

# 사이버 보안과 핵티비즘: 동향과 시사점

유영상

본 보고서는 ETRI ICT전략연구소 기본사업인  
“국가 지능화 기술정책 및 표준화 연구”를 통해 작성된 결과물입니다.



## ◆ 요약 ◆

본 고에서는 2024년에 주로 많이 발생할 것으로 예상되는 사이버 위협과 관련된 핵티비즘에 대해 살펴보았다. 핵티비즘은 정치적 또는 사회적 목적을 위한 해킹으로 정의되며, 그 동기는 복잡하고 미묘하나 일반적으로 정치적 행동주의, 사회적 정의, 보복 및 복수 등을 포함하고 있다. 핵티비즘이 미치는 영향은 매우 다양하여, 불의를 폭로하고 변화를 일으킨다는 긍정적인 측면과 동시에 불법적 행위로 인해 무고한 개인이나 집단에 피해를 주는 범죄라는 부정적 측면이 공존한다.

현재 많은 국가에서 정치화된 핵티비즘을 사이버 보안과 연결하여 잠재적 위협으로 보기 시작했으며, 미국의 경우 핵티비스트를 사이버범죄자 집단으로 규정하고 있다. 본 고에서는 대표적 핵티비스트인 어나니머스와 롤즈젝의 활동 사례를 통해 핵티비즘의 동기와 공격 방식 등 실제 전개 과정을 살펴보았으며, 사이버 보안 관점에서 핵티비즘과 사이버 테러와의 차이 및 사이버 테러의 변화 양상을 알아보았다. 핵티비스트의 사이버 공격에 대응하기 위해서는 법 집행 기관의 적극적 대응과 국제협력, 사이버 보안 관련 조직 및 개인의 역할, 윤리적 해킹, 그리고 AI를 이용한 사이버 보안 기술의 개발이 중요하다.

## 📌 들어가며

2024년은 전 세계적으로 역대 가장 많은 선거가 치러지는 해로 정치·사회적 이슈를 악용하는 사이버 위협이 크게 고조될 것으로 전망된다.

- 2024년에는 정치·사회적 이슈를 악용하는 사이버 위협이 크게 고조될 것으로 과학기술정보통신부는 전망 [1]
- 2024년은 역대 가장 많은 선거가 치러지는 해로, 전 세계적으로 60여 개 국가에서 40억 명 이상이 투표를 하는 대 격동의 해로 기록될 전망 [2]



\* 출처: 연합뉴스(2023. 12. 26), 2024년 주요국 선거 일정

- 1월의 대만 총통 선거를 시작으로 2월 인도네시아 대선·총선, 3월 러시아 대선, 4월 한국·인도의 총선, 11월 미국 대선 등 국내외에 대규모 정치적 행사가 예정
- 국가적 중요한 행사가 있을 때 사회 혼란을 노리는 세력들의 사이버 위협 가능성 증가와 불순한 목적이나 갈등을 조장하기 위한 다양한 공격이 예상
- 최근 미국 대선을 앞두고 AI로 바이든 대통령의 가짜 목소리를 제작하여 대선 예비 경선 투표를 방해하려 한 정치 컨설턴트에 거액의 벌금 부과 [3]

해티비즘은 정치적 또는 사회적 목적을 달성하기 위해 해킹을 통해 벌이는 정책이나 행동을 의미한다.

- 해티비즘(Hacktivism)은 해킹(hacking)과 행동주의(activism)이 융합된 용어로서 ‘정치적 또는 사회적 목적을 위한 해킹’이라고 정의 [4]
  - New Hacker's Dictionary에서는 ‘해커’를 프로그래밍 가능한 시스템의 세부사항과 기능 확장 방법을 탐색하는 것을 즐기는 사람이라고 정의 [5]
  - 한편으로는 신원 도용을 통해 사람들에게 피해를 주기 위해 정보를 훔치거나 시스템을 다운시키거나, 몸값을 받기 위해 시스템을 인질로 잡는 경우와 같이 범죄를 저지르기 위해 자기 능력을 이용해 시스템이나 네트워크에 무단으로 액세스하는 사람을 의미하기도 함 [6]
  - ‘행동주의’는 ‘정치적, 사회적 변화를 가져오기 위해 활발한 캠페인을 벌이는 정책이나 행동’ [7], 또는 ‘정치적 또는 사회적 목표를 달성하기 위해 직접적이고 눈에 띄는 행동을 사용하는 것’ [8] 등으로 정의
  - 따라서 해티비즘은 ‘정치적 또는 사회적 목표를 달성하기 위해 컴퓨터와 인터넷 기술을 사용하여 해킹, 프리킹(phreaking), 또는 새로운 기술을 생성하는 정책이나 행동’을 의미
    - ※ 프리킹(phreaking): 전화 시스템을 표적으로 삼는 해킹의 한 형태로서 무료 또는 승인되지 않은 전화를 걸기 위해 전화 시스템을 조작하거나 해킹하는 행위
  - 해티비즘에는 웹사이트 훼손, 서비스 거부 공격, 특정 문제에 대한 인식 제고 또는 특정 의제를 홍보하기 위한 데이터 유출 등이 포함

### ④ 해티비즘의 동기

해티비즘의 주요 동기에는 정치적 행동주의, 사회적 정의, 보복과 복수 등이 포함된다.

- 해티비스트의 행동 이면에는 단순한 이념보다 더 복잡하고 미묘한 경우가 많으며, 가장 일반적 동기에는 정치적 행동주의, 사회 정의, 보복 및 복수가 포함 [9]
- 정치적 행동주의
  - 많은 해티비스트 그룹은 언론의 자유부터 정부 투명성에 이르기까지 모든 것을 위해 싸우는 정치적 행동주의에 의해 동기를 부여받음
  - 이러한 그룹은 정부 기관, 군대, 기타 억압적이거나 사악하다고 판단되는 조직을 대상으로 공격을 가하는 경우가 많음
  - 일례로 2010년에 Anonymous(어나니머스)는 내부 고발자 웹사이트인 WikiLeaks에서 서비스를 철회한 회사의 웹사이트에 대해 일련의 공격인 ‘Operation Payback’을 시작했고, 이것은 표현의 자유와 정부 투명성에 대한 공격에 대한 보복으로 수행 [10]
  - 또한 ‘아랍의 봄’ 붐기 동안 어나니머스는 튀니지와 이집트 같은 국가의 민주화 운동을 지원하기 위한 노력의 일환으로 해당 국가의 정부 기관 웹사이트를 표적화
- 사회적 정의

