한국컴퓨터정보학회 하계학술대회 논문집 제28권 제2호 (2020. 7)

북한의 사이버조직 관련 정보 연구 (조직 현황 및 주요 공격사례 중심으로)

김진광O
O합동군사대학교
e-mail: whiteseas@naver.comO

North Korea's cyber organization-related information research (Based on organization status and major attack cases)

Jin Gwang KimO
OJoint Forces Military University

● 요 약 ●

우리나라에 대한 사이버 공격의 배후로 추정되는 북한의 사이버조직에 우리는 얼마나 알고 있을까? 사이버 공간의 특성상 공격 흔적이 남지 않기에 언론사들은 북한의 사이버조직과 관련하여 일관된 정보를 거의 제공하지 못하고 있다. 따라서 갈수록 진화하는 북한의 사이버 공격에 효과적으로 대비하기 위해 본 논문에서는 비록 인터넷에 공개된 자료(논문, 기사 등)라 할지라도 이를 통해서 북한 사이버조직 현황 및 주요 공격사례를 중심으로 관련 정보를 살펴보고자 한다.

키워드: 북한(North Korea), 사이버조직(Cyber Organization), 사이버 공격(Cyber Attack)

I. Introduction

과학기술의 발전에 따른 문명 혜택은 우리의 삶을 풍족하게 해주었지만 반대로 지구온난화, 미세먼지, 신종 질병 등의 부작용 또한 초래하였다. 컴퓨터 등의 정보통신기술을 이용한 사이버 공격(또는 침해)도 이러한 부작용 중의 하나이며 그 대표적인 사례가 보이스 피싱이다. 심지어 2013년 K방송사의 예능 프로그램에서는 보이스 피싱을 소재로 한 '황해'라는 코너가 크게 화제가 되었는데 보이스 피싱 다양한 유형을 소개를 통해 많은 사람들이 유사한 사고를 예방할 수 있었다고 한다. 이처럼 과학기술의 발전은 양날의 검과 같아서 분명 이점이 있지만 이를 일부 악용한 사람들에 의해 다양한 피해가 발생하고 있다.

그 중 특히, 사이버 공격은 상대적으로 물리 노동력보다는 컴퓨터, 악성 프로그램 등의 도구를 이용하기 때문에 우리가 흔히 말하는 가성비(가격 대 성능비)가 좋아 좀처럼 줄어들지 않고 다양한 형태로 진화하고 있다. 또한 <그림 1>과 같이 2011년 농협 전산망 사이버 테러, 2016년 군 기관 대상 해킹 등을 통해 알 수 있듯이 공격대상은 개인뿐만 아니라 기업, 국가까지 확대되어가고 있어 이에 따른 대책이 필요하다. [1]

시기	내용
2009.7.7	- 디도스 공격 - 청와대 등 정부 기관 대상
2011.3.4	- 디도스 공격 - 정부기관, 금융기관, 인터넷기업
2011.4.12	- 농협 전산망 해킹
2013.3.20	- 방송, 금융 기관 전산장비 파괴
2013.6.25	- 디도스 공격 - 정부기관과언론사 대상
2014.12.9	- 한수원 원전 해킹
2014.12.24	- 소니픽쳐스사 해킹
2015.10	- 서울 지하철 1-4호선 서버 해킹
2015.10.20	- 청와대, 국회, 통일부 대상 해킹
2016.1	- 청와대 사칭 악성코드 유포

Fig. 1. North Korea Cyber Attack Casea(2009~2016)

하지만 사이버 공간의 특성상 그 흔적을 찾기 쉽지 않고 예방 역시 쉽지 않기에 우리는 공격세력의 현황조차도 제대로 파악하기 어려운 실정이다. 실제로 우리나라에 대한 사이버 공격의 배후로 추정되는 북한 사이버조직에 대해서도 언론사마다 제시하는 현황이 달라 일관되고 정확한 정보를 제공하지 못하고 있다.

따라서 비록 인터넷에 공개된 자료(논문, 기사 등)라 할지라도 효율적인 사이버 공격 대응을 위해서는 북한의 사이버조직 현황에 대해서 파악할 필요가 있으며 조직 현황 및 주요 공격사례를 중심으로 자료

조사와 사회연결망 분석 방법을 통해 관련 정보를 살펴보고자 한다.

