퍼지추론을 이용한 정량적 사이버 위협 수준 평가방안 연구

이 광 호*, 김 종 화**, 김 지 원**, 윤 석 준***, 김 완 주***, 정 찬 기****

요 약

이 연구에서는 사이버 위협을 평가할 시 복합적인 요소들을 고려한 위협 수준의 정량적 평가방안을 제안하였다. 제안된 평가방안은 공격방법과 행위자, 위협유형에 따른 강도, 근접성의 4가지 사이버 위협 요소를 기반으로 퍼지이론을 사용하여 사이버 위협 수준을 정량화하였다. 본 연구를 통해 제시된 사이버 위협 수준 평가는 언어로 표현된 위협 정보를 정량화된 데이터로 제시해 조직이 위협의 수준을 정확하게 평가하고 판단할 수 있다.

A Study on the Quantitative Threat-Level Assessment Measure Using Fuzzy Inference

Kwang-ho, Lee*, Jong-Hwa, Kim**, Jee-won, Kim**, Seok Jun, Yun***, Wanju, Kim***, Chan-gi, Jung****

ABSTRACT

In this study, for evaluating the cyber threat, we presented a quantitative assessment measures of the threat-level with multiple factors. The model presented in the study is a compound model with the 4 factors; the attack method, the actor, the strength according to the type of the threat, and the proximity to the target. And the threat-level can be quantitatively evaluated with the Fuzzy Inference. The model will take the information in natural language and present the threat-level with quantified data. Therefore an organization can accurately evaluate the cyber threat-level and take it into account for judging threat.

Key words : Fuzzy Inference, Cyber Threat, Quantitative Threat-Level Model

접수일(2018년 5월 6일), 수정일(1차: 2018년 6월 26일, 게재확정일(2018년 6월 29일)

* 아주대학교 NCW학과(주저자)
** 아주대학교 NCW학과
*** 국방부 육군
**** 아주대학교 NCW학과(교신저자)

1. 서 론

사이버 위협은 악성코드, 해킹메일, 취약점을 이용한 해킹 외에도 최근에는 가상화폐 채굴형 악성코드가 유포되는 등 끝없이 진화와 변화를 거듭하고 있다. 또한 위협의 주체는 개인 해커, 사이버 범죄그룹, 세계 각국의 국가 지원 해킹그룹으로 분류되며, 이들은 다양한 공간, 방법, 조직을 활용해 사이버 위협을 발생시키고 있다. 하지만 이처럼 공개되거나 획득된 정보를 바탕으로 사이버 위협에 대응하기 위해서는 위협정보를 정확하게 평가하고 정량화할 수 있는 체계를 필요로 한다. 모든 사이버 위협을 단순히 위협이라고 정의하게 된다면 어떻게 사용해야 하는지 조직의 한정된 인력과 자원을 사용해야 하는지 정확하게 판단하기 어렵다. 따라서 본 연구에서는 우리 군의 사이버 위협과 대응, 사이버 위협에 대한 군사적 연구의 필요성에 대해 살펴보고 지금까지의 선행 연구를 바탕으로 퍼지추론을 이용한 정량적 사이버 위협 평가 항목을 제시하고자 한다.

2. 본 론

2.1 북한의 사이버 위협과 대응

2013년 5월 삼성 SDS 등 군 전술망 네트워크 체계와 전술지휘통제 자동화 체계 관련 기술을 가진 국내 방위산업체 두 곳의 전산 시스템이 북한 또는 중국으로 추정되는 세력으로부터 해킹을 당했다. 2015년 8월에는 국방부 바이러스 백신 프로그램 공급업체 하우리가 북한으로 추정되는 해커그룹으로부터 해킹을 당했으며, 2016년 9월에는 군 내부 전산망이 북한 추정 해커그룹으로부터 해킹을 당하여 일부 군사자료가 유출된 것으로 판단하고 있다. 2017년 5월 12일에는 전 세계 150여개국가 20만대 이상의 컴퓨터가 워너크라이(Wanna Cry) 랜섬웨어(Ransomeware)에 감염되었으며, 그 배후도 북한으로 지목되고 있다.[1] 이와 같이 국방 분야에 대한 지능화 · 고도화된 사이버 공격은 단순히 기술적 수단만이 아닌, 사람을 대상으로 하는 사회공학적 공격과 결합된 APT(Advanced Persistent Threat, 지능적 지속위협) 유형으로 치밀한 계획 하에 조직적으로 발생되고 있다.

