사이버 '전쟁'?
새로운 조약이 필요한 이유

아산정책연구원
김길동 연구원
2017.03.13

*본 보고서는 전략분석실 김진우 박사 지도하에 작성되었습니다.

백악관 지하 좁은 사무실, 보좌관들에 둘러싸인 오바마 대통령은 이란의 나탄즈(Natanz) 우라늄 농축시설의 컴퓨터시스템에 대한 사이버 공격을 비밀리에 승인했다. 후에 스턱스넷(Stuxnet)이라 명명된 웜바이러스(worm virus)는 고농축 우라늄 원심분리기가 스스로 파괴될 때까지 임의로 감속 또는 가속시키도록 만들어졌다. 여기서 주목할 점은 시설관리자들 중 그 누구도 악성코드가 이를 조정했을 것이라고 의심하지 않는다는 것이다. 그들에게는 그저 일상적인 고장으로 보여졌기 때문이다. '올림픽 대회 작전'(Operation Olympic Games)이라고 불렀던 이 작전의 성공에 고무된 오바마 대통령은 더 큰 규모의 사이버 공격을 지시했다.[1]

백악관과 6,000마일 떨어진 나탄즈의 원자력 과학자들은 화창한 여름날의 일상을 보내고 있었다. 모든 것이 정상적으로 돌아가고 있었다. 그런데 갑자기 1,000대 정도의 원심분리기가 통제불능 상태에 빠지더니 폭발하고 말았다. 이들은 급작스럽게 벌어진 상황에 당황하며 문제를 규명하기 위해 컴퓨터 앞에 앉았지만 모니터에는 모든 것이 정상적으로 작동되었다고만 나왔다. 이들은 원인도 모르는 채 눈앞에서 시스템이 무너지는 것을 속수무책으로 지켜볼 뿐이었다.[2]

---

[1] David Sanger, "Obama Order Sped Up Wave of Cyber Attacks against Iran," *The New York Times,* June, 12, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[2] Ibid; Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired,* Nov. 03, 14,https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

올림픽 대회 작전이 완벽하게 마무리되는가 싶던 찰나 예기치 못한 일이 벌어졌다. 스턱스넷이 인터넷을 통해 삽시간에 퍼지기 시작한 것이다. 이 말웨어(malware)는 나탄즈 원자력 시설 밖으로 나가지 못하도록 설계되었으나 스턱스넷 파일이 들어간 유에스비(USB)가 인터넷에 연결된 컴퓨터에 꽂히면서 말웨어는 순간적으로 자기복제를 하며 전 세계로 퍼져 나갔다. 그제야 이란은 나탄즈 원자력 시설이 누군가에 의해 고의로 파괴되었음을 알게 되었다.[3]

속수무책으로 당한 이란은 문제의 악성코드를 손에 넣고 무기화했다. 이란은 재공격의 우려 때문이었는지 미국에 대한 직접적인 보복보다는 중동에서 미국과 가장 가까운 동맹국인 사우디아라비아를 표적으로 선택했다. 2012년 8월, 이란은 세계에서 가장 큰 석유회사인 사우디아라비아의 아람코(ARAMCO)에 사이버 공격을 감행했다. 이 공격으로 아람코의 35,000개 컴퓨터 하드드라이브의 데이터가 삭제되었고 디지털 인프라는 심각한 타격을 입었다. 세계 석유의 10퍼센트를 담당하던 아람코의 공급능력이 한 순간에 훼손되었다.

이것이 바로 새롭게 등장한 '불편한 진실'이다. 전쟁은 이제 폭탄과 총탄으로만 수행되는 것이 아니다. 비트와 바이트는 토마호크 미사일 못지않은 파괴력을 갖게 되었다. 클릭 한 번으로 수천 마일 떨어진 국가의 원자로를 마비시켜 경제를 곤경에 빠트릴 수 있다. 특히 비대칭 능력을 지닌 국가들은 새로운 전쟁 수단이 된 사이버 공격의 유혹을 뿌리치기 힘들다. 작전 비용이 적고, 공격 주체 식별이 거의 불가능하기 때문이다. 이미 29개국에서는 군에 사이버 부대를 신설했고, 통상적인 전쟁 수행 계획에도 사이버 무기를 포함시켰다. 비관론자들은 사이버 무기 확산은 불가피하다고 주장한다.[4] 미국 국가안보국(NSA) 사이버 지휘부(Cyber Command)의 책임자였던 키스 알렉산더(Keith Alexander)는 "두고 보라. 앞으로 더 심해질 것이다"라고 할 정도였다.[5]

---

[3] Ibid.

