미국의 사이버안보 거버넌스 구축과 ‘워너크라이'(WannaCry)’ 대응

홍건식(중앙대학교 국익연구소)

목차

I. 서론
II. 사이버공간과 안보거버넌스
 1. 사이버안보
 2. 사이버 공간과 사이버안보 거버넌스
III. 미국의 사이버안보 전략(거버넌스-안보로의 전환)
 1. 오바마 행정부: 백악관 중심의 사이버안보거버넌스
 2. 트럼프 행정부: DHS 중심의 사이버안보거버넌스
IV. 미국의 ‘워너크라이'(WannaCry)’ 대응: 사이버안보 거버넌스
 1. 북한의 사이버안보 전략과 능력
 2. 미국의 ‘워너크라이'(WannaCry)’ 대응: 사이버안보 거버넌스
V. 결론

요약문

2017년 5월 사이버 공간에서 워너크라이(WannaCry) 랜섬웨어의 급속한 확산은 전 세계를 공포로 몰아넣었다. 워너크라이는 전 세계에 무차별적으로 퍼졌으며, 병원, 학교, 기업 및 가정에서 수십만 대의 컴퓨터를 암호화하고 쓸모없게 만들었다. 워너크라이 랜섬웨어 해결의 특이점은 정부, 민간 그리고 국제적 차원의 협조 체계를 바탕으로 하는 안보거버넌스 체계를 바탕으로 한다. 미국의 국토안보부는 국제적 차원에서 영국, 일본, 호주 등 사이버 공격의 직접적인 피해 국가들과 파트너 체계를 구축하며 공동의 대응을 보이며 적극적으로 문제를 해결하는 움직임을 보였다. 이에 본 연구는 워너크라이 대응과정에서 보인 미국의 사이버안보 거버넌스 구축 과정을 추적하고 워너크라이 사건에 실질적으로 어떠한 대응을 보였는가를 분석한다.

I. 서론

사이버 공간에서 북한의 능력은 증대되고 있으며 그 영향 또한 광범위하다. 북한은 사이버 공간에서 사이버 범죄를 통해 국제 제재 조건에서 정치자금을 조달하기 위한 통로로서 그리고 유사시 적을 혼란에 빠뜨릴 수 있는 비대칭 전력으로 고려한다. 북한에게 사이버 전력은 북한의 국력을 구성하는 핵심 전력이라 할 수 있다. 김정은 정권은 집권 초기 첨단 과학기술 강화, 정보통신망 구축, 전국 범위의 과학기술 보급과 사이버 보급 등으로 북한의 산업 현장과 민생 수요를 반영하는 한편 사이버 전력에 대한 정책적 지원을 지속하고 있다(정영애 2019). 북한의 사이버 공격의 대표적인 사례는 2017년 5월 워너크라이(WannaCry) 랜섬웨어의 공격이라 할 수 있다.

2017년 5월 사이버 공간에서 워너크라이(WannaCry) 랜섬웨어의 급속한 확산은 전 세계를 공포로 몰아 넣었다. 워너크라이는 전 세계에 무차별적으로 퍼졌으며, 병원, 학교, 기업 및 가정에서 수십만 대의 컴퓨터를 암호화하고 쓸모없게 만들었다. 특히 워너크라이는 영국의 국가보건의료서비스(NHS)의 시스템에 대한 심각한 손상을 입히며 의료체계를 마비시키고 시민의 생명을 위협했다. 이는 사이버 테러가 실질적으로 현실 공간의 시민들의 생명을 위협한 사례로 기록되고 있으며, 익명을 통한 무차별적 공격에 대한 책임의 문제, 지적 재산권의 문제, 안보의 문제, 재난의 문제 등 국내 그리고 국제적 차원에서 전략적 의미를 부여하는 계기가 되었다(장노순 2017)

워너크라이 랜섬웨어 해결의 특이점은 정부, 민간 그리고 국제적 차원의 협조 체계를 바탕으로 하는 안보거버넌스 체계를 바탕으로 하고 있다. 특히 미국의 트럼프 행정부의 국토안보부는 워너크라이 발생을 인지하고 국내의 마이크로소프트(Microsoft), 구글(Google) 그리고 페이스북(facebook) 등의 민간 IT 서비스 제공자들과의 정보 공유를 통해 적극적인 대응 체계를 구축했다. 이와 함께 미국의 국토안보부는 국제적 차원에서 영국, 일본, 호주 등 사이버 공격의 직접적인 피해 국가들과 파트너 체계를 구축하며 공동의 대응을 보이며 적극적으로 문제를 해결하는 움직임을 보였다. 이에 본 연구는 워너크라이 대응과정에서 보인 미국의 사이버안보 거버넌스 구축 과정을 추적하고 워너크라이 사건에 실질적으로 어떠한 대응을 보였는가를 분석하고자 한다.

사이버안보 거버넌스 그리고 북한의 사이버 능력에 대한 연구는 다수를 이룬다. 최근에는 북한의 사이버 공격과 그에 대한 대응(정영애 2020), 북한의 사이버 조직 현황을 사회연결망을 통해 분석한 연구(김진광, 2020), 북한의 사이버테러에 대비한 법·제도 개선방안 연구(김융영, 양철호 2020), 중국의 사이버안보 전략을 바탕으로 북한에 적용한 연구(박차오름, 부승찬 2020) 등 다양한 시각과 방법론을 바탕으로 연구들이 있다. 그러나 이들 연구는 북한의 사이버 능력에 대한 분석 그리고 사이버 공간에서 거버넌스의 중요성을 강조하는데 머물고 있으며, 실제적 차원에서 사이버 공격에 대한 안보 거버넌스적 대응이 어떠한 형태로 이루어지는가에 대한 면밀한 분석을 제공하지 못한다는 한계를 가진다.

