https://doi.org/10.14400/JDC.2017.15.6.51

사이버위기에 대응하기 위한 국가정보기관의 사이버위협정보 공유 역할에 대한 고찰

김대건*, 백승수*, 유동희**
고려대학교 정보보호대학원*, 경상대학교 경영정보학과**

Sharing the Cyber Threat Intelligence on Cyber Crises: The Appropriate Role of the National Intelligence Agency

Daegeon Kim*, Seungsoo Baek*, Donghee Yoo**
Center for Information Security Technologies, Korea University*
Dept. of Management Information Systems, Gyeongsang National University**

요 약 국가는 전통적으로 국토를 방위하고 국민의 생명과 재산을 보호하는 사명을 가지고 있으며, 이러한 방위의 범위는 지상, 공중, 바다, 우주에 이어 제5의 영역인 사이버 영역을 포함한다. 사이버 영역으로 국가 방위의 범위가 확대 되었지만, 사이버 영역에 있어서는 국가보다는 민간이 더 많은 사이버 관련 출처와 수집수단을 보유하는 정보역전 현상 때문에 정부 주도의 사이버 영역 방위에 어려움을 겪고 있다. 이를 해결하기 위해, 본 논문에서는 먼저 사이버위협정보를 정의하고 그 특성을 분석하였다. 다음으로 정보역전 현상을 극복하기 위한 각국의 노력과 우리나라의 현 주소를 조사하였고, 그 결과를 바탕으로 정부 주도의 사이버 방위를 위한 국가정보기관의 역할과 사이버위협정보의 민간 공유 모델을 제안하였다. 제안된 모델을 국가정보기관에서 활용한다면 사이버위기에 보다 효과적으로 대응할 수 있는 기반 체계가 마련될 것을 기대해 볼 수 있다.

주제어 : 사이버위협정보, 사이버정보, 정보역전, 사이버위기, 국가정보기관

Abstract The role of government is to defend its lands and people from enemies. The range of that defense has now extended into the cyber domain, regarded as the fourth domain of the conventional defense domains (i.e., land, sea, sky, and universe). Traditionally, a government's intelligence power overrides that of its civilians, and government is exclusively responsible for defense. However, it is difficult for government to take the initiative to defend in the cyber domain because civilians already have a greater means for collecting information, which is known as being "intelligence inverse" in the cyber domain. To this end, we first define the intelligence inverse phenomenon and then analyze its main features. Then we investigate foreign countries' efforts to overcome the phenomenon and look at the current domestic situation. Based on these results, we describe the appropriate role of the National Intelligence Agency to handle cyber threats and offer a cyber threat intelligence model to share with civilians to help protect against these threats. Using the proposed model, we propose that the National Intelligence Agency should establish a base system that will respond to cyber threats more effectively.

Key Words : Cyber threat intelligence, Cyber intelligence, Intelligence inverse, Cyber threat, National intelligence agency

Received 5 April 2017, Revised 18 May 2017
Accepted 20 June 2017, Published 28 June 2017
Corresponding Author: Donghee Yoo
(Gyeongsang National University, BERI)
Email: dhyoo@gnu.ac.kr

ISSN: 1738-1916

1. 서론

사이버공간은 지상, 공중, 바다, 우주에 이어 국토의 제5영역으로 인정되고 있다. 최근 사이버 범죄나 공격으로 인해 개인에서부터 기업, 그리고 국가에 이르기까지 여러 유형의 경제적 피해가 발생하고 있으며 동시에 국가안보까지 위협받고 있는 실정이며[1], 공격 형태 또한 점점 지능화되어 가고 있다[2]. 이와 관련하여 미국을 포함한 세계 주요 국가들은 이미 사이버공간을 중요한 국가 영역으로 인정하는 법안을 만들고 있으며 각국의 실정에 적합한 사이버 정책들을 준비하고 있다[3, 4, 5].

특히 여러 분야에서 동시다발적으로 발생하는 국가적 규모의 사이버 위기에 효과적으로 대응하기 위해서는 광범위한 사이버위협정보의 수집에서부터 분석, 처리, 그리고 대응에 이르는 일련의 활동을 통해 생성된 정보의 활용과 공유가 필수적이다[6].

그러나 사이버위협정보에 대한 정보보유 측면에서 국가정보기관과 민간기관을 비교했을 때 타 유형의 정보와는 달리 정보역전현상이 발생한다. 여기서 정보역전현상이란 일반적으로 타 유형의 정보는 출처가 분산되어 있거나 국가가 핵심 정보를 수집하는 자산을 보유하고 있어 정보의 주도권이 국가기관에 있는 반면, 사이버위협정보는 출처와 수집수단 보유 측면에서 민간이 우위를 점하고 있기 때문에 결과적으로 정보가 국가기관에 종합된다 하더라도 정보의 주도권을 민간에서 보유하는 현상을 의미한다.

