JDFR Journal of Data Forensics Research
데이터포렌식연구, 2권 1호, 2025년 6월, 95-109면
Journal of Data Forensics Research, Volume 2, Issue 1, June 2025, Pages 95-109.
https://doi.org/10.12972/JDFR.2025.2.1.6
Print ISSN 3058-9460
Online ISSN 3058-9479

원저

국가 간 사이버 공격의 구조적 양상 분석: 연결망 기반 실증적 접근

김동환[1], 김대환[2], 김지온[3]

[1]한림대학교 융합과학수사학과 석사, [2]한림대학교 융합과학수사학과 학사, [3]한림대학교 융합과학수사학과 교수

교신저자: 김지온, jion972@hallym.ac.kr

요약

본 연구는 2014년부터 2024년까지의 주요 사이버 공격 데이터를 기반으로, 국가 간 사이버전의 구조적 양상을 사회연결망분석(SNA) 기법으로 분석하였다. CISSM Cyber Event Database를 활용하여 공격국, 피해국, 피해 산업, 공격 행위자 유형 간 관계를 네트워크로 모델링하고 시각화한 결과, 러시아·북한·중국은 주로 지정학적 적대국과 전략적 산업 부문(공공행정, 금융, 정보 등)을 주요 공격 대상으로 삼았다. 권위주의 국가는 국가주도형·범죄형 공격을, 민주주의 국가는 핵티비스트 유형의 공격을 주로 수행하는 경향이 나타났다. 특히 북한·러시아·이란의 공격 네트워크를 분석한 결과, 러시아와 이란은 한국을 직접적으로 공격하지 않으면서도 북한과 다수의 공통 공격 대상국을 공유하고 있어, 향후 대북정책 수립 시 양국과의 외교적 협력이 간접적인 사이버 갈등 완화에 기여할 수 있음을 시사한다. 본 연구는 사이버전을 개별 사건이 아닌 구조적 관계 속에서 해석함으로써, 국제 사이버 안보 전략 및 갈등 대응체계 설계에 실증적 근거를 제공한다.

주제어

데이터포렌식, 사회 연결망 분석, 사이버전, 국제정세

Open Access

Received: June 18, 2025
Revised: June 30, 2025
Accepted: June 30, 2025
Published: June 30, 2025

© 2025 Korean Data Forensic Society

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

Structural analysis of inter-state cyber attacks: A network-based empirical approach

Donghwan Kim[1], Daehwan Kim[2], Jion Kim[3]

[1]Master's Student, Department of Forensic Science, Hallym University, Republic of Korea
[2]Undergraduate Student, Department of Forensic Science, Hallym University, Republic of Korea
[3]Professor, Department of Forensic Science, Hallym University, Republic of Korea

Corresponding Author: Jion Kim, jion972@hallym.ac.kr

ABSTRACT

This study conducted a social network analysis (SNA) of cyberattack data from 2014 to 2024. By leveraging the CISSM cyber event database, it models networks among attacker states, victims, industries, and actors. The findings reveal that Russia, North Korea, and China primarily target geopolitical adversaries and strategic sectors, such as public administration, finance, and information. Authoritarian states tend to favor state-led or criminal attacks, whereas democracies are more commonly associated with hacktivist activities. Notably, Russia and Iran share numerous targets with North Korea, despite not directly attacking South Korea, suggesting that diplomatic ties with these states may indirectly ease cyber tensions. This structural approach offers empirical insights into shaping global cybersecurity strategies and conflict response systems, highlighting the strategic value of network-based analysis in understanding cyber-conflict dynamics and informing diplomatic engagement.

KEYWORDS

Data forensics, social network analysis, cyber warfare, international dynamics

I. 서론

현대 국제사회는 인터넷 통신의 발달로 인해 기존 물리적 무력 충돌을 넘어 사이버 공간에서도 전쟁이 이루어지는 사이버전이 병행되는 하이브리드전이 활발하게 이루어지고 있다[1]. 사이버 공간은 데이터 송·수신 및 원거리 통신 환경에서 벗어나 국가 간 경쟁과 대립이 벌어지는 전장과 같은 기능을 하고 있으며, 이러한 흐름 속에서 사이버 범죄와 국가 주도의 사이버전 양상은 점차 심화되고 복잡해지고 있다. 북한은 정찰총국 산하의 라자루스(Lazarus) 집단을 필두로 스피어피싱, 악성코드 배포, 주요 인프라 공격 등의 사회혼란 목적의 사이버 공격을 자행하였다. 또한 국제 사회의 경제적 제제속에서 금융 인프라 탈취, 암호화폐 거래소 해킹 등의 경제 이윤 탈취 목적의 사이버 공격을 자행하였다[2]. 우크라이나와 러시아 전쟁에서도 사이버 공격이 활발하게 병행되었다. 2022년 러시아 해커들은 우크라이나의 은행, 정부 기관등을 상대로 DDoS 공격, 악성코드 유포 등 사이버 공격을 시행하였으며, 이에 대한 대처로 우크라이나 역시 정부 주도의 민간 IT 전문가들을 모집하여 'IT의용군'을 창설하였으며 국제 해킹조직인 어나니머스와 빅테크 기업들의 지원으로 대응하였다[3]. 이란과 이스라엘 간 지속적인 사이버 공방 역시 이러한 현대의 사이버 공격이 단순한 기술 침해를 넘어서 정치적·전략적 목적을 가진, 마치 전쟁과 같은 행위로 자리 잡아가고 있다는 것을 보여준다.

이러한 사이버 공격 대상은 국가의 물류 인프라, 공공 행정, 정보, 금융 인프라 및 교통 등 국가의 핵심이 되는 시설로 확장되고 있으며, 이를 통한 인프라 마비, 정보 탈취 등과 같은 행위는 국가의 안보를 위협하고 사회적 혼란을 야기하는 등 물리적인 충돌과 더불어 국가에 큰 타격을 주기도 한다. 이러한 사이버 공격들은 국가 간 공개적인 물리 충돌 없이도 실질적인 피해를 발생시키는 공격 수단으로 활용되고 있으며, 국제사회의 사이버 안보 정책 수립에 큰 영향을 미치고 있다.

이처럼 사이버전이 전략적인 공격 수단으로 활용됨에따라, 단일 사건들의 분석을 넘어, 국가 간 그리고 국가 내부 해킹 집단 간의 연계성과 공격 패턴들을 종합적으로 판단하는 분석이 요구된다. 단순히 단일 사건의 내용 분석뿐만 아니라, 각 국가들이 어느 정도의 빈도로 어떤 나라를 공격하였으며, 어떠한 공격 형태를 채택했는지, 국가간 공격과 피해 연결망의 간접적인 관계까지 고려하면 국제정세를 어떻게 평가할 수 있을지 등에 대한 거시적인 분석 역시 동반되어야 국가별 사이버전 동향 및 국가 내부의 하위 해커집단의 공격 동향 에 대한 심도있는 분석이 가능할 것이며, 각국의 사이버 보안 태세의 점검및 효과적인 대응 방안 마련에 있어서도 필수적인 기반이 될 수 있다.

