ISSUE BRIEF

이슈브리프 471호
(2023.10.30)

하마스의 대(對) 이스라엘 사이버 공격과 시사점

제471호

김경숙 신흥안보연구실
홍건식 신흥안보연구실

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

팔레스타인 무장 정파 '하마스'가 지난 10월 7일 이스라엘을 대상으로 전례 없는 기습공격을 감행했다. 이번 하마스의 기습공격은 군사 및 비군사적 조치를 활용했으며 하마스 공격의 조직 규모와 수준을 볼 때 오랫동안 철저히 계획되고 준비되었음을 알 수 있다. 하마스의 테러 감행을 전후로 하마스 측의 핵티비스트들은 활발한 활동을 보이며, 이스라엘 측의 주요 인프라에 대한 직접적인 사이버 공격과 소셜미디어(SNS)를 활용한 선전전(propaganda) 그리고 가짜 뉴스 확산을 시도했다. 하마스의 공식 사이버 부대(Hamas Cyber Unit)는 이스라엘의 주요 표적에 대한 사이버 공격을 수행하였으며, SNS 공식 계정 텔레그램을 활용해 사이버 공간에서 이스라엘과 유대인에 대한 분노를 부추기는 선전전 및 국제 여론전을 전개했다. 이와 함께 러시아의 지원을 받는 킬넷(Killnet)과 어나니머스 수단(Anonymous Sudan) 등 친팔레스타인 공세를 주도하는 다양한 핵티비스트 그룹도 이들 사이버 공격에 동참했다. 결국 핵티비스트 그룹과 불특정한 집단의 사이버 전쟁 참여는 하마스와 이스라엘의 전쟁 양상을 더욱 어렵게 하고 있다. 러시아-우크라이나 전쟁 그리고 하마스의 테러 감행 초기 대(對) 이스라엘에 대한 사이버 공격을 통해서 사이버 공간의 중요성을 재확인한 우리도 국가 안보적 관점의 사이버 전략 마련이 필요하다. 이에 대비해 우리는 사이버 복원력과 국제 사이버 협력 강화 그리고 '가짜뉴스' 대응 체계 마련이 필요하다. 특히 물리적 충돌 등 위기 상황에서 정부 및 주요 핵심 인프라와 함께 주요 기업도 표적이 된다는 점을 고려해 민관 협력체계 구축으로 복원력 강화를 위한 전략도 함께 모색해야 한다.

핵심어 : 하마스, 이스라엘, 핵티비스트, 가짜 뉴스, 사이버 복원력

지난 10월 7일 하마스 무장 대원들은 이스라엘을 향해 최소 미사일 5,000발 이상을 발사했으며, 하마스와 이슬라믹 지하드로 구성된 침투 병력은 육로, 공중, 바다 등을 이용해 가자(Gaza) 지구와 이스라엘 사이에 설치된 장벽을 넘어 이스라엘에 침투했다. 하마스 공격의 조직 규모와 수준을 볼 때 오랫동안 철저히 계획되고 준비되었음을 알 수 있다.[1] 이스라엘 내부로 침투한 하마스는 군인과 민간인 수백 명을 인질로 잡고 소셜미디어(SNS)를 통해 관련 영상을 공개하며 공포감을 극대화했다. 사이버 공간에서는 하마스 해커들의 사이버 공격 활동도 증가했다.

하마스의 대(對) 이스라엘 테러 그리고 지난 러시아-우크라이나 전쟁에서 나타난 것처럼 국가는 국가 간 분쟁에서 적을 무력화시키고 군사 전략 목적을 달성하기 위해 사이버 전략을 적극적으로 활용하고 있다. 러시아의 우크라이나 침공 당시 러시아 정보기관 GRU은 침공 당일 미국에 본사를 둔 위성통신 업체 비아샛(Viasat)을 해킹한 것과[2] 같이 이번 하마스의 테러도 사이버 전력을 다양하게 활용했다. 하마스의 공식 사이버 부대(Hamas Cyber Unit)는 이스라엘의 주요 표적에 대한 사이버 공격을 수행하였으며 텔레그램 공식 계정을 통해 잘못된 정보 및 선전을 확산시켰다.