이와 같은 사이버위협정보의 특성을 극복하면서 국가적 규모의 사이버위기에 신속히 대응하기 위하여 각국에서는 유관기관을 대상으로 한 거버넌스(governance)를 형성하고 사이버위협정보 수집을 위한 법률 제정 등과 같은 다각도의 노력을 기울이고 있다.

본 논문에서는 먼저 사이버위협정보를 정의하고 그 특성을 다른 정보 유형과 비교분석함으로써 정보역전현상의 발생을 설명한다. 이어서 이를 극복하기 위한 각국의 노력을 살펴보고 국가기관의 사이버위협정보 수집을 위한 우리나라의 현 주소와 발전적인 사이버위협정보 공유모델을 제안한다.

2. 사이버위협정보

2.1 사이버위협정보 정의

사이버위협정보(Cyber Threat Intelligence, CTI)는 여러 정보 유형 중에서도 상대적으로 최근에 부각된 정보 유형으로, 다양한 정보보호 업체들에서 자사의 제품에 사이버위협정보에 관한 보안의 장점을 부각시키기 위해 관련 정의를 사용하였다. 이 중 대다수는 사이버위협정보를 첩보수준으로 정의하고 있으나, McMillan은 (사이버)위협정보를 아래와 같이 정의하였다.

"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard[7]."

위 정의를 기준으로 사이버위협정보를 구분해 보면 <Table 1>과 같다. 협의의 사이버위협정보는 주로 기술정보를 나타내며 악성코드정보, 악성 네트워크 트래픽 정보, 그리고 이를 가공한 기술분석정보 등이 해당된다. 광의의 사이버위협정보는 사이버 위협과 관련된 공격자(그룹)인 인물정보와 동향정보 등과 같은 비기술정보를 포함하고 있다.

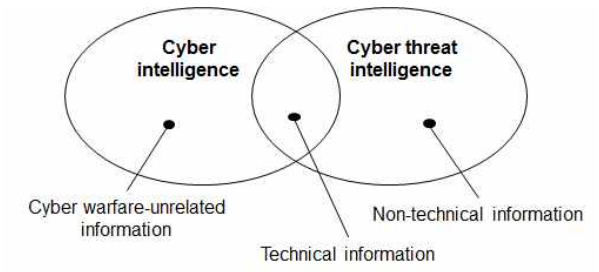
<Table 1> Classification of cyber threat intelligence

Classification	Example
Technical Information (Narrow sense)	Malicious code information, Network information, Technical analysis information
Non-technical Information (Broad sense)	Personal information, Trend information

본 논문에서는 사이버위협정보와 사이버정보(Cyber Intelligence, CYBINT)를 구분하여 사용하고자 한다. 전통적으로 분류되는 6대 정보 유형에는 인간정보(Human Intelligence, HUMINT), 신호정보(Signal Intelligence, SIGINT), 영상정보(Imagery Intelligence, IMINT), 지리공간정보(Geospatial Intelligence, GEOINT), 계측 및 기호정보(Measurement and Signature Intelligence, MASINT), 공개정보(Open Source Intelligence, OSINT)

가 있으나[8], 최근에는 사이버정보를 추가적인 정보 유형으로 분류하기도 한다[9].

사이버정보는 사이버 공간상에서 수집 가능한 모든 유형의 정보를 의미한다. 예를 들어 인터넷 검색을 통해 수집 가능한 공개정보, 해킹을 통해 수집한 전자적 형태의 정보, 입수된 저장매체에서 추출한 정보 등이 사이버정보에 해당한다. 사이버정보는 정보를 수집하는 공간을 기준으로 그 특성이 구분되며 수집된 정보의 성격은 특성에 크게 반영되지 않는다. 따라서 사이버정보는 사이버위협정보를 일부 포함하는 개념으로 이해할 수 있다. 그러나 사이버위협정보에는 사이버적인 수단이 아닌 별도의 수단으로 수집된 사이버 조직과 공격주체와 같은 정보들이 포함될 수 있으므로 사이버정보를 사이버위협정보보다 포괄적인 개념으로는 정의할 수 없다. 따라서 본 논문에서는 사이버정보와 사이버위협정보의 범위를 [Fig. 1]과 같이 표현하고자 한다.



[Fig. 1] Scope of cyber intelligence and cyber threat intelligence

2.2 사이버위협정보 특성

본 장에서는 앞서 언급한 6대 정보 유형들 중 공개정보를 제외한 정보 유형들과 사이버위협정보를 비교하고자 한다. 여기에서는 협의의 사이버위협정보 관점에서 관련 정보가 유통되는 매체(매질)의 특성을 정보 유형에 따라 비교하였다. 공개정보와 비기술적 사이버위협정보는 정보전달 매체가 한정된 것이 아니므로 정보가 유통되는 매체를 기준으로 비교할 수 없어 비교 대상에서 제외하였다. 각 유형의 정보가 전달되는 매체는 <Table 2>와 같이 분류될 수 있다.