본 연구는 2장의 이론적 검토를 통해 사이버 공간의 특수성과 안보 거버넌스의 필요성, 3장을 통해서 오바마 행정부 이후 트럼프 행정부로 이어지는 안보 거버넌스 구축 과정 그리고 4장을 통해 북한의 사이버안보 전략 능력과 미국의 대응을 분석한다. 본 연구는 오바마 행정부 이후 미국의 사이버안보 거버넌스 구축 체계를 미 행정부의 사이버 정책과 입법 체계를 바탕으로 분석하고 실제적 차원에서 워너크라이 사건을 통해 대응 과정을 분석함으로써 사이버안보 거버넌스의 정책적 효용성을 제시한다.

II. 사이버공간과 안보거버넌스

1. 사이버안보

안보(security)는 안보를 연구하는 학자들에 따라 다양하게 정의된다. 안보를 연구하는 학자들은 2차 세계 대전 이후 국내외적 위협에 국가를 어떻게 보호할 것인가에 대한 논의가 심도 있게 이루어졌다(Wolfers 1952; Yergin 1978). 이 시기 국가 안보와 군사력에 초점을 둔 전통적 안보 개념은 국제관계이론 중 현실주의(realism) 이론을 기반으로 했다. 이들 안보 개념은 군사력과 같은 물리적 수단을 통해 적대 세력에 손해를 입히거나 생존을 위협하는 것을 전제로 하고 있다. 따라서 전통적 안보 연구는 군사력의 사용과 통제 그리고 위협의 연구이며(Walt 1991,212) 안보란 국가 최고의 이익, 즉 생존에 대한 위협을 감소시키는 것을 의미한다(Williams 2008, 5). 이 같은 안보 연구는 냉전 기간 동안 황금기(1955~1965년), 쇠퇴기(1960년) 그리고 르네상스라는 시간적 경과를 통해 이론적 그리고 경험적 견고함을 확보해 왔다(Walt 1991) 그러나 탈냉전 이후 국가와 힘의 관계를 중심으로 하는 전통적 안보 개념은 비군사적 영역에서 발생되는 새로운 안보 환경 변화에 따른 안보 위협을 설명하기 어렵게 되었다. 특히 냉전의 해체, 세계화 그리고 정보화는 국경과 영토를 바탕으로 하는 국민국가의 개념에 대한 상대적 약화에 대한 논의를 불러 일으켰다(김상배 2002, 312). 이와 함께 안보의 대상이 국가에서 인간으로 확대됨에 따라 안보 주체와 그 대상이 확대됨에 따라 국가와 국가 이외의 행위자를 포함하는 포괄적 안보 개념으로 확대되었다(Bajpai 2003, 223).[1] 따라서 포괄적 안보란 전통적인 군사안보와 비군사적 요소를 적절히 조화롭게 하여 효과적인 안보 정책을 달성하는 것을 의미한다(채재병 2013, 176).

과학기술의 발전은 물리적 공간을 바탕으로 했던 전통적 안보 개념에도 한계를 만들어 내고 있다. 정보통신 발전은 사이버 공간을 통한 안보적 위협의 주체와 수단을 다양화시키고 있으며 사이버의 가상의 공간이라는 특성은 위협의 주체와 형태를 모호하게 만들고 있다(유호근·설규상 2017). 사이버 공간은 물리적 그리고 가상의 특성이 결합된 특별한 특성으로 컴퓨터로 연결된 인터넷 뿐만 아니라 인트라넷, 휴대폰 그리고 케이블을 통한 정보 교환과 같은 커뮤니케이션 모두를 포함한다(Martain Libicki 2009, 12). 이는 2000년대 이후 정보통신 관련 하드웨어와 소프트웨어의 발전으로 사이버 공간은 점차 확대되었으며 개인과 국가 모두 정보통신 기술에 더욱 의존하게 되었으며, 국가적 차원에서 타국의 행동에 영향을 미칠 수 있는 자원이 되고 있다(유호근·설규상 2017, 237-239).

사이버 공간은 인터넷 그리고 월드와이드웹(the World Wide Web)에서 만들어진 가상의 공간을 의미했다(Muller 2017, 419) 이는 점차 인터넷, 정보통신 네트워크, 컴퓨터 시스템 등이 네트워크로 상호의존하는 형태로 발전되었다. 그러나 사이버 공간은 단순히 인터넷으로 연결된 공간이상으로 정보기술, 인프라 구조, 통신 네트워크 등을 변화시키는데 중요하게 작동하며 이들을 인간과 인간 그리고 인간과 사물이 세계적 차원에서 상호 작동하는 공간이다. 이처럼 네트워크를 통해 상호 작동하는 사이버 공간은 영토라는 경계를 바탕으로 하는 국가주권을 핵심적 이익으로 고려하는 국가에게는 사이버안보를 국가안보와 동일시 한다. 특히 사이버 안보 환경은 그 위협의 방식과 수단이 확대 및 다양화되어 전통적 안보 영역을 넘어서고 있다

1) 탈냉전기 안보의 복합성 그리고 안보 담론의 규범성에 대한 논의는 베리부잔(Berry Buzan)을 중심으로 하는 코펜하겐(COPRI: Copenhagen Peace Research Institute) 학파가 대표적이다(김상배 2016. 80)

(장노순 2019, 5). 다시 말해 사이버안보는 군사적 영역 뿐만 아니라 비군사 영역으로 확장된 안보 개념을 가지고 있으며, 외교적 차원에서도 사이버 역량은 강압적 수단으로 사용되며, 안보의 위협 또한 대상과 범위가 기존 전통적 안보보다 더욱 넓다. 특히 사이버 공간을 통한 상호 연결성을 통한 사이버 위협은 전통적 안보보다 복잡한 다단한 특성을 만들어내고 있다. 국가들은 정보통신 기술의 발달에 따른 사이버 공간의 확대속에서 국가 안보를 위협하는 새로운 수단과 방식을 경험하면서 사이버 영역에 대한 안보적 대응과 목표를 어떻게 설정해야 하는가가 모호해졌다.