본 연구는 국가 대 국가 및 국가 내부 해킹 집단 간의 구조적 연계성을 분석하여 사이버전의 전략적 양상을 도출하는 것을 목적으로 한다. 미국 해리스컴퓨터(Harris Computer) 社의 i2 Analyst's Notebook(관계정보를 노드와 엣지로 시각화하여 다양한 분석을 할 수 있는 정보분석 도구로 전 세계 형사사법기관에서 사용중)을 분석 도구로 활용하여 2014년부터 2024년까지의 사이버공격을 크롤링하여 기록한 데이터를 네트워크 시각화한다. 이후 사회 연결망 분석(Social Network Analysis, SNA) 및 공격 이벤트 세부 분석을 진행하여 기존의 사건 중심 분석과 더불어 거시적인 분석을 함께 진행하여 기존 분석들의 한계를 보완하며, 사이버전의 전개 양상과 국제 정세 간의 관계를 전체적인 네트워크를 통한 전반적인 사이버 공격 양상에 대한 거시적 관점과 세부적인 국가 단위의 사이버 공격 행위에서 도출될 수 있는 미시적 관점에서의 분석을 통합적으로 조망하고자 한다.

II. 이론적 배경 및 관련 연구 분석

2.1. 이론적 배경

사이버전(Cyber Warfare)이란 디지털 환경에서 발생하는 정치적, 군사적 목적의 공격 행위를 의미하며, 정보 시스템에 대한 파괴, 교란 등을 포함한다[4]. 기존 연구에서는 주로 국가 간 갈등에 초점을 맞추었으나, 2015년 연구에서는 정의를 넓혀 해커집단 또는 개인들 역시 의도를 가지고 사이버전에 참여할 수 있다는 점에서 사이버전의 개념의 확장을 주장하였다[5].

하이브리드전(Hybrid war)이란 기존의 무력투쟁인 정규전과 여러 분쟁형태인 비정규전의 이분법적 구분을 넘어서 다양한 수단이 통합적으로 운용되는 현대전의 새로운 형태이다. 해당 선행 연구에서는 하이브리드전을 물리적 전투뿐 아니라, 정치적 사회적 불안을 조성하고 국가의 주요 인프라등을 마비시켜 상대국가의 전력을 초기에 약화시키는 비전투적인 공격으로 정의하였다[6]. 사이버 해킹 공격은 이러한 하이브리전의 비전투적인 수단 중 하나로 간주되며, 따라서 물리적 충돌과 별개로 대상 국가의 인프라 및 사회에 혼란을 야기하는 비전투 도구로 활용된다.

사회연결망 분석이란 정치적, 경제적, 사회적 구조 환경에서 나타나는 다양한 사회적 실체간의 관계와 그 관계의 패턴을 분석하고 결과를 도출하는 연구방법론으로서, 다양한 행위자들 간의 중심성, 밀도, 집단 형성 등의 관계 지표를 활용하여 정량적인 분석을 가능하게 해주는 도구이다[7]. 최근에는 사이버 보안 및 사이버 범죄 분야에서도 사회연결망분석 방법론이 활발하게 활용이 되고 있으며, 해커 조직의 관계 구조 파악, 사이버상에서의 이상 행위, 피해자 연결성 등을 분석하는 데 사용되어지고 있다[8,9]. 실제로 국내의 여러 수사전문가들은 SNA 및 응용 프로그램을 활용하여 실제 범죄자들을 추적하고 검거하는데에 활발하게 사용하고 있다[10,11].

2.2. 선행연구 분석

Anastopoulos[8]는 MISP(Malware Information Sharing Platform)를 기반으로 수집된 위협 정보를 활용하여, 조직 간 공유하는 위협 공간(shared threat space)을 사회연결망분석(이하 SNA라고 한다.) 기법으로 분석하였다. 본 연구는 이와 유사하게 SNA 기법을 적용하되, 동일한 IP 주소나 인프라로부터 공격받은 피해자 그룹을 식별하는 방법론을 설계하고자 하였다.

Sarkar et al.[9]는 대규모 사이버 공격의 증가에 대응하여, 소셜 플랫폼을 활용해 공격을 사전에 예측하고 방어할 수 있는 방안에 대해 연구하였다. 이들은 다크웹 포럼에서 사용자의 답변 구조에 SNA를 적용함으로써, 전문가 사용자를 중심으로 한 상호작용 패턴을 분석하고, 전문가의 중심성과 영향력을 정량적으로 평가하였다.

Péter Kacziba[12]는 국제관계 분야에서 증가하는 국가 및 비국가 행위자 간 상호작용의 복잡성을 설명하기 위한 방법론으로 SNA의 활용 가능성을 제시하였다. 그는 기존의 국제관계 이론들이 복잡다변한 국제 시스템의 상호작용을 충분히 설명하는 데 한계가 있다고 보고, SNA가 이러한 복잡한 상호작용 구조를 보다 체계적으로 분석할 수 있는 대안적 접근임을 강조하였다. 특히 외교 네트워크 데이터를 활용하여 국가 간 외교관계의 밀도, 상호성, 중심성과 같은 핵심 네트워크 지표를 실증적으로 도출하였으며, 이를 통해 국제 체계 내에서 개별 국가의 상대적 영향력과 위상을 정량적으로 평가하는 분석틀을 제시하였다.

한편, 미국의 싱크탱크인 CSIS(Center For Strategic & International Studies)는 2006년부터 시작된 정부, 빅테크 기업 및 국가 경제를 대상으로 한 사이버 공격에 대한 사실들을 기록

해 놓은 Significant Cyber Incidents 보고서[13]를 정기적으로 공개하고 있다. 해당 보고서에는, 다양한 국가들의 국제사회 사이버 공격에 대한 사례들을 포함하고 있으며, 특히 러시아-우크라이나 간 분쟁을 비롯하여, 북한의 해킹 공격 등 여러 국가들의 사이버 갈등 양상을 기록하고 있다. 해당 보고서는 다양한 국가간의 사이버 갈등에 대한 내용을 포함한다는 점에서 본 연구와 깊은 관계가 있다.

국내에서도 SNA를 활용한 사이버 범죄 연구가 진행된 바 있다. 수사정보분석에 SNA 방법론을 최초로 활용한 김지온[14]의 연구에서는 중심성(Centrality)과 하위집단(Cohesive subgroup) 원리가 다양한 수사사례에 어떻게 적용될 수 있는지를 개괄적으로 소개하였다. 문병훈과 곽기영[10]은 사이버 도박 범죄 수사에 사회 연결망 분석을 적용하여 조직 구조와 핵심 인물을 식별하는 성과를 도출하였다. 김현철과 윤지원[11]은 사이버 금융범죄 수사 중 조건만남 사기 사건을 중심으로 SNA 방법론을 활용하여 계좌정보, 메신저 계정, 접속 IP등에 대한 수사 단서를 네트워크 시각화하였으며, 이를 통해 범죄 조직 간의 연결성을 분석하여 수사단서들과 중심노드의 연관성을 식별하여 수사 진행에 실질적인 기여를 하였다.