특히 북한의 사이버전 인력은 약 6800명으로 추산되고 있으며, 미국 워싱턴대 국제문제연구소 평가에서는 북한 해커부대 전력이 미국 사이버사령부가 보유한 4900명보다 많으며, 중국에서 활동하는 해커인력만 600~1000명 수준인 것으로 추정하고 있다. 최근 발표에 따르면 북한 정보기관인 정찰총국이 180부대라는 해커조직을 운영해 각종 사이버테러에 성공하고 있다.[1] 이를 종합해보면 북한에 의한 사이버 위협이 지속적으로 증가될 것으로 예측된다.

군은 증가하는 사이버 위협에 대응하기 위해 2010년 사이버사령부를 창설, 2016년에는 각 군 사이버방호센터를 창설하였으며 북한을 비롯한 전 세계의 사이버 위협으로부터 군의 정보체계를 안정적으로 보호하기 위한 다양한 정책들을 추진하고 있다.

2.2 사이버 위협에 대한 군사적 연구의 필요성

사이버 위협에 대한 다양한 기술적, 개념적 연구들이 진행되어 왔음에도 불구하고 우리 군에 적용 가능한 사이버 위협에 대한 개념과 측정에 대한 연구는 미비한 실정이다. 모든 사이버 위협을 단순히 '위협'이라고 정의하게 된다면 그에 따른 언어적 불확실성을 가지게 되며 그 대상과 실체가 명확하더라도 위협이 어떤 위험과 영향을 주는지에 대한 측정이 불가능하고 조직의 효과적인 대응을 어렵게 한다.[2][3][4]

최근까지 국내에서 발표된 다양한 연구에서는 사이버 위협정보를 공유하는 방법과 수집된 사이버 위협정보를 분석하는 방법, 그에 따른 위험도를 측정하는 방법에 대해 연구되었다. 또한 수집된 위협정보를 어떠한 프레임으로 체계화하여 공유할 것인지에 대해 초점이 맞추어져 있다. 또한 대부분의 일상적 사이버 위협은 군과 같은 공공분야보다는 상대적으로 보안관리가 허술하고 금전적 이득을 취할 수 있는 민간분야를 대상으로 발생되고 있다.[5] 민간분야에서 사용되는 보호되지 않거나 개방된 인터넷 네트워크는 조직의 규모에 따라

비용 및 기술부족한 실정이며 위협을 인식하고 신속한 조치를 하지 않아 군의 사이버 환경과는 특성이 다르다. 이를 고려해 볼 때 군의 사이버 환경을 고려한 군사적 사이버 위협에 대한 연구는 위협에 대한 인식과 대응에서 차이를 가지고 있다. 따라서 발생 가능한 사이버 위협을 개념적으로 분류하고 정량적 측정을 통해 위협을 인식한다면 조직의 전사적 대응을 가능하게 한다. 또한 측정된 정보를 공유해 한정된 자원을 효율적으로 사용하고 효과적 대응을 가능하게 하며 명확한 위협에 대한 분류와 평가지표를 바탕으로 정책결정자나 조직관리자의 의사결정에 영향을 줄 수 있다.