사이버안보(cybersecurity)는 '정보통신 기술에 대한 비인가된 접근 또는 접근 시도로부터 보호'하는 것을 의미한다(U.S. Department of Defense 2010). 사이버안보는 사이버 정보활동, 사이버 범죄, 사이버 전쟁 그리고 사이버 테러로 분류될 수 있으며(Ny2 2011), 사이버안보 공격과 피해 유무에 따라 사이버 공격(cyber attack)과 사이버 악용(cyber exploitation)으로 구분하기도 한다(Goldsmith 2011). 그러나 국제사회 차원에서 사이버안보 개념을 정립하고자 하는 움직임은 계속되고 있지만 아직 합의점을 찾지는 못하고 있으며 국가들 역시 이에 대해 명확한 정의는 보류하고 있다. 한편으로 사이버안보를 위한 국제적 차원의 협력은 다양한 수준에서 진행되고 있다. 1997년 G8과 국제형사경찰기구(INTERPOL)와의 비상연락망 설치하였으며(Choucri, Madnick, Ferwerda 2014), 경제협력기구(OECD), 국제전기통신연합(ITU), 북대서양조약기구(NATO) 등이 사이버안보를 위한 대응 조치와 전략을 협의한 바 있다(Nastasiu 2016). 정부간 기구 차원에서 사이버안보에 대한 국제규범 논의는 UNGGE(GGE: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in The Context of International Security)가, 그리고 소다자적 차원에서 유럽안보협력기구(OSCE: Organization for Security and Co-opeatioan in Europe)와 상하이 협력기구(SCO: Schanghai Cooperation Organization)가 있다.

사이버 공간은 가상의 공간이라는 특성으로 현실 세계와의 경계가 모호하지만 정보통신의 발전을 통한 상호의존의 확대는 현실에서 작동하는 실질적 공간으로 만들고 있다. 이로 인해 과거 비전통 안보로 고려되던 사이버안보를 명확히 규정하기에는 어렵다. 그러나 전통적 안보 관점에서 사이버안보를 고려한다면 결국 국민과 국가의 최고의 이익을 유지 방어하는 능력이라고 할 수 있다. 다시 말해 사이버안보는 사이버 공간에서 발생되는 위협으로부터 방어하고 보호하는 능력이다(배영자 2017). 보다 구체적으로 사이버범죄(cyber crime), 사이버 첩보(cyber espionage), 사이버테러(cyber terror), 사이버전쟁(cyber warfare) 등의 위협에 대앙하는 것으로 정의된다(Nye 2011, 21). 이 같은 네트워크 특성을 바탕으로 하는 사이버 공간은 기존 국가를 중심으로 하는 대응 체계 이상의 탈중심적인 사이버안보 거버넌스 형태와 복합적인 대응 체계를 요구하고 있다.

2. 사이버 공간과 사이버안보 거버넌스

인터넷 거버넌스(Internet Governance)란 "정부, 민간 부문 및 시민사회가 인터넷의 발전과 사용을 형성하는 공유 원칙, 규범, 규칙, 의사결정 절차 및 프로그램을 각각의 역할에 따라 개발하고 적용하는 것"을 말한다(WGIG 2005). 따라서 인터넷 거버넌스에서는 정부, 민간 부문 그리고 NGO와 같인 시민사회 모두가 각자의 역할을 하게 된다. 인터넷 거버넌스는 ICANN이 다루는 인터넷 이름과 주소와 함께 중요한 인터넷 자원, 인터넷 안전과 보안 그리고 인터넷 이용과 관련된 개발 등의 공공정책 문제를 포함한다(Shahan 2005). 인터넷 거버넌

스와 관련해 누가 행위 주체가 되어야 하는 문제는 국가가 중심이 되는 다자주의(multilateralism)과 국가와 함께 민간기업 그리고 시민 사회가 동등한 입장에서 관련 이익과 가치를 공동으로 고려해야 한다는 입장으로 나뉜다(Mauer 2011). 그럼에도 불구하고 인터넷은 사용자 중심의 개방적인 생태계를 바탕으로 인터넷 공간에서의 사용 주체들이 자발적으로 공동의 목표와 문제를 해결하기 위해 동등하게 참여하는 것을 특징으로 한다.

일반적으로 사회과학에서 정의하는 거버넌스 개념은 국가 중심의 국정운영 방식에 대한 한계를 바탕으로 등장했다. 이는 국가와 사회 관계를 위계적 형태로 유지했을 때 보다 국가와 사회가 네트워크를 통한 수평적 관계로 정립된다면 사회 운영과 조정이 보다 효율적이라고 설명한다(Amoore 1997; Strange, 1995; 1996; Cerny 1990). 특히 정보기술 차원에서 ICT 관련 기술은 기술 집중형 네트워크에서 탈집중형 네트워크를 가능하게 한다. 때문에 거버넌스의 탈집중 네트워크형 관리 구조는 디지털 시대에 적합한 내재적 속성을 가진다(김상배 2002, 318).

네트워크를 특성으로 하는 사이버 공간의 복잡성은 전통적 안보적 관점에서 국가의 힘을 바탕으로 물질적 차원의 절대우위를 통한 안보구조의 안정적 관리는 어려워 졌다. 또한 사이버 위협을 만들어 내는 주체가 국가 뿐만 아니라 사물에 이르기까지 다양해지며 변화된 사이버안보 환경에 대한 개별 국가 차원의 대응 전략은 어렵게 되었다. 특히 정보통신기술의 발달과 함께 독자적으로 발전하는 정보기술들은 융합하고 네트워크화 하면서 탈집중화 그리고 거버넌스 형태의 제도환경을 만들어 내고 있다. 상이한 정치 행위자들은 위계적인 연결성을 가지기보다는 다양한 복합적 관계를 갖게 된다. 이들은 '네트워크'를 통해 연결되며 이들은 국가와 사회의 위계적 접근보다는 이들의 수평적 연결성에 초점을 두고 거버넌스 개념을 통한 접근이 필요하다.