- 어나니머스와 같은 그룹은 동물 실험이나 인권 유린과 같은 일에 연루되어 개인이나 단체를 착취하고 있다고 느끼는 기업과 조직을 표적으로 삼는 경우가 많으며, 이는 자신들이 취약한 사람들을 보호하고 사회에 해로운 권력 구조를 재조정하기 위해 노력하고 있다고 생각하는 경우가 많기 때문
- 2012년 미국 오하이오주 스투벤빌(Steubenville)의 고등학교 축구팀의 선수 두 명이 16세 소녀를 성폭행하였으나 경찰이 사건을 축소, 은폐하려 하자 어나니머스는 구단 홈페이지와 SNS 계정을 해킹해 팀원과 코치들의 개인정보를 유출했으며, 이를 성폭력 문화 문제와 고등학교 스포츠에서 지속되는 방식에 대해 사회적 관심을 끌어내는 방법으로 간주 [11], [12]

### ○ 보복과 복수

- 일부 해커비스트 그룹은 보복과 복수를 동기로 삼으며, 이러한 그룹은 경력이 파괴된 내부 고발자나 환경법 준수를 거부한 회사 등 어떤 방식으로든 잘못했다고 생각하는 개인이나 조직을 표적화
- 일례로 2011년 민간 정보회사인 Stratfor를 해킹하고 WikiLeaks에 데이터를 공개한 혐의로 10년의 징역형을 받은 해커비스트 Jeremy Hammond의 경우, Stratfor가 불법 활동에 연루되어 있고 활동가들을 염탐하고 있다고 믿었기 때문에 Stratfor를 표적으로 삼았다고 주장 [13]
  - ※ 이 Stratfor 해킹으로 인해 60,000개의 신용카드 번호가 유출되었고, 신용 카드 번호 중 일부는 사기 혐의로 70만 달러에 달하는 피해를 유발

어나니머스는 Chanology Project, Operation Payback 등을 수행했을 뿐만 아니라 아랍의 봄, 러시아-우크라이나 전쟁에도 관여하였다.

Project Chanology는 사이언톨로지 교회가 유튜브에서 특정 파일을 삭제하도록 압력을 가한 행위를 인터넷 검열로 보고 사이언톨로지 교회를 인터넷에서 추방하고자 시작되었다.

## 📖 주목할 만한 해커비스트 그룹

### ○ 어나니머스(Anonymous)

- 가장 잘 알려진 해커비스트 그룹 중 하나인 어나니머스는 ‘느슨하게 연결된 활동가와 해커비스트 단체의 국제 네트워크’로 이 그룹과 관련된 웹사이트는 이를 ‘지시보다는 아이디어에 따라 작동하는 매우 느슨하고 분산된 명령 구조를 갖춘 인터넷 모임’이라고 설명 [14]
- [Project Chanology] 2008년 어나니머스는 톰 크루즈(Tom Cruise)와의 인터넷 인터뷰 자료를 삭제하려는 사이언톨로지 교회의 시도에 대응하는 ‘Project Chanology’ 실시 [15], [16]
  - ✓ Chanology는 4chan\*과 Scientology의 합성어로서 이 프로젝트는 2008년 1월 영화배우이자 사이언톨로지 교인인 영화배우 톰 크루즈(Tom Cruise)와의 인터넷 인터뷰 자료를 삭제하려는 사이언톨로지 교회의 시도에 대응하여 시작
    - ※ 4chan은 익명의 영어 이미지 보드(이미지 게시에 중점을 두는 일종의 인터넷 포럼) 웹 사이트로서 어나니머스가 2003년 이 4chan에서 시작(출처: Wikipedia)
  - ✓ 2008년 1월 14일, 영국 사이언톨로지 교회가 제작한 톰 크루즈의 인터뷰를 담은 영상이 유튜브에 게재되었고, 이 영상 속에서 크루즈는 교통사고 후 도와줄 수 있는 사람은 사이언톨로지스트뿐이며 범죄자를 교화하거나 중독자들

을 마약에서 벗어나게 하는 권한은 사이언톨로지스트에게만 있다는 등의 진술을 한 바 있음 [17]

- ✓ 사이언톨로지 교회는 유튜브와 다른 웹사이트에 유출된 비디오 자료가 사이언톨로지 회원들을 위해 제작된 3시간 분량의 비디오에서 "해적·편집된" 것이라고 주장하였고, 유튜브는 소송 위협 아래 크루즈 비디오를 그들의 사이트에서 삭제
- ✓ 어나니머스는 이러한 사이언톨로지의 행위를 인터넷 검열로 보고, 사이언톨로지 교회를 인터넷으로부터 추방하려는 의도로 Chanology 프로젝트를 시작
- ✓ 2008년 1월 21일 유튜브에 게시된 "Message to Scientology"라는 동영상을 시작으로 분산 서비스 거부 공격(DDoS)이 이어졌으며, 곧이어 블랙 팩스, 장난 전화 및 기타 조치로 사이언톨로지 교회의 운영을 방해 [18]

*Operation Payback은 미국 정부의 비밀 외교 전문을 공개한 WikiLeaks에 대해 제재를 가한 기관을 대상으로 DDoS 공격 등을 통해 어나니머스가 전개한 활동이다.*

- [Operation Payback] 2010년 WikiLeaks에 대해 제재를 한 조직에 대해 Operation Payback 캠페인 전개

※ Operation Payback은 원래 인터넷 불법 복제에 반대하는 음악산업과 관련된 회사를 대상으로 한 일련의 보복 사이버 공격이었으나 나중에 WikiLeaks의 기밀 데이터 공개에 대한 반발 이후 새로운 목표를 포함하도록 확대

- ✓ 2010년 11월 WikiLeaks가 유출된 미국 외교 전문 수십만 건을 공개하기 시작하자 미국 정부로부터 비밀 외교 전문을 공개하는 것을 중단하라는 강력한 압력을 받았으며, Amazon, PayPal, Bank of America, 스위스 금융회사 PostFinance, MasterCard 및 Visa와 같은 기업은 정치적 압력으로 인해 WikiLeaks와의 협력을 중단하거나 고객의 기부금을 동결 [19]
- ✓ 이에 대응한 어나니머스의 DDoS 공격으로 PayPal 웹사이트, 그리고 WikiLeaks에 대한 서비스를 거부한 PostFinance, 웹 호스팅 회사인 EveryDNS, 그리고 서비스 중단을 지지했던 미국 상원의원 조 리버만(Joe Lieberman)의 웹사이트가 다운되었으며, 이어서 2010년 12월 8일 Operation Payback의 조직적인 DDoS 공격으로 Visa 및 MasterCard의 웹사이트가 다운
- ✓ PayPal은 이로 인해 회사에 550만 달러의 손실이 발생한 것으로 추산하였고, 나중에 공격자 1,000명의 IP 주소를 FBI에 제공하여 최소 14명이 체포 [20]

- [Westboro Baptist Church] 2012년 어나니머스는 극단적 증오 단체로 알려진 웨스트보로 침례교회(Westboro Baptist Church)에 대해 교인 신상 공개 및 DDoS 공격 실시