<Table 2>와 같이, 인간정보는 인간과 인간 사이의 관계에서 정보가 유통되고 그 외 정보들은 전자기파, 영상, 레이저 등 각자 파장이 다른 파동에 의해 정보가 유통된다. 그러나 사이버위협정보는 사이버공간에서 유통되는 정보로써 네트워크망, 호스트와 서버, 정보보호장비, 그리고 저장매체 등에 의해 정보가 유통되며 이러한 전달매체가 사이버공간에서 점유하는 위치에 따라 정보주체가 달라진다. 네트워크망을 통해 유통되는 정보는 주로 ISP에서, 호스트에 존재하는 정보는 호스트 보호 서비스를 제공하는 백신 업체 또는 해당 호스트를 보유한 기관에서, 서버에 존재하는 정보는 IDC 또는 직접 서버를 운영하는 기관에서, 정보보호장비에서 탐지되거나 저장되는 정보는 해당 장비를 운영하는 네트워크 운영주체가, 그리고 각 저장매체에 저장된 정보는 매체의 소유주가 정보의 주체가 된다.

<Table 2> Transmission medium according to Information types

Type	Transmission medium
HUMINT	Human
SIGINT	Wave (Electromagnetic waves)
IMINT	Wave (Image & Photography)
GEOINT	Wave (Image & Radar)
MASINT	Wave (Electro-optical & Radar)
Cyber threat intelligence	Network, Host and Server, Equipment for information security, Storage

3. 정보역전현상 및 각국의 극복노력

3.1 정보역전현상

<Table 2>에서 보는 바와 같이, 사이버위협정보를 제외한 정보 유형의 경우 정보 수집에 사용되는 전달매체는 국가 차원의 인프라 구축을 통해 수집되기 때문에 수집된 정보가 정보기관을 중심으로 국가에 집중되는 특성을 지니고 있다. 그러나 사이버위협정보는 통합데이터센터와 같은 국가시설을 통해 관련 정보가 직접 수집될 수 있지만, 동시에 민간영역에서도 다양한 사이버위협정보가 수집될 수 있다. 여기에서 민간영역에서 수집된 사이버위협정보의 주도권을 국가가 직접 행사하기에는 여러 가지 제약이 발생한다. 또한, 국가시설이라 할지라도 백신과 ISP의 서비스를 사용하지 않을 수 없기 때문에 국가에서 독자적으로 보유한 사이버위협정보의 양은 소수일 수밖에 없다. 따라서 정보출처와 수집수단의 보유 측면에서 국가보다 민간에서 사이버위협정보 보유에 대한

우위를 점하게 되는 정보역전현상이 발생하게 되는 것이다.

사이버위협정보의 수집을 목적으로 국가에서 주도적으로 수집수단을 운영하는 경우도 있다. 에드워드 스노든(Edward Joseph Snowden)에 의해 공개된 바와 같이 미국 정보기관은 법적인 활동의 보장이 제한되는 정보수집을 사이버 공간에서 수행 중에 있다[10]. 이러한 활동을 확장하기 위해 범국가적인 인터넷 공간에서 사이버위협정보를 포함한 다양한 정보를 수집하는 XKeyscore[11], 토르(Tor)와 같은 다크넷 사용자를 추적하기 위한 Egotistical Giraffe[12] 등과 같은 비밀 프로젝트들을 수행하기도 하였다. 이와 같이 국가적 차원의 사이버위협정보 수집수단이 존재할 경우 타 유형의 정보와 같이 국가에서 정보의 주도권을 보유할 수 있다.

사이버위협정보의 주도권을 보유한 민간업체의 궁극적인 목표는 이익 창출이기 때문에 사이버 침해 발생 시 자사 서비스의 지속성 유지를 위해 상호호혜적 관계 속에서 각자 보유한 정보에 대한 공유가 이루어지고 있다. 반면, 국가에서 사이버위협정보를 효율적으로 수집하기 위해서는 법적, 제도적 근거를 기반으로 정보주체들로부터 관련 정보들을 제공 받아야하는 실정이다.

3.2 정보역전현상 극복을 위한 각국의 노력

사이버위협정보에 대한 정보역전현상을 극복하기 위해 각 국은 정보 수집 관점에서 다양한 노력을 기울이고 있다.

3.2.1 미국

미국은 앞서 언급한 XKeyscore 및 Egotistical Giraffe와 같이 국가주도의 사이버위협정보 수집을 위한 비밀 프로젝트 외에 민간에서 유통되는 사이버위협정보를 국가에서 합법적으로 수집하기 위한 근거를 마련하고 있다.

