韓國IT서비스學會誌
第15卷 第1號
2016年 3月, pp.67-79

Journal of Information Technology Services
http://dx.doi.org/10.9716/KITS.2016.15.1.067

# 북한의 사이버공격과 대응방안에 관한 연구

정민경* · 임종인** · 권헌영***

# A Study on North Korea's Cyber Attacks and Countermeasures

Min Kyung Chung* · Jong In Lim** · Hun Yeong Kwon***

■ Abstract ■

This study aims to present the necessary elements that should be part of South Korea's National Defense Strategy against the recent North Korean cyber-attacks. The elements proposed in this study also reflect the recent trend of cyber-attack incidents that are happening in the Unites States and other countries and have been classified into the three levels of cyber incidents: cyberwarfare, cyberterrorism and cybercrime. As such, the elements proposed are presented in accordance with this classification system.

In order to properly take into account the recent trend of cyber-attacks perpetrated by North Korea, this paper analyzed the characteristics of recent North Korean cyber-attacks as well as the countermeasures and responses of South Korea. Moreover, by making use of case studies of cyber-attack incidents by foreign nations that threaten national security, the response measures at a national level can be deduced and applied as in this study. Thus, the authors of this study hope that the newly proposed elements here within will help to strengthen the level of Korea's cyber security against foreign attacks, specifically that of North Korea such as the KHNP hacking incidents and so on. It is hoped that further damage such as leakage of confidential information, invasion of privacy and physical intimidation can be mitigated.

Keyword : North Korea, DPRK(Democratic People's Republic of Korea), Cyber Attacks, SPE(Sony Pictures Entertainment) Hacking, Cyber Attacks on Estonia, Stuxnet, KHNP(Korea Hydro & Nuclear Power Plant) Hacking

Submitted : December 29, 2015 1st Revision : January 6, 2016 Accepted : January 8, 2016

* 고려대학교 일반대학원 사이버국방학과 석사과정
** 고려대학교 정보보호대학원 교수
*** 고려대학교 정보보호대학원 부교수, 교신저자

# 1. 서 론

정보화사회가 고도화됨에 따라 현대사회는 정보통신기술로 인해 편리해지고 복잡해졌다. 컴퓨터와 인터넷이 점차 발전함에 따라 네트워크를 통한 사이버공격의 위협은 점차 증가하고 있으며, 사이버공격으로 인한 피해도 증가하고 있다. 한국은 2009년 7.7 사이버테러, 2011년 3.4 사이버테러와 농협 해킹사건, 2012년 7.7 사이버테러 등 북한으로부터 대규모 사이버공격을 당해오고 있다.

2014년 12월엔 한국수력원자력이 해킹되어 개인용 컴퓨터(PC) 8대 감염 및 5대 하드디스크 초기화, 한수원 임직원 정보 및 원전 관련 정보 공개, 시민을 인질로 한 사회불안 야기 등의 피해를 발생시켰다. 해커는 총 10회에 걸쳐 122건의 문서를 인터넷상에 공개하며 협박과 심리전을 병행했다. 정부합동수사단은 북한소행으로 발표하고 수사를 종결했다.

사이버공격이 사이버공간에 국한되지 않고 실질적으로 피해를 끼치는 사건들은 우리나라 외에도 전 세계적으로 발생하고 있다. 본 논문에서는 해외 국가들이 국가안보를 위협하는 사이버공격에 대한 대응사례를 분석하여 한국의 사이버공격에 대한 대응전략을 제시하고자 한다. 해외의 사례로는 미국의 소니 해킹사건, 북대서양조약기구(NATO)의 에스토니아 해킹사건, 마지막으로 이란의 스턱스넷(Stuxnet) 사건을 살펴볼 것이다.

논문의 구성은 다음과 같다. 제 2장에서는 사이버공격의 정의와 북한 사이버공격의 특징, 그리고 한국의 북한 사이버공격에 대한 대응조치를 살펴본다. 제 3장에서는 미국의 소니 해킹사건과 미국의 대응사례, 북대서양조약기구의 에스토니아 사건과 북대서양조약기구의 대응사례, 이란의 스턱스넷 사건과 이란의 대응사례를 살펴볼 것이다. 제 4장에서는 사이버공격에 대한 한국의 국가적 대응전략을 제시하고 제 5장에서 결론을 정리한다.

# 2. 북한의 사이버공격과 한국의 대응조치

## 2.1 사이버공격의 정의

### 2.1.1 사이버전쟁

사이버전쟁(Cyber warfare)에 해당하려면 사이버공격을 국가가 수행하거나 국가의 지원을 받아야하며(Kwon, 2015), 사이버공격의 수준이 전통적인 의미에서의 무력공격에 해당하거나 무력충돌의 상황에서 발생했을 경우에만 사이버전쟁에 해당한다고 볼 수 있다(Hathaway et al., 2012). 무력사용과 자위권의 발동에 관한 사항은 현 국제법상 유엔헌장(United Nations Charter)에 규정되어 있으며, 어느 정도의 수준이 사이버공간에서 무력사용에 해당하는지는 국제적인 합의가 필요하다(Hoisington, 2009). Schmitt(2013)은 사이버공간에서의 국가가 무력을 행사하는 경우에 대한 국제법(Jus ad bellum)과 무력충돌행위를 규율하는 국제법 또는 전쟁법(Jus in bello)에 대한 적용방안을 제시하였으며, 국제인도법, 헤이그조약, 관습법 등 기존의 국제법들을 사이버공간에서 어떻게 적용할 것인지에 대해서도 학술적으로 논의되고 있다(Schaap, 2009; Kelsey, 2008). 사이버전쟁에 관한 대부분의 자료들은 사이버범죄를 다루지 않는데, 그 이유는 군사적인 문제이거나 법집행과 관련된 문제 때문이며 사이버전쟁과 사이버범죄는 서로 다른 기관에서 담당한다(Carr, 2011).