[4] Jennifer Valenito-Devries and Danny Yadron, "Cataloging the World's Cyberforces," *The Wall Street Journal*, Oct. 11, 2015, *http*://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710; McAfree Report, In the Crossfire: Critical Infrastructure in the Age of Cyber War, 2010, 11, http:// resources.mcafee.com/content/NACIPReport.

[5] Andrea Shalal-Esa, "Top General Says U.S. under Constant Cyber Attack Threat," *Reuters*, May, 14, 2013, http://www.reuters.com/article/us-cyber-summit-alexander-idUSBRE94D12L20130515.

사이버 공격이 세계로 확대되자 각국의 지도자들과 법률가들은 스턱스넷과 같은 최악의 파괴적인(destructive) 사이버 공격을 두려워하며 이에 대한 대비책을 마련하는 데 한 목소리를 내고 있다. 그러나 오늘날에는 물리적인 피해를 초래하지는 않지만 사회·경제·정부에 심각한 타격을 입히는 교란성(disruptive) 사이버 공격에 대한 규제가 절실히 요구된다. 본 보고서에서는 이런 공격을 '전쟁에는 못 미치는 사이버 공격(cyber-attacks-short-of-war, 이하 CASoW)'이라는 새로운 용어로 부르기로 한다. 즉 **'정치적인 이유로 국가 및 비국가가 민간 또는 공공재산을 표적 삼아 수행하는 사이버 공격으로 실제 물리적 피해는 없어도 사회·경제·정부에 심각한 혼란을 일으키려는 목적으로 실행되는 공격'**을 의미한다.[6] 물리적 피해나 인명 손실을 초래하는 사이버 공격은 전통적인 전쟁법 관장 범위에 들어갈 수 있다. 그러나 CASoW는 무정부·비규제 공간에서 수행되며, 이 공간을 관장할 강제적인 법규는 현재 없다. 현대 사회에서 가장 큰 위협이 되는 것은 사이버 전쟁이 아니라 바로 CASoW이다.

유엔 헌장과 사이버 전쟁

전쟁 선포의 정당성(jus ad bellum)과 전쟁 행위의 정당성(jus in bello)에 대한 이론은 상당히 오랫동안 유지되었다. 그러나 유엔 헌장 제2조 4항에는 '영토 보전이나 정치적 독립에 대하여 (중략) 무력적 위협이나 무력행사를 삼간다'라고 명시되어있어 전쟁 선포의 정당성은 더 이상 논하지 않아도 되게 되었다.[7] 제51조에는 '유엔 회원국에 대하여 무력 공격이 발생한 경우 이 헌장의 어떠한 규정도 (중략) 개별적 또는 집단적 자위의 고유한 권리를 침해하지 아니한다'는 예외 조항도 있다.[8] 한마디로 자위를 제외한 합법적인 무력 사용은 안전보장이사회의 결의를 받아야만 한다는 것이다.

유엔 헌장에서는 '무력 사용'(use of force)과 '무력 공격'(armed attack)을 구체적으로 정

[6] 이 용어를 사이버범죄와 혼동해서는 안 된다. 사이버범죄는 개인적 경제적 동기로 수행하는 행위며 일반적으로 파급효과가 덜하다.

[7] United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, available at: http://www.refworld.org/docid/3ae6b3930.html

[8] Ibid.

