Crisisonomy Vol.13 No.11, 105-118
ISSN 2466-1198 (Print) ISSN 2466-1201 (Online) http://dx.doi.org/10.14251/crisisonomy.2017.13.11.105

Crisisonomy

Implications on National Security Strategies of the Strategic Use of Cyber Capabilities of Foreign Governments

- The Case of Alleged Russian Interference in the 2016 US Election -

Jeong Yoon Yang[+], Kyudong Kim, So Jeong Kim

National Security Research Institute, P.O. Box 1 Yuseong, Daejeon, Korea

Abstract

As the cyberspace is recognized as the national security domain such as air, sea, and space, countries are growing their efforts to expand their influences in cyberspace and cyber capabilities targeting the integrity of information resources in an attempt to influence the political decision making process at the state level. It is assumed that Russian interference in the 2016 US election took place as a part of this effort. The US government imposes sanctions on Russia through legislative and administrative measures in conjunction with investigations of intelligence and investigate agencies and parliamentary commissions of inquiry. This paper aims to gain insight of national countermeasures against strategic cyber attacks from other countries by reviewing US countermeasures of the Russian interference in the 2016 US election case. This paper examines the facts centering on reports published by US intelligence agencies and examine the domestic measures and derive national security strategic implications on strategic cyber attacks from foreign governments.

Key words: cyber attack, cybersecurity strategy, US, Russia, South Korea

Ⅰ. 서 론

사이버공간을 영토, 영해, 영공, 우주에 이은 국가안보영역으로 인식하여 사이버안보 태세를 강화하는 국가들이 증가하고 있다(DoD, 2014; CAC, 2016). 많은 국가들이 사이버 공간을 활용하여 국가 영향력을 전 세계적으로 투사할 목적으로 사이버 역량을 강화하고 있으며, 정보자원의 무결성을 공격해 국가 정책 결정과정에 영향을 미쳐 정책결정자가 잘못된 정책결정을 내리도록 유도하거나 자국에 유리한 방향으로 국가정책이 실행되도록 조정하는 국가차원의 전략적 공격이 증가하고 있다(Coats, 2017; Clapper, 2016).

2016년 11월 치러진 미국 대통령 선거과정에서 민주당전국위원회(Democratic National Committee, 이하 DNC)의 서버가 해킹되어 정보가 유출되고, 상대후보를 비방하는 허위사실이 유포되는 등 대통령 당선에 영향을 미칠 수 있었던 중대한 일련의 사건이 발생한다. 2017년 8월 현재 사건의 조사가 진행중이나, 미 정부

[+] Corresponding author: Jeong Yoon Yang, Tel. +82-42-870-2114, Fax. +82-42-870-2222, e-mail. jyyangrok@nsr.re.kr

및 미국의 보안전문기업들은 사건의 배후를 러시아로 지목하고 있다(Strohm, 2016). 이에 따라 미 정부는 입법과 행정조치 등을 통해 러시아에 대한 제재를 취하는 한편 정보・수사기관과 의회 조사위원회를 통한 조사를 병행하고 있다.

정보통신기술의 발달에 따라 급격히 팽창된 사이버공간은 국가에 새로운 위협이자 기회의 공간으로 대두되고 있다. 사이버공간의 공시성(共時性), 통공성(通空性), 편재성(偏在性)과 같은 특징들은 국가위협의 구성요소인 위협의 구체성, 위협의 공간적 근접성, 위협의 시간적 근접성, 위협이 현실화 될 수 있는 개연성, 위협에 따른 이익 침해의 심각성을 충족하여 국가안보위협으로 자리매김하고 있다(Ha & Kim, 2006; Lee, *et. al.*, 2015).

본 논문에서는 美 대선 러시아 개입사건을 중심으로 타국의 전략적 사이버공격에 대한 국가적 대응방안을 살펴보도록 한다. 수사가 종료되지 않은 사건에 대한 분석이 시기상조로 비춰질 수 있으나, 2016-17년을 전후하여 치러졌거나 치러질 예정인 네덜란드, 독일, 프랑스 대선에도 러시아 개입 의혹이 잇따르고 있으며, 북한발 대남 사이버공격이 증가되고 공격방식의 변이가 일어나고 있다. 단순 정보활동이나 혹은 사보타지가 아닌 타국의 국내문제에 대한 적극적 개입 시도가 급증하고 있는 현실에서 대선 이후 약 6개월 간 미국의 신속하고 적극적인 대응방식은 타국의 전략적 사이버공격에 대한 국가적 대응방안에 시사점을 내포한다.

본 논문은 이론적 배경과 사실관계 검토 후 미 정보기관의 보고서 발표, 이에 대한 입법적 대응과 행정명령 등 미국이 취한 국내적 조치들에 대해 살펴본다. 타국의 전략적 사이버공격에 대한 일국의 국가적 대응방식을 살펴보는 과정을 통해 한국의 국가 사이버안보전략에 미치는 시사점을 도출한다.

II. 이론적 배경

1. 국가안보와 사이버안보

새로운 공간의 출현은 국가에 안보적 위협과 기회라는 도전과제를 부여한다. 20세기 초 비행기의 발명은 공역(空域)이라는 새로운 공간을 출현시켰고, 잠수함의 보급은 해저공간을, 20세기 후반 로켓 기술의 발달은 우주공간이라는 새로운 공간을 출현시켰다(Jang & Han, 2013). 새로 출현된 공간은 국가이익 추구의 장(場)이 되어 공간의 전략적 활용을 위한 국가간의 경쟁이 발생한다. 탈냉전시대의 안보개념 변화에 따른 포괄적안보 대상의 구성요소로 생각되던 사이버안보는 주요기반시설의 운영을 위협하여 국가의 정상적인 기능을 저해할 수 있는 국가의 치명적(vital)이익에 대한 위협으로 발전하고 있다. 사이버안보 위협의 중차대함을 반영하듯 현재 전 세계 70개 이상의 국가에서 사이버안보전략을 공포하였으며, 한국도 사이버안보전략을 수립 중인 것으로 알려져 있다. 미국, 중국, 일본, 러시아, 영국, 독일, 프랑스 등 주요국 역시 사이버안보 분야의 전략을 마련하여 국가안보적 차원의 사이버위협에 대비하고 있다.

사이버안보 위협의 가시적인 확대에도 불구하고 아직 국내외적으로 사이버안보의 용어에 대한 통설은 존재하지 않는다. 미국과 러시아 연구기관의 공동연구에 따르면 사이버공간은 '정보의 생성・전송・수신・저장・처리・삭제가 이루어지는 전자적 매체'라 정의된다(Godwin III, 2014). 최근 연구에 따르면 사이버안보라는 용어의 원형이라고 할 수 있는 영어 표현인 사이버시큐리티(cybersecurity)에 따라 사이버안보를 '정보의 생성・전송・수신・저장・처리・삭제가 이루어지는 전자적 매체가 지닌 의도적・비의도적 위협에 대항하고 대응・복구할 수 있는 속성'으로 정의한다. 또한 사이버보안은 '정보의 비밀성, 무결성, 가용성을 유지하기 위하여 사이버공간에 발생하는 공격으로부터 정보, 정보시스템 및 정보통신망을 보호하는 것'으로 정의한다(Park, *et. al.*, 2017).