사이버 공격에 대응하기 위한 조사와 네트워크의 안전성을 보장하기 위하여 민간업체에서 수집한 네트워크 트래픽 정보를 정부와 공유하도록 규정한 「사이버정보 공유 및 보호법(Cyber Intelligence Sharing and Protection Act, CISPA)」은 미 의회에서 2011년에 최초 발의된 후 상원을 통과하지 못하였으나 2013년과 2015년에 재발의 되어 검토되고 있다[13]. 그 후, 이와 유사한 법안인 「사이버안보 첩보 공유법(Cybersecurity Information Sharing Act, CISA)」이 2014년에 미 상원에서 발의된 후 2015년에 재발의 되어 현재 상원을 통과하였으며 CISPA가 CISA의 형태로 돌아왔다고 평가될 만큼 두 법률은 내용상 매우 유사하다[14]. 이 법안들의 핵심은 민간영역과 공공영역에서 발생하는 사이버 침해와 관련된 정보가 국토안보부(Department of Homeland Security, DHS)로 종합되도록 한 것이다. 표면적으로는 DHS에서 사이버위협정보가 종합되는 것처럼 보일 수 있으나 이 정보들은 결국 NSA와 FBI와 같은 국가 정보기관에 공유될 것이라는 의견이 지배적이다. 또한 사이버위협정보 내에 포함될 수 있는 개인정보의 처리 또는 가공에 대한 의무사항을 포함하지 않고 있어 무차별적인 개인정보 수집이 가능하다는 점이 이 법안에서 가장 논쟁이 되는 부분이다.

이와 같은 법적 노력뿐 아니라 사이버위협정보 공유의 중요성에 대한 인식을 바탕으로 표준화된 정보공유 가이드를 적용하기 위하여 미 국립표준기술연구소(National Institute of Standards and Technology, NIST)에서는 「사이버위협첩보 공유를 위한 가이드(Guide To Cyber Threat Information Sharing)」를 발간하였다[15].

3.2.2 일본

일본의 국가기관들은 기관마다 정보보호기능을 수행하는 자체 기구를 운영하였으나, 2001년 IT 강국으로 발전을 위한 'e-Japan 중점계획 2002'의 일환으로 국가차원의 사이버전을 수행할 능력을 구비하기 위해 정보보안대책 추진실을 내각관방실에 신설하였다. 2005년에는 이 조직을 국가정보보호센터로 발전시켰으며 2008년에는 네트워크 관리와 자위대 컴퓨터에 대한 사이버 방호 임무를 수행하는 지휘통신시스템대를 창설하는 등 사이버전에 대비한 조직개편을 가속화하였다.

이러한 가운데 경제산업성(Ministry of Economy, Trade and Industry, METI)이 주관하는 사이버 보안과 경제에 관한 연구회가 2010년 3월에 개최되었고, 그 결과로써 '표적 공격에 대한 대책'이 발표되었는데 이중에는 조직 간의 정보 공유를 위한 그룹에 대한 논의가 포함되어 있었다. 2011년에 일본 내에서 발생한 다양한 사이버 침해사건들로 인해 이 그룹에 대한 필요성이 가중되었으며, 그 결과 2011년 10월 25일에 정보처리진흥사업기구(Information-technology Promotion Agency, IPA) 주관으로 '국가적 사이버 보안을 강화하고 파트너십을 공유

하며 사이버 보안을 위한 정보를 공유하기 위한 이니셔티브(The Initiative for Cyber Security Information Sharing Partnership of Japan, J-CSIP)'가 설립되었다. 이에 따른 실적으로 5개 산업과 3개 기관 간의 정보공유 제도가 2012년에 수립되었고, 2012년 4월부터 2013년 3월 사이 160건의 사이버 침해시도에 대한 정보공유가 이루어졌다[16].