의하지 않았지만 지난 수십 년간 국제사법재판소(ICJ)의 판결은 방향과 선례를 제시해주고 있다. 즉 '무력 공격'보다 범위가 넓은 '무력 사용'은 미사일 실험, 무인지대 폭격 등이 포함된다. 국제사법재판소에서 가장 '심각한 형태의 무력 사용'[9]으로 규정하고 있는 '무력 공격'에는 공중 폭격, 지상공격, 마사일 타격, 영토 침략 등이 속한다.

특정 공격 행위를 '무력 사용'과 '무력 공격' 중 어느 것으로 규정하느냐가 관건이다. 그 결과에 따라 피해국은 공격국에 대해 적정하고, 합법적이고, 정당한 대응을 할 수 있다. 다시 말해 '무력 사용'이 있었을 경우 피해국은 경제 제재 등의 대응 조치를 취할 수 있으나 '무력 공격'을 해서는 안 된다. '무력 공격'이 있었을 경우에는 제51조의 자위 조항에 따라 피해국은 비례(proportionality)와 필요(necessity)의 원칙에 따른 무력으로 보복하는 것이 적법하다.

그렇다면 국제법은 어떤 기준으로 사이버 공격을 '무력 사용' 혹은 '무력 공격'으로 규정하는가? 이 질문에 답을 제시하는 가장 권위 있는 연구 문서는 <사이버 전쟁에 적용할 수 있는 국제법에 관한 탈린 매뉴얼>(2013)이다. <탈린 매뉴얼은> 비록 법적 구속력은 없지만 나토(NATO)가 지원한 학술연구이다.[10] 이 매뉴얼에서 사이버 공격은 규모와 효과가 '무력 사용'에 상응하며 비사이버 작전에 준할 때 '무력 사용'에 해당한다고 간주한다.[11] 즉, 폭탄과 동일한 결과를 초래할 때 '무력 사용'으로 간주되는 것이다. 그리고 '무력 공격'으로 간주되려면 공격 결과로 인한 재산의 물리적 피해나 인명 손실이 있어야 한다.[12] 이에 상응하는 사이버 공격의 종류로는 ① 원자력 발전소 사고를 유발하는 작

---

[9] 국제사법재판소(ICJ), Military and Paramilitary Activities in and against Nicaragua (Nicaragua *v.* United States of America), accessed at: http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5

[10] 2009년, NATO의 북대서양조약기구(NATO) 산하 사이버방어협력센터(CCDCOE)는 국제법전문가 그룹을 구성하여, 기존의 국제법으로 새로이 등장하는 공격 기술을 다룰 수 있는가를 조사하도록 하였다. 탈린매뉴얼 전문은: https://ccdcoe.org/tallinn-manual.html 에서 읽을 수 있다.

[11] For more detail: https://ccdcoe.org/tallinn-manual.html

[12] Michael N. Schmitt, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, (New York: Cambridge University Press, 2013).

전, ② 인구 밀집지역 상류에 위치한 댐 수문을 열어 시설물 파괴와 인명 손실을 초래하는 작전, ③ 항공교통 관제시스템의 장애를 일으켜 항공기 추락을 유발하는 작전 등이있다.[13] 다행스럽게도 아직까지 이런 시나리오는 현실화 되지 않았지만 그렇게 된다면 그 결과는 가시적이고 구체적이며 측정 가능할 것이다.

사이버 공격이 실질적인 재산 피해나 인명 손실로 이어지지 않을 경우에는 어떻게 되는가? 이런 사이버 공격은 자위권을 발동케 하는 '무력 사용' 또는 '무력 공격'으로 간주될 수 있을까? 그렇지 않다면 이에 대한 적정한 대응은 무엇인가? 만약 사이버 공격이 국가가 지원하는 비국가 대리인에 의해 수행된다면 무력사용과 무력공격에 관한 국제법을 적용할 수 있는가?

전쟁에는 못 미치는 사이버 공격(Cyber-Attacks-Short-of-War)

퇴역 장성인 찰스 던랩(Charles Dunlap) 소장은 담담하게 소견을 피력했다.