기존에 사이버안보에 관한 다수의 연구가 있으며 이러한 연구들은 사이버안보 법제에 관한 연구와 정책 및 전략에 관한 것으로 분류된다. 사이버안보 위협성격을 통해 사이버안보 전략을 분석한 선행연구로는 Jang,

et. al.(2017), Jang & Kim(2016), Yoon, *et. al.*(2015) 등이 있다. Jang, *et. al.*(2017)에 따르면 선거개입의 경우 국가가 사이버위협의 행위자로서 사이버심리전에 해당하는 사이버공격에 해당된다. 다수의 연구에서 국가 사이버안보 강화방안에 대해 제시하고 있으나, 본 연구에서는 선거개입 사건에 주안점을 두어 국가 사이버안보 전략을 분석하는 한편, 기존의 법제개선과 체제개편에 대한 논의를 차치하고 국가차원에서 실행가능한 실증적 방안들을 고찰하고자 한다.

2. 대선개입 사건의 사실 관계

사건의 발단은 2015년 여름 러시아 정보기관으로 추정되는 공격자가 미 정부 및 정치단체 종사자를 대상으로 약 1,000여건의 악성코드가 담긴 이메일을 발송한데에서 비롯되었다(Strohm, 2016). WikiLeaks가 DNC와 관련된 20,000여개의 이메일과 8,000여개의 파일을 유포하는 것으로 사건은 본격적으로 점화되고, CrowdStrike, Fidelis, Mandiant, SecureWorks, ThreatConnect 등 미국의 보안업체들은 WikiLeaks의 이메일 유포가 러시아 정보기관과 관련이 있다고 발표한다(Alperovitch, 2016). WikiLeaks, DC Leaks, Guccifer 2.0 등은 지속적으로 민주당과 관련된 비밀문서들을 공개하고 버니 샌더스 후보와 힐러리 후보의 민주당 경선이 힐러리 후보쪽에 편파적이었다는 내용이 공개되는 등 민주당 내부의 분열이 발생하게 된다. 2016년 10월 오바마 전 대통령은 미-러 핫라인(red phone)을 통해 푸틴 대통령에 대선 해킹에 대해 경고한다. 이후 2016년 11월 치러진 대통령 선거에서 도널드 트럼프는 제45대 미국 대통령으로 당선된다. 미국은 대선 개입에 대한 보복성 조치로 정보요원으로 추정되는 러시아 외교관 35명을 추방하고 정보활동의 본거지로 추측되는 주미 러시아 시설 2개에 대해 폐쇄조치를 내린다. 2016년 12월 국토안보부(Department of Homeland Security, 이하 DHS)와 연방수사국(Federal Bureau of Investigation, 이하 FBI)은 러시아의 대선개입에 관한 합동분석보고서를 발표하고, 2017년 1월 국가정보국장(Director of National Intelligence, 이하 DNI)은 FBI, 중앙정보국(Central Intelligence Agency, 이하 CIA), 국가안보국(National Security Agency, 이하 NSA) 합동 조사를 통한 美 대선 러시아 활동 보고서를 발표한다(DHS, FBI, 2016; DNI, 2017). 이후, Michael Flynn 국가안보위원회(National Security Council, 이하 NSC) 보좌관 사임(2월), 하원청문회 개최(3월), 러시아 해커 체포(4월), James Comey FBI 국장 해임(5월), NSA 보고서 유출(6월), 트럼프 측근인물 조사(7월) 등 활발한 수사가 진행 중이다.

미 정보기관과 보안업체들의 주장에 따르면 해킹 주체는 연방보안국(Federal Security Service, 이하 FSB), 정보총국(Main Intelligence Directorate, 이하 GRU)인 러시아 민간부문 및 군 정보기관(Russian civilian and military Intelligence Services, 이하 RIS)[1]으로 추정된다. 이들은 웹사이트 취약성, 서버 취약성을 이용하여 DNC 서버를 해킹하고 해킹된 자료를 유포하거나 소셜미디어 및 웹사이트 등을 통해 건강이상설 등 힐러리 후보 관련 허위정보를 유포하여 힐러리 후보를 폄훼한다. 또한 러시아 국영 뉴스 RT 등 다양한 채널을 통해 트럼프를 선전하는 방식으로 미국 대선에 영향력을 행사하였다고 알려진다(DNI, 2017).

미국은 사건의 해결을 위해 국내적으로 행정부와 의회가 각각 다양한 노력을 개진하였다. 상하원은 외국에 의한 정치적 개입에 대응하기 위한 법안을 입안, 가결하는 한편, 사건에 대한 이해도 제고를 위해 우크라이나 시찰, 대통령에 대한 정보요구, 군사위원회와 정보위원회를 통한 조사를 실시한다. 2017년 1월 상원 정보위원회는 조사에 착수하여 공동성명[2]을 발표하고, 조사과정에 문제가 있다고 판단된 FBI 국장과 NSC 국가

1) 정보기관을 행정 영역별로 분류할 시 국방부나 군 관련 부처가 아닌 일반 행정부처 소속 정보기관 및 대부분의 국가 중앙정보기관을 의미(예: DNI, CIA, FBI 등)(GAO, 2014). 국방부나 육・해・공군 등 각 군에 소속되어 군의 정보업무를 수행하는 군 정보기관과 대별됨. 러시아 경우, 국내 첩보 수집 및 방첩 임무 수행하는 국가 중앙정보기관인 FSB는 민간부문 정보기관에 해당하고, 러시아 연방군 내 정보부서로 국내외 군사정보 수집 및 대외 비밀공작 업무 수행하는 GRU는 군 정보기관에 해당(Han, 2011)

안보보좌관의 사임을 요구한다.

Ⅲ. 美 국내적 대응조치

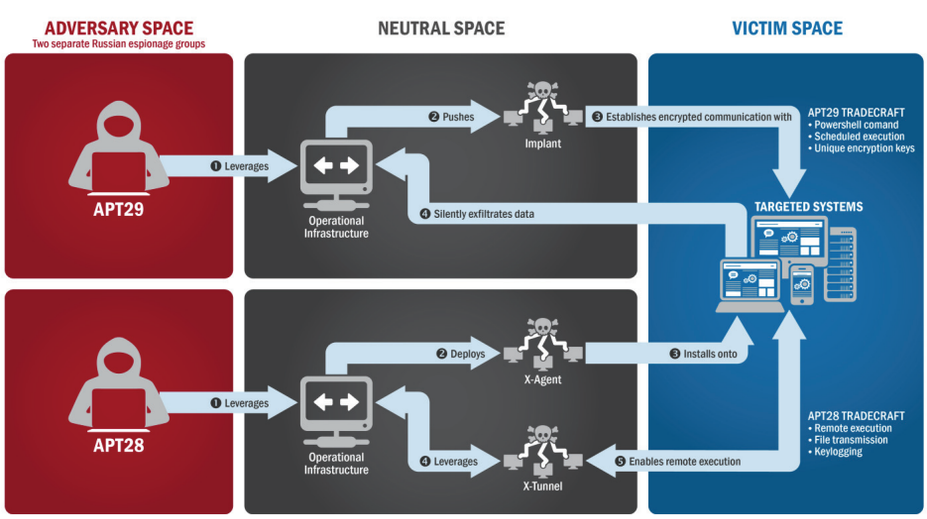
1. 정보기관의 조사

미국은 러시아의 대선 개입 의혹에 강경한 입장을 취하였다. 대선 개입 의혹이 공론화되기 시작하였던 2016년부터 오바마 전 대통령은 G20 정상회담 시 푸틴 대통령에 우회적으로 경고를 전달하였으며, 10월 말 미-러 핫라인을 통해 푸틴 대통령에 미 대선개입에 대하여 경고하며 '무력충돌에 대한 것을 포함하여, 국제법이 사이버공간에도 적용'되며, 이러한 국제법적 기준에 따라 러시아에게 책임을 물을 것이라고 경고한 것으로 알려졌다(Rampton & Mason, 2016; Arkin, *et. al.*, 2016). 또한 대선 개입 조사 명령과 함께 수집 정보를 연방기관에 전달하여 사건 조사가 적극적으로 진행되도록 촉구한다.