### 2.1.2 사이버테러

사이버테러(Cyber terrorism)는 컴퓨터의 이용을 통한 테러리즘의 수행이라고 볼 수 있는데(Ember-Seddon, 2006), 테러리즘에 관한 국가들의 법률상의 정의를 보면 '정치적인, 종교적인 또는 이념적인 동기를 가지고 국민 또는 정부를 강요하거나 공포를 조장하기 위해 민간에 가하는 폭력'이라는 내용을 공통적으로 포함하고 있다는 것을 알 수 있다(Golder and Williams, 2004). 따라서

사이버테러란 "사이버공간에서 정치·종교·사상의 목적을 가지고 집단 혹은 불특정 일반대중에게 사회적 공포심이나 불안감을 조성하기 위해 의도되거나 계획된 행위"라고 정의할 수 있다(Park, 2014). 핵티비즘(Hacktivism)은 사이버테러와 마찬가지로 정치적인 목적을 위해 수행되지만 민간에 대한 직접적인 피해를 동반하지 않는다는 점에서 사이버테러와 구분된다(Weimann, 2004). 또한 사이버테러는 정치적인 영향을 미치기 위한다는 목적을 가진다는 점에서 사이버범죄와 구별된다(Stohl, 2006). 일국은 사이버범죄와 사이버테러에 대한 대응을 구분할 필요가 있다(Brenner, 2007). 법률적인 차원에서 사이버테러리즘은 대부분 국내법을 적용하지만, 국제적인 법률을 적용해야 하는 상황도 분명히 존재한다(Young, 2006).

#### 2.1.3 사이버범죄

사이버범죄(Cyber crime)는 컴퓨터범죄(Computer crime)를 대체한 용어로써 컴퓨터와 기술과 연관된 모든 범죄들을 포함한다(Moore, 2010). 사이버범죄의 유형을 분류할 때 '컴퓨터를 대상으로 한 범죄', '컴퓨터를 이용한 범죄', 그리고 '컴퓨터 안에서의 범죄'로 구분하는 경우가 많은데(Fafinski et al., 2010), 일반범죄와 유사한 범죄유형과 컴퓨터로 인해 새롭게 생긴 범죄유형을 구분하여 분류하면 '컴퓨터의 무결성에 대한 범죄', '컴퓨터를 활용한 범죄', '컴퓨터 콘텐츠에 대한 범죄'로 구분할 수 있다(Wall, 2007). 사이버범죄는 일반범죄와 비슷한 면도 있지만 고유의 특수성을 갖기 때문에 기존의 일반범죄이론을 적용가능한지 여부에 관해 논란이 있으며, Yar(2005)는 사이버범죄가 일반범죄이론과 비슷한 점과 고유한 특수성을 갖는다는 특징을 보여주며 사이버범죄를 일반범죄이론만으로 다루기에는 한계가 있음을 설명한다. <Table 1>은 사이버공격이 분류되는 사이버전쟁, 사이버테러, 그리고 사이버범죄의 유사점과 차이점을 보여준다.

〈Table 1〉 Taxonomy of Cyber Attacks

| | Cyber warfare | Cyber terrorism | Cyber crime |
|---|---|---|---|
| Entity | State actor | Non-state actor | Non-state actor |
| Target | Nation | Civilians | Civilians |
| Motive | National interest | Political aim | Personal profit |
| Applicable law | International | International/ Domestic | Domestic |

### 2.2 북한 사이버공격의 특징

#### 2.2.1 공격대상

북한의 사이버공격은 2000년도 초기엔 개인용 컴퓨터(PC) 및 웹사이트를 중심으로 한 공격이 이뤄졌었는데, 2011년부터 금융사 및 언론사의 전산시스템을 공격하는 사이버공격들이 발생했으며, 2014년도 후반에는 국가사회기반시설을 대상으로 한 공격이 발생했다. 2004년 국가 및 공공기관 전산망 해킹사건, 2006년 한국 국방부 및 미국 국방성 해킹사건, 2009년 7.7 디도스 공격, 2011년 3.4 디도스 공격 사건들은 공공기관과 민간기관의 웹사이트를 공격한 사건들이다. 금융사 및 언론사를 대상으로 한 공격은 2011년 농협 전산망 해킹사건, 2012년 중앙일보 해킹사건, 2013년 3.20 사이버테러, 2014년 9.25 디도스 공격 등이 있다. 2014년 12월에는 한국수력원자력발전소가 해킹되어 원전 관련 기밀자료 유출, 한수원 임직원 개인정보 유출, 원전 가동중지 협박 등 기반시설을 대상으로 공격이 발생했다.

#### 2.2.2 공격방법

북한의 사이버공격 방법은 바이러스와 해킹을 이용한 공격방식에서 디도스 공격방식으로, 그리고 지능형지속위협(Advanced Persistent Threat) 공격방식으로 발전한다. 북한은 2009년 7.7 디도스 공격사건, 2011년 3.4 디도스 공격사건, 2014년 9.25 디도스 공격사건에서 디도스 공격방식을 사용하였다. 북한이 처음으로 지능형지속위협 공격방식을 사용한 것은 2011년 4월 농협은행 해킹사건 때이며(Lee et al., 2015), 2012년 중앙일보 해킹사건, 2013년 3.20 사이버테러 및 6.25 사이버테러에서 지능형지속위협 공격방식을 사용하였다.