"기본적으로 사이버 공격은 여타 공격에 적용되는 교전수칙이 똑같이 적용된다."[14]

하지만 그는 '같은 수칙이 적용되는 것이 타당한가'라는 중요한 질문을 간과하고 있다. 현재 벌어지고 있는 사이버 공격은 사회·경제·정부의 '심각한 교란'을 초래하는 것이 사실이지만 스턱스넷을 제외하고는 어떤 사이버 공격도 물리적 피해를 초래한 경우는 없다. 또 국가가 사이버 공격을 수행한 경우가 거의 없다는 점도 문제를 더욱 어렵게 만든다. 대부분의 경우 국가가 사이버 공격을 기획하고 수행하지만 애국심이 투철한 해커들을 고용하여 사후 책임을 부인할 여지를 남겨두기 때문이다. 또한 CASoW는 유엔 헌장의 권한에 속하지 않으며 그리고 전쟁 선포의 정당성 원칙을 발동하는 것이 아니기 때문에 적용 가능한 새로운 법규가 요구된다.

그렇다면 CASoW는 정확히 무엇인가? 여기에 포함되는 공격 행위는 사이버 첩보, 사이

[13] Harold H. Koh, "International Law in Cyberspace," *Harvard International Law Journal* (2012) Vol. 54

[14] Peter W. Singer, Allan Friedman, *Cybersecurity: What Everyone Needs to Know,* (Oxford University Press: New York), 2014.

버 사보타주, 사이버 국가 전복 등이 있다. 특정 사이버 공격이 CASoW에 해당되는지 판단하려면 ① 공격자의 의도, ② 공격자와 정부와의 관계, ③ '심각한 교란'의 수준과 범위 등 세 가지를 검토해야 한다. 여기서 앞의 두 항목에 더 큰 비중을 두는데, 그 이유는 공격자의 의도와 소속기관은 비교적 신속하게 파악할 수 있지만 '심각한 교란'에 대해서는 그 자체가 주관적이고 측정이 어렵기 때문이다. 따라서 공격자가 정부와 긴밀한 관계이거나 '심각한 피해'를 입힐 만큼 정치적 동기가 있다는 것이 입증될 경우 CASoW로 규정할 수 있다. 다음 사례는 CASoW의 심각한 결과를 구체적으로 보여준다.

최대 규모의 부의 이전

국가간 첩보 행위 때문에 전쟁을 하지는 않는다. 하지만 첩보원이 국가 안보에 직접적인 위협을 가할 수 있는 정보를 훔치다가 발각되면 어떻게 될까? 미국은 매년 사이버 공격으로 인해 3,500억 달러의 손실을 본다. 키스 알렉산더는 이를 '역사상 최대 규모의 부의 이전'이라고 표현했다.[15]디지털 혁명 덕분에 세계 각국은 더 이상 값비싼 위성, 항공기, 잠수함, 첩보원 등 대규모 물량을 투입하지 않고도 초고속 인터넷이 연결된 노트북 몇 대와 유능한 해커 몇 명만으로 중요한 정보를 확보할 수 있게 되었다. 이렇듯 진입 장벽이 낮아지면서 사이버 첩보 확산을 촉진시키고 있다.

작전의 규모보다 더 심각한 문제가 있다. 유출된 정보는 민감성과 경제적 중요도에 따라 한 국가의 안보와 경쟁력에 큰 타격을 가할 수 있다. 2009년 5월, 미국 국방부는 정부와 군수업체들의 전산망에 중국 해커들이 침투했다고 발표했다.[16] 이들이 가져간 정보 중에는 미국이 향후 55년간 사용할 차세대 전투기인 F-35의 설계도 및 제작 공정에 관한 정보도 포함되어 있었다. 미국은 차세대 전투기 개발 사업에 14년간 약 1조 5천억

[15] Josh Rogin, "NSA Chief: Cybercrime Constitutes the Greatest Transfer of Wealth in History," *Foreign Policy*, July 9, 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/
https://www.wsj.com/articles/SB10001424127887324328904578621880966242990.

[16] Office of the Secretary of Defense, "Military Power of the People's Republic of China 2009," accessed at:
https://www.defense.gov/Portals/1/Documents/pubs/China_Military_Power_Report_2009.pdf.

