 보고서가 발표되기도 했고(동아일보, 2024/02/20), MS 위협분석센터(MTAC)는 중국 해커들이 미국과 대만에서 사회적 긴장을 고조시키기 위한 표적 캠페인에 AI를 활용하고 있다는 조사 결과와 중국이 한국과 미국, 인도에서 치러지는 주요 선거에 AI로 만든 허위 조작 정보를 퍼뜨려 영향력을 행사할 수 있다고 분석을 내놓기도 했었다. (Microsoft, 2024/04/04) 현재 생성형 AI 기술이 급속하게 발전하는 상황에서 향후 어떤 형태의 공격이 이루어질지 예상하기 어렵고 그 피해 역시 가늠하기 힘들다. 그러나 AI와 연계한 사이버 위협 경고는 이미 몇 년 전부터 나오기 시작했고 실제로 신·변종 공격과 이에 관한 방어를 위해 AI 기술을 활용하고 있다. 생성형 AI는 사이버 공격의 알고리즘을 학습해 더욱 빠르게 시스템의 취약점을 찾아내 대규모 공격을 감행하고 동시에 자율적 피드백을 통해 좀 더 진화한 방식의 공격 루트와 최적화한 방식을 찾아낼 수 있다. 물론 이와 반대의 상황과 역할로 위협 패턴을 찾아내 분석하고 새로운 위험 요인을 사전에 감지해 대응 역시 가능하다. 관건은 기술력에 있는데 중국이 관련 기술과 발전 속도 면에서 가히 타의 추종을 불허하고 있다는 점이다. 중국의 대학과 연구기관, 기업 등은 이미 특허, 간행물 수 부문에서 미국을 압도하고 있다. 이런 추세가 계속되어 기술을 축적하고 적용한다면 중국은 사이버 공간에서 독보적인 영향력을 행사하며 장악할 수 있는 것이다.

2)분석 그룹의 명명에 따라 Barium 또는 Shadow Hammer, Shadow Pad 또는 Wicked Panda로도 알려져 있으며, NetSarang(2017), CCleaner(2017) 및 ASUS(2019) 공격의 유사성으로 중국 배후 해킹그룹으로 분류됨 (WIRED, 2019). 2023년 상반기 사이버 위협 동향 보고서, p.49. 재인용

〈그림 3〉 생성형 AI 주요 현황




자료: 세계지식재산권기구(WIPO)

# Ⅲ. 결론 및 시사점

2024년 4월 19일, 중국은 전략지원부대를 폐지하고, 정보지원(信息支援), 군사우주(军事航天), 사이버 공간(网络空间)과 관련한 부대를 새롭게 창설한다는 것을 선포했다. 그와 동시에 “사이버 안보가 전 지구적 도전이고 중국이 직면하고 있는 엄중한 안보 위협이며, 사이버 안보 방어 수단을 적극적으로 개발하는 것이 중국의 사이버 주권과 정보 안전을 수호하는 데 매우 중요한 의미가 있다.”라고 강조했다. (中国国防部, 2024/04/19) 중국은 사이버 역량을 강화하는 데 총력을 기울이고 있다. 이 같은 노력은 사이버 공간에서 권력 균형을 무너뜨리고 국제사회에서 중국의 영향력을 강화하는 데 유효한 결과를 담보할 수 있다. 국제사회가 사이버 공간의 표준과 규범을 만드는 과정에서 중국이 기술적인 우위와 장악력을 활용한다면 자국의 전략적 의도를 반영하기 쉬워진다. 따라서 중국의 전략을 살피고 동시에 고도화된 사이버 공격 기술에 대한 방어와 대응 능력을 마련하는 데 초점을 맞추어 투자와 연구를 지속해서 확대해야 할 필요가 있다. 또한, 사이버 공간에 대한 재평가와 전략 수립은 물론 국제사회와 협력을 강화하는 것은 필수적이다.