그러나 상기 연구들은 모두 분석 대상을 조직 또는 개인 수준에 한정하고 있어, 본 연구에서 진행하려고자 하는 국가 단위의 사이버 사건에서의 복합적인 상호작용 구조 분석에 그 차이점이 존재한다. 또한 많은 연구들이 공격의 사전 탐지나 핵심 인물 식별 등 기술 중심의 분석에 집중되어 있는 반면, 탐지 이후의 전략적 대응 체계나 거시적 정책 설계로까지 논의를 확장한 사례는 비교적 드물다.

III. 데이터 수집 및 전처리

3.1. 데이터 수집

본 연구는 국가 간 사이버 갈등의 구조를 분석하기 위해 CISSM Cyber Event Database[15,16](이하 CISSM 데이터셋)를 주요 분석 자료로 활용하였다. 해당 데이터베이스는 미국 메릴랜드대학교 산하 국제안보 및 과학기술정책연구소(Center for International and Security Studies at Maryland, CISSM)에서 구축한 것으로, 2014년 이후 발생한 주요 사이버 사건에 대한 공격 행위자 및 대상, 동기, 공격 유형 등의 정성적 정보를 포함하고 있다.

해당 데이터베이스의 사건 데이터는 Python 기반의 자동 수집 스크립트를 통해 오픈 인터넷 및 다크웹 상의 특정 웹사이트로부터 크롤링되어 확보되었으며, 이후 CISSM의 연구진들의 수작업 검토를 거쳐 사건 정의 기준에 부합하는 항목만이 포함되었다. 이렇게 수집된 데이터는 CSV 형식으로 제공되며, 주요 변수로는 공격 국가(actor_country), 공격자 유형(actor_type), 공격 동기(motive), 사건 유형(event_type), 피해 산업(industry) 및 피해 국가(country) 등이 포함된다. 특히 각 사건은 description 항목에 정성적 설명을 포함하고 있어, 사건 간 유사도 분석 및 분류 작업 등에 활용이 가능하였다.

본 연구에서는 2025년 3월 기준으로 공개된 최신 버전의 데이터셋을 활용하여 연구를 수행하였다.

3.2. 데이터 전처리

원천 데이터는 분석 목적에 적합하도록 추가적인 정제 및 전처리 과정을 요구하였고, 이에 본 연구에서는 다음과 같은 전처리를 수행하였다.

먼저, 원본 데이터에는 동일한 사건이 서로 다른 행으로 중복 기재되어 있는 사례가 다수 확인되었다. 이는 시각화 및 네트워크 분석 시, 하나의 사건이 다수의 간선으로 인식되어 구조 왜곡을 초래할 수 있으므로, 다음과 같은 기준을 설정하여 중복 사건을 병합하고자 하였다

먼저 motive, event_type, actor_country 항목이 동일하고 description 간 유사도(Similarity Ratio)가 0.95 이상일 경우 동일 사건으로 간주하였다. 이러한 기준에 따라 중복 사건을 병합하였으며, 이 과정에서 하나의 사건이 복수의 피격 국가를 포함하는 경우, 병합 이후 각 피격 국가를 기준으로 사건을 분리하였다. 이로써 사건-국가 간 관계 단위를 명확히 하여 네트워크 분석의 정밀도를 확보하였다.

CISSM 데이터셋은 사이버 사건을 다루기에 행위자의 익명성과 오픈소스 한계 등 사건의 특성상 공격자의 신원이나 국적을 명확히 식별하기 어려운 사례가 다수 존재한다. 이는 데이터셋 내에서 'Undetermined'로 표기되어 있었고, 본 연구에서는 이를 결측치로 간주하여 주요 분석 변수인 country 및 actor_country, motive 컬럼에서 Undetermined 값을 포함한 행을 제거하였다. 이 과정은 행위자 노드가 불확실한 경우 네트워크 분석에서 오류를 유발할 가능성을 사전에 차단하고, 구조 해석의 신뢰성을 확보하기 위한 조치였다.

아울러, 동일 국가가 다양한 명칭으로 표기된 경우(예: 'South Korea', 'Korea (Republic of)')를 통일하고, 일부 범주형 변수 값의 정규화 작업도 병행하였다.

마지막으로, 본 연구의 분석 목적과 직접적으로 관련되지 않는 industry_code, source_url 등의 컬럼은 분석에 기여하지 않는다고 판단되어 제외하였다. 이를 통해 전체 데이터 구조를 단순화하고, 후속 모델 설계 및 시각화의 효율성을 제고하였다.

3.3. 선행연구와의 차별점 및 연구설계

CISSM 데이터셋을 활용하여 연구를 진행한 선례들의 경우, 사건 발생의 빈도나 유형 분포에 초점을 맞춘 기술통계적 접근에 집중된 경향이 있었다[17,18]. 이에 반해 본 연구는 사건 간 행위자 관계와 구조적 연결성에 집중하며, 관계에 초점을 둔 새로운 시각으로 사이버 사건에 접근하고자 하였다.

본 연구를 위해 총 3가지의 분석 사양을 설계하였다. 연구 가설로써 2014년부터의 사이버 공격 관련 이벤트들을 기록한 데이터셋으로 국가 대 국가, 국가 대 산업 그리고 국가 대 공격행위 유형의 데이터를 시각화 한 후 현재 국제적인 정세 속에서 국가들이 어떠한 관계가 있는지, 이러한 관계가 사이버전에서도 유사하게 형성이 되는지에 대한 연구 가설을 설정하였다. 이에 따라, 표면적으로 보이는 국제 정세뿐 아니라 사이버전과 같은 표면적으로 드러나지 않은 정세도 종합적으로 분석하여 ① 공격국가와 피해국가의 네트워크 분석을 위해 노드1과 노드2를 각각 공격 국가와 피해국가로 설정하였으며, 링크의 방향은 공격을 한 국가에서 공격대상 국가로 설정하여 공격 방향을 시각적으로 쉽게 파악할 수 있게 하였다. 또한, 공격을 많이 수행한 국가일수록 링크의 굵기를 굵게 시각화하여 한눈에 파악하기 용이하게 설계하였다. ② 공격국가와 피해산업군 분석사양은 노드1과 노드2에 각각 공격 국가와 피해 산업군을 설정하였으며 링크는 위와 동일하게 설정하였다. ③ 공격국가와 공격행위자 유형은 노드1과 2를 각각 공격국가와 공격 행위자 유형으로 설정하였으며, 링크의 방향은 공격 국가에서 공격 행위자 유형으로 화살표가 표현되도록하여 각 공격 국가들이 어떠한 공격행위자 유형의 빈도가 높은지를 분석하는 분석 모델을 설계하였다.