달러를 투입했다.[17] 중국은 이 정보를 바탕으로 개발 비용 없이 중국산 J-31 전투기를 제작할 수 있었다.[18] 미국 국방부의 기술·군수 책임자였던 프랭크 켄달(Frank Kendall) 전 차관은 "이로써 적이 들여야 할 비용과 리드타임을 줄여줬고, 적에게 괄목할 만한 우위를 내주고 말았다."[19] 라고 말했다.

미국 국방부의 핵심 자문기관인 국방과학위원회(Defense Science Board)는 미국이 수십 년간 경험하며 개발한 운용개념 및 시스템 사용(자동화 및 인간 조종 프로세스)에 대한 지식, 즉 실험실이나 공장에서 생성될 수 없는 경험적 지식을 중국이 확보한 것이 가장 심각한 문제라고 지적했다. 중국은 이 정보 덕분에 신기술에 대응하는 기술을 단기에 개발할 수 있었다.

웨스트버지니아주(West Virginia)의 조 만친(Joe Manchin) 상원의원은 중국에 대해 보복 조치를 하지 못한 오바마 정부를 신랄하게 질타했다.

"중국은 우리 덕분에 유례없는 속도로 비약적인 발전을 하고 있다. 우리도 이 점을 잘 알고 있지만 우리는 어떠한 대응도 하지 않고 있다."[20]

오바마 정부는 작전을 수행한 세 명의 민간인 해커 중 한 사람인 수 빈(Su Bin)만을 기소했으며, 법원은 겨우 5년 징역형을 선고했다.[21] 공식적인 외교채널을 통한 항의도 없었고, 유엔안보리에 결의안을 상정하지도 않았으며, 경제 제재 조치도 없었다.

---

[17] Naval Air Warfare Center, "Joint Strike Fighter F-35 Lightning II Fact Sheet," accessed at: http://www.jsf.mil/news/docs/20160324_Fact-Sheet.pdf.

[18] Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," *DOD*, January 2013, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[19] David Alexander, "Theft of F-35 Design Data Is Helping U.S. Adversaries," *Reuters*, June, 19, 2013, http://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619.

[20] Brendan McGarry, "Lawmaker: Chinese J-31, J-20 Mirror American F-35, F-22," *Defensetech*, September, 29, 2015, https://defensetech.org/2015/09/29/lawmaker-chinese-j-31-j-20-mirror-american-f-35-f-22/.

[21] Justin Ling, "Man Who Sold F-35 Secrets to China Pleads Guilty," *Vice News*, March 25, 2016, https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty.

에스토니아의 대규모 사회 혼란

2007년, 러시아와 에스토니아는 에스토니아의 수도 탈린(Tallinn)에 있는 소비에트연방 전쟁기념 동상 철거를 두고 충돌했다. 에스토니아의 러시아계 국민들은 이를 제2차 세계대전 전사자를 추모하는 기념물로 생각했고, 에스토니아인들은 50년간 지속된 소련 점령의 상징으로 여겼다. 에스토니아 정부가 동상 철거를 고려하자 러시아계 국민들은 거리로 나와 반대 시위를 벌였다. 러시아의 푸틴 대통령은 '되돌릴 수 없는 결과'를 초래할 것이라는 경고로 겁박했다.[22] 그럼에도 불구하고 에스토니아 정부는 2007년 4월 27일 문제의 동상을 탈린 국군묘지로 이전했다.