- ✓ 웨스트보로 침례교회는 아프가니스탄 미군 전사자, 살해당한 동성애자, 에이즈 병사자, 애리조나 총기 난사 사건 희생자, 버지니아 공대 총기 난사 사건 희생자, 보스턴 마라톤 폭탄 테러 사망자 등의 장례식에서 혐오스러운 피켓 시위나 조롱을 지속 해왔으나 미국 대법원은 이를 표현의 자유로 인정 [21], [22], [23]
- ✓ 특히 2012년 총격 사고로 어린이 20명과 성인 6명이 살해당한 미국 코네티컷 주의 샌디훅 초등학교에서 웨스트보로 침례교회가 피켓 시위로 하나님의 심판을 찬양할 것이라고 게시하자, 어나니머스는 교회 신도들의 이름, 전화번호, 이메일 및 집 주소를 공개하고 DDoS 공격으로 웹사이트를 다운 [20]

*어나니머스는 극단적 증오단체로 알려진 웨스트보로 침례교회를 대상으로 신도들의 개인 신상을 공개하고 DDoS 공격으로 웹사이트를 다운시켰다.*

아랍의 봄은 2010년 시작된 아랍권 민주화 시위로 중동 전역에서 해커비스트 활동을 급증시켰으며, 해커비스트는 시위대를 조직하고 동원하는 데 핵심적인 역할을 하였다.

- [Arab Spring] 어나니머스는 아랍권 민주화 시위인 ‘아랍의 봄’에도 참여해 튀니지, 이집트, 리비아의 봉기를 지원 [24]
  - ✓ 아랍의 봄(Arab Spring)은 2010년 12월 17일 튀니지 혁명 이후에 폭발하여 2011년에 절정, 그리고 2024년 현재까지도 여파가 미치고 있는 아랍권의 민주화 시위 [25]
  - ✓ 2009년 이후 세계 금융위기가 본격화되고, 2010년 러시아의 흉작으로 식량, 특히 밀 수출을 막기 시작하면서 국제 식량 가격의 폭등과 여기에 달러화 약세까지 겹쳐 아랍권의 경제와 식량 사정이 더욱 악화
  - ✓ 민중들은 정부에 곡물 가격 문제 해결을 요구하기 시작하면서 각지에서 소규모 시위, 분신 시도 등이 벌어졌고 이것이 혁명의 시발점으로 작용
  - ✓ 어나니머스는 튀니지인들이 정부 감시로부터 웹 브라우저를 보호하는 데 사용할 수 있는 스크립트를 만들었고, 튀니지 정부 웹사이트에 대한 DDoS 공격을 시작했으며 또한 튀니지 반체제 인사들이 봉기에 대한 비디오를 온라인으로 공유하도록 지원 [20]
  - ✓ 아울러 활동가 그룹인 Telecomix와 협력하여 반체제 인사들이 정부 검열을 우회하고 서로 및 외부 세계와 소통할 수 있도록 지원하였으며, 계속해서 바레인, 이집트, 리비아, 요르단, 짐바브웨의 정부 웹사이트 공격에 가담
  - ✓ 아랍의 봄은 중동 전역에서 해커비스트 활동을 급증시켰고, 해커비스트는 시위대를 조직하고 동원하는 데 핵심적인 역할을 했으며, 이들의 활동은 이 기간에 발생한 많은 봉기의 성공에 필수적 역할 수행
  - ✓ 다른 해커비스트 그룹도 아랍의 봄에 참여하여 정부 웹사이트를 공격하고 시위대에 기술 지원을 제공했으며, 이들 그룹의 활동은 봉기와 관련 문제에 대한 인식을 높이는 데 일조

어나니머스는 최근 러시아의 우크라이나 침공에 대한 보복으로 러시아 연방을 상대로 한 Operation Russia를 전개하였다.

- [Operation Russia] 최근에는 러시아의 우크라이나 침공에 대한 보복으로 러시아 연방을 상대로 ‘사이버 작전’을 시작
  - ✓ 어나니머스는 러시아 선전 방송국인 RT News의 웹사이트를 해킹하여 다운시켰고 국방부 데이터베이스를 해킹하였으며, 러시아의 우크라이나 침공 시 러시아에 물류 지원을 제공한 벨라루스 무기 제조업체 Tetradr로부터 200GB 상당의 이메일을 유출 [26]
  - ✓ 또한 러시아 TV 채널을 해킹하여 우크라이나 음악을 재생했으며, 우크라이나에서 일어난 사건에 대한 무수정 뉴스를 상영 [27], [28]

### ● 룰즈섹(LulzSec)

룰즈섹은 단기간 활동한 해커비스트 그룹으로 기업의 보안 결함을 노출하여 기업을 조롱하고 당혹스럽게 만드는 것이 주된 관심사라고 밝혔다.

- 룰즈섹은 소규모 어나니머스 그룹에서 분파한 해커비스트 그룹으로 2011년 세간의 이목을 끈 소니 플레이스테이션 네트워크를 공격한 것으로 알려진 단기간 활동한 해커비스트 그룹
  - ※ LulzSec은 웃음(lol)을 뜻하는 lulz와 보안을 뜻하는 security에서 따온 신조어
- 이 그룹은 범죄 목적이거나 금전적 이익을 위해 해킹한 것으로 보이지는 않으며, 주된 동기는 혼란을 야기하여 재미를 느끼는 것, 즉 보안 결함을 노출하여 기업을 조롱하

- 고 당혹스럽게 만드는 것이 주요 관심사 [29], [30]
- ✓ LulzSec은 해킹된 사용자 이름을 공개하거나 취약한 웹사이트를 대중에게 알림으로써 사용자에게 다른 곳에서 악용될 수 있는 이름과 비밀번호를 변경할 기회를 제공하고 기업은 경각심을 가지고 보안을 강화하게 될 것이라고 주장
- ✓ 그러나 이들은 자신들이 위반하고 공개한 데이터의 오용에 대한 책임을 부인하는 대신 여러 웹사이트에서 비밀번호를 재사용하는 사용자와 보안이 제대로 이루어지지 않은 회사를 비난 [31]
- 룰즈섹은 2011년 5월부터 6월까지 다양한 기업, 공공기관, 정부 기관을 해킹 [32]
  - ✓ 2011년 5월에 Fox.com을 해킹하여 여러 개의 비밀번호, LinkedIn 프로필 및 73,000명의 X Factor 참가자 이름을 유출
  - ✓ 영국 내 3,100대의 ATM기기의 거래 로그에 침투하여 개인 은행 계좌 정보를 탈취
  - ✓ Sony Japan의 데이터베이스 내부를 공개
  - ✓ 미국의 PBS 방송국이 부정적인 WikiLeaks 다큐멘터리를 방영하자 PBS의 비밀번호를 훔치고 래퍼 Tupac이 살아 있다는 가짜 기사 게시
  - ✓ 2011년 6월 Sony의 음악 코드, 쿠폰, 고객 정보를 훔치면서 Sony의 보안 결함에 대해 최대한의 당혹감을 주기 위해 이들을 공개할 것이라고 주장
  - ✓ 사용자 로그인 및 서버 구성 파일과 같은 '기본 정보'가 손상되었다고 보고하는 Sophos를 통해 미국 상원 등 정부 웹사이트를 해킹
  - ✓ 2011년 6월 LulzSec은 CIA에 대한 DDoS 공격을 통해 3시간 동안 웹사이트를 다운 [33]
- 2011년 6월 26일 LulzSec은 'lulz의 50일' 성명을 발표하여 LulzSec이 6명의 멤버로 구성되어 있으며 해당 웹사이트가 폐쇄될 것임을 확인 [34]
  - ✓ 이들은 처음부터 50일 동안만 활동할 계획이었다고 주장하며, 법 집행이 두려워서 그만두는 것이 아니라 언론이 그들을 지루하게 만들고 있고, 그들 자신도 지루하게 만들고 있다고 주장 [35]
  - ✓ 해당 그룹의 구성원들은 AntiSec 작전을 계속하기 위해 어나니머스 구성원들과 합류한 것으로 알려짐 [36]