정보기관들은 이례적으로 조사 결과에 대한 보고서를 공개하여 러시아 개입을 입증하고자 시도하였다. 이들 보고서들은 기술적 분석과 재무관계 조사를 통해 사실관계를 밝히고, 대선 개입 배경에 대한 분석을 시도하였다.

선제적으로 본 사건과 관련하여 DHS와 국가정보국(Office of Director of National Intelligence, ODNI)은 선거보안에 관한 공동성명을 발표하고, 이에 대한 후속 작업으로 DHS와 FBI는 공동의 합동분석보고서(Joint Analysis Report, JAR)인 'GRIZZLY STEPPE-Russian Malicious Cyber Activity'를 발표한다(DHS & ODNI, 2016; FBI & DNI, 2016). 보고서에서는 2016년 선거와 관련하여 RIS의 악의적 사이버 활동을 GRIZZLY STEPPE라 통칭하며, RIS가 미국 대선 개입 사건을 주도하였다고 밝히고, RIS가 연방정부, 민간기관 등의 네트워크에 침입하기 위해 사용한 공격기술 공개한다.

보고서는 이번 대선 개입 사건의 주요 공격 주체로 추정되는 APT28과 APT29의 활동을 분석한다. APT28은 스피어피싱 기법을 사용하는데, 이메일 수신자가 가짜 웹메일 도메인에서 비밀번호를 변경하도록 속여 비밀번호를 탈취하고, 탈취된 정보를 통해 민주당 고위인사들의 콘텐츠에 접속하여 정보를 유출하였다. APT29도 스피어피싱 기법을 사용하여 민주당 컴퓨터 시스템을 감염시킨 후 시스템에 침투한 멀웨어를 통해 이메일을 유출하고 원격제어(RATs) 악성코드를 통해 추적을 회피하였음을 밝힌다.



※ Source: GRIZZLY STEPPE-Russian Malicious Cyber Activity

Figure 1. The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems

2) Joint Statement on Committee Inquiry into Russian Intelligence Activities (2017.1.13.) (https://www.burr.senate.gov/press/releases/joint-statement-on-committee-inquiry-into-russian-intelligence-activities)

보고서는 또한 해킹에 사용된 침해지표(Indicators of Compromise, IOCs) 및 악성코드 시그니처(Yara Signature)를 통하여 분석의 근거를 제시하였으며, 추가적으로 후속 피해를 미연에 방지하기 위한 보안 강화 권장사항들을 제시한다.

동 보고서는 미국 정보기관이 해킹증거자료를 제시하였다는 점에서 이례적이라고 할 수 있다. 한편 일부 보안 전문가들은 보고서 내용의 부실성, 침해지표 수준이 낮은 점, 악성코드 시그니처의 특이성이 낮은 점 등에 따라 동 보고서로 러시아의 개입을 주장하는 것은 무리가 있다고 판단한다(Arghire, 2017). 보고서의 내용으로 판단할 시 제시된 자료가 러시아의 행위임을 결정적으로 입증하는 증거들로 보기에는 어려움이 따른다. 그러나 정보기관의 입장에서는 기존에 수집된 침해지표를 모두 공개하여 대조한 증거들을 대중에 제시할 수 없는 것이 사실이다. 또한 사이버공격에 대한 국가의 개입은 많은 경우 기술적 정보만으로는 입증이 어려우며, 이에 대한 판단에는 피해국의 정보역량과 고도의 상황분석이 병행되어야 한다. 이러한 사이버공격의 특성은 국가의 대응활동에 딜레마를 야기한다.

이후 DNI는 FBI, CIA, NSA가 합동으로 수집한 정보를 통해 본 사건에 관한 분석보고서(Assessing Russian Activities and Intentions in Recent US Elections, 2017. 1. 6)를 발표한다. 동 보고서는 사이버 도구와 언론 보도를 이용하여 미국 여론에 영향을 미치고자 한 러시아의 의도 및 동기 분석에 주력하여, 사건에 대한 전반적인 분석 결과를 담는다. 이는 앞서 발표된 보고서의 기술정보에 더해 행위의 동기와 정황 등을 제시함으로써 미 정부의 주장을 보완해주는 것으로 볼 수 있다.

선거 개입을 통해 달성하고자 한 목표는 미국 민주주의 과정에 대한 대중과 전 세계의 신뢰 저하와 힐러리 후보의 당선 가능성을 감소시키기 위함으로 판단된다. 힐러리 후보는 2011년 미 국무장관 시절부터 지속적이고 공개적으로 푸틴 대통령을 비판해왔으며 푸틴 대통령의 세력 확장에 부정적 인물로 언론에 분석되어 왔다. 보고서는 푸틴 정부가 트럼프 후보를 분명히 선호하였다고 기술하며 트럼프 후보가 힐러리 후보에 비해 러시아에 우호적인 정책을 개진할 것이라 판단하였을 것이라 추정한다. 우크라이나 사태 이후 서방 세계의 대러 외교・경제 제재와 러시아 접경 지역에서 북대서양조약기구(North Atlantic Treaty Organization, NATO)의 군사적 대응태세 강화는 주요 경제지표의 하락 등 러시아에 위기를 초래하게 된다(Koh, 2017; Cha, *et. al.*, 2015). 이러한 대러 제재를 완화하기 위해서는 미국의 대러 정책 전환이 필요하고 힐러리 후보에 비해 러시아에 우호적인 정책을 구사할 것이라는 기대하에 트럼프(공화당) 후보의 당선을 지지하게 되었다는 분석이다.

또한 동 보고서는 선거 개입의 원인으로 미국 대선 과정에 대한 영향력 행사(influence campaign)를 푸틴 대통령이 직접적으로 지시하였을 것으로 분석한다. 이러한 목적을 달성하기 위해 러시아가 실행한 선거 개입 활동은 다음과 같다. 첫째, 정보기관을 통한 비밀 정보 활동이다. 러시아 GRU가 수집된 정보를 "Guccifer 2.0"과 "DCLeaks.com"를 이용하여 언론 매체에 배포하고 "위키리크스"에 전달하는 방법을 통해 정보를 유포하였을 것으로 추정된다. 둘째, 정부기관・국영미디어・제3중개자・유료소셜미디어 사용자 및 트롤(trolls)[3]의 역량을 활용한 전략적 유포 전략(messaging strategy) 활동이다. 러시아 국영선전기관 RT은 국내외에서 크렘린 궁의 입장을 대변하는(Kremlin messaging)의 창구 역할을 수행하는 것으로 분석된다.