하마스의 핵심 인프라에 대한 사이버 공격 시도

하마스의 테러를 전후해 하마스의 공식 사이버 부대와 함께 친팔레스타인 공세를 주도하는 다양한 핵티비스트[3] 그룹도 사이버 공간을 통해 분쟁에 가담했다.[4] 특히 분쟁 발발 당시 하마스 내무장관

1) BESA 센터 관점 보고서는 가자 지구로 후퇴한 테러리스트까지 포함해 전체 공격에는 약 3,000명의 테러리스트가 침투하였으며 의도적으로 이스라엘군(IDF)의 유니폼이나 이와 유사한 패턴의 유니폼을 입고 있었다고 밝혔다. https://besacenter.org/the-gaza-terror-offensive-october-7-8-2023/

2) https://www.bbc.com/korean/international-60887580

3) 핵티비즘은 해킹(Hacking)과 정치행동주의를 뜻하는 액티비즘(Activism)의 합성어로 정치·사회적 목적을 위한 사이버 공격을 의미하며, 핵티비스트(Hactivist)는 이러한 목적을 위한 정치적 사이버 해킹 활동가라는 점에서 해커와는 차이가 있다. https://www.ciokorea.com/news/271653

4) Register는 "최소 15개의 알려진 사이버 범죄, 랜섬웨어 및 핵티비스트 그룹이 이스라엘과 팔레스타인의 기관과 그 지지자를 표적으로 삼는 파괴적인 공격에 적극적으로 참여하고 있다"고 발표하였다. https://www.theregister.com/2023/10/09/hacktivism_middle_east/; https://www.csoonline.com/article/655223/israel-palestine-conflict-extends-to-cyberspace.html

대변인은 이스라엘에 대한 사이버 공격을 지시하는 듯 “우리는 가자지구뿐 아니라 전세계 모든 팔레스타인 소프트웨어 기술자들에 이스라엘 웹사이트를 공격해 무력화시키라고 요청했다”고 밝혔다. 이를 전후해 친하마스 핵티비스트 그룹들의 활동이 확대되었고, Cyber Av3nagers와 AnonGhost 등이 보고되었으며, 러시아의 지원을 받는 킬넷(Killnet)과 어나니머스 수단(Anonymous Sudan) 등도 친팔레스타인 공세를 주도하는 해커 그룹으로 알려졌다.[5)]

Av3nagers는 이스라엘 전력망 시스템 운영 기관인 Noga Independent Systems Operator 해킹하고 디도스(DDoS) 공격을 했으며, 이외에도 DORAD 발전소 해킹, Mekorot과 ORPAK의 CCTV 엑세스 권한도 확보했다고 주장했다. 또 다른 친하마스 AnonGhost 핵티비스트 그룹은 이스라엘 미사일 경보 서비스 Red Alert 앱을 해킹해 ‘핵폭탄이 다가오고 있다’라는 가짜 경고를 배포했다.[6)] 한편 러시아 해커그룹 어나니머스 수단(Anonymous Sudan)은 이스라엘의 경고 어플리케이션에 대한 DDoS 공격을 했으며, 킬넷(Killnet)은 이스라엘 정부의 공식 웹사이트에 대한 공격을 감행했다. 이외에도 팔레스타인 해킹 그룹 블랙 쉐도우(Black Shadow)는 이스라엘 국방부를 포함한 이스라엘 웹사이트 및 조직에 대해 여러 차례 공격을 감행했다고 주장하였다.[7)] 마이크로소프트(MS)는 「디지털 방어 보고서 2023(Digital Defense Report 2023)」을 통해 가자지구에 기반을 둔 스톰-1133 해커그룹을 추적한 결과를 공개하기도 했다.[8)] 이들 핵티비스트들은 하마스의 테러 감행과 동시에 이스라엘의 공공기관과 주요 기반 시설에 대한 디도스(DDoS) 공격, 해킹 그리고 데이터 갈취 등을 감행하며, 이스라엘의 주요 인프라에 대한 무력화를 시도했다.