2.3 사이버 위협에 대한 군사적 정의

사이버 위협에 대한 개념을 이해하기 위해서는 먼저 군사적 개념의 위협에 대한 이해가 필요하다. 군사용어사전에서 위협이란 적의 공격기도, 군사적 능력, 환경으로 인해 받는 심리적인 긴장상태, 침투 및 도발이 예상되는 적의 능력과 기도가 드러난 상태를 말한다.[6] 국방과학기술용어사전에서는 침투 및 도발이 예상되는 적의 능력과 기도가 드러난 상태로 정의하고 있다. 하지만 사이버 위협은 공격자를 규정하기가 어렵고 기도와 능력이 사전에 드러나지 않는다.[7] 따라서 사이버 위협이란 우리의 정보체계에 위협이 되는 기술적 수단이나 사이버 공간에서 공격 행위가 드러난 상태로 정의할 수 있다.[8]

2.4 사이버 위협 평가에 대한 선행 연구

김애찬과 이동훈은 사이버 위협정보(Cyber Threat Intelligence)란 조직의 자산에 손실 또는 잠재적인 위협이 될 수 있는 지식, 문맥, 메커니즘, 식별자에 대한 주체의 실행 가능한 조언 또는 의사결정을 지원하는 정보라고 정의했다.[5] '사이버 위협정보 공유에 관한 법률(안)'에서는 정보통신망 · 정보통신기기 및 정보보호시스템 등에 의해 해킹, 바이러스, 서비스방해, 전자기파 등 정보통신망을 마비 · 파괴하거나 정보를 절취할 수 있는 행위에 관한 정보로 정의하고 있다. Enter Greg Reith는 사이버 위협은 실행속도, 강도, 놀라움의 세가지 요소를 가지고 있으며, 사이버 위협 정보의 역할은 사전의 경고를 통해 작전, 전략, 전술적 혼란을 줄이는 것이라고 정의하였다.[9] Martin Libicki는 '중요한 사이버 공격에는 반드시 동기가 있다'라고 하였으며 특히 공격주체가 국가라면 국가안보에 영향을 줄 것이라고 정의하였다.[10]

Irving Lachow는 그의 연구에서 사이버 위협을 테러로 규정하고 위험을 정량적으로 측정하기 위해 3가지 수준으로 분류 하였으며, 위협 수준을 <표 1>과 같이 단순, 발전된, 복합적 위협으로 정의하였다.[11]

<표 1> 위협 수준 분류

구분	단순	발전	복합
범위	단일 시스템 네트워크	다양한 시스템, 네트워크	복합적 네트워크
분석	없음	기초적	자세함
통제	약함	중점적	확장적
필요 자원	부분적 컴퓨터 능력	고급 프로그래머, 단순 테스트 환경	전문적 프로그래머, 분석가, 기획자 복잡한 테스트 환경
필요 조직	없음	없음	동조화된 팀
잠재 사용	괴롭힘	전술적 공격	전략적 공격

위협치를 산출해내는 척도로는 위협평가 파라미터가 있다. 많은 연구논문들에서는 위협을 평가하는데 사용하고 있는 파라미터를 <표 2>와 같이 세 종류로 분류하고 있다.[12] 방어 자산에 대한 타겟의 근접도를 나타내는 Proximity 파라미터, 자산의 피해를 입히는 정도를 나타내는 Capability 파라미터, 타겟의 의도를 나타내는 Intent 파라미터로 분류되고 있다. 다음 표는 위협평가에 사용하는 파라미터를 표로 정리한 것이며, 이와 같은 파라미터들의 연관성 및 관계성을 통하여 위협평가를 수행한다.[13]

<표 2> 위협 파라미터

Parameter	Examples
Proximity	Euclidean Distance, CPA
Capability	Target type, Weapon envelope
Intent	Speed, Heading