이후 DHS의 국가사이버안보・통신통합센터(National Cybersecurity and Communications Integration Center, 이하 NCCIC)는 16년 12월 발간한 "GRIZZLY

3) 보고서에서는 troll이란 말이 여러 차례 등장하는데, 인터넷 트롤은 일반적으로 인터넷에서 고의적으로 논쟁이 되거나 선동적, 파괴적 행동을 하는 해커를 의미하나, 보고서 상 미 대선에 개입할 목적으로 러시아 정부를 대변하여 허위정보 유포 활동을 수행한 주체를 의미.

Table 1. Analysis of russian interference in the 2016 US election case utilizing cyber kill chain

Phase	Description
Reconnaissance	using network vulnerability scanning, credential harvesting, and typo-squatting methods, actors determine the best attack vector for compromising targets
Weaponization	actors have embedded malicious code into file types. Weaponization methods have included ① Code injects in websites as watering hole attacks, ② Malicious macros in Microsoft Office files, ③ Malicious Rich Text Format (RTF) files with embedded malicious flash code
Delivery	actors used spear-phishing emails to deliver malicious attachments or URLs that lead to malicious payloads
Exploitation	actors have developed malware and target Microsoft Office exploits
Installation	actors have leveraged several different types of implants using PHP and RTF files
Command and Control	actors leveraged their installed malware through Command and Control (C2) infrastructure
Actions on the Objective	utilizing malware, actors conducted extensive data exfiltration of sensitive files, emails, and user credentials

STEPPE-Russian Malicious Cyber Activity"의 미흡한 사항을 보완하려는 노력의 일환으로 이에 대한 후속 문건으로 "Enhanced Analysis of GRIZZLY STEPPE Activity(2017. 2. 10)"를 발표한다. 동 보고서는 2015-2016년 APT28, APT29의 활동을 사이버 킬체인(Cyber Kill Chain) 모델을 통해 분석한다. 사이버 킬체인이란 사이버공간에서 정찰(Reconnaissance), 무기화(Weaponization), 유포(Delivery), 공격(Exploitation), 설치(Installation), 명령・제어(Command and Control), 목표물 타격(Action on the Objective)에 이르는 전 과정을 의미하는 데, 이를 통한 미 대선 러시아 개입사건에 대한 분석은 다음과 같다(Hutchins, *et. al.*, 2010; Cha, *et. al.*, 2010).

또한 동 보고서는 추가적으로 해킹에 사용된 침해지표 및 악성코드 시그니처를 공개하여, 사건에 사용된 사이버 위협에 대한 전반적 이해도를 높이도록 노력하였다. 이러한 조사결과 공개를 통해 조사 사실의 실효성 및 입증성을 높이는 한편 사건의 객관화를 시도하였다.

2. 입법적 대응

1) 외국선전 및 허위정보 대응법(Countering Foreign Propaganda and Disinformation Act of 2016)

사이버공간을 통한 러시아의 악의적 활동에 대응하기 위하여 2016년 3월 '정보전대응법(Countering Information Warfare Act)(H.R.5181)'이 입안된다. 입법취지는 러시아와 중국을 비롯한 외국 정부가 허위정보 및 선전을 통해 미국과 미 동맹국의 이익을 저해하는 것에 대한 포괄적이며 전략적인 대응 방안을 마련하기 위함이다. 이 법안은 2016년 5월 '외국선전 및 허위정보 대응법(Countering Foreign Propaganda and Disinformation Act of 2016)'으로 발의(초당적 법안)되고 2016년 12월 2017 국방수권법(National Defense Authorization Act for Fiscal Year 2017, 이하 NDAA)에 병합되어 통과된다[4].

NDAA 2017에 포함된 러시아발 허위정보 및 선전에 대한 전략적 대응 체계 마련의 주요 골자에는 세계참여센터(Global Engagement Center, 이하 GEC)의 설립이 있다. 법률 제정 후 180일 이내 국무부장관은 국방부장관 및 관련 연방부처 및 기관들과 협의하여 국무부 내에 GEC를 설립하여야 하는데, 이는 외국정부 또는 비국가단체가 선전 및 허위정보활동을 통해 미국의 국가안보이익을 저해하는 활동을 저지하기 위한 연방정부의 활동들을 주도, 통합, 조정하기 위함이다. GEC는 미국, 미동맹국, 파트너국의 국가안보이익을 위협하는 허위정보활동을 추적・검증하고, 이를 위한 국제적 노력을 통합한다. 또한 미국 정부기관, 동맹국, 파트너국,

4) 국방수권법은 1961년 케네디 대통령 시절부터 현재까지 지속적으로 제・개정이 진행중인 美 국방부 예산을 정하기 위해 매년 제정되는 연방법으로, 관련 법안 규정들을 병합하여 제정되기도 한다.

싱크탱크, 대학 연구기관, 시민사회단체, 비정부기구의 첩보・정보・해석정보를 분석하고 필요시, 선전 및 허위사실에 대응하기 위한 활동의 일환으로 사실 정보(fact-based narratives) 및 분석 자료의 유포를 지원한다. 또한 선전 및 허위정보 활동의 최신경향을 식별하고 허위정보 및 오류정보의 기법, 기술, 과정을 대중에 공개한다. 적극적으로 사실 기반 정보 및 정책을 해외에 알리고, 연방정부부처 및 기관 간 전문지식을 공유하고 외부소스의 전문 기술을 습득하며 모범사례를 공유하여 포괄적 기술 및 기법의 활용을 촉진한다. 선전 및 허위정보로부터 강건성을 갖추기 위한 미국의 역량 개선 사항을 확인 및 권고하고, 기관 간 보급되는 정보를 통해 국가와 국민들이 선전과 허위정보로부터 가장 취약한 부분을 확인한다. 또한 정보접근기금(Information Access Fund)을 관리하는 한편 중복 조사를 피하기 위해 미 동맹국 및 파트너국과 공조한다. 외국정부 또는 비국가단체가 선전, 허위정보 등을 통해 공공외교를 행사하는 것에 대한 연구를 수행하고, 데이터 분석을 위한 정보를 수집・배포한다. 이러한 연구 및 데이터 분석은 프라이버시와 시민의 자유를 수호하는 범위 내에서 행해질 것임을 명시한다.

GEC의 장은 대통령에 의해 임명된 연방기관의 장이 수행하고 직원은 연방정부 공무원 및 개인 서비스 계약자(personal service contractor)로 구성된다. 센터운영을 위해 국방부는 국무부에 2017년, 2018년 각각 $60,000,000를 제공하게 된다.

GEC는 정보접근기금을 통하여 시민사회단체, 미디어콘텐츠제공자, 비정부기구, 연방기금출연연구개발센터, 민간기업, 대학연구소에 예산을 지원한다. 이를 통하여 ① 외국 허위정보 및 정보조작 활동에 반대하는 지역 독립 미디어의 활동 지원, ② 허위정보, 오류정보, 선전과 관련된 인쇄물, 온라인, 소셜미디어 정보의 수집 및 저장, ③ 허위정보, 오류정보, 선전을 이용한 외국 정보전 기술, 기법, 과정을 분석 및 보고, ④허위정보, 오류정보, 선전을 통해 사회・정치적 안정성을 저해하는 것에 대응하는 센터의 활동을 지원하는 역할을 수행토록 한다. 법안에서 센터 활동은 법 제정 이후 8년이 지난 시점에 종료하도록 되어 있다.