### 2.2.3 공격목적

북한 사이버공격의 목적은 크게 정치적인 목적, 기밀정보 취득, 금전적인 이익으로 구분된다. 1.25 인터넷 대란, 국가 및 공공기관 전산망 해킹, 7.7 디도스 공격, 3.4 디도스 공격, 위성위치파악시스템(GPS) 교란, 중앙일보 해킹, 3.20 사이버테러, 6.25 사이버테러, 9.25 디도스 공격, 한수원 해킹사건은 사회혼란유발 등 정치적인 목적에 의해 발생한 공격이다. 그리고 군사기밀정보, 기업기밀정보 등 기밀정보 취득이 목적인 공격들이 있으며, 금전적인 이익을 위한 공격들도 존재한다. <Table 2>는 북한 사이버공격의 공격대상, 공격방법, 공격목적을 보여준다.

## 2.3 사이버공격에 대한 한국의 대응조치

### 2.3.1 정책적 대응조치

한국은 사이버공격에 대한 정책적 대응조치로 2009년 범정부 사이버위기 종합대책, 2011년 국가 사이버안보 마스터플랜, 2013년 국가 사이버안보 종합대책, 2014년 국가 사이버안보 태세 강화 대책을 발표했다. 7.7 디도스 공격, 3.20 사이버테러, 한수원 해킹사건 등 대규모 사이버공격 사건이 발생한 후 종합대책을 발표하였다.

〈Table 2〉 Characteristics of North Korea Cyber Attack

| Date | Incident Name | Targets | Means | Motive |
|---|---|---|---|---|
| 2003-01-25 | 1.25 Internet chaos | KT telephone company | Slammer worm | Political aim |
| 2004-07-13 | National · public organizations hacking | National · public organizations's PC | Malicious code | Political aim |
| 2006-07 | Korea MND, U.S. DoD hacking | Korea MND, U.S. DoD | Malicious code | Confidential information |
| 2008-09 | Korea military officer targeted trojan horse mail sending | Army colonel | Malicious code | Confidential information |
| 2009-03-05 | Korea military chemical weapon information hacking | Third republic of Korea Army headquarters | Malicious code | Confidential information |
| 2009-07-07 | 7.7 DDoS attack | U.S, ROK's public institutions, press, firms, banks, portals | DDoS | Political aim |
| 2009-12 | Leakage of military operation 5027 | Military system | Hacking | Confidential information |
| 2011-03-04 | 3.4 DDoS attack | NIS and the Blue House | DDoS | Political aim |
| 2011-04-12 | DDoS attacks on Nonghyup bank | Nonghyup bank | APT | Political aim |
| 2011-05-30 | Military academy reunion site hacking | Military academy man | Malicious code | Confidential information |
| 2011-11-06 | Korea university email hacking | Korea university email system | Malicious code | Confidential information |
| 2011-08-04 | Game company hacking and auto program production by north korean hacker | Lineage game, dungeon and fighter, maple story etc. | Malicious code | Monetary profit |
| 2010-2012 | GPS jamming | GPS receiver | GPS jamming | Political aim |
| 2012-06-09 | Joongang daily intranet hacking | Joongang daily | APT | Political aim |
| 2012-06-28 | Spread of malicious codes from North Korea's general bureau of reconnaissance | Computer games | Malicious code | Monetary profit |
| 2013-03-20 | 3.20 Cyber-terror | Broadcasting · financial companys | APT | Political aim |
| 2013-06-25 | 6.25 Cyber-terror | National computing and information agency | APT | Political aim |
| 2013-10-16 | S corporation hacking through foreign branch | S corporation | Liaison with insider | Confidential information |
| 2014-09-25 | 9.25 DDoS attack | Finance · press · education · medical · shopping etc | DDoS | Political aim |
| 2014-12-15 | Korea Hydro & Nuclear Power Co. hacking | Korea Hydro & Nuclear Power Co. | Malicious code | Political aim |
| Characteristics | | 1. PC/websites<br>2. Finance·press companies<br>3. National infrastructure | 1. Malicious code<br>2. DDoS<br>3. APT | 1. Confidential information<br>2. Political aim<br>3. Monetary profit |

### 2.3.2 실무적 대응조치

사이버공격에 대한 실무적 대응조치로는 백신프로그램 설치, 방화벽 설치 등 기술적인 조치와 노트북 보안관리, 비밀번호 변경 등 관리적인 조치를 취하였다. 또한 디도스 공격 대피소 구축, 디도스 대응인력 보강 등 디도스 공격에 대비한 대응전략을 확대하였다. 그로 인해 2009년 7.7 디도스 공격 사건 때보다 2011년 3.4 디도스 공격에서 피해 규모를 대폭 줄일 수 있었다.

### 2.3.3 외교적 대응조치

한국은 2004년 국가 및 공공기관 전산망 해킹사건 때는 중국에 공동수사를 요청하였고, 2014년 12월 한수원 해킹사건이 발생했을 당시에도 미국, 중국, 일본, 태국 등 경유지 국가들과 국제 공조수사를 추진했지만 성과를 보지 못했다. 2010년부터 2012년 사이에 북한이 위성위치확인시스템 수신기를 교란시켰을 때는 항의서한을 북측에 전달하기도 하였다. <Table 3>은 북한의 사이버공격에 대한 한국의 대응조치를 나타낸다.