바로 그 날, 에스토니아는 대대적인 디도스(DDoS, 분산 서비스 거부) 공격을 받았다. 그 결과 신용카드 거래와 은행계좌가 동결되었고, 뉴스 매체의 방송도 중단되었다. 뿐만 아니라 주요 기관의 홈페이지가 다운되었고, 이동통신망도 마비되면서 국민들은 공포에 휩싸였다. 손발이 마비된 에스토니아 정부는 국민들과 소통할 방법이 없었다. 결국 거의 3주 후 에스토니아의 사이버 비상대응팀(Cyber Emergency Response Team)이 침입자들을 제거하고 핵심 서비스를 복구하며 최악의 상황을 끝냈다. 다행히 물리적 피해나 인명 손실은 없었지만 두려움과 공황 상태에 빠졌던 에스토니아인들은 이 사건을 자신들의 9·11사태라고 표현한다.[23]

에스토니아 당국은 공격의 근원지로 러시아를 지목하였으나 러시아 정부는 자신들과는 무관한 일이며 친정부 해커집단인 나시(Nashi)의 소행이라고 화살을 돌렸다.[24] 초기에 에스토니아는 집단방위를 규정한 나토 제5조를 발동할 것을 고려하였으나 다른 나토 국가들이 사이버 공격을 '무력 공격'으로 간주하는 것을 꺼리며 한 발 물러섰다.[25] 에스

---

[22] Gary Peach, "Statue Symbolizes Grudges Against Russia," *The Associated Press,* April, 22, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/04/22/AR2007042200617_pf.html.

[23] Patrick Howell O'Neill, "The Cyberattack that Changed the World," *The Daily Dot,* May 20, 2016, http://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/.

[24] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, *Berkeley Journal of Law* (27), 2009, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil

[25] Scheherazade Rehman, "Estonia's Lessons in Cyberwarfare," *US News,* Jan. 14, 2013, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

토니아는 달리 보복할 방법이 없자 국내법과 규정에 의거하여 피의자들을 기소하였다. 러시아와 에스토니아는 사법 공조협정에 따라 범죄 수사에 상호 협조할 의무가 있었지만 러시아 대검찰은 에스토니아의 범죄인 인도 요청을 거절하였다. 에스토니아 정부는 결국 탈린에 거주하는 러시아계 학생 한 명을 처벌하는 것으로 이 일을 마무리했다. 에스토니아 전국을 최악의 혼란으로 빠뜨린 이 학생은 고작 1,642달러 벌금형을 받았다.

러시아는 넘지 말아야 할 선을 넘은 것인가

2016년 10월, 오바마 정부는 러시아가 미국 대선에 개입했다고 주장했다. 이보다 앞선 두 달 전, 미국 정보당국은 러시아가 대선 개입을 시도한다고 경고하였고 결국 우려는 현실이 되고 말았다. 러시아가 민주당국가위원회(DNC)의 컴퓨터를 해킹하고, 힐러리 클린턴의 이메일을 위키리크스(WikiLeaks)에 흘린 것 이다.[26] 러시아는 이를 완강히 부인하였지만 미국 국가안보국(DHS)과 연방수사국(FBI)은 문제가 되는 공격은 러시아 정부를 대리한 에이피티(APT, Advanced Persistent Threat)29와 에이피티28의 소행임을 확인했다.[27] 중앙정보국(CIA)은 이들의 공격 목적을 도널드 트럼프(Donald Trump)의 당선으로 분석했다.[28] 러시아의 개입이 대선의 결과에 직접적으로 영향을 미치지 않았을 수도 있지만 사이버 공격이 분명히 있었음은 부인할 수 없다.[29]오바마 대통령도 이 점에 동조했

[26] Adam Entous, Ellen Nakashima, and Greg Miller, "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House," *The Washington Post*, Dec. 9, 2016, https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.8253de2f0c12; 아싼지(Assange)는 반복적으로 이메일이 러시아 정부에서 온 것이 아니라고 주장했다. 그러나 12월 Hannity의 라디오방송에서 인터뷰를 하면서 그는 Guccifer 2.0(실제 이메일을 유출시킨 해커)의 활동은 러시아와 관련이 있을 수 있다는 가능성을 부인하지 않았다. https://www.washingtonpost.com/news/fact-checker/wp/2017/01/05/julian-assanges-claim-that-there-was-no-russian-involvement-in-wikileaks-emails/?utm_term=.b18da842ee3a.

[27] President Obama stated, "These data theft and disclosure activities could only have been directed by the highest levels of the Russian government."

[28] Miller, "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House."

[29] Philip Rucker and Ashley Parker, "Trump Admits to Russian Hacking Even as He Attacks U.S.