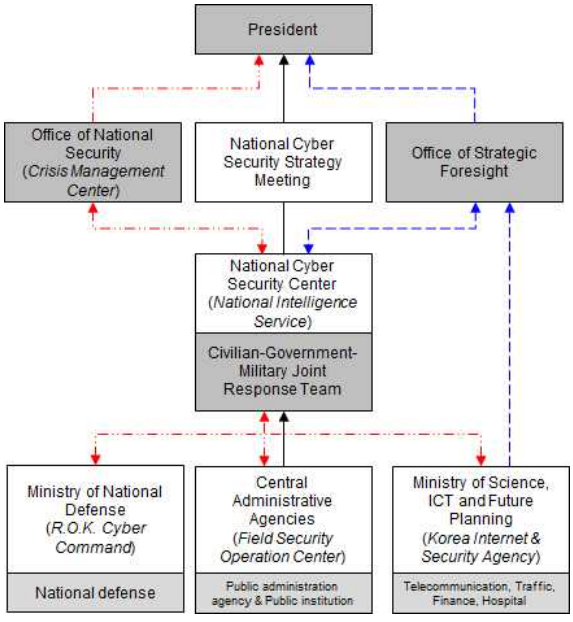
3.2.3 NATO 및 EU

NATO는 2007년 에스토니아전을 통해 사이버전에 대한 중요성을 체감한 결과 일찍이 사이버 위협에 공동으로 대응하고 정보를 공유하기 위한 조직을 운영하게 되었다. 2002년 프라하에서 열린 NATO 회원국 정상회담에서 NATO의 사이버 방어 프로그램의 필요성에 합의한 결과 2008년 3월 북대서양 이사회의 승인 하에 NATO 회원국 간의 통합적인 사이버 대응을 컨트롤하기 위한 사이버 방어 지휘부(Cyber Defence Management Authority, CDMA)가 조직되었다. CDMA는 사이버 방어와 정보공유의 최적화, 협업 및 상호운용성과 관련된 일체의 지원을 제공한다. 또한, 2008년에 창설된 NATO 산하 사이버 방어협력센터(Cooperative Cyber Defence Centre of Excellence, CCDCOE)는 회원국의 사이버 대응능력, 상호협력, 사이버정보 공유 등을 강화하는 실행기구의 성격을 지닌다[17].

EU의 경우 2004년에 유럽 정보보호원(European Union Agency for Network and Information Security, ENISA)을 설립하였다. ENISA는 정보보호에 대한 데이터 수집과 분석 기능을 수행하고, 유럽연합 국가들에 정보보호와 관련된 전문기술과 경험을 제공한다. 아울러 ENISA는 주요 관련 기관의 조정역할을 수행하며 정보보호 표준화 활동을 통해 네트워크와 정보시스템의 연동을 조화시키는 역할을 담당한다[18].

3.3 우리나라의 현 주소

국가적 사이버위협에 대응하기 위한 우리나라의 법적 기반은 2005년 제정된 「국가사이버안전관리규정(대통령훈령 제141호)」에 근거하고 있다[19]. 2009년에 발생한 '7.7 DDoS 공격'은 국가적 사이버공격에 대응하기 위한 선제적 예방과 침해 시 피해를 최소화하기 위한 범정부차원의 포괄적 대책의 필요성에 대한 공감대를 형성하였고, 이에 따라 마련된 「국가사이버위기종합대책」이 국가사이버안전 전략회의에서 확정되었다[20]. 본 종합대책에서는 국가정보원(이하 국정원)이 사이버 위기대응에 대한 총괄업무를, 방송통신위원회는 악성코드를 퍼트리는 좀비 PC 제거와 국민을 대상으로 사이버안전에 관한 홍보 등의 업무를, 국방부는 사이버부대를 새로 편성하여 국방영역의 사이버전을 대비하게 했다. 이 종합대책을 구현하기 위해 제정된 「국가사이버안전관리규정」은 지속적으로 보완되고 개선되어 현재에 이르고 있다. 2013년에는 '3.20 사이버테러'와 '6.25 사이버공격' 등 국가 안보를 위협하는 사이버 위협이 발생함에 따라 「국가사이버안보종합대책」이 수립되었으며[21], 이 종합대책에서는 [Fig. 2]와 같이 사이버안보의 컨트롤타워는 청와대가, 실무총괄은 국정원이 담당하도록 조정되었고, 주요 사이버침해사고에 대해서는 '민, 관, 군 합동 대응팀'을 중심으로 상호협력과 공조를 강화하도록 규정되었다.



[Fig. 2] Response system for national cyber security[21]

사이버위협정보의 공유 측면에서 「국가사이버안보종합대책」이 갖는 큰 의미는 기존에 관련기관 간 원활한 정보공유가 부족하다는 지적에 따라 유관기관들의 스마트 협력체계를 마련하기 위한 국가차원의 '사이버위협정보 공유시스템'을 2014년까지 구축하고, 이를 토대로 민간 부문과의 정보제공과 협력을 강화해 나가기로 한 점이다. 이에 대한 추진결과로 민간부분에서는 미래부

산하 한국인터넷진흥원(KISA) 주관으로 '사이버 위협정보 분석 공유 시스템(C-TAS)'을 운용하여 사이버위협정보를 공유하게 되었다.

여기에서 체계에 의한 정보 공유뿐만이 아니라 국가적 사이버위협정보의 수집과 공유를 위한 입법도 추진된 바 있다. 2015년 발의되었다 종료된 「사이버위협정보 공유에 관한 법률안」은 국정원 산하에 '사이버위협정보 공유센터'를 설치하여 관련정보를 공유하고, 공유센터의 장은 공유된 사이버위협정보를 종합분석하고 그 결과를 사이버위협정보 공유기관과 관련업체에게 제공하여야 한다고 규정하였다[22].