정보통신기술의 발전은 사이버 영역에서 두 가지 특성을 만들어 내고 있다(김상배 2002, 314-315). 첫째로 '무어의 법칙(Moore's Law)'과 같이 컴퓨터 정보처리 능력의 획기적인 발전 속도로 하드웨에서 소프트웨어와 서비스·컨텐츠로 이행되고, 더 나아가 빅데이터를 바탕으로 하는 네트워크 체제는 기존 국경안에서의 사이버 공간을 이제는 국제적 차원으로 탈영역화하고 있다. 세계의 수 많은 컴퓨터들이 상호 접속 가능하기 위해서는 컴퓨터 시스템의 데이터 흐름과 명령어의 작동을 제어하는 아키텍처(architectural)와 함께 인터넷 데이터 교환을 위한 공동프로토콜(common protocl) 의 기술 표준이 요구된다. 1980년대 초에는 인터넷 프로토콜로서 TCP/IP(Transmission Control Protocl/Internet Protocol)이 등장했으며 이후 인터넷을 위한 핵심적 기술요소로서 기능해 왔다(Froomkin 1997). 둘째로 디지털 융합으로서 커뮤니케이션, 방송 그리고 컴퓨터 등의 정보통신 분야가 네트워크를 통해 하나의 실술적 핵심으로 수렴 및 융합되는 특성을 가진다.

정보 기술 표준은 탈집중 네트워크 형태로 연결되어 거버넌스 제도 환경 만들어내며, 인터넷 또한 비대칭 그리고 비집중적인 형태로 결합되어 탈집중 관리 구조를 요구하는 느슨한 결합 체계로 발전해왔다(김상배 2002, 315). 컴퓨터 아키텍처와 인터넷 프로토콜의 표준화, 하드웨어와 소프트웨어 그리고 서비스·컨텐츠가 디지털 네트워크로 연결되어 융합된 하나의 시스템으로 작동하면서 기술 공간의 거버넌스 역할을 한다. 이와 함께 인터넷상의 데이터가 각기 다른 네트워크 경로를 통해 수신자가 사용할 수 있는 형태로 재조립되면서 이를 통제하거나 관리하려는 시도는 어렵게 되었다. 결국 정보기술의 발달은 네트워크형 관리구조를 만들면서 탈집중화를 만들면서 정보기술에 적합한 거버넌스 제도 환경을 요구하는 특성을 가진다.

사이버안보에 대한 거버넌스적 접근은 2005년 '튀니스 아젠다(Tunis Agenda for the

Information Society)'를 통해 확인할 수 있다(ITU 2005). 또한 인터넷 거버넌스에서 다주의적 입장을 보이는 ITU에서도 인터넷 거버넌스는 "정부, 민간, 시민사회가 각자의 역할, 공유된 원칙, 규범, 규칙, 의사결정 절차 그리고 인터넷의 진화와 이용을 형성하는 프로그램의 개발과 응용"으로 정의한다. ITU는 인터넷과 관련된 공공정책 문제에 대한 권한은 국가가 가지면서 민간, 시민, 사회, 정부 그리고 국제기구가 인터넷의 안정과 관련 정책 개발을 위해 각자의 역할을 수행해야 함을 밝히고 있다. 결국 인터넷 거버넌스에서 정부, 민간부문 그리고 시민사회의 관계에 대해 위계에 기초한 질서 보다는 상호 동등한 관계를 바탕으로 개방성, 참여성 그리고 투명성을 특징으로 하며 상호 포용적인 관계를 통해 다양한 공론장에서 서로의 이익을 창출하는 과정을 통해 이들의 의견을 수렴한다. 이들 각각의 행위자들이 거버넌스를 구성하고 그 운영과정에 참여하는 것이 다자이해당사자주의이다(유인태 2019; 유호근·설규상 2017, 248; ITU 2005).이는 한국을 비롯해 미국, 영구, 호주, 일본 브라질, 멕시코 등 여러 국가들에 의해 지지를 받고 있다.

글로벌 거버넌스 차원의 사이버 공간은 국가와 함께 초국경 행위자들과 함께 서로의 자율적 통제를 바탕으로 사이버 위협을 최소화하고자 한다. 특히 사이버 공간의 행위자들은 형성된 네트워크를 바탕으로 자율적인 상호조정과 협의를 통해 갈등을 조정하고 피해를 최소화하고자 하며(홍석훈 2019, 53), 이는 다자주의 형태로 나타난다(유호근·설규상 2017, 249). 다자주의는 정부의 대표성을 인정하면서 정부가 주도적으로 국제적 이슈에 종합적이고 다자적 해결방식으로 국제적 사이버 쟁점에 대해 종합적이고 다자적인 해결방식을 추구하는 것을 말한다. 국제전기통신연합(ITU)에서 국가는 일국 일표주의 원칙을 통해 상대적으로 수평적 관계를 가지면서 미국 주도의 인터넷 질서를 견제한다. 이 같은 사이버안보 차원의 두 거버넌스 유형은 유엔 정보안보 정부전문가그룹(GEE: Group of Governmental Experts on Developments in the Field of Inforamtion and Telecommunication)을 통해 국제적 차원의 안보 국제규범화를 위한 설정의 논의가 진행되고 있다(장노순 2016, 10)

결국 사이버안보 문제는 사이버 공간의 사용자와 제공자 그리고 국가의 세 행위자 모두를 동시에 고려해야 하는 사안이며 이들의 파트너십을 기본 축으로 거버넌스 관계를 바탕으로 접근해야 하는 사안이다. 특히 4차 산업 혁명 이후 복잡 다단하고 빠르게 변하는 IT 환경에서 정부의 제도화 능력의 더딤은 이들의 협조체계가 절대적인 사안이라 할 수 있다. 결국 사이버 공간에서 사이버 위협에 국가 차원에서 체계적이고 종합적인 대응 위해서도 사이버안보거버넌스 구축은 필요조건이다.