〈Table 3〉 Korea's Response Action Against North Korea's Cyber Attacks

| Date | Incident Name | Politic Action | Practical Action | Diplomatic Action |
|---|---|---|---|---|
| 2004-07-13 | National · public organizations hacking | - | Blocking IP stopover, anti-virus programs installation | Requesting assistance in criminal investigation to Chinese Ministry of Foreign Affairs, propel investigation cooperation with Police, Interpol, the Chinese Ministry of Public Security |
| 2009-03-05 | Korea military chemical weapon information hacking | - | Firewall installation, extensive security checks, etc. | - |
| 2009-07-07 | 7.7 DDoS attack | A comprehensive government-wide cyber-crisis measures | Building DDoS attack shelters, offer free vaccines | - |
| 2011-03-04 | 3.4 DDoS attack | National cyber security master plan | DDoS response personnel reinforcement, investment expansion, etc. | - |
| 2011-04-12 | DDoS attacks on Nonghyup bank | - | Strengthening management by laptop security management, administrator password changes, etc. | - |
| 2011-08-04 | Game company hacking and auto program production by north korean hacker | - | Cracking down illegal program | - |
| 2010-2012 | GPS jamming | - | - | Delivering protest letter from the Korea Communications Commission to North Korea |
| 2012-06-09 | Joongang daily intranet hacking | - | - | Criticizing a hacker through a newspaper |
| 2013-03-20 | 3.20 Cyber-terror | Comprehensive national cyber security measures | Information Security Management System (ISMS) response system, APT corresponding solutions, etc. | - |
| 2013-06-25 | 6.25 Cyber-terror | | | - |
| 2013-10-16 | S corporation hacking through foreign branch | - | Scrutinizing military computer system | - |
| 2014-09-25 | 9.25 DDoS attack | - | Changing DNS recursion query settings | - |
| 2014-10-29 | North Korea smartphone hacking | - | Blocking hacking stopover, antivirus updates | - |
| 2014-12-15 | Korea Hydro & Nuclear Power Co. hacking | Strengthening national cyber security measures | - | Requesting assistance in criminal investigation to United States, China, Japan, Thailand, Netherlands, etc. |
| Characteristics | | Announce comprehensive measures after large-scale cyber attacks | Minimize damage from DDoS attacks due to DDoS confrontational strategy | No cases international cooperation investigations success |

# 3. 사이버공격에 대한 국제적 대응 사례

## 3.1 미국

### 3.1.1 소니 해킹사건

소니 해킹사건은 미국의 소니 픽쳐스 엔터테인먼트사가 해킹되어 소니 임직원 및 할리우드 영화배우 등 4만 7천 명의 개인정보가 유출되고 '퓨리', '애니', '스틸 앨리스', '미스터 터너' 등 미개봉영화를 포함한 영화 5편이 온라인 사이트에 유포되어 100만 건 이상의 불법다운로드가 발생한 해킹사건이다. 또한 해커는 김정은 북한 제 1비서의 암살내용이 포함되어 있는 영화인 '인터뷰(The interview)'의 상영을 중단할 것을 소니사에 요구하며 911테러를 기억하라고 언급하면서 물리적인 테러위협을 하였다(Haggard, 2015). 이 사건은 미국 헌법이 규정하고 있는 표현의 자유를 침해하였다는 연유로 미국 연방수사국(FBI)이 수사를 담당하였으며 조사결과 북한소행이라고 발표하였다.

### 3.1.2 미국의 대응조치

3.1.2.1 한국과 악성코드 관련 정보 공유

미국 연방수사국은 소니 해킹사건을 북한소행으로 발표한 근거로 ①2013년 한국의 3.20 사이버테러와 6.25 사이버테러 사건 당시 사용된 악성코드와 유사한 점, ②소니 해킹사건에서 쓰인 악성코드와 북한 관련 인터넷 프로토콜(IP)이 교신한 점을 근거로 들었다.

3.1.2.2 금융제재 행정명령 발표

2015년 4월 2일, 오바마 대통령은 사이버공격을 시도한 개인과 단체에게 자산동결 및 은행접근을 제한하는 행정명령(Executive order)을 발표하였다. 제재 대상은 미국에 대한 사이버위협 활동에 직간접적으로 가담하거나 책임이 있는 사람 및 단체로, 외국에 거주하고 있는 자 또는 외국에 거주하고 있는 자로부터 지시를 받는 국내 거주자 및 단체라고 규정하였다. 제재 행위는 주요 국가기반시설을 지원하는 조직의 컴퓨터 및 컴퓨터 네트워크를 공격하거나, 서비스 제공을 방해하는 모든 행위로 규정하고 있다. 해당 행정명령을 통해 미 재무부는 필요하다고 판단될 경우 미국 기업 등을 공격한 외국의 국가나 개인, 기업 등을 대상으로 강도 높은 금융제재를 할 수 있게 된다.

3.1.2.3 국내 사이버 위협정보 공유 법안 통과

2015년 2월 오바마 대통령은 사이버 위협정보통합센터(Cyber Threat Intelligence Integration Center) 설립을 승인하고 정부기관과 민간부문 간 사이버보안 위협과 관련된 정보공유를 촉진하는 행정명령 제13691호를 발표하였다. 또한 2015년 12월 18일 오바마 대통령은 '사이버보안 정보공유법(CISA : Cybersecurity Information Sharing Act)'에 서명하였고, 법안이 발효되었다. 업체가 사이버보안, 테러, 범죄 등의 위협에 대해 정부기관과 정보를 공유한다는 내용을 담고 있다. 정보를 공유한 업체는 해킹사건에 대해 면책권을 주는 내용을 포함하고 있으며, 정보를 공유하지 않고 사건이 발생했을 경우 책임을 물을 수 있다는 내용도 포함한다.