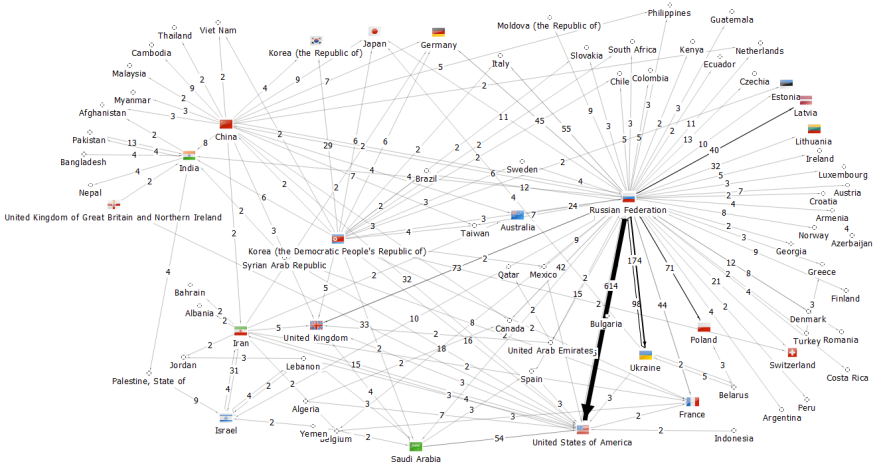
IV. CISSM 데이터셋 기반 네트워크 분석

4.1. 공격 국가와 피해 국가 분석

네트워크 분석 결과, 사이버 공격을 가장 활발하게 수행한 국가로 러시아가 도출되었다. 러시아는 총 60여 개 국가를 대상으로 공격을 시도하였으며, 그 중에서도 특히 미국을 대상으로 한 공격이 614건으로 가장 높은 빈도를 차지하였다. 이어서 우크라이나, 폴란드, 프랑스, 스페인, 독일 등 주로 유럽과 북미의 서방 국가들이 집중적인 피해를 입은 것으로 나타났다.

이러한 공격 패턴은 러시아가 지정학적 갈등이 존재하는 국가들을 전략적으로 목표물로 삼고 있음을 보여준다. 특히 나토(NATO) 회원국이자 정치 및 군사적으로 미국과 협력 관계에 있는 국가들이 주요 타겟으로 확인되었다는 점에서, 러시아의 사이버 공격이 군사 및 안보적으로 밀접하게 연관되어 있음을 유추해볼 수 있다. 또한, 과거부터 이어져온 러시아-우크라이나 분쟁 및 현재 진행 중인 러-우 전쟁으로 인하여 러시아와 우크라이나 두 국가는 특히 많은 사이버 공격을 수행 중인 것을 확인 가능하다. 또한 러시아는 폴란드에게도 눈에 띄는 사이버 공격을 수행한 것을 확인할 수 있다. 폴란드는 지정학적으로 우크라이나에 인접하게 위치해있는 국가이며, 나토(NATO) 회원국이자, 우크라이나에 우호적인 국가이다. 2022년 러-우 전쟁이 발발하였고, 이에따라 수많은 난민들이 발생하였다. 폴란드는 이러한 난민들을 우호적으로 받아들이며 우크라이나를 지원하였고[19], 전쟁 발발 이후 가장 많은 무기를 우크라이나에 지원하며 NATO 연합의 선봉에서 우크라이나를 지속적으로 지원해왔다[20]. 이러한 사실을 비추어봤을 때, 러시아의 폴란드에 대한 사이버 공격이 서방 국가 중에서 특히 높은 빈도를 보인다는 것을 확인하였다.

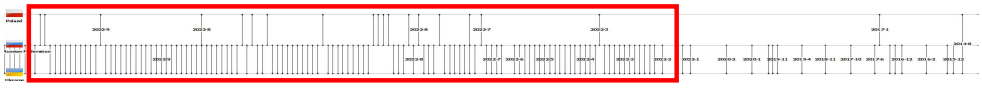
한편 다양한 사이버 공격을 포함하는 CSIS의 보고서의 러시아 공격 사건들을 분석해 본 결과 러시아의 여러 국가들에 대한 공격 내용들은 파악할 수 있었지만, 러시아가 다른 국가들과의 어떠한 관계에 놓여있는지에 대한 지정학적 분석 결과를 도출할 수 없었다. 이에 반해, 본 연구의 시각화 된 네트워크 데이터는 단순 사례나열을 넘어 각 국가의 공격·피해 관계와 그 배경이 되는 국제사회의 정세를 파악하여 보다 심층적인 분석을 진행할 수 있다는 강점을 지닌다.



<Figure 1> 공격국가-피해국가 네트워크

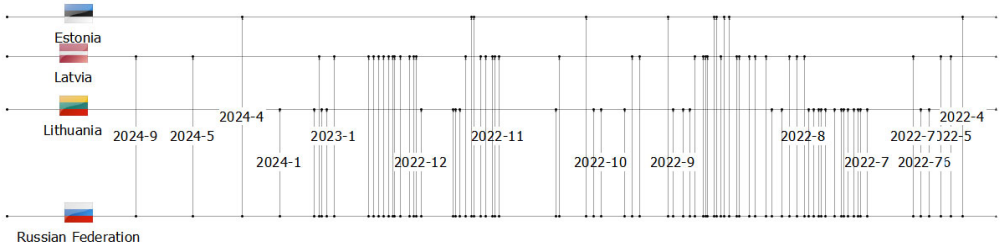
<Figure 2>의 Ukraine-Russia-Poland의 타임라인 네트워크 분석 결과이며 빨간 상자는 2022년 2월 이후의 러시아의 공격 링크를 보여준다. 2022년 2월 러시아와 우크라이나의 전쟁

발발 전까지 소수의 사이버 공격이 진행이 되던 부분에 반해 2월 이후부터 급격하게 증가한 러시아의 우크라이나에 대한 사이버 공격이 확인되었다. 2022년 이전까지의 사이버공격 빈도수는 2022년 한해 발생한 우크라이나에 대한 사이버 공격 빈도수보다 적은수의 공격이 확인되었으며, 2022년 2월 전쟁 시작을 기점으로 우크라이나의 NATO 연합 우방국이자 지원을 많이 한 폴란드에 대한 사이버 공격의 빈도도 급격하게 늘어나는 것을 본 타임라인 네트워크를 통해 확인하였다.