위키리크스는 해커비즈니스 그룹은 아니나 해커비즈니스 운동에 상당한 영향력을 미쳤다.

#### ○ 위키리크스(WikiLeaks)

- 위키리크스는 엄밀히 말하면 해커비즈니스 그룹은 아니나 해커비즈니스 운동에 상당한 영향력을 행사한 조직
  - ✓ 위키리크스는 2006년 호주의 인터넷 활동가인 Julian Assange가 설립한 비영리 단체로 기부금과 미디어 파트너십을 통해 자금을 조달 [37], [38]
  - ✓ '중요한 뉴스와 정보를 대중에게 전달하여 대중이 세상을 형성하는 사건에 대해 스스로 결정을 내릴 수 있도록 하는 것'을 목표로 기밀 정보와 민감한 정보를 게시하는 것으로 알려져 있으며, 그 활동은 전 세계의 많은 해커비즈니스 그룹에 영향



- 수년에 걸쳐 위키리크스는 2010년 미국 군사 및 외교 기밀 문서 공개를 포함하여 여러 차례 중요한 유출에 연루되었으며, 이 조직의 활동이 국가 안보를 위협한다는 비난을 하는 사람과 투명성과 표현의 자유를 옹호한다고 칭찬하는 사람 등이 있어 논란의 여지가 있음

**해티비즘이 언론의 자유와  
 검열에 대한 논쟁을  
 불러왔고, 현대 시위에  
 있어서 중요한 역할을  
 해왔으나, 부정적인 결과도  
 초래하고 있어 사회적으로  
 미치는 영향은 관점에  
 따라 매우 복잡하고  
 다양하다.**


## **해티비즘이 사회에 미치는 영향**

- **해티비즘이 사회적으로 미치는 영향은 복잡하고 다양**
  - 흔히 정의의 옹호자라고 자칭하는 해티비스트의 행동은 개인과 조직에 심각한 영향
  - 즉, 누군가에게는 불의를 폭로하고 변화를 일으키는 영웅으로 여겨지지만, 불법 행위를 통해 피해를 주는 범죄자로 여겨지기도 함
  - 그러나 어떤 사람의 입장과 관계없이 해티비즘은 공개 담론을 형성하고 정치 및 사회 구조에 영향을 미치는 것은 분명
- **표현의 자유와 검열에 대한 논쟁**
  - 해티비즘에 대한 주요 논쟁 중 하나는 그것이 언론의 자유인지 검열인지의 여부
  - 많은 해티비스트 그룹은 자기 행동을 권위에 도전하고 언론의 자유를 장려하는 방법으로 보지만, 다른 그룹은 반대 목소리를 침묵시키고 다른 사람에게 자신의 의지를 강요하기 위해 사이버 무기를 사용할 뿐이라고 주장
  - 해티비스트 그룹은 언론의 자유를 장려하는 것과 다른 사람에게 해를 끼치는 불법 활동에 가담하는 것 사이에서 아슬아슬하게 줄타기하는 경우가 많음
- **현대 시위에서 해티비즘의 역할**
  - 해티비즘은 현대 시위에서 점점 더 중요한 역할을 해왔으며, 예를 들어, 어나니머스와 같은 해티비스트 그룹은 Occupy Wall Street\* 시위 중에 시위대를 조직하고 동원하는 데 중요한 역할을 수행
    - ※ Occupy Wall Street(OWS)는 2011년 9월 17일부터 11월 15일까지 59일 동안 뉴욕 시를 중심으로 발생한 경제적 불평등과 기업법 부패에 대한 항의 시위
  - 해티비스트 그룹은 또한 전 세계적으로 경찰의 폭력과 기타 문제에 반대하는 시위를 조직하는 데 참여
    - ✓ 일례로 미국 미니아폴리스 경찰의 조직적인 소수 인종 차별과 과도한 무력 사용 관행으로 2020년 체포 중 사망한 조지 플로이드 사건에 대한 보복으로 어나니머스가 미니아폴리스 경찰청 웹사이트 서버 마비 [39]
  - 해티비스트 그룹은 암호화된 통신 및 기타 보안 조치를 사용하여 시위대의 신원을 보호하고 그들이 법 집행 기관이나 기타 그룹의 표적이 되는 것을 방지
- **해티비스트 행위로 인해 의도하지 않은 부정적 결과 초래 가능**
  - 비록 해티비스트의 의도는 숭고할 수 있지만 그들의 활동은 의도하지 않은 결과를

초래할 가능성

- ✓ 예를 들어, 해커비스트 그룹이 수행한 많은 공격으로 인해 민감한 정보가 노출되어 잠재적으로 개인이나 조직이 위험에 직면할 가능성이 있음
- ✓ 또한, 웹사이트에 대한 DDoS 공격으로 인해 합법적인 사용자가 사이트에 액세스하지 못하게 되어 불만이 발생하고 불편을 겪는 등 해커비스트 행위는 무고한 개인이나 조직에 부정적인 영향을 미칠 수 있음
- ✓ 또한, 해커비스트 행위로 인해 법 집행 기관이나 기타 그룹의 감시 및 모니터링이 강화되어 잠재적으로 개인의 개인 정보 보호 권리가 침해될 가능성 존재

해커비즘과 사이버 테러는 여러 측면에서 상당한 차이가 있으며, 사이버 테러의 경우 변화 양상에 주목할 필요가 있다.