사이버위협정보 수집과 관련된 조항을 포함한 또 다른 관련 법률안인 「국가 사이버테러 방지 등에 대한 법률안」은 위 법률안과 비교하여 국정원의 능동적인 정보수집 권한을 강화할 수 있도록 규정하고 있다[23]. 본 법률안은 1) 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방 및 대응, 2) 사이버위기관리를 위하여 국정원 소속으로 '국가사이버 안전센터'를 운영하고, 3) 국가차원의 종합판단, 상황관제, 위협요인 분석, 사고 조사 등을 위해 '민, 관, 군 합동 대응팀'을 설치·운영할 수 있다고 규정하고 있다. 이러한 법률안은 현재 실행되고 있는 「국가 사이버안보종합대책」 상의 사이버안보 대응 체계도에 법률적으로 명문화되어 있는 것으로 보인다([Fig. 2] 참고). 하지만 이 법률안이 논란에 휘말리고 있는 이유는 사이버안보 대응 체계도의 전반적인 프로세스와 상호협력 측면을 부각하기 보다는 대응 체계상에서 국정원의 역할과 권한에 대한 측면을 강조하는 것처럼 느껴지기 때문이다.

가장 최근에 국정원 주도의 「국가사이버안보법(안)」에 대한 정부입법추진도 예정되어 있다[24]. 이 법률안에서도 '사이버위협정보 공유센터'를 국정원 산하에 설치하도록 명시하고 있다. 이 경우 국정원이 '사이버위협정보 공유센터'로의 정보공유 의무가 없는 상태에서는 향후 사이버위협정보가 국정원으로 보다 집중될 가능성이 높아진다.

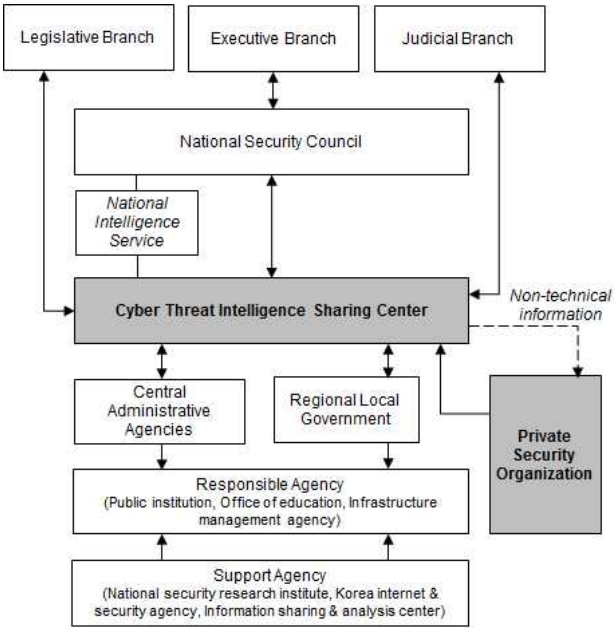
4. 국가정보기관의 역할

국가적 사이버 위기에 효과적으로 대응하기 위해서는 국가 차원에서의 정보 수집과 분석을 통해 지도자의 결심을 지원하고 신속한 대응을 위해 국가정보기관의 정보지원이 필요하다. 사이버전의 진행과 확산은 타 유형의 국가 위기유형과 비교했을 때 상당히 빠르게 이루어지므로 신속한 상황파악과 대응을 위한 정보 지원이 상당히 중요할 수밖에 없다. 또한 민, 관, 군 별로 독립된 대응체계로는 한계가 있기 때문에 전 국가적 차원의 사이버전 대응체계가 필요하며[25], 전략적 요소, 운영적 요소, 기술적 요소 등을 고려하여 위협 요인에 관한 체계적인 분석이 필요하다[26, 27].

특히 사이버 위기에 대한 대응은 특정 국가기관에서 실시할 수 있는 것이 아니라 관련기관들의 노력이 국가 전 영역에서 필요하다는 측면에서 사이버위협정보는 단순히 수집과 분석의 대상이 아닌 대응방법을 도출하기 위해 필요한 요소가 되어야 한다. 이러한 측면에서 사이버위협정보와 관련된 국가정보기관의 역할 중 수집측면과 더불어 공유측면의 역할이 강조되어야 하는 시점으로 보인다. 사이버 위협에 대한 국민적인 공감대는 상당부분 형성되어 있으며 이에 대한 효과적인 대응을 위한 정보공유의 중요성에 대해서도 인식이 확산되어 있는 점에 대해서는 긍정적인 상황으로 분석할 수 있다. 그러나 국가기관의 사이버위협정보 수집을 법률로 명문화하더라도 일방적으로 정보를 제공받기만 한다면 과거에 형성된 비난여론은 지속될 수밖에 없을 것이다.