## 3.2 북대서양조약기구

### 3.2.1 2007년 에스토니아 사건

에스토니아는 온라인상에서 세금을 신고하고 휴대전화로 쇼핑과 주차요금 지불을 할 만큼 인터넷 강대국이었다(Shackelford, 2009). 2007년 4월, 에스토니아에서는 구소련 지배 시절에 세워졌던 소련군 군인의 동상을 철거하는 문제로 러시아계 시민들이 격렬한 시위를 벌이는 중이었고, 유혈사태까지 발생한 상황에서 100만대 이상의 좀비 PC가 동원되어 대통령궁을 비롯한 행정부 · 의회 · 정당 · 언론 · 은행 등의 사이트와 전산망에

피해가 발생했다(Son, 2013). 에스토니아의 침해사고대응팀(Computer Emergency Response Team)은 수사결과 인터넷 프로토콜(IP) 주소와 러시아어로 쓰여진 블로그 등 러시아인에 의한 소행이라는 증거를 발견했으며(Evron, 2008), 에스토니아 정부는 러시아를 범인으로 지목하였으나 러시아 정부는 책임을 거부했다(Lesk, 2007).

#### 3.2.2 북대서양조약기구의 대응조치

3.2.2.1 사이버상의 교전규칙 출간

북대서양조약기구는 사이버방어센터(Cooperate Cyber Defence Centre of Excellence)를 탈린에 세우고 마이클 슈미트(Michael Schmitt) 교수를 비롯한 25명의 국제법 관련 전문가를 소집하여 3년 간 논의하여 '탈린매뉴얼(Tallinn Manual)'이라는 사이버 교전수칙을 출간했다. 해당 연구에는 미국, 영국, 독일 및 캐나다의 군사교본이 참조되었으며, 미국 사이버사령부(United States Cyber Command), 국제적십자위원회(International Committee of the Red Cross), 북대서양조약기구가 연구에 참가하였다. 내용은 만장일치로 합의된 95개의 규칙과 각 규칙에 대한 주석으로 구성되어 있으며, 사이버공간에서의 주권과 국가책임, 무력사용과 자위권 등의 내용을 다루는 국제사이버안보법과 무력충돌, 교전규칙 등의 내용을 담고 있는 사이버 무력충돌법으로 구분되어 있다(Schmitt, 2013). 무력충돌에 이르지 않는 평시에 적용 가능한 탈린매뉴얼 두 번째 버전도 논의 중에 있다.

3.2.2.2 사이버안보 컨퍼런스 주최

북대서양조약기구의 사이버방어센터는 에스토니아의 수도인 탈린에서 2013년부터 매년 사이버안보 컨퍼런스인 '사이콘(CyCon)'을 주최하고 있다. 사이콘은 세계 최고 수준의 사이버안보 컨퍼런스로 자리매김하고 있으며, 정책・전략・법・기술 등 다양한 분야의 연구를 다룬다(Son, 2013).

### 3.3 이란

#### 3.3.1 2010년 스턱스넷 사건

스턱스넷은 미국과 이스라엘이 이란의 핵시설을 파괴하기 위해 제작한 사이버무기이다. 미국과 이스라엘은 2009년에서 2010년에 합동으로 스턱스넷이라는 웜을 개발하여 인도, 인도네시아, 중국 등 전 세계 60,000대의 컴퓨터를 감염시켰으며, 그 중 반 이상이 이란에서 발견되었다(Farwell and Rohozinski). 스턱스넷은 국가의 산업 및 주요기반시설에 주로 사용되는 감시 제어 데이터 수집 시스템(Supervisory Control And Data Acquisition system)을 감염시키며, 감시 제어 데이터 수집 시스템은 인터넷에 연결되어 있지 않기 때문에 플래시 드라이브(Flash drive)를 통해 스턱스넷의 최초 감염이 시작되었을 것으로 추정된다(Chen and Abu-Nimeh, 2011).

#### 3.3.2 이란의 대응조치

3.3.2.1 사이버공간최고위원회 발족

이란에서 사이버공간을 다루는 가장 높은 정부기관은 사이버공간최고위원회(High Council of Cyber-space)로, 이 조직이 2012년에 설립된 이후로 사이버작전과 연관된 다른 모든 기관들이 이 기관의 정책을 실현하기 위해 움직인다. 대통령, 사법부와 국회의장, 국영 라디오-텔레비전의 장, 이란혁명수비대(The Islamic Revolution Guards Corps)와 경찰의 최고사령관, 정보요원, 통신, 문화, 과학의 장관들 등 최고 관계자들로 구성되어 있다(Cordesman and Gold, 2014).

3.3.2.2 사이버방어/역공격능력 강화

이란은 미국과 이스라엘의 사이버공격을 계기로 내부전산망과 주요 인프라시설에 대한 사이버보안을 강화했다. 사이버공간 최고위원회를 출범시킨 이후로 이란의 사이버전 수행 역량이 급성장했는데, 사이버공간최고위원회는 이란의 전산망 방어를 관장하고 미국이나 이스라엘과 같은 적대국의 사이버공격에 대응하며, 상황에 따라서는 역침투하는 업무를 수행한다.