 **해커비즘과 사이버 테러**

- 해커비즘과 사이버 테러 모두 컴퓨터 네트워크를 사용하는 것은 유사하지만 둘 사이에는 상당한 차이가 존재 [9]
  - 첫째, 해커비즘은 종종 정치적 또는 사회적 행동주의로 인해 동기가 부여되지만, 사이버 테러는 해를 입히거나 특정 정치적 또는 이념적 의제를 촉진하려는 욕구에 의해 동기가 부여
  - 둘째, 해커비스트가 사이버 공격을 수행할 수 있지만 그들의 목표는 지속적인 피해를 주기보다는 인식을 높이거나 불편을 끼치는 것인 경우가 많음
    - ✓ 예를 들어, 해커비스트 그룹은 특정 정책에 항의하기 위해 정부 웹사이트에 DDoS(분산 서비스 거부) 공격을 수행
  - 셋째, 해커비스트 활동은 불법인 경우가 많지만, 사이버 테러는 일반적으로 주요 인프라 파괴와 같은 명시적인 범죄 행위를 수반
    - ✓ 사이버 테러리즘은 인명 손실을 포함한 심각한 결과를 초래할 수 있으며 많은 정부와 조직에서 주요 위협으로 간주
    - ✓ 사이버 테러리즘은 극단주의자들과 기타 단체들이 자신들의 목표를 추진하고 혼란을 야기하기 위해 컴퓨터 네트워크를 사용하면서 전 세계적으로 점점 더 위협이 커지는 추세
    - ✓ 사이버 테러리스트의 가장 일반적인 목표에는 민감한 정보를 훔치고, 중요한 인프라를 파괴하고, 폭력적인 이데올로기를 조장하는 것이 포함
- 사이버 테러의 경우 변화 양상에 주목할 필요가 있음 [40]
  - 공격 대상이 정부 기관과 군, 금융기관에서 사이버 절도 유형의 공격으로 변화
    - ✓ 기존의 사이버 테러는 정보 탈취 및 국가기능의 마비가 목적이었으나, 점차 암호화폐나 금융기관의 해킹을 통한 경제적 이익을 노린 사이버 절도 유형의 공격으로 변화
    - ✓ 북한의 경우 정부 기관 및 금융 기관, 정부출연연구소 등에 대한 해킹 및 DDoS 공격, 악성 코드 유포 등에서 은행 전산망, 암호화폐 및 가상화폐거래소 등으로 변화

- 공격 주체가 개인이나 해커조직에서 국가 주도의 사이버 테러로 전환
  - ✓ 과거의 개인이나 해커조직이 주도하는 사이버 테러 방식은 자기 과시적 목적이거나 금전적 이익을 목적으로 하였다면 국가 주도의 사이버 테러의 경우 사이버전 및 지능형 지속공격(APT) 기법을 사용한다는 점이 특징
  - ※ 지능형 지속공격(APT: Advanced Persistent Threat): 해커가 특정 타깃을 선정한 후 소셜 엔지니어링 등 다양한 방법을 이용해 네트워크에 침입한 후 공격이 성공할 때까지 (혹은 완전히 불가능해지기 전까지) 짧게는 수 주, 길게는 수 년에 걸쳐 줄기차게 공격하는 방식 (출처: 기획재정부 시사경제용어사전)
  
- 테러 단체가 마약 밀매나 인신매매, 무기 밀매 등 범죄적 수법을 통해 테러 자금을 모집하는 것과 같은 ‘범죄와 테러의 결합 가속화’
  - ✓ 사이버공간에서의 범죄와 테러의 결합은 현실 세계의 결합을 뛰어넘어 사이버 범죄에서 사용되는 수법을 이용하되 파급력은 범죄보다 더 큰 경우도 많음
  - ✓ 사이버범죄가 악성 코드를 이용하여 사용자 정보나 산업기밀 등을 훔치거나 시스템 접근을 차단하는 방식이라면, 사이버 테러에서는 발전시설의 전원공급장치를 차단하는 등 중요한 인프라를 손상시키는 방식으로 사용
  - ✓ 사이버범죄에서 신원 절도를 통해 사이버 사기를 저지른다면, 사이버 테러에서는 절취한 타인의 신원을 이용해 테러범의 신분을 위장하고 테러 자행에 사용
  
- **해커비스트의 공격 방식과 대응 방법**
  - 해커비스트의 사이버범죄에는 웹사이트 훼손, 웹사이트 리디렉션, 서비스 거부(DoS) 공격 또는 분산 서비스 거부(DDoS) 공격, 악성 코드 배포, 데이터 도난 및 공개, 방해 행위 등이 포함되며, 이러한 모든 전술에는 대상의 시스템, 웹사이트 및 데이터에 대한 무단 액세스가 포함 [41]
  - 미국 FBI는 해커비즘을 이념적, 사회적, 정치적 목적을 달성하기 위해 사이버 활동을 수행하는 사이버범죄자 집단으로 규정 [42]
    - ✓ 해커비스트는 자신의 목적을 위해 공격을 수행하려는 모든 사람에게 사이버 공격 방법론 및 기술에 대한 도구와 지침을 제공
    - ✓ 웹페이지 및 소셜 미디어 프로필 훼손과 함께 공개 웹사이트에 대한 DDoS 공격이 많이 선호되는 전술
    - ✓ 이러한 DDoS 공격은 일반적으로 기회주의적이며 DDoS 완화 단계를 통해 피해자에게 미치는 운영상의 영향은 최소화되나 해커비스트들은 종종 소셜 미디어에 대한 공격의 심각성을 홍보하고 과장
    - ✓ 결과적으로 DDoS 공격의 심리적 영향은 서비스 중단보다 더 큰 경우가 많으며, 실제 운영 중단보다 더 큰 영향을 미칠 것으로 인식되는 대상을 주로 선택
  - DDoS 공격은 지속 시간이 다양하며 네트워크 성능이 비정상적으로 느리거나, 또는 특정 웹사이트를 사용할 수 없거나 어떤 웹사이트에도 액세스 할 수 없는 경우 등으로 식별할 수 있으며, 다음과 같은 조치로 DDoS 공격을 완화

DDoS 공격 등을 통한 해커비즘은 많은 국가에서 사이버 범죄로 간주되고 있으며, 이에 대응하기 위해서는 정부의 대응뿐만 아니라 국제협력, 개인과 조직의 사이버 보안 의식, 그리고 윤리적 해커의 역할이 중요하다.