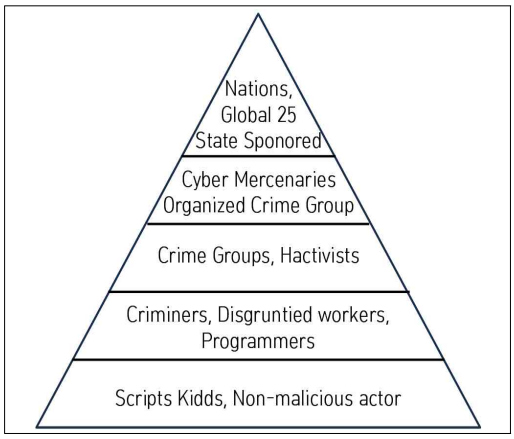
Enter Greg Reith는 그의 연구에서 위협의 범주를 성가신(N : Nuisance) 위협에서 중요한(S : Significant) 위협으로 나누고 세 가지 카테고리로 분류하였다. 분류된 위협은 알려진 취약점을 이용한 쉬운 공격부터 어려운 공격, 알려지지 않은 취약점에 의한 복잡하고 다양한 공격, 창의적으로 생성된 취약점에 의한 복잡하고 다양한 계층에 대한 공격으로 나누었다. 또한 위협을 9가지로 구체화하여 위협을 통제 가능하도록 하였다.[9] 이것을 정리하면 <표 3>과 같다.

<표 3> 위협계층과 유형

구분		위협 유형
S ↑	Creates vulnerability, Unique multi staged full spectrum attacks	Automated Analytic attack
		APTs
		SE+HUMINT
N	Attacks unknown v ulnerability, Complex multi vector attacks	Exploit kit Malware
		Ransomeware
		Spear Phishing
↓ L	Attack known vulne rability, Easy to diff icult exploits	DDoS
		Social Engineering
		Phishing, Viruses

또한 위협 행위자에 대한 프로파일링을 통해 위협의 강도를 제시하고 있으며, 이를 정리하면 아래 <표 4>와 같다.

<표 4> 위협 프로파일링



3. 사이버 위협 수준 평가 모델 제시

종합적인 사이버 위협수준을 평가하기 위해 항목별 위협수준을 아래 <표 5>와 같이 제시하였다.

<표 5> 위협 수준 평가 항목

행위자 / 방법 / 근접성 강도		S			C			K		
		H	N	L	H	N	L	H	N	L
H	H	A	A	B	A	A	C	B	B	C
	N	A	A	B	B	B	C	C	C	D
	L	B	B	B	C	C	C	D	D	D
N	H	A	B	B	B	B	D	D	D	E
	N	A	B	B	B	D	D	E	E	E
	L	B	B	C	D	D	D	E	E	E
L	H	B	B	C	C	C	D	D	D	E
	N	C	C	C	C	D	D	E	E	E
	L	C	C	C	D	D	D	E	E	E

또한 평가 항목을 제시함에 있어 퍼지추론의 방식을 이용하였다. 퍼지추론이란 몇 개의 모호함이 포함된 언어적 명제로부터 하나의 다른 근사적 명제를 도출하는 근사추론 방식이다.[14] 특히 퍼지이론을 이용한 사이버 위협 평가 항목은 보안 영역에서 다양한 연구에서 적용되어 왔다.[15][16][17][18][19][20][21]

세로축의 근접성은 사이버 위협이 있을 시 군이 보유한 정보체계 자산에 영향을 줄 수 있는 취약점인가에 대한 평가로 영향을 줄 수 있는 가능성이 높을 시(H : High), 일반적(N : Normal), 낮을 시(L : Low)의 위협으로 분류하였다. 또한 그 취약점에 의해 발생될 피해의 강도가 높을 시(H : High), 일반적(N : Normal), 낮을 시(L : Low)로 구분하였다. 가로축의 행위자는 국가 지원해커(S : State Sponsored), 범죄그룹(C : Crime Group), 비악의적 행위자(K : Script Kids)로 분류하였으며, Enter Greg Reith 위협분류에 따라 높을 시(H : High), 일반적(N : Normal), 낮을 시(L : Low)로 구분하였다. 이와 같이 위협을 평가하기 위한 행위자, 방법, 강도, 근접성의 4가지 분류는 각각 3개의 언어적 변수로 나누어 표현하였다. 이에 따라 위협 수준에 대한 평가는 81개의 평가결과로