II. Preliminaries

2.1. 사회연결망 분석

사회연결망 분석은 연결망 형태의 특징을 도출하고 관계성으로 특성을 설명하거나 체계를 구성하는 단위의 행위를 설명하는 것이다. 따라서 사회연결망 분석은 복잡한 관계를 보다 더 쉽게 설명해준다. 그 분석의 대상은 사회나 조직 간 관계 또는 조직 내부의 관계일 수도 있고, 개인 이웃 간 연결일 수 있다. 더불어 최근 사회연결망 분석의 범위는 인간관계뿐만 아니라 단어의 관계로까지 확장되고 있으며 컴퓨터 계산 속도와 시각화 방법이 발전함에 따라 이전까지 고려하기 어려웠던 관계와 그들 간 상호작용을 이해하고 분석할 수 있게 되었다.

한편, 사회연결망 분석을 생각하면 일반적으로 떠올리는 것이 점과 선으로 된 연결망 그래프인데 이는 분석적 의미를 표현할 뿐만 아니라, 시각화된 패턴을 통해 더 많은 해석의 가능성을 열어준다. 연결망 그래프를 잘 표현하면 복잡하게 얽혀있는 연결망 구조를 한눈에 파악하여 씨알과 쏠림, 소외와 고립 부분 등을 쉽게 확인할 수 있다. [2]

2.2. 북한의 사이버 공격 일반사항

국가정보원은 북한이 2018년 4월 판문점선언 및 9월 평양 정상회담의 남·북간 평화 분위기 속에서도 우리나라에 대한 사이버 공격(또는 해킹) 시도가 있었다는 의혹을 제기한 바 있다. 이처럼 북한의 사이버 공격은 왜 끊이지 않을까? 다양한 이유가 있겠지만 북한 김책공업대학에서 컴퓨터를 전공했던 김흥광 NK지식인연대 대표는 '섣부른 물리적 공격은 국가 간의 전쟁으로 발전할 가능성이 있어 어렵다고 보고 자신의 피해를 최소화하면서 최대한 이득을 취할 수 있는 것이 바로 사이버 공격'이라고 언급한 바 있다. [3]

실제로 북한의 김정은 위원장은 2013년 '사이버전이 핵·미사일과 함께 군대의 무자비한 타격능력을 담보하는 만능의 보검'이라고 말한 바 있으며, 이를 증명하듯 러시아의 보안업체(카스퍼스키)가 제공한 북한 사이버조직 중 하나로 추청되는 라자루스(Lazarus)의 악성 프로그램도 <그림 2>와 같이 지속 증가하며 활발한 활동을 하고 있다. [4]

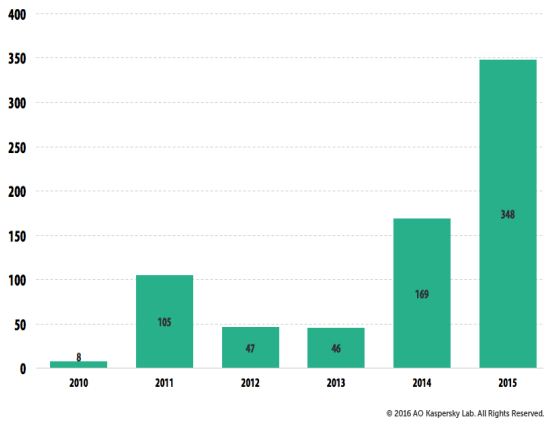

Fig. 2. Lazarus Malware Status(2010~2015)

이에 따라 우리나라는 정보해킹과 적대세력 및 가상 적국에서 들어오는 사이버 공격에 대한 대응조직으로 2010년 1월 1일 사이버사령부(現 사이버작전사령부, 2019년 2월 26일 명칭 변경)를 설립하여 운영 중이다. 하지만 2013년 11월 국회 국정감사에서 당시 사이버사령부는 북한의 해커 등 사이버전 관련 인력이 3,000여 명으로 우리 군(400여 명)의 7배 수준이라고 발표한 적이 있으며, 2018년 국방백서 상에는 2배가량 늘어난 6,800여 명으로 명시되어 있어 북한의 사이버 공격에 대한 우리의 현실은 생각보다 어려운 상황일지도 모른다.

III. North Korea Cyber Organization Information

분석 대상자료는 인터넷을 통해 주요 언론사와 정부기관 공개자료 및 논문, 웹사이트(38 north 등)에서 총 761건(언론사 뉴스 기사 691건, 논문 5건, 기타 검색자료 65건)을 수집하였고 이를 기반으로 북한 사이버조직 관련 정보를 정리하였다.