〈Table 4〉 Each Countries's National Responses

| | USA | NATO | Iran |
|---|---|---|---|
| Cyber warfare | | - Held 'Cycon'<br>- Published 'Tallinn Manual'<br>- Accused the International Court of Justice | |
| Cyber terrorism | - Sharing malware-related information with ROK<br>- Pass domestic cyber threat information sharing legislation | | |
| Cyber crime | - Accedes to Cybercrime Convention | | - Established the Supreme Council of Cyberspace |

# 4. 국가적 대응전략 제언

## 4.1 사이버전쟁 차원의 대응전략

### 4.1.1 사이버공격 방지를 위한 국제규범 제정

북대서양조약기구의 사이버방어센터에서 발간한 탈린매뉴얼처럼 사이버공격을 억지하기 위한 국제규범을 제정해야 한다. 탈린매뉴얼은 북대서양조약기구를 포함한 일부 국가에서만 검토가 이루어졌으며 완전한 합의를 이르지도 못하였다. 국제적 차원에서 합의가 이루어진 사이버공격을 금지하는 규범을 만들 필요가 있으며, 무력사용의 한계점을 넘은 행위에 대한 규제뿐만 아니라 그 수준을 넘지 않는 공격을 포괄할 수 있는 규제 제정이 필요하다. 이는 공격국가로 식별된 국가에 도덕적 비난을 제공하는 근거가 될 것이다.

### 4.1.2 사이버안보 컨퍼런스 주최

에스토니아의 수도 탈린에서 열리는 사이버안보 컨퍼런스 사이콘은 국제 컨퍼런스로 입지를 구축하였다. 한국은 아 · 태지역과 유럽지역 그리고 국제기구 등 36개 국가 또는 기구의 차관급 국방관료와 석학들이 참가하여 안보현안에 대해 토의하는 '서울안보대화(Seoul Defense Dialogue)'를 개최하고 있으며, 사이버는 일부 세션의 형태로 포함되어 있다. 사이버안보 컨퍼런스의 주최는 사이버안보 역량을 강화하며 한국의 국제적 위상도 높일 것이다.

### 4.1.3 국제사법재판소 회부

북한의 사이버공격을 귀속시키기 위해서 국제사법재판소에 기소하는 방법도 있다. 네덜란드 헤이그에 있는 국제사법재판소(International Court of Justice)는 1986년 6월 27일 '니카라과에 대한 군사적, 준군사적 활동'(니카라과 vs 미국) 사건에 대해 "미국은 다른 나라에 무력을 사용해서는 안 된다는, 다른 나라의 국내 문제에 개입해서는 안 된다는, 그리고 다른 나라의 주권을 침범해서는 안 된다는 국제법상의 의무를 위반했다."라고 판결했다. 미국의 국제법 위반을 판결내리며 미국이 니카라과에 손해배상금을 지불할 것을 포함하였다. 북한을 국제사법재판소에 기소하는 것은 향후 북한발 사이버테러의 심각성에 대한 여론을 환기시키고 북한 사이버테러를 국제사회 담론으로 끌어들이는 계기를 마련한다는 점에서 의미가 있을 것이다. 국제사법재판소 회부와 관련해서는 개인 차원에서 진행하기에는 어려움이 있으므로 국가차원의 조직구성 및 예상편성의 필요성이 제기된다.

## 4.2 사이버테러 차원의 대응전략

### 4.2.1 국가사이버안전에 관한 총괄 입법체계 구성

한국은 국가사이버안보 종합대책에 따라 청와대를 컨트롤타워로 지정하고 국가 · 공공분야는 국정원, 민간분야는 한국인터넷진흥원, 국방분야는 국방부가 담당하는 체제를 택하고 있다. 이란은 사이버

공간최고위원회를 중심으로 사이버방어능력 및 공격능력을 성장시켰으며 사이버전 역량을 강화하였다. 우리나라는 대통령 훈령으로 중앙행정기관과 국정원 등의 역할과 의무 사항만을 규정한 상태이며, 국가 사이버안전에 관한 총괄 입법체계가 부재한 상태라고 할 수 있다(Kwon, 2015). 효과적이고 체계적인 사이버안전 대응체계를 구축하려면 국가사이버안전에 관한 총괄 입법체계를 구성해야 한다.

#### 4.2.2 복원력 중심의 연구개발 수행

사이버공간의 특성상 사이버공격의 발원지를 찾아 특정 국가나 단체에 귀속시키기에 어려움이 따른다. 따라서 사이버공격의 주체를 식별하기 어렵다면 사이버공격의 주체와 상관없이 피해를 최소화하여 회복력을 강화하는 복원력 중심의 연구개발이 수행되어야 한다. 미국 국방부 산하 방위고등연구계획국(Defence Advanced Research Projects Agency)은 군사 클라우드를 활용하여 군장비의 복원력을 강화하는 연구를 진행하고 있다. 클라우드 서비스와 기반시설을 이용하여 사이버공격에 대한 탐지 및 진단, 대응을 수행하여 생존력을 강화하는 것을 목표로 한다. 국내에서도 복원력을 강화할 수 있는 연구가 진행되어야 한다.

#### 4.2.3 국내 사이버 위협정보 공유

앞 장에서 살펴봤듯이 미국은 정부기관과 민간부문 간 사이버보안 정보공유법이 통과되었다. 국내에서는 '사이버 위협정보 공유에 관한 법률안'이 국회에 계류 중이다. 사이버 위협정보 공유는 국가 차원에서 국내 위협정보를 공유하여 사이버위협을 조기에 탐지할 수 있도록 하며, 위험을 빠르게 식별하여 신속한 대응을 할 수 있다는 장점이 있다. 정보공유를 하기에 앞서 개인의 프라이버시와 기업의 기밀정보 등에 관한 문제를 검토해야 할 필요가 있다.