- ✓ 비정상적인 트래픽 흐름을 감지하고 네트워크에서 트래픽을 리디렉션하는 서비스 거부 보호 서비스에 등록
- ✓ 인터넷 서비스 제공업체(ISP)와 파트너십을 맺고 ISP와 협력하여 이벤트 중에 네트워크 트래픽을 제어
- ✓ 공격 발생 시 성공적이고 효율적인 통신, 완화 및 복구를 보장하기 위한 재해 복구 계획을 수립
- ✓ DDoS 공격 도중과 이후에는 다른 네트워크 자산을 모니터링하여 2차 공격을 나타낼 수 있는 추가적인 비정상적이거나 의심스러운 활동이 있는지 모니터링

▶ 핵티비즘과 사이버 테러의 비교 ◀

구분	핵티비즘	사이버 테러
개념	<ul style="list-style-type: none"> <li>• 정치적 또는 사회적 목표를 달성하기 위한 해킹</li> </ul>	<ul style="list-style-type: none"> <li>• 국가의 핵심 기반시설을 마비시키거나 정부 또는 민간인을 강제, 위협하기 위하여 컴퓨터 네트워크를 사용하는 행위 [43]</li> </ul>
동기	<ul style="list-style-type: none"> <li>• 정치적 행동주의</li> <li>• 사회적 정의</li> <li>• 보복과 복수 등</li> </ul>	<ul style="list-style-type: none"> <li>• 국가 핵심 기반 시설 마비 및 파괴</li> <li>• 암호화폐, 금융 기관 해킹 등 사이버 절도</li> </ul>
공격 주체	<ul style="list-style-type: none"> <li>• 개인이나 그룹 등 해커 조직</li> </ul>	<ul style="list-style-type: none"> <li>• 국가 배후 또는 국가 주도로 변화</li> </ul>
공격 대상	<ul style="list-style-type: none"> <li>• 개인, 기업, 단체 홈페이지 등</li> </ul>	<ul style="list-style-type: none"> <li>• 정부, 군, 인프라</li> <li>• 은행, 전산망, 암호화폐 및 가상화폐 거래소</li> </ul>
공격 방법	<ul style="list-style-type: none"> <li>• 해킹·컴퓨터바이러스·논리폭탄·메일 폭탄·서비스 방해 등 전자적 수단 [44]</li> </ul>	<ul style="list-style-type: none"> <li>• 해킹·컴퓨터바이러스·논리폭탄·메일 폭탄·분산 서비스거부 공격(DDoS), 랜섬웨어, 트로이 목마 등 [43]</li> <li>• 지능형 지속 공격(ATP)</li> </ul>
국제 조직	<ul style="list-style-type: none"> <li>• 어나니머스</li> <li>• 룰즈섹</li> <li>• 락비트 [45]</li> <li>• 켈빈시큐리티 [46]</li> </ul>	<ul style="list-style-type: none"> <li>• 북한 정찰총국·총참모부 [47]</li> <li>• 중국 인민해방군·국가안전부·공안부</li> <li>• 러시아 군 정보총국</li> <li>• 이란 혁명수비대</li> </ul>
국내 규정	<ul style="list-style-type: none"> <li>• 정보통신망법</li> <li>• 국가사이버안전관리규정(대통령훈령)</li> <li>• 국가정보안전기본지침(국가정보원)</li> <li>• 정보보안기본지침(콘텐츠진흥원)</li> </ul>	<ul style="list-style-type: none"> <li>• 테러 방지법·형법</li> <li>• 정보통신기반보호법·정보통신망법</li> <li>• 신용정보의 이용 및 보호에 관한 법률</li> </ul>

\* 출처: 저자 재정리

- 핵티비즘과 사이버 테러에 맞서 싸우기 위해서는 다음과 같은 방법을 고려할 필요가 있음 [9]
  - ✓ (정부 및 법 집행 기관의 대응) 전 세계 정부와 법 집행 기관은 핵티비즘과 사이버 테러에 맞서 싸우기 위해 노력해 왔으며, 여기에는 사이버범죄자를 처벌하기 위한 새로운 법률 개발, 사이버 공격 조사를 위한 법 집행 기관의 역량 강화 등이 포함
  - ✓ (국제협력의 강화) 초국가적 범죄 성격의 사이버 테러에 대응하기 위해서는 국제공조를 위한 사이버범죄 협약 가입 등 초국가적 협력 증진 노력이 필요 [43]
  - ✓ (사이버 보안의 역할) 조직과 개인은 강력한 비밀번호 사용, 소프트웨어 최신

상태 유지, 적절한 경우 암호화 사용 등 공격으로부터 디지털 정보를 보호하기 위한 조치가 필요

- ✓ (윤리적 해킹) 윤리적 해킹은 해티비즘과 사이버 테러에 맞서 싸우는 데 중요한 역할을 수행할 수 있으며, 윤리적인 해커는 컴퓨터 시스템에 대한 지식을 활용하여 공격을 방어하고 조직이 사이버 보안을 개선하도록 지원
- ✓ (전문 인력의 양성) 사이버 수사 전문 인력 및 사이버 보안 인력 양성이 필요

해티비즘과 같은 사이버 공격은 관련 법률에서 범죄로 규정하고 있다. 특히 해티비즘의 결과가 사이버 테러의 도구로 사용될 가능성이 높다는 점에서 이를 방지할 수 있는 기술의 개발이 필요하다.

## 해티비즘에 대한 법적 조치

- 영국과 미국은 정치화된 해티비즘을 잠재적인 위협으로 보기 시작
- 영국의 2000년 테러법(Terrorism Act 2000)은 테러리즘을 “전자 시스템을 심각하게 방해하거나 교란하기 위해 심각하게 설계된 행동의 사용 또는 위협”으로 정의 [48]
- 미국의 2001년 애국법(Patriot Act 2001)에서는 컴퓨터 네트워크 침입에 대한 최고 형량을 5년에서 10년으로 상향하였고, 2002년 사이버 보안 강화법(Cyber Security Enhancement Act 2002)은 무모하게 누군가의 죽음을 초래하거나 시도한 해커에 대해 최대 종신형을 선고할 것을 요구 [49]
- 미국은 러시아와 우크라이나의 전쟁에서 외국 정부 또는 비정부 컴퓨터를 해킹하는 미국 내 개인에 대해 연방법인 컴퓨터 사기 및 남용법(Computer Fraud and Abuse Act; CFAA)과 중립법(Neutrality Act)에 따라 민사 및 형사 처벌될 수 있음을 경고 [50]
- 국내의 경우, 이혼한 배우자에게 양육비와 위자료를 지급하지 않은 사람들의 신상을 공개함으로써 사적 제재를 가한 배드파더스(bad fathers) 인터넷 사이트 운영자에 대해 대법원에서는 정보통신망법상 명예훼손 혐의로 유죄 판결 [51]

## 시사점

- 해티비스트의 행동은 정치적, 사회적 이슈에 대해 공개 담론을 형성하는 등 긍정적 측면도 있으나, 개인과 조직에 심각한 영향을 미치는 부정적 측면을 간과할 수 없음
  - 표현의 자유는 존중받아야 할 기본권이지만 절대적 권리는 아니며, 표현의 자유라는 이름으로 말하거나 행하는 데에는 분명한 한계가 있음
  - 해티비스트의 공격으로 인해 민감한 정보가 노출되어 잠재적으로 무고한 개인이나 조직이 위협에 직면할 가능성이 있으며, 이는 사이버 테러에 이용될 가능성도 존재