3.1. 사회연결망 분석 결과

시각화는 사회연결망 도구인 Netminer(4.4.1.c)를 이용하였으며, 수집한 자료에서 '북한, 사이버' 관련 키워드가 등장하는 관계를 2모드 네트워크로 작성한 후 중심성 분석방법 중 페이지랭크(PageRank) 중심성로 다음의 <그림 3>과 같이 시각화하였다. [5]

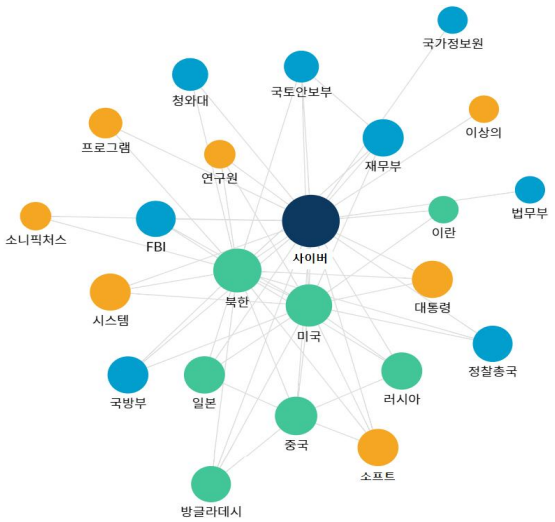

Fig. 3. Network of PageRank Centrality (North Korea-Cyber detail)

<그림 3>을 간략하게 살펴보면 우선 남색 원은 중심 키워드인 '사이버'를 나타내고 녹색 원은 장소, 청색 원은 기관, 황색 원은 기타 키워드를 의미한다. 이를 통해서 북한과 관련된 사이버 공격의 주요 대상국가는 미국, 일본, 방글라데시까지 다양하며 관련기관에는 북한 정찰총국과 미국 FBI, 우리나라 청와대 등 많은 국가 기관이 연관되어 있음을 알 수 있다.

또한, 다음의 <표 1>에서 '북한-사이버' 관계를 페이지랭크 중심성 연결 정도 수치를 통해서 보면 국가 중에서는 미국이 0.67로 북한을

제외하고 제일 높으며 기관 중에는 우리나라 국방부가 0.20으로 가장 높아 북한 사이버 공격 대상의 국가 및 기관임을 확인할 수 있다.

Table 1. PageRank of 'North Korea-Cyber'

키워드	연결 정도	키워드	연결 정도
사이버	0.95	정찰총국	0.17
북한	0.82	FBI	0.17
미국	**0.67**	청와대	0.14
중국	0.33	국토안보부	0.13
일본	0.22	프로그램	0.12
러시아	0.21	소니픽처스	0.10
미사일	0.21	연구원	0.10
국방부	**0.20**	이상의	0.9
시스템	0.20	법무부	0.9
대통령	0.18	이란	0.9
재무부	0.18	국가정보원	0.9
방글라데시	0.17	-	

3.2. 사이버조직 연혁 및 체계

북한은 1986년 '군 지휘자동화대학'(평양 미림동 위치하여 '미림대학'으로 불리하며 2000년 현 '김일 군사대학'으로 명칭 변경)을 설립하여 100여 명의 컴퓨터 전문요원 양성을 시초로 사이버 부대 준비를 시작하였다. 그리고 1991년 걸프전이 미국 주도 하 연합국 승리로 끝난 후 현대전에서 전자전의 중요성을 인식하고 '총참모부' 직속으로 '지휘자동화국'과 각 군단에는 '전자전 연구소'를 신설하였다.

1995년에는 100여 명 수준의 '중앙당 35호실 기초자료조사실'을 설비하여 중앙당 부서에 필요한 다른 나라 국가기관, 단체, 개인에 관한 기밀자료를 인터넷을 통해 수집하였다. 1998년에는 사이버부대(121소) 창설 및 1999년에는 200여명 수준의 사이버심리전부대인 적공국 204소를 설립하여 국군과 남한의 청소년, 일반인을 대상으로 사이버 심리전을 펼치고 있다. 또한, 2004년 중반부터 중국 단둥을 거점으로 사이버 부대를 운영하기 시작하였고, 2010년 인민부력부 정찰국, 노동당 작전부, 중앙당 35호실 등을 통합하여 정찰총국을 창설 및 사이버부대(121소)를 병력(500명→3,000명) 증강과 더불어 사이버지도국(121국)으로 개편하였다. 2012년에는 전략사이버사령부 창설하여 병력을 약 6,000명 규모로 확대하였다.