나타나며 위협 수준을 나타내는 언어적 변수는 매우 심각(A), 심각(B), 보통(C), 낮음(D), 매우 낮음(D)로 나타내고, 이를 나타내는 수치는 0.9, 0.7, 0.5, 0.3, 0.1로 정의할 수 있다.

예를 들어 국가지원 해커가(State Sponsored) 피싱 이메일과 같이 알려진 일반적 방법(Normal)으로 랜섬웨어(Normal)를 유포 중이지만, 해당 취약점은 군이 사용하는 체계와 달라 근접성이 낮다면(L) 위협 수준은 보통(C)으로 정량화시 0.3으로 표현할 수 있다. 또는 범죄집단의 해커(C : Crime Group)가 랜섬웨어를 유포해 금전 취득을 노리는 경우(N : Normal), 랜섬웨어 감염대상과 군 정보체계의 근접성이 낮다면(L : Low), 감염시 피해가 크더라도(H : High), 언어적으로는 보통(C)이며 정량적 수치는 0.3으로 표현할 수 있다. 즉, 본 연구에서 제시하는 평가항목을 통해 사이버 위협 수준을 다각적으로 평가하여 정량적으로 비교 가능하다.

4. 결 론

본 연구에서는 사이버 위협을 정량적으로 평가할 수 있는 항목들을 모델화 하여 제시하고자 하였다. 이를 위해 언어적으로 표현된 위협의 항목들을 분류하고 위협에 해당되는 여러 가지 정성적 영향 요소들을 복합적으로 적용해 위협수준을 평가하고자 하였다. 또한 이를 퍼지추론법을 적용한 종합적 모델로 제시하고자 하였다. 하지만 퍼지 이론을 응용하기 이해서는 실험적 검증이 중요하다.[22] 따라서 향후 연구에서는 퍼지 이론을 적용하기 위해 항목을 세밀화 하고, 정성적 평가 항목간의 연관성 검증과, 유효성과 타당성을 제시하는 추가 연구를 통해 검증한다면, 객관적 사이버 위협 수준 평가 항목을 제시할 수 있을 것이다.

사이버 위협 수준 평가항목을 통해 군의 사이버 방호 조직간 사이버 위협을 정량적으로 평가하고 공통된 위협 인식이 가능할 것이며, 이를 바탕으로 민간, 공공기관간의 사이버 위협정보를 공유하고 공동으로 대응할 수 있는 정량화된 근거로 제시될 수 있을 것이다.

참고문헌

[1] 이광호, 김홍택. “사이버 안보를 위한 軍 정보보호 전문인력 양성방안”, 융합보안논문지, 제17권 제2호, pp.145-152, 2017.

[2] L.A. Zadeh, "Fuzzy Set", Information and Control 8. pp.338-353, 1965.

[3] L.A. Zadeh, "The Concept of a Linguistic Variable and its Application to Approximate Reasoning", Information Science 8. pp.199-249, 1975

[4] Burrough & R.A. McDonnel, "Principle of Geographical Information System, Oxford University Press, 1998.

[5] 김애찬, 이동훈, “효과적인 사이버위협 정보공유체계 수립을 위한 요구사항의 우선순위 도출에 관한 연구”, 정보보호학회지 제26권 제1호, pp.61-67, 2016.

[6] 이태규, ‘군사용어사전’, 일월서각, 2012

[7] 국방기술품질원, ‘군방과학기술용어사전’, 2011

[8] 윤석준, 김종화, “사이버 작전 수행을 위한 사이버 작전 모델 제안”, 합참지 Vol.74 2018.1월(겨울호), pp.55-60, 2018.