친이스라엘 해커들도 하마스의 사이버 공격에 대응했다.[9)] 인도에

5) https://www.newsis.com/view/?id=NISX20231013_0002482094
6) https://www.bitdefender.com/blog/hotforsecurity/hacktivists-send-fake-nuclear-attack-warning-via-israeli-red-alert-app/
7) https://www.secureworld.io/industry-news/hackers-rules-of-engagement-i
8) https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
9) https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/

기반을 둔 핵티비스트 그룹인 인디안 사이버 포스(Indian Cyber Force)는 팔레스타인 정부 웹 서비스에 대한 공격 주체가 자신들이라고 주장했다.[10] ThreatSec은 팔레스타인의 최대 ISP 제공업체인 Alfanet 시스템을 마비시켰으며, 이스라엘은 하마스의 암호화폐 계정을 동결하며 대응했다.[11]

하마스의 소셜미디어(SNS)를 활용한 가짜 뉴스의 확산

하마스와 일부 핵티비즘 집단은 SNS와 해시태그를 활용해 우군 확보와 사기 진작 그리고 심리전을 목적으로 자신들이 지지하는 집단에 대한 긍정적인 여론을 확산시켰다. 이들은 허위 정보, 잘못된 정보 등 가짜뉴스를 사이버 공간에 확산시키며 공포와 혼란을 조장했다.

하마스는 공식 계정 텔레그램과 엑스(X, 이전 트위터) 등을 활용해 이스라엘의 가자지구 공격 당시 상처를 입은 팔레스타인들의 영상을 편집, 배포 및 확산시켰다. 주목할 것은 하마스가 이번 테러에서 납치 인질들의 소셜 미디어 계정을 탈취해 가짜뉴스 확산에 적극적으로 활용했다는 점이다. 이들은 납치한 이스라엘인들의 페이스북, 인스타그램, 왓츠앱 등의 소셜 미디어 계정을 탈취하거나 가짜 계정을 활용해 폭력적인 메세지를 방송하며 이스라엘에 대한 반감을 조성하는 여론전과 심리전을 구사했다.[12]

그러면서도 하마스 집단은 자신들의 인도주의적인 모습을 대비해 보이며 사이버 공간 내에서 이스라엘에 대한 반감 여론을 조성하려 했다. 이들은 국제사회 여론을 의식해 납치된 인질들이 안전하고 정당한 대우를 받고 있다는 모습을 공개(10.16)했다. 이와 함께 가자지구 알아흘리 병원 피격(17일 현지시간)에 대해 이스라엘이 지하드 소행이라는 증거를 제시했음에도 불구하고, 하마스는

10) https://www.theregister.com/2023/10/09/hacktivism_middle_east/
11) https://www.wired.com/story/israel-hamas-war-hacktivism/
12) https://www.nytimes.com/2023/10/17/technology/hamas-hostages-social-media.html

이스라엘군의 소행이라는 관련 동영상을 게시하면서 이스라엘과 유대인에 대한 분노를 부추기는 국제 여론전을 전개했다. 하마스를 지지하는 미스터리어스 팀 방글라데시(Mysterious Team Bangladesh)와 같은 핵티비스트는 텔레그램 등을 통해 하마스 지지를 표명하면서 #FreePalestine, #OpIsraelV2 등 인기 있는 친팔레스타인 해시태그를 사용해 관련 영상 배포에 동참했다.[13)]

이스라엘은 이에 대응해 공식 발표와 공식 계정 X를 통해 하마스의 테러 행위를 규탄하고, 하마스의 허위 정보를 반박하는 증거를 제시했다. 또한 SNS 계정을 통해 '자기방어를 위한 이스라엘의 공격권을 인정한다면 (이 게시물을) 공유해달라'고 요청하는 등 적극적인 대응에 나서고 있다.

하마스의 사이버 공격에서 주목할 것은 납치 인질 활용과 사이버 공간에서 다양한 SNS를 수단으로 사용하고 있다는 점이다. 하마스의 공식 계정, 친하마스, 친팔레스타인 해커 및 핵티비스트, 납치된 인질의 SNS를 통해 가짜뉴스를 확산시켜 이스라엘을 비방하고 자신들의 테러 정당성을 주장하는 선전전을 지속하고 있다. 하마스의 이 같은 사이버 전략은 사이버 공간에서의 여론전을 통해 인질 납치에 대한 국제사회의 비난을 무마하고 가자지구 팔레스타인들의 피해를 부각해 지상군 투입이 임박한 이스라엘군을 압박하려는 의도가 담겨 있다.