그리고 탈북자 김흥광 NK지식인연대 대표(2003년 탈북, 김책공업대학 컴퓨터공학 박사) 말에 따르면 2017년에 사이버전략사령부 창설이 추정되며 이는 사이버지도국(121국)과 사이버심리전부대(204소), 110연구소를 통합한 것을 예상된다. 현재까지 알아본 연혁에 대해서 간략히 정리하면 다음 <그림 4>와 같다.

- 1986년 : 지휘자동화 대학(현 김일 군사대학)에서 100여명 컴퓨터 전문요원 양성이 시초
- 1991년 : 총참모부 직속 지휘자동화국, 각 군단 전자전연구소 창설
- 1995년 : 중앙당 35호실 기초자료조사실 창설
- 1998년 : 사이버부대(121소) 창설
- 1999년 : 사이버심리전부대 창설(적 공국 204소 조직)
- 2004년 : 사이버부대 거점 운영(거점 : 중국 단둥)
- 2010년 : 정찰총국 창설(인민무력부 정찰국 + 노동당 작전부 + 중앙당 35호실)
- 2010년 : 사이버부대(121소) → 사이버지도국(121국)으로 개편(병력 500명 → 3000명으로 증강)
- 2012년 : 전략사이버사령부 창설
- 2017년 : 사이버전략사령부 창설 추정(121국 + 204소 + 110연구소 통합 추정)

Fig. 4. North Korea Cyber Organization History

다음으로 사이버조직 체계에 대해 알아보면 연혁을 통해 쉽게 알 수 있듯이 수년간 다양한 임무를 수행하는 조직이 창설 및 통합되었다. 특히, 2010년 이후 조직의 변화가 잦았는데 이는 그만큼 사이버조직의 확대에 많은 노력을 기울인 것으로 보인다.

현재까지 기사 및 논문 등의 연구자료를 통해 확인한 결과 전반적으로 유사하지만 조금씩 제시하는 조직체계가 달랐고 인터넷에서 검색되는 약 15여 개의 조직도를 확인하고 기존 연구 등을 통해 분석결과 일반적으로 <그림 5>과 같이 구성되어 있음을 알 수 있었다. [6]

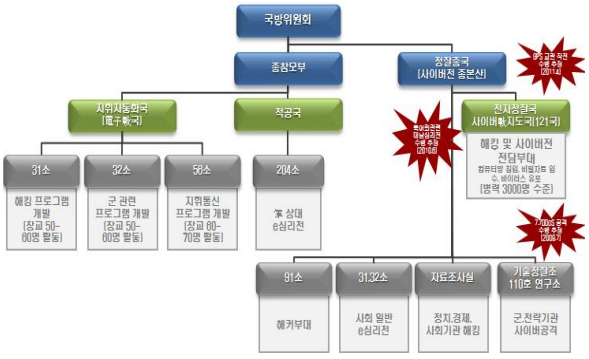

Fig. 5. North Korea Cyber Organization structure

3.3. 사이버 공격 유형 및 방법

2009년부터 지금까지 지속되고 있는 북한의 사이버 공격을 유형을 전반적으로 분석하면 크게 다음 다섯 가지로 볼 수 있다. 우선은 소니픽처스 해킹에서 알 수 있듯이 '북한의 소위 최고존엄을 지킨다'이며, 두 번째는 사이버전을 대비하는 '군사적 목적'이 있다. 세 번째는 은행 및 금융권 등을 대상으로하는 '외화벌이 목적'이며 네 번째는 댓글선동 등을 통한 '대남공작 목적', 마지막 다섯 번째는 한국수자원공사 원전 해킹 등의 '최신국방 및 자연과학기술 탈취 목적'으로 구분할 수 있다.

주요 공격방법은 이메일을 통한 악성 프로그램 유포가 많으며 북한은 핵실험으로 인한 경제 제재 이후 외화벌이 목적이 두드러지고 있는데 대표사례로는 2017년 컴퓨터 파일을 암호화한 후 복호화 대가로 금전을 요구했던 '워너크라이(Wanna Cry)'가 있다. 특히, 워너크라이의 배후로 다수의 보안업체들이 '라자루스'를 추정하고 있는데 그 이유는 워너크라이에는 과거 라자루스가 사용한 악성 프로그램과 일부 코드가 공유되었기 때문이다.