III. 미국의 사이버안보 전략(거버넌스-안보로의 전환)

1. 오바마 행정부: 백악관 중심의 사이버안보거버넌스

오바마 행정부는 국가 안보에 대한 사이버 위협의 주체와 방법이 다변화됨에 따라 사이버 위협을 미국에게 가장 심각하고 실질적인 국가위험 중 하나로 인식했다. 오바마 행정부는 취임과 함께 사이버 보안 정책에 대한 포괄적인 검토를 지시했다. 2009년의 사이버 공간정책 검토(2009 Cyberspace Policy Review)는 기술에 대한 미국의 의존도가 높아지는 반면에 사이버와 관련된 범죄, 테러 그리고 공격에 점차 취약해 지고 있으며 미국 정부와 민간 부문은 이에 대처할 준비가 되지 않았다고 보고했다. 이에 오바마 행정부는 미국의 사이버 공간에서의 정부와 민간의 역량과 조율을 강화하고 시민의 자유를 보호와 혁신이 이뤄지느 가운데 취

약성 해소가 가능한 국제 규범 개발을 추진할 것임을 밝혔다.

오바마 행정부는 점증하는 사이버 위협에 대응하기 위해 '정부 전체(whole-of-government)'적 접근 방식을 보였다(White House 2015). 무엇보다도 오바마 행정부는 부시 행정부 시기 국토안보안보부(DHS)가 총괄했던 사이버안보 업무를 국가안보위원회(NSC)산하 사이버안보국 내의 사이버안보조정관에게 총괄하도록 했다. 이와 함께 사이버 인프라 조직들이 실시간으로 사이버 위험을 공유하고 대응할 수 있도록 관련된 실무부처의 통합성과 민관협력을 바탕으로 하는 사이버안보 거버넌스 대응체계를 구축하고자 했다. 이는 연방정부의 사이버안보 능력 향상과 정부와 민간의 사이버안보 협력체계 구축을 핵심으로 하는 사이버안보거버넌스 구축 전략이라 할 수 있다.

오바마 행정부는 부시 행정부의 포괄적인 국가 사이버안보이니셔티브(CNCI: the Comprehensive National Cybersecurity Initiative)의 사이버안보 문제 인식을 공유한다. 부시 행정부는 2000년 9.11 테러 발생 이후 주요기반 시설에 대한 사이버 테러 가능성을 인지하고 이에 대한 보호의 중요성을 강조했다. 2002년 11월 국토안보법, 12월 연방정보보안관리법(FISMA)을 제정하고 사이버 공격에 대해 국토안보부(DHS: Department of Homeland Security)가 주도하는 대응 체계를 갖추었다. 특히 2009년 5월에는 미국 사이버안보 전략의 근간이 되는 CICI를 통해 사이버 공간에서 즉각적이고 발생가능한 위협에 대한 방어체계와 함께 미래 사이버 보안 환경 강화를 명령했다.

오바마 행정부는 부시 행정부의 사이버 위협에 대한 인식을 공유하며 사이버안보가 미국의 경제와 안보를 심각하게 위협하는 요인 중 하나이지만 여전히 정부 그리고 국가 차원에서 이에 대한 대응이 취약하다고 인식했다(White House 2010). 오바마 행정부는 사이버안보에 대한 총괄 책임을 백악관으로 하며 사이버안보 확보를 위해 연방 정부의 역할을 강화하고 민간부문과의 협력을 제도화해 나갔다. 오바마 행정부는 CICI를 바탕으로 미국의 정보통신 및 디지털 기반 시설 보안에 대한 포괄적 대응을 검토했으며, 이는 2009년 미국의 사이버안보 전략의 근간이 되는 '사이버공간 정책보고서(CPR: Cyberspace Policy Review)'와[2] 2013년 행정명령 136369Execute Order(EO) 136369, Improving Critical Infrastructure Cyversecurity) 그리고 정책 지침(Presidential Policy Directive, PDD 21, Critical Infrastructure Security and Resilience)으로 도출되었다. 오바마 행정부는 부시 행정부 시기 국토안보부에 있던 국가 사이버보안의 총괄·지휘를 백악관으로 이전시키고 사이버 보안 조정관(Cybersecurity Coordinator) 임명과 함께 국가안보위원회(NSC: National Security Council) 사이버보안국(Cybersecurity Directorate)을 신설했다.[3]

오바마 행정부는 '효과적인 정보 공유 및 사고 대응체계' 구축의 일환으로서 사이버 침해사고 대응계획을 수립하고 민관 파트너십 향상을 위한 대화를 촉진할 수 있도록 했다. 사이버 사고를 예방·탐지·대응하기 위해 민관 협력 프로세스를 개발하고 다자간 협력 강화를 위해 네트워크 사고 및 취약성 정보 공유 확대를 실행계획으로 두었다(The White House. 2009) 사

2) 이는 ①최상의 리더십 발휘 ② 디지털 국가 역량 구축 ③ 사이버 보안 책임 공유 ④ 효과적인 정보공유 및 사고대응체계 구축 ⑤ 혁신 촉진이라는 5개의 아젠다와 10개의 단기·14개의 중기 실행계획으로 구성되어 있다.

3) 사이버보안 조정관은 국가안보위원회의 일원이자 대통령 특별 보좌관으로 대통령에게 사이버보안 관련 사안을 정기적으로 보고한다. 연방정부 최고기술책임자(CTO: Chief Tecnology Officer)와 최고정보책임자(CIO: Chief Information Officer)와 협력하여 정책 개발 및 입법 방향을 정립하며 사이버 보안 정책간 우선 순위와 기관 간 협업을 조정하는 역할을 한다. 오바마 대통령은 사이버 조정관으로 부시 행정부의 국가 사이버보안 자문을 했던 하워드 슈미츠(Howard Schmidt)를 임명한 바 있다.