다.

"어느 누구도 대선 기간 동안 러시아의 해킹이 트럼프보다는 힐러리의 선거운동에 지장을 줬다는 것을 부인할 수 없다."[30]

국가안보국(NSA)의 국장이자 사이버컴(CYBERCOM) 총사령관인 마이클 로저스(Michael S. Rogers)도 같은 의견이었다.

"이번 사건은 무심코 저지른 행동도 우발적인 행동도 아니며, 무작위로 표적을 택한 것도 아니다. 분명히 한 국가가 특정한 효과를 노리고 의도적으로 저지른 행동이다."[31]

트럼프 대통령조차도 처음에는 러시아를 지목한 주장을 가짜 뉴스(fake news)라고 일축했으나 나중에는 러시아가 공격의 배후에 있다고 인정했다.[32]

이렇듯 러시아의 심각한 침해 행위가 있었음에도 불구하고 오바마 정부의 대응은 너무나 약했다. 2016년 12월 29일, 미국 정부는 러시아 외교관 35명을 추방하고, 러시아 정보관리들을 해외자산통제국(OFAC)의 특별 제재 지정 대상 리스트(SDN List)에 포함시킨다고 발표했다.[33] 그리고 첩보 활동에 이용된 러시아 레저 단지 두 개를 폐쇄했다. 오바

Intelligence Community," *Washington Post*, Jan. 11, 2017, https://www.washingtonpost.com/politics/trump-admits-to-russian-hacking-even-as-he-attacks-us-intelligence-community/2017/01/11/40941a34-d817-11e6-b8b2-cb5164beba6b_story.html?utm_term=.945272cd7e98

[30] Scott Detrow, "Obama on Russian Hacking: We Need to Take Action. And We Will." *NPR*, December 15, 2016, http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will

[31] Eric Lipton, David Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[32] Philip Rucker and Ashley Parker, "Trump Admits to Russian Hacking Even as He Attacks U.S. Intelligence Community," *Washington Post*, Jan. 11, 2017, https://www.washingtonpost.com/politics/trump-admits-to-russian-hacking-even-as-he-attacks-us-intelligence-community/2017/01/11/40941a34-d817-11e6-b8b2-cb5164beba6b_story.html?utm_term=.945272cd7e98.

[33] The White House, "Fact Sheet: Actions in Response to Russian Malicious Cyber Activities and Harassment," December, 29, 2016, accessed at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and.

마 대통령은 미국이 비밀리에 보복할 것이라고 했다. 그러나 많은 사람들은 존 매케인(John McCain, R-AZ) 상원의원과 린지 그레이엄(Lindsey Graham, R-SC) 상원의원과 같은 견해를 보였다.

"이번 제재 조치는 미국의 민주주의를 무모하게 공격한 러시아의 파렴치한 행동에 대한 대가로는 너무나 가볍다."[34]

권고: CASoW를 위한 새로운 사이버 조약

위의 세 가지 CASoW의 예를 통해 사이버 공격의 잠재적 파괴력을 살펴보았다. 사이버 공격은 피해국에 '심각한 피해'를 초래하지만 기존의 전쟁법으로는 사이버 공격을 다룰 수 없기 때문에 재발을 억제할 만한 대응책을 찾지 못한다. 따라서 본 보고서는 새로운 국제조약 도입을 촉구한다. 이 조약을 통해 모든 사이버 공격의 판단 기준과 응분의 결과를 명확하게 규정하여 대리인의 행동에 대해서도 해당 국가가 책임을 지도록 해야 한다.

우선 CASoW로 분류하기 위한 요건을 명확히 하고 보복의 비례성을 정의한다면 가해국과 피해국은 사이버 공격의 대가를 사전에 인지할 수 있을 것이다. 합의된 기준과 결과를 구속력 있는 조약으로 성문화하여 피해국이 상응하는 대응 조치를 취하는 것이 법적으로 허용되어야 한다. 이보다 더 중요한 것은 가해국으로 하여금 CASoW를 수행하기 전에 결과에 대해 계산하도록 만드는 것이다. 가해국은 과연 이 공격을 통해 '응분의 대가'라는 커다란 위험보다 더 큰 '상당한 수준의 이득'을 취할 수 있는지 반드시 계산해야 할 것이다.