이와 관련하여, 본 연구에서는 [Fig. 3]과 같이 국가정보기관이 보유하고 있는 사이버위협정보를 민간기관과 공유하는 사이버위협정보 모델을 제안하고자 한다. [Fig. 3]에서는 국가사이버안보와 관련된 정보들이 국가정보기관을 중심으로 공유되고 그 중 일부는 민간기관에 공유하는 것을 보여주며 화살표는 각 기관을 통해 정보가 전달되는 방향을 나타낸다. 여기에서 기존의 「국가사이버안보법(안)」과의 차이점은 사이버위협정보센터와 민간 보안업계와의 정보공유 채널을 포함시킨 부분이다. 기존에는 '민관군 통합사이버위협대응팀' 활동을 통해 일부 공공기관 및 민간분야의 사이버위협정보를 공유해 왔으나, 국가사이버위협정보공유체계 내에 민간분야를 포함시킴으로써 상시 가동되는 사이버위협정보를 보유할 수 있게 된다. 이때 사이버위협정보의 공유 범위는 국가(공공)기관의 경우 기관의 취약점이 노출 될 수 있는 정보공유는 기본적으로 제한하되 악용되고 있는 취약점 정보

는 출처를 익명화한 후 공개가 가능할 것이다. 민간분야의 사이버위협정보 공유 범위는 기관(업체)의 자율에 맡기되, 공유정보의 양과 질에 따라 호혜관계가 유지될 수 있어야 할 것이다. 또한, 정보역전현상으로 인해 국가정보기관에서 민간기관에 제공 가능한 기술적 사이버위협정보가 제한된다 하여도 타 유형(인간, 신호정보 등)에서 수집된 비기술적 사이버위협정보의 경우는 공유 가능할 것으로 판단된다. 또한 국가정보기관에서는 민간기관이 주도권을 보유한 사이버위협정보를 지속적으로 수용할 수 있는 방안들이 마련되어야 한다. 이를 통해 국가정보기관은 전국가적인 사이버위기에 보다 효과적으로 대응할 수 있는 능력을 보유하게 되며 국가정보기관의 사이버위협정보 수집에 관한 긍정적인 여론 형성도 기대해 볼 수 있다.



[Fig. 3] Cyber threat intelligence sharing model

그러나, 현재 발의된 「국가사이버안보법(안)」에서와 같이 사이버위협정보가 국정원에서 독점되고 국가적으로 환류되지 않는 부작용을 예방하기 위해서는 청와대 국가안보실(사이버안보비서관) 등의 기관에서 사이버위협정보공유센터의 역할을 정기적으로 감독하고 이를 개선 및 발전시킬 역할을 부여하는 것이 검토되어야 한다.

5. 결론

사이버위협정보는 정보가 유통되는 매체의 특성상 국가와 민간의 정보역전현상이 발생할 수 있다. 이를 극복하기 위하여 세계적으로 법령제정과 범정부적인 거버넌스 형성 등과 같은 다양한 노력을 기하고 있으며 국내에서도 효과적인 사이버 위기 대응을 위한 정보공유 측면의 노력을 기울여 왔다. 하지만 국내에서 추진된 다양한 노력들은 국가정보기관의 사이버위협정보 수집 측면의 권한을 부여하는데 집중하고 있는데 비해 이러한 정보를 국내 유관기관에 제공하고 공유하는 역할은 아직 미흡한 실정이다.

이와 관련하여, 본 논문에서는 정보역전현상을 설명하기 위해 사이버위협정보를 정의함과 동시에 그 특성을 다른 정보 유형들과 비교분석하였다. 또한 정보역전현상을 극복하기 위한 각국의 노력을 조사하였고, 이를 참고하여 우리나라에 필요한 사이버위협정보 공유모델을 제안하였다. 제안된 모델과 같이 국가정보기관의 사이버위협정보 수집에 대한 명분을 강화하기 위해서는 자체적인 정보 수집 뿐 아니라, 민간 및 공공 분야에서 사이버위협정보를 보다 원활하게 수집할 수 있게 해주는 다양한 노력들을 함께 병행함으로써 국가정보기관의 필요성을 부각시킬 필요가 있음을 언급하였다.

본 논문에서는 사이버위협정보의 공유에 있어서 국정원의 역할을 중심으로 그 내용들을 기술하였다. 향후 연구에서는 국정원을 포함한 여러 국가정보기관들의 역할을 면밀히 분석하여 국가적 사이버 위기에 보다 성공적으로 대응할 수 있는 통합적인 사이버위협정보 모델 개발에 관한 연구를 진행하고자 한다.

REFERENCES

[1] H. Rha and H. Chung, “A Theoretical Comparative Study of Human Resource Security Based on Korean and Int’l Information Security Management Systems,” Journal of Convergence for Information Technology, Vol. 6, No. 3, pp. 13-19, 2016.

[2] M. Gu and Y. Li, “A Study of Countermeasures for Advanced Persistent Threats attacks by malicious code,” Journal of Convergence for Information

Technology, Vol. 5, No. 4, pp. 37-42, 2015.

[3] D. T. Kuehl, "From cyberspace to cyberpower: Defining the problem," In F. Kramer, S. Starr, & L. K. Wentz (Eds.), Cyberpower and national security, pp. 24 - 42, Washington, DC: National Defense University Press, 2009.

[4] K. Lee, "Cyber security strategies for world and security policy direction for Korea - focused on U.S.A.," ICT & Media Policy, Vol. 23, No. 16, pp. 1-27, 2011.