<Figure 2> Ukraine-Russia-Poland 타임라인 네트워크

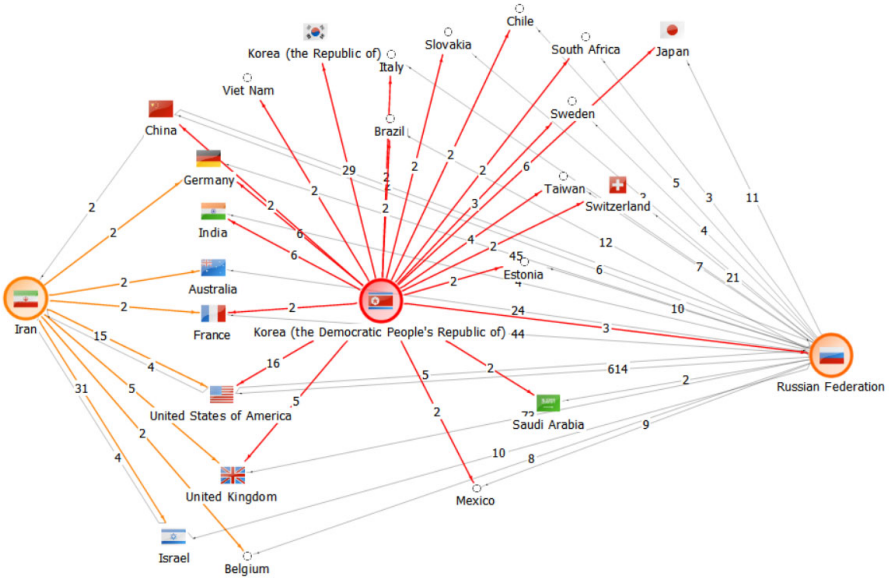
<Figure 3>의 Baltic States-Russia의 타임라인을 보면 2022년 러시아-우크라이나 전쟁 이후 발트 3국에 대한 러시아의 높은 빈도의 사이버 공격이 진행되었다. 발트 3국은 러시아 국경에 위치한 에스토니아, 리투아니아, 라트비아 3개국으로 이루어져 있으며, 2022년 러시아의 우크라이나 침공 직전인 2월 21일 러시아의 도네츠크와 루한스크의 독립국 공식 승인 직후 유럽연합(EU)이 러시아에 대한 강력하고 신속한 제재를 단행해야 한다고 주장하였으며, 러시아에 대한 강경한 대응 입장을 가진 국가들이다[21]. 이러한, 발트 3국에 대하여 러시아는 NATO 회원국이자 우크라니아와 연대하는 리투아니아, 라트비아, 에스토니아에 다수의 사이버 공격을 2022년 이후 수행한 것으로 분석된다.



<Figure 3> Baltic States-Russia 타임라인 네트워크

SNA의 이론적 관점에서 볼 때, 여러 종류의 국가를 높은 빈도로 공격했던 러시아가 공격 국가-피해 국가 네트워크에서 가장 높은 연결 중심성(Degree Centrality)을 지닌 노드로 확인이 되었다. 러시아는 단일국으로는 가장 많은 피해 국가들과 직접적으로 연결되어 있으며, 그 다음 높은 빈도로 국가와 연결되어 있는 국가는 북한이다. 북한의 상위3개의 공격 빈도가 높은 국가를 분석해 보면 1위 대한민국, 2위 미국, 3위 일본으로 구성되어 있으며, 이 3개국은 모두 지정학적으로 밀접하게 연관되어 있는 국가이며, 한미일 안보 협력체제의 핵심 축이다. 이러한 네트워크를 바탕으로 볼때, 북한은 현재 휴전 중인 대한민국에 대해 빈번하게 사이버 공격을 수행하였으며, 이는 대한민국의 국가 안보 및 사회적인 혼란을 야기하기 위한 수단으로 사이버 공격을 활용하였음을 유추해볼 수 있다. 특히나, 북한의 경우 일반 개개인의 인터넷 통신 접속이 불가능한 부분에 있어서 본 사이버 공격은 북한 정부 주도의 사이버 공격임을 시사한다. 또한, 한미일 연합체제인 미국과 일본에 다수의 사이버 공격을 수행한 점에서 한미일 연합체제에 대해 위협으로 간주하고 있음을 보여준다. <Figure 4>의 북한-러시아-이란 공격 네트워크를 분석한 결과 러시아와 이란은 한국을 공격하지 않으면서도 북한이 공격하는 많은 나라들을 공통적으

로 공격하고 있는 점을 확인할 수 있다. 이는 러시아와 이란이 북한과 공통의 목적과 방법을 추구하고 있다는 것을 유추할 수 있고 그럼에도 불구하고 러시아와 이란은 우리나라를 공격하지 않고 있으므로 우리나라가 북한과의 관계 개선을 위한 정책을 추진할 때 먼저 러시아와 이란과 우호적인 관계를 형성한다면 간접적으로 북한과의 관계가 개선될 수 있을 것이라는 대북정책의 시사점을 도출할 수 있었다.



<Figure 4> North Korea-Russia-Ukraine 공격 네트워크

중국은 북한 다음으로 높은 연결 중심성(Degree Centrality)을 보였으며, 중국과 러시아의 공통점을 파악해보면 지정학적으로 근접한 국가를 더 많은 빈도로 공격한 것이 확인되었다. 즉, 러시아와 중국을 중심으로 피해 국가들의 클러스터가 각 형성되었으며, 특히 중국은 같은 아시아계열의 동아시아 및 동남아시아, 러시아는 미국과 우호적인 관계를 맺고 있는 서방국 중심으로 클러스터가 형성된 것을 확인할 수 있었다. 중동 국가 지역에서는 이란이 높은 연결 중심성(Degree centrality)을 보였으며, 이란과 이스라엘 간의 공격 빈도수가 높은 것을 확인하였다. 2000년대 들어 이란과 이스라엘은 직접적인 군사적 충돌은 없었지만, 이란의 핵 개발 폭로, 이라크라는 공통의 적의 몰락이 양국의 정치적인 내러티브로 표현되며 두 국가는 현재 각 국을 위협의 대상으로 인식하게 되었다[22]. 이 같은 현상이 국가 간의 사이버 정세에서도 반영이 되며 두 국가의 빈도수가 높게 확인이 되었다. 폴란드-러시아-우크라이나의 관계는 러시아라는 노드를 중심으로 우크라이나와 폴란드 그리고 러시아가 서로 긴밀하게 연결되어있다는 것을 본 시각화 네트워크를 통해 분석이 가능했으며 여러 국제 정세 선행 연구들을 통해 그 해당 국가들 간의 관계를 명확히 할 수 있었다.