시사점 : 국가 안보 전략 수준의 사이버 전략 고려 필요

러시아-우크라이나 전쟁 이후 사이버 공간은 전략 목적을 달성하기 위한 필수적인 전장이 되었다. 특히 이번에도 하마스의 테러 감행을 전후로 핵티비스트들과 해커들이 이스라엘의 핵심 인프라에 대한 사이버 공격을 감행하였다. 하마스는 자신들의 테러 정당성 확보를 목적으로 사이버 공간에서 SNS를 통한 '가짜뉴스'도 확산시켰다.

13) https://www.newsis.com/view/?id=NISX20231013_0002482094

이를 고려했을 때 우리도 국가 안보 전략 수준에서 사이버 전략 마련이 필요하다. 사이버 전략은 이제 사이버 공간의 평화와 안정을 구축하는 전략이 아닌 국가 안보 차원의 전략적 접근이 필요하다. 우선, 사이버 복원력(resilience) 강화가 필요하다. 사이버 복원력이란 사이버 위협에 적응하는 역량으로 사이버 공격을 예상·감지하며 공격 후 이를 복구하는 대비 수준을 말한다. 이는 사이버 위협 가해자의 위협 의도를 사전에 억제함과 동시에 위협이 발생하더라도 그 비용을 최소화해 공격자의 목표 달성을 제한하는 기능을 할 수 있다. 지난 2022년 EU는 사이버 복원력법(EU Resilience Act)을 제정했으며, EU의 통합적인 대응과 사이버 위협을 최소화하는 데 초점을 두고 있다. 북한의 사이버 위협에 상시 노출되어 있는 우리는 전력망, 통신망, 해저케이블 등 핵심 인프라의 사이버 시스템 안정성 구축을 위해 관련 소프트웨어에 대한 지속적인 기능 개선이 필요하다. 이를 통해 보안 취약성을 해결하고 성능을 최적화할 필요성이 있다.

둘째, 핵티비즘화하는 사이버 위협은 글로벌 문제로 국제 사회의 공동 대응이 절대적이다. 악의적 국가·비국가 행위자의 사이버 위협에 대비해 미국을 중심으로 우방국과 국제적 공동 대응 체계 구축을 지속해야 한다. 한국과 미국은 지난 4월 체결한 '전략적 사이버안보 협력 프레임워크'를 기반으로 사이버 위협에 대한 공동 대응 체계를 보다 강화할 필요가 있다. 미 국방부는 「사이버 전략(Cyber Strategy)」을 통해 동맹국·파트너 국가와 사이버 위협 정보에 대한 정보 공유 강화를 정책적으로 추진할 것임을 밝힌 바 있다. 따라서 한미 간 사이버 협력체계를 강화하는 한편 한미일 사이버 정보 공유 협력도 증대해 북한의 사이버 위협 등에 적극적으로 대응할 필요가 있다.

셋째, 사이버 공간에서의 '가짜 뉴스' 확산에 대한 체계적인 대응 마련도 필요하다. SNS에 가짜뉴스, 특히 인공지능(AI) 기반 가짜 뉴스가 범람하면서 이를 막기 위해 SNS 플랫폼에 대한 규제 조치도 이어지고 있다. 유럽연합(EU)은 디지털서비스법(DSA)를 근거로 X,

페이스북 모회사 메타플랫폼(이하 메타) 등 주요 SNS 플랫폼에 가짜뉴스와 테러 관련 게시물 삭제를 요구하는 등 '가짜뉴스' 차단을 강화하는 조처를 하고 있다.[14] 관련해 우리 정부도 헌법이 보장한 개인의 기본권을 보장하면서도, 인터넷 기업의 효율성과 안전한 사이버 공간을 구축할 수 있는 인터넷 규제와 지원책 마련이 필요하다. 인터넷 플랫폼 내에서 허위 정보 확산 방지와 이를 모니터링하는 시스템 개발과 '가짜뉴스' 대응을 위한 '특별운영센터' 등을 운영해 건전한 인터넷 공간을 구축할 수 있어야 한다.

//끝//

본 내용은 집필자 개인의 견해이며,
국가안보전략연구원의 공식입장과는 다를 수 있습니다.

14) DSA를 위반한 SNS 플랫폼은 연간 글로벌 수익의 최대 6%를 과징금으로 내야 한다. https://www.yna.co.kr/view/AKR20231014004500091?section=international/all