2) 2017 러시아 적대행위 대응법(Counteracting Russian Hostilities Act of 2017)

'2017 러시아 적대행위 대응법(S.94)'은 러시아 발 사이버 침해행위 및 적대 행위를 제재하기 위해 2017년 1월 발의되었다. 이는 2017년 4월 위원회 송부 후 검토 중인 법안으로 러시아 美 대선개입 사건과 관련된 EO 13694[5], PPD 41[6], EO 13757[7]을 발전시키고 및 러시아 발 사이버 침해행위에 대한 제재방안 구축에 대한 내용이 주요 골자이다.

세부내용으로 컴퓨터 네트워크 또는 시스템을 통한 공공 및 민간 기반시설에 대한 침해행위를 사이버침해행위로 정의하여 민주적 제도에 위해를 가해 사이버안보를 저해하는 행위에 대한 제재의 구체적인 방식에 대해 정한다.

법안에 따른 사이버침해행위에 대한 제재는 자산 동결과 미국 비자 등과 같은 공문서 발급 제한으로 행해진다. 사이버침해행위 가담자에 대한 세부 제재 방안은 ① 미 수출입은행으로부터 상품과 서비스의 신용 보증・보험・연장 금지, ② 수출 제재, ③ 미 금융기관으로부터 대출 금지, ④ 국제금융기관으로부터 대출 금지, ⑤ 정부 관련 금융 업무 수행 금지, ⑥ 정부 구매 업무 관련 종사 제재, ⑦ 외국환 거래 제재, ⑧ 은행 거래업무 제재, ⑨ 부동산 거래 제재, ⑩ 주식투자 및 대출 제재, ⑪ 취업 금지, ⑫ 요직 취임 금지이다.

---

5) Executive Order 13694, 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities'

6) Presidential Policy Directive United States Cyber Incident Coordination

7) Executive Order 13757, 'Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities'

3) 2017 정보수권법(Intelligence Authorization Act for Fiscal Year 2017)

정보수권법은 美 정보기관의 예산에 관한 법으로 첩보, 대테러, 전쟁, 사이버안보 관련 정책 및 자원을 식별한 법이다. '2017 정보수권법(H.R.6480)'(이하 IAA 2017)은 대선 개입 사건에 대한 정책적 대응방안을 담은 내용이 포함되어 2016년 12월 발의되었다. IAA 2017은 여러 차례 수정을 거쳐 2017 통합세출법(Consolidated Appropriations Act, 2017)에 병합되어 제정되었다.

2017 통합세출법에 담긴 IAA 2017의 러시아 관련 주요 내용은 정부기관을 대상으로 하는 러시아 비밀첩보활동에 대한 대응 임무를 명시하고, 주미 러시아 외교관 및 영사의 이동시 사전 통지 의무를 부과하는 것이다. 동 법은 러시아 비밀 첩보활동에 대한 적극적 대응 의지를 나타내는데, 대응 대상 행위로는 기금조성, 비밀선전, 미디어 조작, 방첩행위 방해, 암살, 테러행위를 명시한다. 이러한 활동들을 관련위원회인 정보위원회, 상하원 군사위원회, 상하원 외교위원회 등에서 관리하고 국가정보국장, 국무부장관, 국방부장관, 재무부장관, 법무부장관, 에너지부장관, FBI 국장, 기타 대통령이 임명한 정부기관 수장이 관련 업무를 수행한다.

또한 동 법에서 주미 러시아 외교관 및 영사의 이동시 사전 통지 의무를 부여하는데, 국무부장관은 FBI 국장 및 국가정보국장과 협의하여 주미 러시아 외교관 및 영사관에 이동시 사전 통지 의무를 부여하고 이를 어길 시 필요한 조치를 통해 제재될 것임을 나타낸다. IAA 2017 법안(H.R.6393) 발의 시, 주미 러시아 외교관 및 영사관의 이동을 근무지로부터 25마일(약 40km)로 제한하고 이탈 금지의 해제를 위해서 FBI 국장의 서면 허가를 득해야 하는 것으로 되어 있었으나, 하원 통과 과정에서 제재가 다소 완화되었다. FBI 국장과 국가정보국장은 ① 주미 러시아 외교관 및 영사의 이동에 관한 사항과 ② 불이행 내역에 관한 서면의 정보공유 메커니즘을 구축하게 된다.

4) 미국민주주의수호법(안)
(Protecting Our Democracy Act)

'미국민주주의수호법(안)(H.R.356)'은 '2016 대선 해외 개입에 관한 국가위원회(National Commission on Foreign Interference in the 2016 Election)' 설립을 목적으로 발의된 법안이다. 세부 내용으로는 위원회의 설립 목적, 구성, 기능, 권한 등 명시하고 있다. 법안은 2017년 1월 6일 발의되었으나 5월 철회되었다. 그러나 대선 개입 사건과 관련하여 조속히 국가위원회 구성안을 제시하고 다수의(의안 서명 의원 218명)의 합의를 이끌어냈다는 점에서 의의가 있다.

5) 제재를 통한 미국의 적성국가 대응법
(Countering America's Adversaries Through Sanctions Act)

미 하원은 2017년 7월 미국에 적성국가로 분류되는 북한, 이란, 러시아에 포괄적 제재를 가할 수 있는 법적 근거가 되는 '제재를 통한 미국의 적성국가 대응법(안)(H.R.3364)'을 발의하였다. 동 법안은 하원과 상원의 폭넓은 지지를 받아 승인되어 대통령 서명 이후 공포될 것으로 예상된다. 동 법안의 미 대선 러시아 개입 사건과 관련 부분에 관련하여 EO 13694, PPD 41, EO 13757을 계승하고 DNI 보고서 분석을 원용한다. 법안은 대러 제재 및 외교정책과 관련된 결정에 대한 의회의 권한을 강화시키는 한편 대통령의 권한을 축소시켜 미국 대선 러시아 개입 사건이 장기화 될 것임을 시사한다.

3. 행정조치

1) 행정명령 13694

행정명령 13694 – '중대한 악의적 사이버 활용 활동에 가담하는 자의 재산 차단(Executive Order 13694, 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities')'은 사이버공간에서 미국의 국가안보, 외교정책, 경제안정에 심각한 위협을 가하는 개인과 단체에게 자산동결

등 강력한 금융제재를 취할 수 있는 근거를 마련하기 위한 목적으로 발표되었다. 시행 배경은 주요기반시설 및 기업을 표적으로 한 외국 사이버공격 증가에 있다. 주요 내용으로 사이버공격에 대한 제재 대상, 제재 행위, 제재 방식 등을 명시한다.

제재 대상에는 미국에 대한 사이버위협 활동에 직간접적으로 가담하거나 책임이 있는 사람 및 단체, 외국에 거주하는 자 또는 외국에 거주하고 있는 자로부터 지시를 받은 국내 거주자 및 단체이다. 제재 대상은 신중하게 선정될 것이며 봇넷에 감염되어 사이버공격에 이용된 컴퓨터 소유자와 같이 의도치 않은 피해자들은 제재 대상에서 제외된다. 또한 사이버공격에 대응하는 과정에서 온라인 상 표현의 자유 및 인터넷 자유를 제한하지 않을 것임을 강조한다.

제재 행위는 국가주요기반시설을 운영하는 기관의 컴퓨터 및 컴퓨터 네트워크를 공격하거나, 서비스 제공을 방해하는 모든 행위, 경쟁 우위나 금융상 사적 이익을 취하기 위해 무역 기밀, 개인 정보, 금융 정보 등을 악용하는 모든 행위이다.