4.2. 공격 국가와 피해 산업 분석

CISSM 데이터셋에는 피해 산업이 미국의 NAICS(North American Industry Classification System)[23]에서 분류한 기준에 따라 기록되어 있으며 NAICS는 북미산업분류시스템으로 미국 연방 통계기관들이 미국 비즈니스 경제와 관련된 통계를 수집, 분석, 공표하기 위해 설정한 분류체계이다. <Table 1>은 본 연구 분석을 위해 시각화한 네트워크 중 유의미

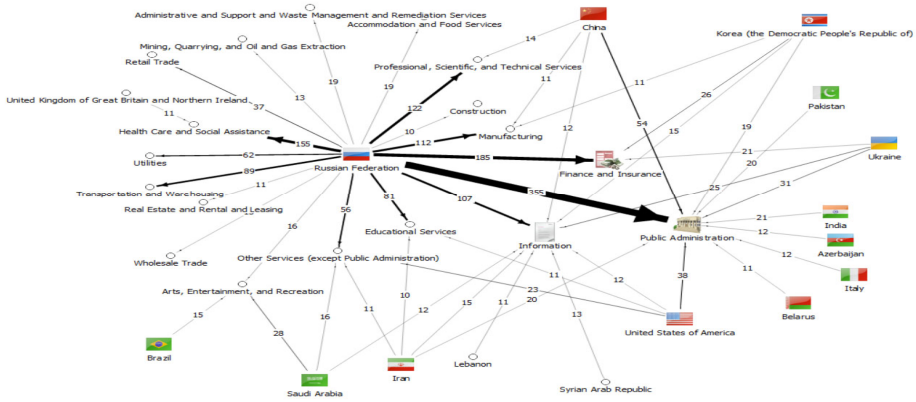
한 분석내용이 도출 된 산업군에 대한 설명을 포함한다.

<Table 1> 피해 산업군 설명 테이블

산업군	요약 설명
Public Administration	정부가 정책을 집행하고 법을 제정 ·판단하며 공공프로그램을 관리하는 기관들로 구성
Finance and Insurance	금융 자산을 생성, 청산, 소유권 이전 등 금융거래를 수행하는 기관들로 구성
Information	정보를 생산·유통, 전송 수단 제공, 데이터 처리를 수행하는 기관들로 구성
Utilities	전력, 천연가스, 증기, 수도, 하수 처리 등의 공공 서비스를 제공하는 기관들로 구성
Transportation and Warehousing	여객 및 화물 운송, 창고 보관, 관광 운송, 운송 지원 활동을 수행하는 기관들로 구성
Health Care and Social Assistance	개인을 위한 보전의료 및 사회복지 서비스를 제공하는 기관들로 구성

데이터 분석 결과, 여러 산업에 사이버 공격을 가장 활발하게 수행한 국가로 4.1.과 같은 러시아가 도출되었다. 러시아 기반의 해커 집단들은 특히 공공 행정 분야(Public Administration)에 가장 많은 약 350건 가량의 공격을 시도했으며 뒤를 이어 금융 및 보험(Finance and Insurance) 분야가 185건, 정보(Information)분야가 107건으로 나타나, 러시아의 사이버 공격이 정부 기관뿐 아니라 경제적 가치와 민감한 정보가 밀집된 산업 분야에서도 광범위하게 이루어지고 있음을 보여준다. 또한, 유틸리티(Utilities), 운송 수단(Transportation and Warehousing), 건강 및 사회보험(Health Care and Social Assistance)분야에서도 유의미한 공격 횟수를 발견할 수 있었다. 이를 통해, 러시아는 국가 운영에 필수적인 사회 기반 분야 및 보험, 금융 등과 같은 필수 서비스 분야에도 다수의 공격을 수행하였다는 점을 확인할 수 있다. 러시아는 특정 분야만이 아니라, 사회, 경, 정치적으로 전략적 중요성을 가진 다수의 산업군을 체계적으로 공격하고 있었다. 해당 분석 결과를 토대로 러시아의 사이버 공격에 많이 노출되었던 폴란드, 우크라이나, 미국이 해당 산업의 피해를 많이 받았다는 점을 추론할 수 있었다.

사회연결망분석 관점에서 볼 때, 러시아는 공격 네트워크에서 중심성(centrality)이 가장 높은 노드(node)로 보여진다. 특히 러시아는 공격의 빈도 및 연결 관계 측면에서 연결 중심성(degree centrality)이 매우 높아 공격 네트워크에서 핵심적인 위치를 차지하고 있으며, 중국과 이란, 북한 등 다른 공격 국가들 역시 상대적으로 연결성이 높은 산업군에 집중적으로 공격을 가하는 형태의 구조가 도출되었다. 가령, 러시아와 연결된 다양한 특수 산업군(소매업, 부동산, 문화 산업, 건설업) 등에는 추가적으로 다른 연결된 국가가 극소수이거나 전혀 없는 구조를 통해 북한, 중국 미국 등은 해당 산업보다는 공공 행정 및 정보, 금융 분야에 다수의 공격을 가하는 것을 확인하였다.



<Figure 5> 공격국가-피해산업군 네트워크

4.3. 공격 국가와 공격행위자 분석

해당 분석은 공격을 수행한 국가들이 어떤 유형의 사이버 공격 행위(Actor type)를 주로 활용했는지를 분석하였다. 행위자 유형은 총 5가지로 구분되며, 테러리즘(Terrorisom)유형, 범죄조직(Criminal)유형, 핵티비스트(Hacktivist) 유형, 국가주도(Nation-state)유형 그리고 개인 동기(Hobbyist)유형으로 이루어져 있다. CISSM 데이터셋을 초기 구축한 연구자들은 5가지의 유형에 대한 세부 설명[15]을 정리하였다. <Table 2>는 5가지 유형을 설명과 함께 정리한 표이다.

<Table 2> 공격행위자 유형 설명 테이블

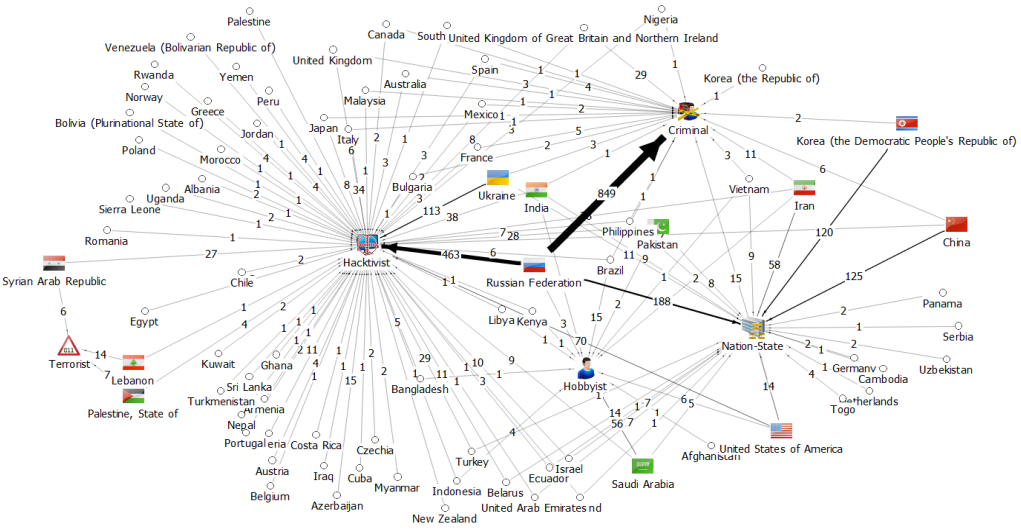
공격행위자 유형	요약 설명
Hacktivist	사회적 또는 정치적으로 행동주의에 의해 동기부여된 개인 또는 집단
Nation-State	정부기관, 군대, 또는 그에 소속된 집단
Terrorism	민간인을 대상으로 공격을 감행하여 정치적 또는 군사적 조건에 영향을 미치려는 비국가 행위자
Criminal	금전적 이득을 목적으로 불법적으로 공격을 시도하는 행위자
Hobbyist	호기심 또는 명예욕에 의해 동기부여된 개인