- 대부분의 국가에서는 해킹비즈니스를 사이버범죄로 규정하고 있으며, 해커비즈니스의 행위로 인해 법 집행 기관이나 기타 그룹의 감시 및 모니터링이 강화되어 잠재적으로 개인의 개인 정보 보호 권리가 침해될 가능성 존재
- 우크라이나와 러시아 간 전쟁의 지속으로 미국 등 제3국의 해커비즈니스 활동이 증가하고 있으며, 미국의 경우 외국 컴퓨터 시스템과 관련하여 금지된 활동에 참여하거나 군사 임무를 수행하는 것을 금지한 연방법 위반이 될 수 있음
- 해커비즈니스의 활동으로 인한 정보 절도 및 유포는 사이버 테러의 도구가 될 가능성이 농후하고, 종교적 극단주의 뿐만 아니라 인종차별, 젠더 갈등, 이주민 갈등, 동물권·낙태권 등의 폭력적 극단주의는 정치적 의제로도 확장되고 있어 대책이 필요
- AI를 이용한 딥페이크 역시 잘못된 정치적 행동주의의 결과로 볼 수 있으며, 이를 추적·방지할 수 있는 AI 사이버 보안 기술의 개발이 필요

## 참고문헌

- [1] 과학기술정보통신부 보도자료 (2023), “2023년 사이버 보안 위협 분석 및 2024년 전망 발표,” 2023. 12. 18.
- [2] 연합뉴스 (2023. 12. 26), [그래픽] 2024년 주요국 선거 일정 (<https://www.yna.co.kr/view/GYH20231226000800044>)
- [3] YTN (2024. 5. 24), “바이든 ‘가짜 목소리’ 벌금 82억 원... 딥페이크 음란물 제재” ([https://www.ytn.co.kr/\\_ln/0104\\_202405241101149356](https://www.ytn.co.kr/_ln/0104_202405241101149356))
- [4] metac0m (2003) “What is hactivism? 2.0” (<http://edshare.soton.ac.uk/8762/2/whathactivism.pdf>)
- [5] New Hacker’s Dictionary (<http://www.catb.org/esr/jargon/oldversions/jarg271.txt>)
- [6] TechTarget, “Hacker” (<https://www.techtarget.com/searchsecurity/definition/hacker>)
- [7] English definitions powered by Oxford Languages (<https://en.bab.la/dictionary/english/activism>)
- [8] Cambridge Dictionary (<https://dictionary.cambridge.org/dictionary/english/activism>)
- [9] John Iannarelli, “What is Hacktivism? Understanding Hacktivists & Cyberterrorism,” August 2, 2023. (<https://fbijohn.com/hacktivism-cyberterrorism/>)
- [10] BBC News (2010. 12. 9), “Anonymous hacktivists say Wikileaks war to continue” (<https://www.bbc.com/news/technology-11935539>)
- [11] Nancy Schwartzman; Nora Zelevansky (2022), “When Anonymous Focused Its Digital Wrath on the Steubenville Rape Case” (<https://lithub.com/when-anonymous-focused-its-digital-wrath-on-the-steubenville-rape-case/>)
- [12] Wikipedia, “Steubenville High School rape case” ([https://en.wikipedia.org/wiki/Steubenville\\_High\\_School\\_rape\\_case](https://en.wikipedia.org/wiki/Steubenville_High_School_rape_case))
- [13] Wikipedia, “Jeremy Hammond” ([https://en.wikipedia.org/wiki/Jeremy\\_Hammond#cite\\_note-Poulson-13](https://en.wikipedia.org/wiki/Jeremy_Hammond#cite_note-Poulson-13))
- [14] ANON OPS: A Press Release (2010. 12. 10), “Who is Anonymous” ([https://www.wired.com/images\\_blogs/threatlevel/2010/12/ANONOPS\\_The\\_Press\\_Release.pdf](https://www.wired.com/images_blogs/threatlevel/2010/12/ANONOPS_The_Press_Release.pdf))
- [15] Richards, Johnathan (2008. 1. 25), “Hackers Declare War on Scientology,” Fox News. (<https://edition.cnn.com/2012/12/16/tech/web/anonymous-westboro-baptist/index.html>)
- [16] The Guardian, “Hackers declare war on Scientologists amid claims of heavy-handed Cruise control” (<https://www.theguardian.com/technology/2008/feb/04/news>)
- [17] Youtube, “Tom Cruise Scientology Video” ([https://www.youtube.com/watch?v=UFBZ\\_uAbxS0](https://www.youtube.com/watch?v=UFBZ_uAbxS0))
- [18] Wikipedia, “Project Chanology” ([https://en.wikipedia.org/wiki/Project\\_Chanology](https://en.wikipedia.org/wiki/Project_Chanology))
- [19] The Guardian, “Anonymous cyber-attacks cost PayPal £3.5m, court told” (<https://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court>)
- [20] Wikipedia, “Anonymous(hacker group)” ([https://en.wikipedia.org/wiki/Anonymous\\_\(hacker\\_group\)](https://en.wikipedia.org/wiki/Anonymous_(hacker_group)))
- [21] CNN (2012. 12. 16), “Anonymous targets Westboro Baptist over threats of Newtown protest” (<https://edition.cnn.com/2012/12/16/tech/web/anonymous-westboro-baptist/index.html>)
- [22] 크리스찬저널 (2011. 3. 4), “웨스트보로 재판, 표현의 자유 인정”

- (<https://www.kcijlogos.org/news/articleView.html?idxno=6389>)
- [23] CBS NEWS (2012. 12. 17), “Hackers Vow To Render Westboro Baptist Church ‘Obsolete’ After Threat To Protest At Newtown School”  
(<https://www.cbsnews.com/newyork/news/hackers-vow-to-render-west-boro-baptist-church-obsolete-after-threat-to-protest-at-newtown-school/>)
- [24] Aljazeera (2011. 5. 19), “Anonymous and the Arab uprisings”  
(<https://www.aljazeera.com/news/2011/5/19/anonymous-and-the-arab-uprisings>)
- [25] 나무위키, “아랍의 봄” (<https://namu.wiki/w/아랍의%20봄>)
- [26] Security Affairs (2022. 2. 26), “Anonymous hacked the Russian Defense Ministry and is Targeting Russian Companies” (<https://securityaffairs.com/128428/hacking/anonymous-russian-defense-ministry.html>)
- [27] iNews (2022. 2. 27), “Anonymous: Russian media channels broadcast Ukrainian songs after hacker group declare cyber war”  
(<https://inews.co.uk/news/world/anonymous-hacker-group-russia-tv-channels-broadcast-ukrainian-songs-1486735>)
- [28] The Guardian (2022. 2. 27), “Anonymous: the hacker collective that has declared cyberwar on Russia”  
(<https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>)
- [29] The New Republic (2011. 6. 14), “Hacking For Fun More Than Profit”  
(<https://newrepublic.com/article/89997/hacking-fun-more-profit>)
- [30] Nate Anderson (2011. 6. 18), “LulzSec manifesto: ‘We screw each other over for a jolt of satisfaction’”  
(<https://web.archive.org/web/20110619214911/http://arstechnica.com/tech-policy/news/2011/06/lulzsec-heres-why-we-hack-you-bitches.ars>)
- [31] Ars Technica (2011. 6. 4), “Lulz? Sony hackers deny responsibility for misuse of leaked data”  
(<https://arstechnica.com/tech-policy/2011/06/lulz-sony-hackers-deny-responsibility-for-misuse-of-leaked-data/>)
- [32] Fox News (2011. 6. 21), “A Brief History of the LulzSec Hackers”  
(<https://www.foxnews.com/tech/a-brief-history-of-the-lulzsec-hackers>)
- [33] The Independent (2011. 6. 16), “Who are the group behind this week's CIA hack?”  
(<https://www.independent.co.uk/news/world/americas/who-are-the-group-behind-this-week-s-cia-hack-2298430.html>)
- [34] Business Insider (2011. 6. 26), “LulzSec, the notorious hacker group that's been on a rampage, just announced that it's disbanding.” (<https://www.businessinsider.com/lulzsec-finished-2011-6>)
- [35] CNN (2011. 6. 27), “Hacking collective LulzSec says it is disbanding”  
(<http://edition.cnn.com/2011/TECH/web/06/26/tech.lulzsec.hackers/index.html>)
- [36] Los Angeles Times (2011. 6. 29), “AntiSec ‘hackers without borders’ claim new hack on Arizona state police”  
(<https://www.latimes.com/archives/blogs/technology-blog/story/2011-06-29/antisecc-hackers-with->