이러한 행위에 대해 재무부는 국무부 및 법무부와 협의를 통해, 제재 대상으로 확정된 개인과 단체의 모든 자산을 동결하고 자산의 이전, 지불 등 금융 거래 행위를 정지시킨다. 또한 제재 대상자들에 대한 비자 발급을 제한하고 제재 대상자들이 미국 기업과 비즈니스 활동을 하는 것을 금지시킨다.

동 행정명령은 EO 13757의 선행 문건으로 러시아 대선 개입 사건과 관련된 단체와 개인에 대한 제재 근거를 마련하였다는 점에서 의의가 있다. 2017년 3월 트럼프 대통령은 동 행정명령의 적용을 1년 연장 할 것임을 발표한 바 있다.

2) 행정명령 13757

행정명령 13757 – '중대한 악의적 사이버 활용 활동과 관련한 국가적 위기를 다루기 위한 추가적 조치의 채택(Executive Order 13757, 'Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities')은 사이버 위협 활동 증가로 인한 적극적 대응 필요성의 증대에 따라 EO 13694 후속 문건으로 마련되었으며, 美 대선 러시아 개입 사건에 대한 대응을 겨냥하여 발표되었다. EO 13694와 비교하여 제재 대상 행위에 '선거 과정이나 기관을 침해하거나 위해를 가할 목적으로 정보를 부적절하게 변경하는 행위'가 추가되었으며(Sec.1(a)(ii)(E)), 5개의 러시아 기관과 4명의 GRU 소속 러시아인이 제재 대상임을 명시하였다.

행정명령에 따른 제재대상기관은 2개의 러시아 정보기관(GRU, FSB)과 이들의 활동을 지원한 3개의 민간단체들(Special Technology Center, Zorsecurity, Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems")이다. 본 행정명령은 美 대선 러시아 개입사건과 관련, 악의적 사이버 활용 활동에 선거과정 및 기관에 대한 침해를 추가하고 러시아 제재를 강화하고 직접적으로 제재 대상을 명시한 것에 의미가 있다.

Ⅳ. 국가 안보전략적 함의

본 사건은 다음의 국가 안보전략적 함의를 내포한다. 첫째, 국가정책 결정과정에 영향력을 행사하는 타국의 전략적 사이버위협에 대한 국가적 대응 방안의 필요성을 일깨워준다. 본 사건에서 보안기업들은 사건 발생 초기에 보안위협사실에 관한 조사자료를 발표하여 수사에 기여하였으며, 국가 정보기관은 사건분석보고서 발표를 통해 사건을 객관화하였다. 또한 국가 원수의 경고, 연방 기관에 대한 수사 지시, 외교적 압박, 허위정보 및 선전에 대한 전략적 대응 체계 마련 및 관련 센터(GEC) 설립, 제재 활동을 위한 예산 마련, 위법적 사이버행위에 대한 제재방식의 구체화 등으로 차후 발생할 수 있는 공격에 대한 대비 태세를 마련하고 이미 발생한 사건에 대한 수사를 강화하였다. 이러한 미국의 다각적 대응 방안 마련은 한국 정책 환경에 부합하는 타국의 전략적 사이버위협에 대한 국가적 대응 방안에

대한 시사점을 준다.

전략은 국가 사이버안보를 위협하는 다양한 공격유형을 포괄할 수 있어야하고 공격수준별 대응을 위한 가이드라인이 될 수 있어야 한다. 또한 대응역량 강화를 위한 사이버안보 체계 및 조직, 인력, 예산에 대한 포괄적 계획이 포함되어야 한다. 한국은 7.7 DDoS공격, 3.4 DDoS 공격, 농협 전산망 사이버테러, 3.20 사이버테러, 6.25 사이버공격, 한수원 해킹 사건과 같은 대대적 사이버공격 발생 시 범정부 사이버위기 종합대책(2009), 국가 사이버안보 마스터플랜(2011), 국가 사이버안보 종합대책(2013), 국가 사이버안보 태세 강화 대책(2013)과 같은 국가 차원의 종합적인 대책을 수립하여 대응하였다(Yang, *et. al.*, 2016). 국가 사이버안보 강화를 위한 대책과 함께 중장기적 국가사이버안보전략이 필요한 시점이다. 2012년 4.11 총선 당시 북한의 사이버 개입이 있었다는 신문기사가 있었으나, 이에 대한 명확한 문제제기나 조사, 선거개입에 대한 대비방안 수립이 부재하였다. 전략수립 및 전략에 따른 세부 시행규칙을 통해 국가의 민주적 정책결정과정에 대한 사이버위협에 대한 대비가 필요하다.

둘째, 사이버공간에서의 국제 질서 수립 과정에 대한 적극적 참여가 필요하다. 사이버공간에서의 문제는 국내법의 문제를 벗어나 국가 간의 갈등으로 발전되어 가고 있으며, 국제규범을 통한 국제 질서 수립에 대한 필요성이 확산되고 있다(Bae, 2017). 그럼에도 불구하고 사이버공간상의 행위에 대한 기존 국제법 규칙 적용의 기술적 어려움과 모호성으로 인하여 해석론과 신규 규범의 필요성 등에 관한 논란은 지속되고 있다. 이는 개별 국가나 진영마다 처한 사이버 위협환경과, 보다 큰 맥락에서의 안보 환경이 상이하기 때문에 법해석과 신규규범의 내용이 이해관계에 영향을 미치기 때문이다. 이는 특히 명백히 위반이 되거나 되지 않는 행위, 예컨대 사이버 공격을 통해 타국에서 대량의 인명 피해를 발생시켜 무력공격으로 판단되거나 혹은 단순히 인터넷을 통해 상대 국가를 비난하는 등에 대해서보다, 그러한 경계에 있는 행위의 영역에서 국가와 진영간 대립의 대상이 되고 있다.

이러한 교착 상황에서 국가들은 그와 같은 회색지대를 점차 자국의 이익을 위해 전략적으로 이용하고, 혹은 대응활동에도 이용하고 있다. 본 사건의 경우에도 국제법과 규범의 위반 여부가 명확하지 않은 영역에 속한다. 즉, 오바마 전 대통령의 성명에서는 이를 "확립된 국제적 행동 규범의 위반(violation of established international norms of behavior)"이라고 표현하였으며, 그 외에도 러시아의 행위를 명백히 국제법의 위반이라고 표현한 적이 없으며, 이는 미국이 의도적으로 최종적 판단을 내리지 않은 것으로 평가된다(Goodman, 2017). 미국의 공식적 국제법 입장을 대변하는 국무부 법률자문관이었던 Harold Koh는 사이버공간에서 국제법이 적용된다는 데 대해 확고한 입장을 표명한 바 있고(Koh, 2012), 그 후임자인 Brian Egan 역시 그러한 입장에 기초하여 타국의 선거 결과를 조작하는 사이버 행위가 명백히 국제법상의 불간섭 원칙을 위반한다는 견해를 표시하였다(Goodman, 2017). 그러나 이번 사건에서는 직접적으로 선거 결과를 조작하였는지 여부가 불명하여 위와 같은 입장만으로는 미 정부가 이를 국제위법행위로 평가하는지 여부는 단정하기 어렵다. 또한 양국 정상 간의 핫라인 통화에서 오바마 대통령이 사이버공간에 대한 국제법 적용을 재확인하고 이에 따라 러시아가 책임을 지도록 하겠다는 발언을 한 것으로 알려졌으나, 그 후 러시아의 법 위반을 미국이 주장한 바 없으며, 국제위법행위에 대한 법적 대응이 후행되지 않았기 때문에, 이 역시 미국이 러시아의 행위를 국제법 위반으로 평가한다는 근거로 보기는 어려울 것이다.