이 5가지 사이버 공격자 유형에 따라 여러 국가들이 어떤 유형의 행위자였는지를 분석하였다. 본 네트워크에서는 국가가 위 5가지 유형 별로 링크되어 있으며, 국가는 해당 유형 타입의 국가이다. 따라서, 러시아의 경우 범죄조직(Criminal)에 849건의 링크합이 연결되어 있으며, 이는 러시아가 범죄조직(Criminal)유형의 사이버 공격을 849회 수행한 것으로 분석된다.

네트워크 분석 결과, 핵티비스트(Hacktivist) 유형은 전체 국가들 중 가장 높은 유형을 보이며, 다양한 국가들에서 광범위하게 보이는 특징이 확인되었다. 특히, 미국, 영국, 캐나다, 호주와 같은 민주주의 제체의 국가들에서 핵티비스트 성향의 사이버 공격 유형이 다수 존재하는 것이 확인되었으며, 이러한 현상은 민주주의 체제 국가들에서 정치적 또는 사회적으로 어떠한 이슈들에 대해서 항의와 반대 의견을 표출하는 수단으로 사이버 공격이 수행된다고 분석할 수 있다.

반면, 범죄조직(Criminal) 또는 국가주도형(Nation-state)의 경우 러시아, 중국, 이란과 같은 국가들에서 높은 빈도를 나타내었다. 이러한 국가들의 경우 사이버 공격을 일종의 정치적 목

적, 정보 수집, 금융 탈취 등과 같은 국가 시설 마비 및 사회 혼란 등과 같은 목적을 가지고 사이버 공격을 다수 수행한 것으로 보여진다.



<Figure 6> 공격 국가-공격 행위자 유형 네트워크

V. 결론

5.1. 결론

본 연구에서는 CISSM 데이터셋을 활용하여, 국가 간 사이버 공격 관계를 네트워크 시각화하고 구조를 분석하였다. 그 결과, 러시아, 중국, 북한 등의 국가들은 공격 네트워크 중심성이 매우 높았으며, 이를 통해 사이버전에서 핵심적인 행위자 역할을 하는 것을 확인하였다. 이 국가들은 지정학적으로 대립관계에 있는 다수의 국가들을 공격 대상으로 삼는 모습을 보였으며, 사이버상에서의 공격 빈도가 실제 해당 국가들의 국제정세와 상호 연관되어있는 모습을 보였다.

러시아의 경우 거시적인 네트워크 구조에서 NATO 회원국 및 미국 중심의 서방국을 공격하는 양상을 보였으며, 중국과 북한은 각각 아시아권 지역과 한미일 안보 협력이 구축된 국가에 대하여 반복적인 사이버 공격을 가하는 특징을 보였다. 이러한 분석 결과는 국제적으로 발생하는 사이버 갈등이 국가 간 세력을 유지하고 정치 및 외교적으로 전략적인 모습을 보인다는 것을 의미한다. 따라서, 사이버전은 물리적 충돌 없이 실질적으로 국가들에 영향을 미치는 비전투 전략 수단으로 활용되고 있으며, SNA 기반 네트워크 모델은 이러한 국제 사이버전 정세를 분석하는 유용한 틀로서 활용될 수 있다.

미시적 분석을 통해서는 개별 국가 간의 사이버 공격 사건을 분석하여, 러시아 우크라이나의 전쟁이 본격화된 2022년을 기점으로 우크라이나의 우방국이었던 폴란드에 대한 공격 빈도가 급증하였으며, 이는 실제로 지정학적 충돌이 러시아-우크라이나 전쟁 뿐만 아니라 사이버 영역으로 확장되었음을 보여준다. 또한, 북한의 한미일 3국에 대한 집중 공격을 통해 정치적 목적이 뚜렷한 공격임을 확인할 수 있다. 대북정책의 관점에서 북한과의 관계 개선을 위해서는 러시아와 이란과 우호적인 관계를 맺는 것이 좋을 것이라는 시사점도 도출할 수 있었다.

피해산업군 분석에서 러시아를 중심으로 공공행정, 금융, 정보 등 정치·경제 핵심 분야에 대한 공격이 집중되었으며, 이는 국가 기능 마비 및 사회 혼란을 목적으로 한 전략적인 공격 양상

을 시사한다. 또한 공격 행위자 유형에 따른 분석 결과, 민주주의 체제의 국가들은 핵티비스트(Hacktivist)유형이 다수를 이루었고, 러시아, 중국, 북한, 이란 등은 국가주도형(Nation-state) 및 범죄조직(Criminal)유형이 주 유형을 차지하였다.

5.2. 연구의 한계 및 문제점

본 연구에서 다루는 주제인 사이버 공격은 타 국가나 기업을 대상으로 수행되는 경우가 많기에 상당히 민감한 정보로 분류 가능하다. 또한 피해 세력은 사이버 공격을 당했다는 피해 사실을 부인 혹은 묵인하려 하는 경우가 많고[24], 이에 사이버 공격에서는 실제 공격 국가나 기타 사건 정보들이 드러나지 않는 경우가 다수 존재한다. CISSM 데이터셋에도 Undetermined로 표기된 값들이 다수 존재하였으며 본 연구에서는 이러한 값들을 결측치로 판단 후 제거하여 분석을 수행하였다. 하지만 이러한 전처리 방식은 현실과 연구 결과 사이에 괴리를 발생시킬 수 있다는 한계를 내포한다.

또한, 본 연구에서는 단일 데이터셋인 CISSM 데이터에 대부분 의존하여 분석을 진행하였다. 이는, 데이터의 일관적인 측면에서는 장점이 존재하나, 데이터 자체에 존재하는 한계점 역시 연구 전체에 반영이 될 수 있다. 앞서 언급한 Undetermined 표기와 같은 불완전한 정보의 비중이 다소 있는 상황에서 교차 검증이 가능한 별도의 데이터를 통한 추가적인 분석이 진행되지 않았다는 점에서 한계가 존재한다.

마지막으로, 본 연구는 사회연결망분석(SNA)을 중심으로 국가 간 사이버 공격의 관계성을 시각화하고 구조를 정량적으로 분석하였다. 이 과정에서, 다양한 국가 관 관계를 분석한 선행연구들을 참고하여 본 연구의 분석 결과에 신빙성을 제고하고자 하였으나 급변하는 국제정세를 충분히 담아내지 못했다.