[9] Enter Greg Reith, "Prioritizing Cyber Threats With Real-Time Threat Intelligence", RFSID., 2018.

[10] Libicki Martin C, "Conquest in Cyberspace : National Security and Information Warfare." Cambridge University Press, 2007

[11] Irving Lachow, "Cyberpower and National Security", Potomac Books Inc., 2009

[12] Jong Min Yun, Sung-Sam Hong and Myung-Mook han, "The Study of Threat Evaluation using Threat Evaluation Parameter and Fuzzy on Air Defence of Army", Proceedings of KIIS Fall conference, vol. 21 no.2 pp.228-229, 2011

[13] 최보민, 한명묵, “베이지안 네트워크 학습을 이용한 방공 무기 체계에서의 위협평가 기법 연구”, Journal of Korean Institute of Intelligent Systems, Vol 22 No. 6 pp.715-721, 2012

[14] 도용태, 김일곤 외 3명 ‘인공지능 개념 및 응용’, 사이텍미디어, 2013.

[15] Ming-Chang, Lee. "Information Security Risk Analysis Methods and Research

Trends: AHP and Fuzzy Comprehensive Method", International Journal of Computer Science & Information Technology (IJCSIT) 6 (1) p. 29-45., 2014
[16] Sjoberg, Lennart., "Consequences of perceived risk: Demand for mitigation." Journal of Risk Research 2.2., 1999
[17] National Research Council of the National Academies., "The Owner's Role in Project Risk Management". Available in:(https://www.nap.edu/read/11183/chapter/7). p. 41., 2005
[18] Hany, Sallam. "Cyber Security Risk Assessment Using Multi Fuzzy Inference System", International Journal of Engineering and Innovative Technology (IJEIT) 4, 8., 2015
[19] Martin McNeill, F., Ellen, Thro. "FUZZY LOGIC A PRACTICAL APPROACH" by Academic Press Professional. San Diego, CA, USA., 1994
[20] Bajpai, Shailendra, et al. "Security Risk Assessment: Applying the Concepts of Fuzzy Logic", Journal of Hazardous Materials, 173 (1-3) 258-264., 2010
[21] Sonia., Singhal, A., Banati, H. "Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD model", IJCSI International Journal of Computer Science Issues, 8 (4) 1., 2011
[22] H. -J. Zimmermann "Fuzzy set theory', 2015

〔저자소개〕

이 광 호 (Kwang-ho Lee)
2007년 2월 육군3사관학교 학사
2016년 3월 연세대학교 정보보호 석사
2017년 2월 ~ 현재
아주대학교 NCW학과 박사과정
email : loveney@naver.com

김 지 원 (Jee-won Kim)
2016년 8월 연세대학교 정보보호 석사
2016년 7월 ~ 현재
육군사관학교 컴퓨터과학과 조교수
2017년 2월 ~ 현재
아주대학교 NCW학과 박사과정
email : jeewonkim@ajou.ac.kr

김 완 주 (Wan-ju, Kim)
1998년 2월 서울과기대 전자공학 학사
2008년 1월 국방대학교 전산정보학 석사
2017년 아주대학교 NCW공학 박사
email : sizipus1@gmail.com

김 종 화 (Jong-hwa Kim)
2001년 3월 국방대학원 전산정보 석사
현 재 아주대학교 NCW학과
박사과정
email : joaakim@hanmail.net

윤 석 준 (Seok-jun Yun)
1995년 9월 Naval Postgraduate School
전산학 석사
2005년 5월 Texas A&M University
전산학 박사
email : talky@hanmail.net

정 찬 기 (Chan-ki Jeong)
1986년 공군사관학교 전자공학 학사
1994년 플로리다공대 전산공학 석사
2001년 플로리다공대 전산공학 박사
2007년 3월 ~ 현재
아주대학교 NCW학과 교수
email : ckjung@gmail.com