이버 공격 및 테러 행위에 대한 경각심이 증가하고 있는 상황에 대응하기 위해 2013년에 발표된 '주요 기반시설 사이버 보안 강화를 위한 행정명령'에서도(CISA 2013) 관할 정부기관과의 유기적인 연계로 사이버 위협 발생 시 관련 정보를 신속하게 전체 기반시설이 공유해 사고 대응에 효율성을 높일 수 있는 대응 시스템을 주문했다. 특히 오바마 행정부 시기 '사이버안보법(the Cybersecurity Act of 2015)'은 공공부문과 민간부문의 정보공유를 촉진시켜 증가하는 사이버 위협에 더 많은 협력과 공조를 이루도록 하고자 했다.[4] 이를 위해 오바마 행정부는 사이버안보 위협에 대한 통합성과 민관 협력 실현을 위해 DNI 산하에는 사이버위협정보통합센터(ctiic)가 설치되어 사이버위협과 사고를 종합적으로 분석하여 유관기관에 정보를 제공케 했다. 예산관리국 내에서는 전자정부사이버과를 설치하여 연방기관의 업무를 감독조율하게 했다. 민관협력 촉진을 위해 정보공유분석기구(ISAOs)를 설치하여, 국토안보부 산하에서 민관 정보 공유를 담당하는 국가사이버안보정보통합센터(NCCIC)와 협력하도록 했다(김상배 2018, 19)

오바마 행정부는 사이버 보안 책임을 공유하기 위해 국제 파트너십 관련 역량 강화를 실행계획으로 두었다(White House 2009). 이를 바탕으로 미국은 EU, 영국, 인도 등 주요국가와 글로벌 기업들과 사이버 보안과 범죄에 대한 협력 관계를 구축과 공동 대응을 마련했다. 미국은 EU와 '미국-EU 사이버보안 및 사이버범죄 워킹그룹(US-EU Working Group on Cyber Security & Cyber Crime)' 출범을(2010, 11) 그리고 인도와는 '제2차 전략회담(Strategic Dialogue)'에서 사이버 테러 정보 공유 등 사이버 보안 협력을 위한 양해 각서 체결(2011.7) 했다. 또한 미국, 영국 등 주요국과 글로벌 기업이 참여한 '국제사이버보안연맹(International Cyber Security Protection Alliance, ICSPA)'를 공식 출범 시켰다(11월 7일).[5]

오바마 행정부는 취임과 함께 사이버안보 체계 구축을 정부의 우선 순위에 두었다. 오바마 행정부는 연두교서(State of the Union Address)를 통해서도 매년 사이버안보의 중요성을 강조하며 사이버안보 확보를 위한 정책을 추진했다. 행정부내에 사이버안보 체계 구축에 있어서는 백악관을 중심으로 사이버안보 관련 정책을 추진하고 국가안보위원회의 사이버안보 조정관이 사이버안보 관련 업무를 총괄하도록 했다. 주요 기반 시설에 대한 시아버 보안 문제도 백악관 주도의 정책 결정으로 이루어졌다(김근혜 2019). 특히 오바마 행정부는 집권기 동안 공공 영역과 민간 부문의 사이버 보안 수준 향상, 미국과 동맹국에 대한 악의적인 사이버 활동 저지, 사이버 보안 사고에 대한 효과적인 대응에 초점두었다.

그러나 오바마 행정부는 거버넌스 형태의 사이버안보 협조체계 구축을 시도했지만 사이버안보 정책 차원에 있어 그 목표는 달성하지 못했다고 평가한다(Fidler 2015). 첫째로 인터넷 혁신이 정부 정책 보다 빠르기 때문에 정부가 사이버안보에 대한 위협에 대응하는데 본질적으로 불가능하하며, 정부가 민간 영역의 사이버안보 또는 보안을 해결하는데 한계가 있다. 무엇보다도 주요기반시설에 대한 사이버안보 보안 체계 구축에 있어서 민관 파트너십에 실패에 있다. 오바마 행정부의 사이버안보 체계 구축은 정보 공유에 있었으며, 행정부 중심의 거버넌스 체계 구축에 대한 의회와 민간 영역의 비협조로 오바마 행정부의 사이버안보 보안 체계 구축

4) 사이버안보법(the Cybersecurity Act of 2015)은 총 4개의 장으로 구성되어 있으며 1장은 사이버시큐리티 정보 공유, 2장은 국가 사이버 시큐리티 발전, 제 3장은 연방 사이버시큐리티 인력 제 4장은 기타 사이버 문제들로 구성되어 있다.

5) 미국, 영국, 캐나다, 호주, 남아공 등 주요국과, 맥아피, 트렌드 마이크로 등 민간기업, 유럽 공동경찰기구 유로폴(Europol) 등이 참여한 비영리 기구로서 사이버범죄에 대응하기 위해 각 정부의 법 집행 역량을 개선하고, 민·관 협력체계를 구축하며, 중국, 러시아, 브라질 등 보안에 취약한 국가들에게 자금 및 기술을 지원하는 것이 목표이다.

에는 한계를 보였다.

2. 트럼프 행정부: DHS 중심의 사이버안보거버넌스

트럼프의 외교 안보기조는 힘을 통한 평화(Peace through Strength)를 통해 자국의 단기적 이익을 추구하는 미국우선주의(American First) 추구했다. 트럼프 행정부는 기존 국제질서를 바탕으로 미국의 힘을 투사 하기 보다는 압도적인 군사력과 선택과 집중의 개입정책을 통해 미국의 재건을 추구하겠다는 입장을 보였다. 출범 초기 트럼프 행정부는 오바마 행정부의 국제주의를 기반으로 하는 일련의 정책을 부정하며 TPP와 파리기후 변화협약을 탈퇴하며 보호주의 그리고 일방주의 정책 기조를 보였다(Trump 2015).

한편 트럼프 행정부는 사이버안보 문제와 관련해서는 보다 적극적인 정책 대응을 취할 것이라는 입장을 나타냈다(Mark 2017). 특히 트럼프 행정부는 오바마 행정부 시기 추진했던 사이버안보 정책 노력에 대한 한계를 지적하고 취임사를 통해 6대 국정 기조와 함께 사이버 공격에 대한 대비책을 언급했다. 미국의 백악관은 사이버 공간을 전쟁의 공간, 즉 국가간 갈등이 발생할 수 있는 새로운 전장으로 인식하고 국가 안보 차원에서 이를 보호하기 위한 조치를 취해야 함을 강조했다. 이와 함께 "우리는 사이버 사령부를 중심으로 우리의 사이버 방어 및 공격 능력 개발을 우선 과제 중 하나로 삼고 최정예 인재들을 모을 것"이라고 설명했다(심인성 2017). 이는 '연방정부의 네트워크와 주요 기반 시설의 사이버보안에 관한 행정명령(EO 13800: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 이하 EO13800)'으로 2017년 5월에 발표되었다(Norton Rose Fulbright. 2017).