5.3. 후속 연구 제언

본 연구에서 활용한 CISSM 데이터는 공개된 정보를 기반으로 사이버 공격 사건들을 수집하였으며, 이에 따라 기본적인 신뢰성을 갖추고 있다. 하지만, 공개된 정보만을 활용하였기 때문에 공격 주체 또는 피해 주체가 명확하지 않은 데이터들이 다소 존재하였다. 이러한 한계를 보완하기 위해 후속연구에서 공격 주체 또는 피해 주체가 명확하게 식별되는 사이버 공격 로그 데이터에 대한 수집을 확대하고, 민간 사이버 보안 기업에서 수집되는 데이터가 존재한다면 이를 활용하여 보다 더 실증적이고 상세한 분석이 가능해질 것으로 본다.

또한, 해당 데이터셋에는 본 연구에서 활용한 피해국가, 공격 국가, 피해산업, 공격 행위자 유형 외에도 공격 동기, 사이버 공격 수행 집단 등 다양한 속성 정보다 추가적으로 존재한다. 후속연구에서는 이러한 속정 정보들을 보다 더 정밀하게 조합한다면, 본 연구에서 발견하지 못한 국가 간 사이버 공격의 숨은 관계 구조나 전략적 특성을 추가적으로 도출할 수 있을 것으로 기대된다.

참고문헌 (References)

[1] Bachmann SD, Gunneriusson H. 2015. Hybrid wars: The 21st-Century's new threats to global peace and security. Scientia Militaria, South African Journal of Military Studies, 43(1), 77-98. https://doi.org/10.5787/43-1-1110

[2] Perdana A, Aminanto ME, Anggorojati B. 2024. Hack, heist, and havoc: The Lazarus Group's triple threat to global cybersecurity. Journal of Information Technology Teaching Cases. https://doi.org/10.1177/20438869241303941

[3] Lee Y, Jeong K. 2022. Russian vs Ukraine cyber war lessons and implications. Journal of Defense Policy Studies, 38(3), 37-79. https://doi.org/10.22883/jdps.2022.38.3.002

[4] Song TE. 2022. The role of cyber warfare in a full-fledged contemporary war: The case of 2022 Russia-Ukraine War. Journal of National Defense Research [국방연구], 65(3), 215-236.

[5] Robinson M, Jones K, Janicke H. 2015. Cyber warfare: Issues and challenges. Computers & Security, 49, 70-94. https://doi.org/10.1016/j.cose.2014.11.007

[6] Simons G, Danyk Y, Maliarchuk T. 2020. Hybrid war and cyber-attacks: Creating legal and operational dilemmas. Global Change, Peace & Security, 32(3), 337-342. https://doi.org/10.1080/14781158.2020.1732899

[7] Wasserman S, Faust K. 1994. Social Network Analysis: Methods and Applications, pp. 1-825. Cambridge University Press. https://doi.org/10.1017/CBO9780511815478

[8] Anastopoulos V. 2022. Using social network analysis for cyber threat intelligence. Proceedings of the NATO CCDCOE, Tallinn, Estonia.

[9] Sarkar S, Almukaynizi M, Shakarian J, et al. 2019. Predicting enterprise cyber incidents using social network analysis on dark web hacker forums.The Cyber Defense Review, Special Edition, 87-102. https://www.jstor.org/stable/26846122.

[10] Moon BH, Kwahk KY. 2022. A case study on the investigation of cyber gambling criminal organization using social network analysis. Information Systems Review, 26(3), 1-22. https://doi.org/10.14329/isr.2024.26.3.001

[11] Kim HC, Yoon J W. 202. A case of cyber financial crime investigation through social network analysis (2-mode concepts). Journal of Digital Forensics, 14(4), 449-465. http://doi.org/10.22798/KDFS.2020.14.4.449

[12] Kacziba P. 2021. The network analysis of international relations: Overview of an emergent methodology. Journal of International Studies, 14(3), 155-171. https://doi.org/10.14254/2071-8330.2021/14-3/10

[13] CSIS (Center for Strategic and International Studies). 2025. Significant cyber incidents. CSIS, Washington DC, USA. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents accessed on 2025. 6. 17.

[14] Kim JO. 2019. A Study on the Application of Social Network Analysis Principles to Criminal Investigation. Journal of Digital Forensics, 13(2), 87-107. http://doi.org/10.22798/kdfs.2019.13.2.87

[15] Harry C, Gallagher N, Samuelsen L. 2023. Cyber Events Database Codebook. Center for International and Security Studies at Maryland. Available at: https://cissm.umd.edu/sites/default/files/2023-03/Cyber%20Events%20Database%20Codebook.pdf accessed on 2025. 6. 17.

[16] Harry C, Gallagher N. 2018. Classifying cyber events: A proposed taxonomy. Journal of Information Warfare, 17(3), 17-31.

[17] Huygen L. 2024. Cyber shocks: Evaluating the immediate and lasting capital market implications of disruptive and exploitive cyber events – An event study. Master's thesis. Tilburg University, Tilburg, Netherland.

[18] Pseftelis T, Chondrokoukis G. 2025. Cyber attack motivations: Connecting actors with event types. Preprints:202505.1003.v1.

https://doi.org/10.20944/preprints202505.1003.v1

[19] Levi N. 2022. The Role of Poland in the Ukrainian War [러시아-우크라이나 전쟁에 대한 폴란드의 대응]. Korea Institute for International Economic Policy [대외경제정책연구원], Sejong, Korea.

[20] EMERiCs Central-Eastern Europe [중동부유럽]. 2023. [Issue Trend] Central and Eastern European countries provide old weapons to Ukraine while introducing new U.S.-made arms [중동부유럽 각국, 우크라이나에 구형 무기 지원하고 미국산 신무기 도입]. Available at: https://www.kiep.go.kr/aif/issueDetail.es?brdctsNo=353783&mid=a30200000000&systemcode=07 accessed on 2025. 6. 10.

[21] Sytas A. 2022. Baltics call for swift EU sanctions on Russia after it recognizes Ukrainian breakaway republics. Reuters. Available at: https://www.reuters.com/world/europe/baltics-call-swift-eu-sanctions-russia-after-it-recognizes-ukrainian-breakaway-2022-02-21/ accessed on 2025. 6. 10.

[22] Kim E. 2022. Political narratives of Israel-Iran relationships. Middle East Studies [중동연구], 41(2), 1-26.

[23] Executive Office of the President of the United States. 2022. North American Industry Classification System (NAICS) Manual. Available at: https://www.census.gov/naics/reference_files_tools/2022_NAICS_Manual.pdf accessed on 2025. 6. 10.

[24] Bair J, Bellovin SM, Manley A. 2018. That was close! Reward reporting of cybersecurity "near misses". Colorado Technology Law Journal, 16(2), 327-364.