새로운 사이버 협정은 책임 귀속 문제도 해결할 수 있다. 디지털 범죄 수사는 지금도 쉽지 않다. 만약 공격자를 밝혀냈다고 하더라도 국가는 개입 사실을 부인하거나 민간인이나 하위 집단에 책임을 전가함으로써 중대한 책임을 회피한다. 따라서 새로운 조약은 국가가 비국가 행위자의 행동에 대하여 부분적 또는 총체적인 법적 책임을 지게 할 것

[34] Senate Press Release. http://www.mccain.senate.gov/public/index.cfm/press-releases?ID=DFAE6FFD-976A-468C-B53B-15D548E46BD7. Accessed February 16, 2017.

이다. 이것은 2001년 아프가니스탄의 탈레반(Taliban)에 대한 공격을 정당화하기 위해 미국이 취했던 접근 방식과 같다. 마지막으로 모든 국가들이 피해국 수사에 협조하도록 의무화하는 조항도 포함시켜야 한다. 범죄 혐의가 있거나 유죄 판결을 받은 해커들에 대한 인도 요청을 할 수 있게 범죄인 인도 조항 역시 이 조약의 중요한 부분이 되어야 한다. 만약 어떤 체약국이든 조약을 불이행할 때는 피의자와 피의자가 활동한 국가가 공모한 것으로 간주될 것이다.

결론

백악관의 사이버 안보 및 테러리즘 보좌관이었던 리처드 클라크(Richard Clarke)의 말에 귀 기울여야 한다.

"내가 제일 걱정하는 것은 지주만 같았던 대대적인 사이버 공격이 아니라 천 개의 작은 상처로 피 흘려 죽는 것이다. 공격받을 때마다 심각하지 않은 것 같아 대응하지 않고 넘기다가 보면 어느 새 손 쓸 수 없는 상황에 이르게 될 것이다."[35]

그의 말은 사이버 문제의 핵심을 찌른다. 전통적인 전쟁법규로는 CASoW 문제를 다룰 수 없다. 사이버 공격은 가시적·물리적 피해나 인명손실을 초래하지 않고도 경제·사회·정부를 심각하게 교란시킬 수 있다. 또 전통적으로 전쟁을 촉발할 정도까지 이르지 않기 때문에 각국은 앞으로 발생할 공격에 대한 억지책을 내놓지 않았다. 문제를 더욱 심각하게 만드는 것은 사이버 공격의 범인들이 '침대에 앉아 있는 체중 400파운드의 누군가'[36]가 아니라 막강한 재력과 기술력을 겸비한 개인이나 전문가 집단이라는 것, 그리고 대부분의 경우 정부가 이들을 용인하고 때로는 드러내 놓고 지원한다는 점이다.[37]

---

[35] Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian Magazine*, April 2012, http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/.

[36] 2016년 1차 대선토론에서 트럼프는 해킹이 "침대에 앉아있는 체중 400파운드의 한 사람(someone sitting on their bed weighing 400 pounds)"의 소행일 수 있다고 말했다.

[37] Remarks by Eugene Spafford in James Fallows, "Cyber Warriors," *The Atlantic*, March

이 보고서에서 제시한 세 가지 사례는 새로운 사이버 조약의 필요성과 조건을 충분히 보여준다. 만약 세계가 CASoW를 관장할 사이버 협정에 합의에 도달하지 못한다면 오늘날 고도로 상호 연결된 각국의 안보와 경제는 심각한 위협을 맞게 될 것이다. 토마스 홉스(Thomas Hobbes)는 '뒤늦게 깨닫는 진실이야말로 지옥'이라고 했다. 이 위험한 상황에 대한 해결책이 시급하다. 사이버 무법시대(Wild West)를 방치하는 것은 인류의 비극을 자초하는 것이다.

2010,https://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/.