#### 4.2.4 국제 사이버 수사공조 절차 마련

국내에서 북한 사이버공격에 대한 외교적 대응조치로 경유지 국가들에게 수사공조를 요청하였으나 원활하게 이뤄지지 않았으며, 미국도 소니 해킹사건에 대한 수사과정에서 중국에 수사공조를 요청하였으나 중국은 미국과 중국 간의 대화가 필요하다며 회피하였다. 한국은 미국의 소니 해킹사건 수사 과정에서 북한의 악성코드 관련 정보를 제공하여 미국 연방수사국의 수사에 도움을 주었다. 한국과 미국 간에 디지털증거와 관련된 사법공조가 이뤄졌듯이 국제적인 협력체계를 구축하면 원활한 수사공조가 이루어질 수 있을 것이다.

### 4.3 사이버범죄 차원의 대응전략

#### 4.3.1 사이버범죄협약 가입 검토

사이버범죄협약은 사이버범죄에 대하여 상세한 규정을 두고, 이를 처벌하도록 한 최초의 국제조약이며, '부다페스트조약'이라고도 한다. 헝가리 부다페스트에서 열린 사이버범죄 국제회의에서 전 세계 20개국이 조약에 서명한 뒤 조약 참가국별로 비준절차를 거쳐 정식으로 발효되었으며 미국, 에스토니아를 포함한 51개 국가가 가입하였다. 조약은 4개의 챕터로 구성되어 있는데, 제 1장은 조약에서 사용되는 용어를 정의하고, 제 2장은 컴퓨터기반 또는 컴퓨터관련 범죄를 정의하고, 절차상의 권력을 요구하며, 관할권을 주장할 수 있는 규칙들을 정립하고, 제 3장은 권력을 사용할 수 있는 협력 프레임워크를 정하고, 마지막으로 제 4장은 유럽회의의 일반적인 부칙들을 포함하고 있다(Weber, 2003).

## 5. 결 론

사이버공격은 사이버전쟁, 사이버테러, 사이버범죄로 구분되며 컴퓨터를 대상으로 한 범죄행위, 컴퓨터를 이용한 범죄행위, 컴퓨터상에서의 범죄행위로 유형이 구분된다. 사이버전쟁은 국가 또는 그 정보요원이 수행한 공격으로써 무력사용의 수준에 이르는 사이버공격이고, 사이버테러는 개인, 단체

또는 국가가 정치적·사회적·종교적인 목적을 가지고 일반대중에게 공포심을 주는 등의 사회적 혼란을 야기하는 공격이며, 사이버범죄는 주로 개인의 금전적인 이익을 목적으로 발생하는 범죄행위를 말한다.

북한의 사이버공격은 공격대상이 개인용 컴퓨터 및 홈페이지에서 금융사 및 언론사로, 그리고 기반시설로 변화하였고, 공격방식은 바이러스에서 디도스, 그리고 지능형지속위협으로 변화하였으며, 공격목적은 정치적인 목적, 기밀정보유출, 금전적인 이익을 목적으로 하는 구분이 있었다. 북한의 사이버공격에 대한 한국의 대응조치는 정책적, 실무적, 외교적 대응조치로 살펴보았다. 대규모 사이버공격 사건이 발생한 이후에는 국가차원의 종합대책을 발표하였고, 디도스 대응전략을 통해 디도스 피해를 줄일 수 있었으며, 중국 등 경유지국가에 수사공조를 요청하였지만 성공하진 못하였다.

사이버공격에 대한 국제 사례로는 소니 해킹사건이 있었던 미국, 에스토니아 사건이 발생했던 북대서양조약기구, 스틱스넷 사건이 있었던 이란을 대상으로 대응조치를 살펴보았다. 미국은 한국과 디지털증거와 관련된 사법공조를 하였고, 금융제재 행정명령을 발표하였으며, 사이버위협 정보공유 법안을 통과시켰다. 에스토니아 사건을 겪은 북대서양조약기구는 사이버상의 교전규칙인 탈린 매뉴얼을 발간하였고, 사이버안보 컨퍼런스인 사이콘을 개최하여 국제적인 사이버안보 컨퍼런스로 입지를 구축했다. 스틱스넷 사건을 겪은 이란은 사이버공간을 다루는 가장 높은 정부기관으로 사이버공간최고위원회를 발족하고 이를 중심으로 사이버방어와 역공격능력을 강화하였다.

결론적으로 북한 사이버공격에 대한 국가적 대응전략으로 사이버전쟁 차원으로는 사이버공격 방지를 위한 국제규범 제정, 사이버안보 컨퍼런스 주최, 국제사법재판소 회부를 사이버테러 차원으로는 국가사이버안전에 관한 총괄 입법체계 구성, 복원력 중심의 연구개발 수행, 국내 사이버 위협정보 공유, 국제 사이버 수사공조 절차 마련을 사이버범죄 차원으로는 사이버범죄협약 가입을 검토할 것을 제안했다.

본 논문은 향후 한국의 사이버공격에 대한 대응방안 마련 및 전략수립에 기여할 것으로 기대된다. 반면 연구가 미국, 북대서양조약기구, 이란에 국한되었다는 한계점이 존재한다. 더 다양한 국가를 대상으로 연구가 수행될 필요가 있다.

## References

Brenner, S.W. and M.D. Goodman, “In Defense of Cyberterrorism An Argument for Anticipating Cyber-Attacks”, *Journal of Law, Technology and Policy*, 2002, 1-57.

Carr, J., *Inside Cyber Warfare : Mapping the Cyber Underworld*, O'Reilly Medea, Inc., 2011.

Chen, T.M. and S. Abu-Nimeh, “Lessons from Stuxnet”, *IEEE Computer*, Vol.44, No.4, 2011, 91-93.