[5] O. S. Saydjari, "Cyber Defense: Art to Science," Communications of the ACM, Vol. 47, No. 3, pp. 53-57, 2004.

[6] T. Ring, "Threat intelligence: why people don't share," Computer Fraud and Security, Vol. 2014, No. 3, pp. 5-9, 2014.

[7] R. McMillan, "Definition: Threat intelligence," Gartner, 2013, https://www.gartner.com/doc/ 2487216/definition -threat-intelligence

[8] Joint Chief of Staff, Joint Publication 2-0, Joint Intelligence, US DoD, 2013, http://www.dtic.mil/ doctrine/new_pubs/jp2_0.pdf

[9] P. Duvenage and S. Solms, "Putting Counterintelligence in Cyber Counterintelligence: Back to the Future," In proceedings of 13th European Conference on Cyber Warfare and Security, Piraeus, Greece, July, 2014.

[10] J. Verble, "The NSA and Edward Snowden: surveillance in the 21st century," ACM SIGCAS Computers and Society, Vol. 44, No. 3, pp. 14-20, 2014.

[11] National Security Agency, XKeyscore: NSA tool collects 'nearly everything a user does on the internet', 2008, https://www.theguardian.com/world /2013/jul/31/nsa-top-secret-program-online-data

[12] National Security Agency, Peeling back the layers of Tor with EgotisticalGiraffe, 2007, https:// www.theguardian.com/world/interactive/2013/oct/ 04/egotistical-giraffe-nsa-tor-document

[13] Congress.gov, H.R.234 - Cyber Intelligence Sharing and Protection Act, 114th Congress, 2015, https://www.congress.gov/bill/114th-congress/hous e-bill/234

[14] Congress.gov, S.754 - Cybersecurity Information Sharing Act of 2015, 114th Congress, 2015. https://www.congress.gov/bill/114th-congress/sena te-bill/754

[15] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," Technical report, NIST, 2016.

[16] Information-Technology Promotion Agency, Initiative for cyber security information sharing partnership of Japan (J-CSIP), Annual Activity Report FY2012, https://www.ipa.go.jp/files/0000 32417.pdf

[17] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/

[18] European Union Agency for Network and Information Security, https://www.enisa.europa. eu/

[19] National Assembly, 『National Cyber Security Management Act』, 2005.

[20] Korea Communications Commission, 『Compre- hensive National Cyber Crisis Plan』, 2009.

[21] Ministry of Science, ICT and Future Planning, 『Comprehensive National Cyber Security Plan』, 2013.

[22] National Assembly, 『Legislative Bill for Cyber Threat Intelligence Sharing』, 2015.

[23] National Assembly, Korea Ministry of Government Legislation, 『Legislative Bill for National Cyber Terror Prevention』, 2016.

[24] National Assembly, 『Legislative Notice: A Fundamental Law for the National Cyber Security 』, 2016.

[25] J. Kim, "National information security agenda and policies," Journal of Digital Convergence, Vol. 10, No. 1, pp. 105-111, 2012.

[26] K. Lee, "Analysis of Threats Factor in IT Convergence Security," Journal of the Korea Convergence Society, Vol. 1, No. 1, pp. 49-55, 2010.

[27] H. Lee, O. Na, S. Sung, and H. Chang, "A Design on Security Governance Framework for Industry Convergence Environment," Journal of the Korea Convergence Society, Vol. 6, No. 4, pp. 33-40, 2015.

김 대 건(Kim, Daegeon)

・2008년 2월 : 육군사관학교 컴퓨터과학과(이학사)
・2012년 7월 : 미. 서던 캘리포니아대학교 컴퓨터과학과(공학 석사)
・2015년 9월 ~ 현재 : 고려대학교 정보보호대학원 정보보호학과 박사과정
・관심분야 : 정보보안, 사이버위협정보, 머신러닝
・E-Mail : dgkim0803@korea.ac.kr

백 승 수(Baek, Seungsoo)

・2002년 3월 : 육군사관학교 전산학과(이학사)
・2007년 9월 : Naval Postgraduate School(전산학 석사)
・2012년 9월 ~ 현재 : 고려대학교 정보보호대학원 정보보호학과 박사수료
・관심분야 : 정보보안, 사이버전, 사이버 정책
・E-Mail : offident79@korea.ac.kr

유 동 희(Yoo, Donghee)

・2002년 8월 : 고려대학교 MIS(경영학사)
・2009년 2월 : 고려대학교 일반대학원 경영학과 MS/IS(경영학 박사)
・2009년 6월 ~ 2013년 5월 : 육군사관학교 전자정보학과 조교수
・2014년 2월 ~ 2015년 2월 : 연세대학교 정보통신기술연구원 연구교수
・2015년 3월 ~ 현재 : 경상대학교 경영정보학과, 부교수
・관심분야 : 정보보안, 지능형웹, 경영정보시스템
・E-Mail : dhyoo@gnu.ac.kr