EO13800는 국토안보부(US Department of Homeland Security)를 중심으로 사이버안보 역량 강화를 추진할 것임을 설명한다. 특히 오바마 행정부 시기 사이버안보 협력과 관련해 총괄 역할을 담당했던 '사이버보안조정관'을 폐지하고 중앙집중화된 정책을 추진하되 연방네트워크와 주요 기반 시설에 대한 사이버안보 강화를 위해 주요 정부 부처의 임무 수행과 책임을 강조한다.[6)]

트럼프 행정부는 국토안보부(US Department of Homeland Security)를 중심으로 하는 사이버안보 전략을 구체화하는 미 국토안보부의 사이버 보안 전략(U.S. Department of Homeland Security Cybersecurity Strategy)을 2018년 5월에 발표했다(DHS 2018). 특히 국토안보부의 사이버안보 전략은 사이버 공간에서의 위험 평가와 관리를 최우선의 역할로 하며 ① 위험 식별(Risk Identification) ② 취약성 감소(Vulnerability Reduction) ③ 위협 감소(Threat Reduction) ④ 결과 완화(Consequence Mitigation) ⑤ 사이버 보안 성과(Enable Cybersecurity Outcomes) 5개의 전략을 통해 연방정부의 정보 시스템 보호와 기관의 취약성을 보완하며 이해관계자들과 협력하여 주요 기반시설을 보호할 것을 주요 목표로 했다. Nielsen 장관은 포괄적이고 체계적인 사이버 보안을 위해 DHS를 중심으로 미국 네트워크를 방어하고 사이버 위협을 극복할 것이라 설명했다(DHA 2018b).

트럼프 행정부는 사이버안보 대응에 대한 통합개념(United of effort)을 바탕으로 통합된 방식의 사이버안보 전략을 추진했다. 국토안보부의 '사이버 보안 전략' 보고서에 따르면 국토안보부는 주요기반시설 관련 이해관계자들과 사이버 보안 정보를 수집, 분석, 공유하기 위해

6) 행정명령에 대한 평가는 보안 강화를 위한 근본적인 조치라는 평가와 함께 가이드라인 없이 강제성 없는 권고 수준이며 대책을 여전히 제시하지 못하고 있다는 비판이 상존한다(Mark 2017).

자동화 된 메커니즘을 어떻게 구축하고 확장할 것인지에 대해 설명하고 있다. 그러나 사이버 위협 상황시 정부가 요청할 경우 민간은 신속하게 정보를 기밀해 제하고 정부에게 제공해야 할 필요성을 설명하고 있다. 국가 사이버 위험 관리를 위해 연방 정부, 주 및 지방정부, 산업 및 국제 사회의 파트너와의 사이버 보안 커뮤니티 간의 협업을 한 기본 지침으로 삼고 있다 (DHS 2018; 2018b). '국가 사이버보안 전략'에서도 글로벌 차원에서 사이버 보안 관련 국제 협력을 이끌어 내기 위해 국무부가 핵심 외교적 노력과 산업 증진 프로그램을 주도하도록 했다는 점도 특징이다. 이와 함께 사이버 보안 위험을 공동으로 해결하기 위해 민간 영역의 참여와 연계를 다루고 있으며 정부 부처와 민간과의 향상된 정보공유 체계를 다루고 있다. 국토안보부의 권한은 '국가사이버보안전략'(National Cyber Strategy of the United States of America),

사이버보안 및 기반시설보호를 위한 전문기관 설립법(CISA, Cybersecurity and Infrastructure Security Agency Act of 2018)[7]을 통해 사이버 중앙 기관으로서 권한은 더욱 강화되었다. 한편 국방수권법(National Defense Authorization Act of 2017, NDAA)은 국토안보부의 사이버 보안의 전 범위의 성공적 임무 수행을 위해서 국제 사이버 보안 파트너들과의 협력 사항을 전략에 포함할 것을 요구한다. 이를 바탕으로 국토안보부가 실무적인 차원에서 정책을 시행하고 있으며 국방부 사이버사령부와 법 집행기관 또한 막강한 권한을 가지게 되었다.

이와 함께 범부처 차원의 사이버 위협 정보 공유 및 위기시 대응 체계 마련을 위해 국가사이버안보통신통합센터(National Cybersecurity and Communications Integration Center: NCCIC), 사이버위협정보통합센터(Cyber Threat Intelligence Integration Center, CTIIC), 국가사이버안보통신통합센터(National Cybersecurity and Communications Integration Center: NCCIC), 정부부처조정위원회(Government Coordinating Councils, GCCs) 및 분야별 전문기관(Sector-Specific Agencies, SSAs)를 설립 했다. 한편 민간분야에서는 주요 기반시설 운영자들을 중심으로 분야별 협력 위원회(Sector Coordinating Councils, SCCs)와 정보공유분석센터(Information Sharing & Analysis Center, ISACs)를 설립해 사이버안보 대응 체계를 구축했다.

트럼프 행정부는 '미국 우선주의'를 바탕으로 사이버 공간을 국가 안보 전략 차원에서 최우선으로 고려한다. 특히 트럼프 행정부는 오바마 행정부 시기 추진되었던 사이버안보 거버넌스 구축 전략을 유지하며 기존의 정책을 보완 및 개선하는 방향으로 추진되었다. 특히 사이버안보 컨트롤 역할을 하는 국토안보부를 설립해 복잡해지는 사이버안보 환경을 효율적으로 관리하도록 하는 한편, 민간기업들과의 적극적인 파트너십을 구축해 사이버안보 거버넌스 대응 체계를 보다 확고히 했다(1263-1264). 한편 국토안보부는 사이버안보 대응에 주도적인 역할을 보이며, 공공영역과 민간 영역의 협력 체계를 통해 인터넷 범죄, 컴퓨터 해킹, 랜섬웨어 등 사이버 공간에서 발생되는 위협에 대한 대응을 보여왔다. 특히 WannaCry와 BTC-e 랜섬웨어 사건 등에 대해서는 사이버안보 거버넌스 체계를 바탕으로 적극적인 대응을 보였다.