out-borders-claim-new-hack-on-arizona-state-police)

- [37] Hindman, Elizabeth Blanks; Thomas, Ryan J (2014), “When Old and New Media Collide: The Case of WikiLeaks,” *New Media & Society*, 16 (4), pp. 541 – 558.  
([https://www.researchgate.net/publication/275487052\\_When\\_old\\_and\\_new\\_media\\_collide\\_The\\_case\\_of\\_WikiLeaks](https://www.researchgate.net/publication/275487052_When_old_and_new_media_collide_The_case_of_WikiLeaks))
- [38] Benkler, Yochai (2011), “A Free Irresponsible Press: WikiLeaks and the Battle Over the Soul of the Networked Fourth Estate,” WORKING DRAFT ([https://benkler.org/Benkler\\_Wikileaks\\_current.pdf](https://benkler.org/Benkler_Wikileaks_current.pdf))
- [39] Time (2020. 6. 1), “After Anonymous Promises Retribution for George Floyd’s Death, Minneapolis Police Website Shows Signs It Was Hacked” (<https://time.com/5845880/anonymous-minneapolis-police-hack/>)
- [40] 박보라 (2022. 5. 16), “사이버 테러 위협의 새로운 양상: 사이버범죄의 연계와 테러 내러티브의 확산,” 국제문제연구소 이슈브리핑 No.181.
- [41] UNODC, “Hactivism” (<https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/hactivism.html>)
- [42] FBI (2022. 11. 4), “Private Industry Notification” (<https://www.ic3.gov/Media/News/2022/221104.pdf>)
- [43] 정도희 (2023), “사이버테러의 개념 및 대응방안,” 법학연구 제26집 제1호.
- [44] 국가사이버안전관리규정 [대통령훈령 제316호, 2013. 9. 2., 일부개정] 제2조 제2호
- [45] 데이터넷 (2024. 2. 21), “세계에서 가장 위험한 랜섬웨어 ‘락비트’, 공격 인프라 중단” (<https://www.datanet.co.kr/news/articleView.html?idxno=191159>)
- [46] BleepingComputer (2023. 12. 11), “Kelvin Security hacking group leader arrested in Spain” (<https://www.bleepingcomputer.com/news/security/kelvin-security-hacking-group-leader-arrested-in-spain/>)
- [47] 중앙일보 (2022. 1. 23), “[월간중앙] 국경없는 사이버테러, 대한민국이 위협하다” (<https://www.joongang.co.kr/article/25042729#home>)
- [48] Terrorism Act 2000, UK (<https://www.legislation.gov.uk/ukpga/2000/11/section/1>)
- [49] Baldi, Stefano; Gelbstein, Eduardo; Kurbalija, Jovan (2003), “Hactivism, Cyber-Terrorism and Cyberwar” (<https://baldi.diplomacy.edu/italy/isl/Hactivism.pdf>)
- [50] Congressional Research Service (2022. 5. 13), “‘Hactivists’ and the Ukraine-Russia Conflict: Legal Considerations” (<https://crsreports.congress.gov/product/pdf/LSB/LSB10743>)
- [51] 한겨레 (2024. 1. 4), “양육비 미지급자 신상공개 ‘배드파더스’ 명예훼손 유죄 확정” ([https://www.hani.co.kr/arti/society/society\\_general/1122950.html](https://www.hani.co.kr/arti/society/society_general/1122950.html))

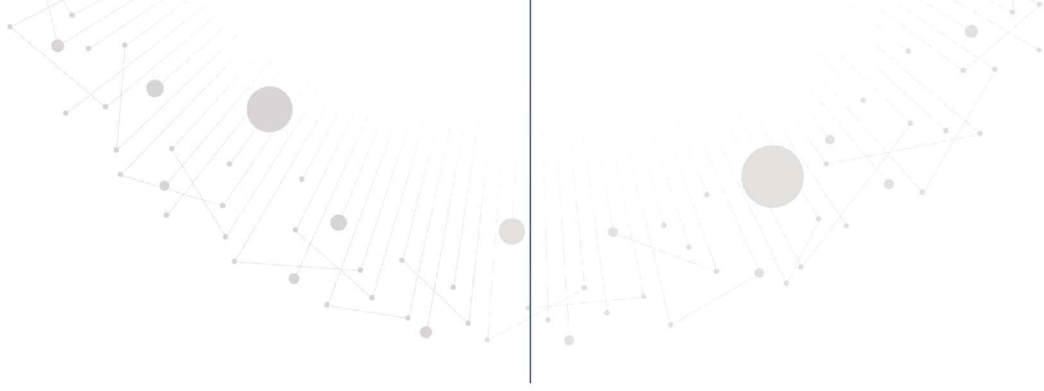
## 저자 소개

**유영상** ETRI ICT전략연구소 기술정책연구본부 기술경제연구실 연구전문위원  
e-mail: heyoo@etri.re.kr Tel. 042-860-6849

## 사이버 보안과 핵티비즘: 동향과 시사점

**발행인** 한 성 수  
**발행처** 한국전자통신연구원 ICT전략연구소  
**발행일** 2024년 6월 30일





[www.etri.re.kr](http://www.etri.re.kr)

본 저작물은 공공누리 제4유형:

출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.



**ETRI** Electronics and Telecommunications  
Research Institute

34129 대전광역시 유성구 가정로 218  
TEL.(042) 860-6114 FAX.(042) 860-6504