이 같은 차원에서 2023년 4월 26일, 한국이 한·미동맹 70주년을 맞아 ‘전략적 사이버 안보 협력 프레임워크(Strategic Cybersecurity Cooperation Framework)’를 공동 발표하고 악의적인 사이버 위협에 공동으로 대응할 것을 천명한 것은 상당히 의미 있는 행보라고 할 수 있다. 이는 사이버 공간에서 일어나고 있는 공격 행위가 미국의 동맹과 파트너에게 지속해서 영향을 끼칠 수 있다는 점에서 더욱 중요하다. 왜냐하면 중국의 사이버 공격 행위는 이미 우리 사회의 여러 분야에서 목도되었고, 사이버 심리전이나 인지전의 방식은 물론 영향력 공작까지 앞으로 더 확대할 수 있다는 우려 때문이다. 중국이 20여 개 그룹 2만여 명에 이르는 핵티비스트·댓글부대 등을 운영하며 친중 영향력을 높이기 위한 공작을 하고 중국의 언론·홍보 업체들이 국내 언론사로

위장해 친중·반미 성향의 여론조작 콘텐츠를 게시하는 일이 이미 정보 당국에 의해 공식화되었다. 그뿐만 아니라 딥페이크 영상, 가짜 뉴스 등 사회 공학적 기법을 이용한 사이버 공격도 증가 추세에 있다는 점에서, 중국산 통신 장비나 기계에서 악성코드가 발견되는 사례 역시 간과할 수 없는 일이며 선제 대응이 필요하다. (국가정보보호백서, 2024, 16)

미국 역시 중국이 벌이는 사이버 공격 행위에 대해 경각심을 갖고 있다. 2023년 미국 국가정보국(Office of the Director of National Intelligence)의 연례 위협 평가 보고서에서 "중국은 미국 정부와 민간 부문 네트워크에 대한 가장 광범위하고, 가장 활발하며, 지속적인 사이버 스파이 위협을 대표하며, 사이버 공간에서 정보의 자유로운 흐름 억제, 전 세계적으로 기술 기반의 권위주의 확산 위협 증가는 물론 중국의 사이버 활동과 관련 기술의 수출은 미국 본토에 대한 공격적인 사이버 작전의 위협을 증대시켜 만약 미국과 심각한 갈등 상황이 발생한다면 미국 본토의 중요 인프라와 전 세계 미군의 주요 자산에 대한 공격적인 사이버 작전 수행을 고려할 확률이 굉장히 높다."라는 분석을 내놓았다. (Annual Threat Assessment, 2023, 10) 이 같은 인식은 2024년 보고서에서도 여전히 동일하게 적시되어 있으며 (Annual Threat Assessment, 2024, 11) 중국과 러시아, 이란, 북한 정부가 자신들의 전략적 목표를 달성하기 위해 사이버 작전을 수행하고 있다고 평가한다.(VOA, 2024/04/06) 이 같은 인식은 미·중 전략경쟁이 심화하고 데이터 유통, 디지털 콘텐츠, 네트워크 등에 대한 서로 다른 통제를 특징으로 하는 플랫폼 지정학이 부상하면서 사이버 공간에서도 진영화를 만들고 있다는 사실과 맥을 같이 한다. (홍건식, 2023, 2) 따라서 사이버 위협에 대응하기 위해 한미 동맹과 한미일 협력을 중심으로 동류 국가(like-minded countries)와 연대하고 공조를 강화하는 것은 반드시 해야 하는 일이다. 다만, 북한의 해킹과 사이버 공격은 물론 중국을 경유해 발생하거나 중국 내부의 범죄 활동에 따른 사이버 공격에 대해서는 중국과의 협력이 필요하다. 중국에 대한 무조건적 경계나 부정적 인식에 기초한 적대적 태도가 아닌 공통의 위협과 대응을 위한 열린 전략 사고가 요구되는 이유이다. 한미 관계에 국한해 외교 안보 이슈로 진영 간 대결 구도 안에서 중국과의 사이버 관계를 이해하는 것이 아닌 사이버 공간의 글로벌 의제 해결을 위한 모멘텀을 만드는 것에 방점을 찍어도 좋을 것이다. 플랫폼은 이미 마련되어 있다. 바로 사이버 안보 분야 역내 협력 증진을 위한 정례 협의체인 한·중·일 사이버 정책협의회이다. 이를 역내 국가 간 미래지향적인 관계 수립과 경색된 양자 관계 회복을 위한 전환점으로 활용한다면 국익을 실현하고 안보를 담보할 유효한 방법이자 기회가 될 수 있을 것이다.

## 〈참고문헌〉


유도진. 2023. "중국 해킹그룹 샤오치잉 사이버 무기체계 대응 방안 연구: SQL Injection 및 OSINT 기반 Known Vulnerability 공격." 한국산학기술학회논문지 24.6

이상현 외 譯, 2023.『사이버안보: 사이버공간에서의 정치, 거버넌스, 분쟁』. 서울:명인문화사.