Cordesman, A.H. and B. Gold, *The Gulf Military Balance : The Conventional and Asymmetric Dimensions,* Rowman & Littlefield, 2014.

Embar-Seddon, A., “Cyberterrorism Are We Under Siege?”, *American Behavioral Scientist*, Vol.45, No.6, 2002, 1033-1043.

Evron, G., “Battling Botnets and Online Mobs Estonia's Defense Efforts During the Internet War”, *Georgetown Journal of International Affairs*, Vol.9, 2008, 121-126.

Fafinski, S., W.H. Dutton, and H. Margetts, “Mapping and Measuring Cybercrime”, *OII Forum Discussion Paper*, Vol.18, 2010, 1-26.

Farwell, J.P. and R. Rohozinski, “Stuxnet and the Future of Cyber War”, *Survival*, Vol.53, No.1, 2011, 23-40.

Golder, B. and G. Williams, “What is ‘Terrorism?’

Problems of Legal Definition", *University of NSW Law Journal*, Vol.27, No.2, 2004, 270-295.

Haggard, S. and J.R. Lindsay, *North Korea and the Sony Hack Exporting Instability Through Cyberspace*, IEEE Computer Society, 2015, 54-57.

Hathaway, O.A., R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel, "The Law of Cyber-Attack", *California Law Review*, Vol.100, No.4, 2012, 817-885.

Hoisington, M., "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International and Comparative Law Review*, Vol.32, 2009, 439-454.

Kelsey, J.T.G., "Hacking into International Humanitarian Law : The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*, Vol.106, No.7, 2008, 1427-1451. Available at http://www.jstor.org/stable/40041623(Accessed December 21. 2015).

Kwon, H.Y., "The need for cyber security laws and legislative strategy", Cyber Security Threats and Countermeasures : the Proceedings of the 18th Hwarangdae International Symposium, Korea Military Academy and Hwarangdae Research Institution, Seoul, 2015, 78-93.

(권헌영, "사이버안보 법제의 필요성과 입법전략", 사이버안보 위협 및 대응전략 : 제18회 화랑대 국제 심포지엄논문집, 육군사관학교, 서울, 2015, 78-93.)

Lee, Y.J., H.J. Kwon, J. Lee, and D.K. Shin, "Development of Countermeasures against North Korean Cyberterrorism through Research Case Studies", *Korean Journal of Defense Analysis*, Vol.27, No.1, 2015, 71-86.

Lesk, M., "The New Front Line Estonia Under Cyberassault", *IEEE Security and Privacy*, Vol.5, No.4, 2007, 76-79.

Moore, R., Cybercrime : Investigating High-Technology Computer Crime, Routledge, Boston, 2010.

Park, K.G., "Cyber Warfare to Cyber-attacks and International Law", *International Law Review*, Vol.32, 2010, 37-83.

(박기갑, "사이버전쟁 내지 사이버공격과 국제법", *국제법평론*, 제32권, 2010, 37-83.)

Schaap, A.J., "Cyber Warfare Operations : Development and Use under International Law Cyberlaw Edition", *Air Force Law Review*, Vol.64, 2009, 121-174.

Schmitt, M.N., *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2013.

Shackelford, S., "From Nuclear War to Net War : Analogizing Cyber Attacks in International Law", *Berkley Journal of International Law,* Vol.25, No.3, 2009, 191-250.

Son, Y.D., *The Endless War Between 0 and 1*, Infothebooks, 2013.

(손영동, *0과 1의 끝없는 전쟁, 인포더북스*, 서울, 2013.)

Stohl, M., "Cyber Terrorism : a Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?", *Crime Law and Social Change*, Vol.46, No.4, 2006, 223-238.

Wall, D.S., *Cybercrime : The Transformation of Crime in the Information Age*, Polity Press, UK, Cambridge, 2007.

Weber, A.M., "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal*, Vol.18, No.1, 2003, 424-

446.

Weimann, G., "Cyberterrorism How Real Is the Threat?", Special Report, United States Institute of Peace, 2004.

Yar, M., "The Novelty of 'Cybercrime' : An Assessment in Light of Routine Activity Theory", *European Journal of Criminology*, Vol.2, No.4, 2005, 407-427.

Young, R., "Defining Terrorism : the Evolution of Terrorism as a Legal Concept in International Law and its Influence on Definitions in Domestic Legislation", *Boston College International and Comparative Law Review*, Vol.29, No.23, 2006, 23-106.

## About the Authors

**Min Kyung Chung (2014020937@korea.ac.kr)**

Min Kyung Chung received the B.S. degree in Information Security from Seoul Women's University in 2014. She is a Master Candidate in Cyber Defense at Korea University. Her current research interests include information security policy.

**Jong In Lim (jilim@korea.ac.kr)**

Professor Jong In Lim is currently a Special Assistant for National Security Affairs to President and a Professor of Graduate School of Information Security at Korea University. He received the B.S. degree in Math from Korea University and MA, Ph.D. degree in Cryptography from Korea University. He received the Red Stripes Order of Service Merit for Day Ceremony of the 1st Information Security in 2012. His current research interests include information security policy.

**Hun Yeong Kwon (khy0@korea.ac.kr)**

Professor Hun Yeong Kwon is currently a Professor of Graduate School of Information Security at Korea University. He received his Ph.D, in Law from Yonsei University in 2005 and LL.M., LL.B. degree from Yonsei University. He is responsible for the Chairman of Government 3.0 Legislation Special Committee, the Chairman of Public Data Strategy Committee. Also, He wrote 'Risks and Countermeasures of the Smart Times' and 'Dissertate the Korea's Internet.'