그러나 이와 같은 모호성은 국가 간의 오인을 부추겨 국제질서의 불안정성을 증대시키는 한편, 국가 간 협력에 대한 장애물로도 작용하고 있다. 국제법과 국제규범은 국가들의 합의에 의해서만이 성립되기 때문에 모든 국가는 자국의 이익에 따라 규범 형성에 참여한다. 따라서 우리나라 역시 국가 사이버안보 강화를 위해 국익에 기초한 종합적 판단을 내리고 이와 같은 국제 규범 형성 활동에 적극적으로 참여하여야 할 것이다.

셋째, 사이버공간을 활용한 심리전 위협에 대한 안보 전략적 고려와 함께 대중의 경각심 제고가 필요하다. 심리전은 국가 정책의 효과적인 달성을 지원하기 위해 타국 및 집단의 견해, 감정, 태도, 행동을 자국에 유리하게 유도하는 선전 및 기타 모든 계획적인 활동을 의미한다(DTaQ, 2011). 기존 전파, 인쇄물을 통한 북한의 심리전 활동은 사이버공간으로 이동되어 김정은 체제 찬양, 선동, 선전만이 아닌 지능화・고도화된 기법으로 다양하게 수행되고 있다. 이러한 활동은 사이버공간을 통해 허위정보를 유포하고 확신시켜 국론분열과 사회 혼란을 조장하여 북한에 유리한 환경을 조성토록 한다(Kim, 2016; Park, 2017). 사이버공간의 심리전에 대한 연구 강화와 함께 미 대선 러시아 개입 사건에 따라 설립된 GEC와 같이 외국정부 및 비국가단체의 선전 및 허위정보로 국가안보이익을 저해하는 활동을 저지하기 위한 역량을 결집하고, 대응활동 총괄조직 구축 등이 필요하다. 북한의 사이버공간을 활용한 심리전 활동 대응을 전담케 하거나 이러한 활동들을 통합하는 노력이 필요하다.

넷째, 사이버공격 조사 특성에 대한 대중의 이해를 확대하는 동시에 공개 가능한 범위 내에서 조사 과정 공개를 통한 조사 내용에 대한 절차적 투명성 확보가 필요하다. 사이버위협에 대한 국가적 대응 방안은 각국의 정책 환경에 적합한 방식으로 구상되어 실행됨과 동시에 사이버위협이 내포하는 고유의 특성이 반영된다. 사이버위협의 특성상 조사기관은 공격에 사용된 도구와 사용기술의 공개를 제한하는데, 이는 공격기법을 공개하면 공격자가 차기 공격 시 공개된 기술을 회피하여 조사를 어렵게 만들뿐만 아니라 조사기관의 역량을 드러내는 결과를 가져올 수 있기 때문이다. 사건 발생 시 미국의 정보기관은 이례적으로 관련 보고서를 공개하지만 동일한 문제의식 하에 DHS와 FBI가 공동으로 발표한 'GRIZZLY STEPPE-Russian Malicious Cyber Activity' 보고서의 공개본은 일반적인 내용으로 일관되었으며 결과적으로 전문가들에 의해 보고서 내용의 부실성 등으로 신뢰성이 의심되었고 이를 보완하기 위해 'Enhanced Analysis of GRIZZLY STEPPE Activity' 보고서가 발표되었다. 이러한 사이버공격 조사는 국가의 대응활동에 딜레마를 야기하는데 사이버공격 조사가 가진 특이성에 대한 대중의 이해가 필요함과 동시에 공개 가능한 범위 내에서 조사 과정을 공개하여 조사 내용에 대한 절차적 투명성 확보가 필요하다.

V. 결 론

미 대선 러시아 개입사건은 사이버공격이 가지고 있는 위험성의 새로운 측면을 부각시킨다. 기존 국가안보적 측면에서의 사이버공격의 위해는 국가주요기반시설 및 주요정보통신기반시설 공격, 전쟁 발생 시 물리전과 사이버전을 동시에 실행하여 하이브리드전 양상으로 전쟁 방식의 변화, 국가적으로 광범위한 경제적 피해 발생 등이 주된 논의의 대상이었다. 그러나 이번 사건은 사이버공간을 통해 일국이 국가 최고정책결정자를 결정하는 국민의 선택과정에 영향력을 행사하여 타국의 국내 정치과정에 개입하고, 자국에 유리한 방향으로 정책결정을 유도하여 국가이익을 확대하고자 한 사건이다. 이에 따른 미국의 신속한 국가적 대응은 추후 새롭게 개진될 미국의 국가사이버안보전략에 반영될 것으로 예상된다. 당시 북한 정찰총국 역시 민주당 해킹을 시도한 정황이 드러남에 따라, 국가 사이버안보전략 발전을 통한 유사한 방식의 북한 공격에 대한 대비가 필요할 것이다.

References

Alperovitch, Dmitri. 2016. *Bears in the Midst: Intrusion into the Democratic National Committee*. Crowdstrike Blog.

Arghire, Ionut. 2017. U.S. Gov's "GRIZZLY STEPPE" Report Fails to Achieve Purpose: Experts. *Security Week*. (http://www.securityweek.com/us-govs-grizzly-steppe-report-fails-achieve-purpose-experts).

Arkin, William M., *et. al*. 2016. What Obama Said to Putin on the Red Phone about the Election Hack. *NBC News*.

(http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116).

Bae, Young Ja. 2017. A Study of International Norms on Cyber-Security. *21st Century Political Association Paper*. 27(1): 105-128.

Bing, Chris. 2017. North Korean Hackers Came Close to Hacking Hillary Clinton's Presidential Campaign. *Cyberscoop*.

Cha, Yoon Hee, *et. al.* 2015. Russia Economic Sanction, Take a New Approach to the Russian Market. *KOTRA Global Market Report 15-033*.

Clapper, James R.(DNI). 2016. *Worldwide Threat Assessment of the US Intelligence Community*.

Coats, Daniel R.(DNI). 2017. *Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence*.

Defense Agency for Technology and Quality(DTaQ). 2011. *Dictionary of Defense Scientific and Technical Terms*.

DHS, FBI. 2016. GRIZZLY STEPPE-Russian Malicious Cyber Activity.

DHS, ODNI. 2016. Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security.

DNI. 2017. Assessing Russian Activities and Intentions in Recent US Elections.

FBI, DNI. 2016. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security.

GAO. 2014. Civilian Intelligence Community: Additional Actions Needed to Improve Reporting on and Planning for the Use of Contract Personnel.

Godwin, III., B. James, *et. al*. 2014. *The Russia-U.S. Bilateral on Cybersecurity-Critical Terminology Foundation, Issues* 2. East West Institute and the Information Security Institute of Moscow State University.

Goodman, Ryan. 2017. *International Law and the US Response to Russian Election Interference*. (https://www.justsecurity.org/35999/international-law-response-russian-election-interference/).

Ha, Young Sun and Sang Bae Kim. 2006. *Networked Knowledge State*. Euryu Munhwasa.

Han, Hee Won. 2011. *National Intelligence*. Beopyul Publishing Company.

Hutchins, Eric M., *et. al.* 2010. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Proc. 6th Int'l Conference*. Information Warfare and Security. Academic Conferences, Ltd.