3.4. 라자루스 관련 정보

라자루스(또는 HIDDEN COBRA) 그룹은 북한이 배후일 것으로 추정되는 기술력과 조직력을 갖춘 사이버(또는 해킹) 위협그룹 중 하나이다. 라자루스 그룹의 대표적인 하위조직에는 블루노로프(Bluenoroff)와 안다리엘(Andariel) 있는 것으로 밝혀졌으며 각 공격 대상이나 목적에 있어서는 다소 차이가 있는 것으로 보인다. 특히 블루노로프는 우리나라를 일부 포함하여 주로 글로벌 금융회사를 대상으로 하고, 안다리엘의 경우는 한국의 소프트웨어 취약점을 이용하여 국내 기업 및 정부기관을 대상으로 하는 공격에 집중하고 있다.

2016년에는 스카크러프트(ScarCruft, Reaper라고도 불림)라는 해킹그룹이 식별되었으며 주로 사이버 스파이 행위와 파괴적인 사이버 공격을 하고 최근 대한민국 대선 때 주요 기관들을 겨냥한 공격들도 발견된 바 있다. 결론적으로 라자루스 그룹 현황 및 관련 정보를 정리하면 다음의 <그림 6>과 같다.

위협 그룹	라자루스	블루노로프	안다리엘	스카크러프트
공격대상	국내 정부, 금융, 방송 기관 등	글로벌 및 국내 금융회사	국내 금융회사, 국방부, 방위산업체	금융기관, 정부기관
목적	사회혼란	경제적 이익	기밀정보 탈취 및 경제적 이익	기밀정보 탈취
주요 활동시기	~ 최근	2015 ~	2014 ~	2016 ~
주요사고	- 7.7. 3.4 DDoS 공격 - 3.20 사이버테러 - 미국 소니 픽처스 엔터테인먼트 - 사 개인정보 유출 - WannaCry 랜섬웨어	- 방글라데시 중앙은행 SWIFT 부정거래 - 폴란드 금융감독원 홈페이지 침해 및 워터링홀 공격 - 금융회사 망분리 환경 공격	- 대기업 자료유출 - 국방망 침해 - VAN사 ATM 악성코드 감염 - 금융회사 노조 악성 코드 유포	- 2016 Erebus 및 Daybreak 작전 (플래시 플레이어 취약점 공격)

Fig. 6. Lazarus Group status

IV. Conclusions

주요 이슈 때마다 SNS를 통해 빠르게 확산되는 '가짜뉴스'가 종종 부정적인 여론을 형성하여 사회적 혼란을 일으키고 있다. 또한, 신속한 정보전달에만 집중하여 남의 기사를 복제하듯이 전파하는 일부 언론사들 때문에 뉴스의 신뢰도 역시 하락하고 있다. 이와 마찬가지로 북한의 사이버조직에 대해서도 검증 및 일관성 없는 기사들이 많아 정확한 정보전달을 위해 본 논문에서는 인터넷에 공개된 자료를 기반으로 북한의 사이버조직 관련 기초적인 수준의 정보를 확인해보았다. 따라서 향후 연구에서는 분석 자료의 확대를 통해 북한 사이버조직에 관한 상세한 연구가 필요하다고 생각한다.

앞으로 북한의 사이버 공격은 더욱 교묘하고 다양하게 우리에게 큰 피해를 줄 것이므로 우리는 사이버 공간에서 전쟁을 대비하는 자세로 강력한 대책을 세워야 할 것이다. 더불어 북한 사이버조직 관련 정보에 대한 지속적인 수집은 물론 2019년부터 실시하는 초등학교 코딩교육처럼 국가적 차원에서 사이버 인재 양성에 지속 노력한다면 우리도 머지않아 튼튼한 사이버 전력 건설을 할 수 있다고 생각한다.

REFERENCES

[1] Hacker Power North Korea.. What Are the Counter-measures?, *http://www.digitaltoday.co.kr*

[2] KIM. YH and KIM. YJ, "Social Network Analysis. 4th edition." Pakyoungsa, pp. 5-130. 2016.

[3] North Korean Cyber Forces and Highest dignity, *https://www.rfa.org/korean/weekly_program*

[4] What is known about the Lazarus Group: Sony hack, military espionage, attacks on Korean banks and other crimes, *https://www.kaspersky.com*

[5] Cyram. NetMiner. 4.4. Seoul: Cyram Inc. 2018.

[6] Korea University Industry-Academy Cooperation Group, Cyber threat scenario development and counter measure study, pp. 55-60. 2014.