채재병 외, 2020. “주요국 사이버 안보 전략과 한국에의 시사점”, INSS 전략 보고, No. 73. 국가안보전략연구원

최원석 외, 2022. “경제 안보 이슈의 부상과 대외 협력 방향”, KIEP 연구보고서 22-28.

홍건식. 2023. “사이버 공간의 진영화와 영향공작”.INSS 이슈브리프 501호.

2024 국가정보보호백서. 국정원.

2023 사이버 보안 위협 전망, 과학기술정보통신부

대만 정부 "대만, 사이버 공격 매일 500만 번 받아…대부분 중국발", https://www.yna.co.kr/view/AKR20230530070000009 (검색일:2024.5.14).

사이버 보안: 왜 서방 국가의 해킹 공격 소식은 드물까?, https://www.bbc.com/korean/international-65995610 (검색일:2024.5.24).

“日 연구기관 등 200곳 사이버 공격 연루 혐의 중국인 입건”, https://www.yna.co.kr/view/AKR20210420131100073 (검색일:2024.5.28).

"사이버 공격이란 무엇인가" 의미와 사례, 동향 분석, https://www.itworld.co.kr/news/145522 (검색일:2024.6.13.).

이란·중국·북한 배후 사이버공격 기승…"보안사고엔 '만약' 없다", https://zdnet.co.kr/view/?no=20230421112257 (검색일:2024.6.13.).

중국 사이버 공격 그룹의 최신 동향, https://www.mandiant.com/resources/blog/chinese-espionage-tactics (검색일:2024.5.20).

중국 욕하면 사이버 공격...미국서 암약한 중국 비밀조직 또 적발, https://www.hankookilbo.com/News/Read/A2023042616320003429?did=NA (검색일:2024.5.17).

美, 중국인 해커 2명 기소… 최소 12개국서 해킹 혐의, https://www.munhwa.com/news/view.html?no=2018122101070830129001 (검색일:2024.5.3).

최근 5년간 외교부 대상 사이버 공격 10건 중 4건이 중국發, https://mn.kbs.co.kr/news/pc/view/view.do?ref=A&ncd=4042031 (검색일:2024.5.20.).

“AI 활용한 랜섬웨어-악성코드로 사이버 공격 늘어” https://www.donga.com/news/Economy/article/all/20240219/123594144/1 (검색일:2024.7.2.).

FBI 국장 “북한·중국, 사이버 작전 통해 미국 위협”, https://www.voakorea.com/a/7558723.html (검색일:2024.7.2.).

Belfer Center for Science and International Affairs Harvard Kennedy School, National Cyber Power Index 2022 (검색일:2024.6.15).

China tests US voter fault lines and ramps AI content to boost its geopolitical

interests,
https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/ (검색일:2024.6.18).
CYBER CAPABILITIES AND NATIONAL POWER:A Net Assessment, THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, p.90.
https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/ (검색일:2024.5.20).
Fact Sheet: 2023 DoD Cyber Strategy,
https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF (검색일:2024.5.20).
2024 Annual Threat Assessment of the U.S Intelligence Community
2023 Annual Threat Assessment of the U.S Intelligence Community
Global Innovation Index 2022, https://www.wipo.int/global_innovation_index/en/2022/ (검색일:2024.3.2).
Mandiant, APT1: Exposing One of China's Cyber Espionage Units,
https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf (검색일:2024.6.8).
China Appears to Warn India: Push Too Hard and the Lights Could Go Out,
https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html (검색일:2024.4.25).
2023年7月14日外交部发言人汪文斌主持例行记者会,
https://www.fmprc.gov.cn/fyrbt_673021/jzhsl_673025/202307/t20230714_11113401.shtml
Stealth Mode: Chinese Cyber Espionage Actors Continue to Evolve Tactics to Avoid Detection, https://www.mandiant.com/resources/blog/chinese-espionage-tactics (검색일:2024.5.10).
起底！中国网安企业人士提供翔实一手资料：印度黑客对我重要部门频密发动网络攻击！,
http://www.news.cn/world/2021-11/20/c_1211454111.htm (검색일:2024.5.26).
国家网络空间安全战略(全文), https://www.cac.gov.cn/2016-12/27/c_1120195926.htm,
https://www.mandiant.com/resources/blog/chinese-espionage-tactics (검색일:2024.6.16).
网络空间国际合作战略（全文）,
http://www.china.org.cn/chinese/2017-03/07/content_40424606.htm
2023年 中国网络安全产业分析报告

*이 글의 내용은 필자 개인의 견해이며*
*한국사이버안보학회의 공식 입장이 아닙니다.*