Jang, Noh Soon and In Taek Han. 2013. Controversial Issues and Research Trends in Cybersecurity. *International Politics Review*. 53(3): 581.

Jang, Noh Soon and So Jeong Kim. 2016. U.S. Choices of Cyber Strategy and Their Security Implications. *Politics · Information Review*. 19(3): 57-91.

Jang, Noh Soon and Sung Kwon Cho. 2017. Cybersecurity Threats and Comprehensive Defense Strategy. *International Area Review*. 20(5): 185-208.

Kim, Yoon Young. 2016. *Changes and Prospects of NK's Phychological Warfare against SK*. 535: 45-51.

Koh, Harold H. 2012. International Law in Cyberspace: Remarks as Prepared for Delivery to the US CYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, Sept. 18, 2012. *54 Harvard International Law Journal*. 1: 1-12.

Koh, Jae Nam. 2017. Putin's 3rd Term Administration's New Diplomatic and Security Strategy. *2016-16 IFANS Policy Research Series*.

Lee, Seong Man, *et. al.* 2015. *National Security: Theory and Practice*. Orum.

Park, Nohyoung. 2017. [Security Column] Korea Needs to Actively Participate in the International Cybersecurity Order. *Etnews*. (http://ciobiz.etnews.com/20170718120009).

Park, Sang Don, Kyudong Kim, and So Jeong Kim. 2017. The New Understanding on the Meaning of Cybersecurity Legal System. *Journal of Security Engineering*. 14(2): 160.

Rampton, Roberta and Mason Jeff. 2016. Obama Blames Putin for Cyber Attacks on U.S. Election. *Fox Business*. (http://www.foxbusiness.com/politics/2016/12/16/obama-blames-putin-for-cyber-attacks-on-u-s-election.html).

Strohm, Chris. 2016. Russia 'Grizzly Steppe' Hacking Started Simply, U.S. Says. *Bloomberg* (https://www.bloomberg.com/news/articles/2016-12-30/russia-s-grizzly-steppe-cyberattacks-started-simply-u-s-says).

US DOD. 2014. *Quadrennial Defense Review 2014*.

Yang, Jeong Yoon, So Jeong Kim, and Il Seok Oh. 2016. Analysis on South Korean Cybersecurity Readiness regarding North Korean Cyber Capabilities. *KIISC WISA*.

Yoon, Oh Jun, *et. al.* 2015. A Study on Measures for Strengthening Cybersecurity through Analysis of Cyberattack Response. *Journal of Information and Security*. 15(4): 71-78.

中华人民共和国国家互联网信息办公室. 2016. 国家网络空间安全战略.

Korean References Translated from the English

고재남. 2017. 제3기 푸틴 정부의 신 외교・안보 전략과 실제. 외교안보연구소 2016-16 정책연구시리즈.

국방기술품질원. 2011. 국방과학기술용어사전.

김윤영. 2016. 북한 대남 심리전 변천 양상과 전망. 北韓. 535: 45-51.

박노형. 2017. [보안칼럼] 사이버안보 국제질서 수립에 적극 참여해야. 전자신문. (http://ciobiz.etnews.com/20170718120009).

박상돈, 김규동, 김소정. 2017. 사이버안보 법제도의 의의에 대한 새로운 이해. 보안공학연구논문지. 14(2): 160.

배영자. 2017. 사이버안보 국제규범에 관한 연구. 21세기정치학회보. 27(1): 105-128.

윤오준 외. 2015. 사이버공격 대응 분석을 통한 사이버안보 강화 방안 연구. 융합보안논문지. 15(4): 71-78.

이성만 외. 2015. 국가안보의 이론과 실제. 오름.

장노순, 김소정. 2016. 미국의 사이버전략 선택과 안보전략적 의미: 방어, 억지, 선제공격전략의 사례 비교 연구. 정치・정보연구. 19(3): 57-91.

장노순, 조성권. 2017. 사이버 안보위협의 성격과 통합적 대응의 전략적 의미. 국제지역연구. 20(5): 185-208.

장노순, 한인택. 2013. 사이버안보의 쟁점과 연구 경향. 국제정치논총. 53(3): 581.

차윤희 외. 2015. 경제제재 1년, 러시아 시장 새롭게 접근하자. KOTRA Global Market Report 15-033.

하영선, 김상배. 2006. 네트워크 지식국가. 을유문화사.

한희원. 2011. 국가정보학원론. 법률출판사.

Received: Aug. 24, 2017 / Revised: Nov. 23, 2017 / Accepted: Nov. 27, 2017

타국의 전략적 사이버공격 대응에 대한 국가 안보전략적 함의

– 美 대선 러시아 개입사건을 중심으로 –

국문초록 사이버공간을 영토, 영해, 영공, 우주에 이은 국가안보영역으로 인식하여 사이버 공간을 활용해 국가의 영향력을 확대하려는 노력이 증가하고 있다. 또한 정보자원의 무결성을 공격해 국가 정책 결정과정에 영향을 미치고자 하는 국가차원의 전략적 공격이 발생하고 있다. 2016년 11월 치러진 미국 대통령 선거과정에 대한 러시아 개입 의혹은 이러한 시도의 일환으로 추정되며 동 사건에서 미 정부는 입법과 행정조치 등을 통해 러시아에 대한 제재를 취하는 한편 정보·수사기관과 의회 조사위원회를 통한 조사를 병행하고 있다. 본 논문에서는 美 대선 러시아 개입사건에 대하여 미 정보기관에서 발표한 보고서를 중심으로 사실관계를 검토하고, 대선 이후 중단기간 미국이 취한 입법적·행정적 대응방식 살펴본다. 타국의 전략적 사이버공격에 대한 일국의 국가적 대응방식을 살펴보는 과정을 통해 한국의 국가 사이버안보전략에 미치는 시사점을 도출한다.

주제어 : 사이버공격, 사이버안보전략, 미국, 러시아, 한국

Profiles **Jeong Yoon Yang** : She is a researcher at the Cybersecurity Policy Department of the National Security Research Institute, Korea. She received her M,A. from Graduate School of International Studies at Seoul National University in 2015. Her areas of research include national cyber security policies, China's cybersecurity strategies, and Russia information security. She has published several papers on cyber security policies, including 'Analysis on South Korean Cyberseuciry Readiness regarding North Korean Cyber Capabilities(2016)'(jyyangrok@nsr.re.kr).

Kyudong Kim : He is a researcher at the Cybersecurity Policy Department of the National Security Research Institute, Korea. He is a Ph.D. candidate at Korea University School of Law, and holds LL.M degrees in public international law and international human rights from Georgetown University Law Center and Korea University, and LL.B. from Korea University. His areas of research include national cyber security strategy, international law. He has written several papers on cyber security legal issues and was part of the Korean delegation to the 4th and 5th UNGGE, the Global Conference on Cyber Space, and other bilateral cybersecurity talks(kyudongkim@nsr.re.kr).

So Jeong Kim : She is head of Cybersecurity Policy Department of the National Security Research Institute(NSR), Korea and has worked at the NSR since 2004. She received her Ph.D. in Engineering from the Graduate School of Information Security at Korea University in 2005. Her primary research focus includes cyber security strategy, policies, and the international security of cyberspace. She has written several papers on cyber security policy issues and has been involved at multiple governmental meetings, most recently including the 4th and 5th UNGGE(sjkim@nsr.re.kr).