IV. 미국의 '워너크라이'(WannaCry)' 대응: 사이버안보 거버넌스

7) 기반시설을 보호하기 위한 우선순위 조치(Priority Action)는 ①책임과 의무 개선 ② 국가위험 식별에 따른 우선순위 결정 ③ 사이버보안 기능 제공자로서 정보통신 기술 제공업체 활용 ④ 미국의 민주주의 보호 ⑤ 사이버 보안 투자 증진 ⑥ 연구 및 개발 투자 우선순위 결정 ⑦ 운송, 해상, 우주공간의 사이버 보안 개선으로 한다.

1. 북한의 사이버안보 전략과 능력

북한의 사이버안보 전략과 능력에 대한 정보는 제한적이다. 그러나 북한의 인터넷 인프라는 세계에서 가장 취약한 국가 중 하나로 알려져 있으며 소수의 사람들만이 국가 인트라넷인 '광명'에 접속할 수 있다(Segal 2016). 북한이 사이버 능력에 관심을 갖게 된 것은 김정은 정권 시기 걸프전(1991), 코소보 전쟁(1999), 이라크 전쟁(2003)에서 보여지는 네트워크 군사에 대한 장점을 인식하면서 시작되었다고 알려져 있다(Jun, Lafoy and Sohn 2015). 북한의 인민군 군사출판사가 2005년에 발간한 '전자전 참고자료'에 따르면 김정일은 "내가 여러 번 이야기했지만 현대전은 전자전이다. 전자전을 어떻게 하는가에 따라 현대전의 승패가 좌우된다고 말할 수 있다"고 말했다. 또한 김정일은 인민군에게 하달되는 『학습제강』을 통해 "현대전은 고도로 확대된 립체전, 정보전(정찰전, 전자전, 싸이버전, 심리전), 비대칭전, 비접촉전, 정밀타격전, 단기속결전으로 특징지어지는 새로운 형태의 싸움이다"고 하면서 현대전에서 정보전의 중요성을 강조한 바 있다(조선인민군 2006).

북한의 전자전 능력 향상은 1986년 미림대학(현 '김일 군사대학')을 평양에 세우고 사이버전 관련 전문 요원을 양성하기 시작했으며, 압록강 군사기술대, 국방대, 공군대, 해군대 등에서도 전자전 요원을 양성하는 것으로 알려져 있다(안용현 2011). 1998년에는 사이버 부대(121소) 창설하였으며 1999년에는 사이버심리전부대인 저공국 204소를 설립하여 사이버 심리전을 펼쳐왔다. 2004년에는 중국 단둥을 거점으로 사이버 부대를 운영하였으며 2010년 인민무력부 정찰국, 노동당 작전부, 중앙당 35호실 등을 통합하여 정찰총국을 창서하였으며 사이버 부대(212소) 병력 증강하여 사이버지도국(121국)으로 개편했다. 북한군 내에는 전자전 특기의 2개 여단(1200여명)을 포함, 약 3만 여명의 전자전 요원이 있으며, 특히 600 여명의 전문 해커들의 능력은 미국 중앙정보국(CIA) 수준으로 추정된다.[8)]

김정은 국무위원장은 사이버전을 핵·미사일과 함께 3대 전쟁 수단으로 규정한다(김형수 2013). 북한은 2013년경부터 사이버 해킹 조직을 신설하고, 재편하기 시작했으며 전문성 제고와 임무 세분화를 목적으로 자금과 인력을 집중하고 있다. 2017년에는 기존 사이버 지도국(121국)과 사이버심리전부대(204소), 110 연구소를 통합해 사이버 전략사령부가 창설되었다고 추정되고 있다(김귀근 2017). 결국 김정은 체제 이후 김정은 정권은 사이버 전을 대비한 안보체계 확립과 함께 전문 인력 규모를 지속적으로 확대했다.

북한의 김정은 정권은 국제 사회의 제재 국면에서도 비대칭 전력 강화와 사이버 심리전을 목적으로 사이버 테러 역량을 강화시키고 있다. 또한 북한은 대북 제재 상황속에서 정치자금과 대량상살무기 프로그램을 위한 자본 확보를 위해 사이버를 적극 활용하고 있으며 사이버 해킹으로 최대 20억달러(약 2조4천 380억원) 규모의 자금을 탈취했다고 보고된 바 있다(United Nation Security Council 2019). 북한은 17개국을 상대로 최소 35건의 사이버 해킹을 했으며 이중 한국은 10건을 기록하며 최대 피해국가였다(이귀원 2019). 북한의 사이버 공격 유형은 크게 다섯 가지 유형으로 이루어져 왔다(김진광 2020, 113). 첫째로 북한의 최고존엄 수호, 둘째, 군사적 목적, 셋째, 은행 및 금융권에 대한 '외화벌이' 넷째, 대남공작, 끝으

8) 정구연.이기대는 북한이 사이버사령부를 설치하고 군과 노동부 산하 7개 해킹 조직에 약 1,700여명의 전문 인력을 두고 있고, 이와는 별도로 10여개의 대남 해킹 지원 조직을 통해 6,000여명의 사이버 공격 인력을 관리하고 있다고 하였다. 북한의 사이버 공격 인력은 7,700여 명으로 추정한다. (정구연, 이기대 2016)

로 국방 및 최첨단 기술 탈취 목적으로 이루어졌다. 특히 북한의 사이버 전문가들이 중동 또는 아프리카로 진출하는 사례도 발생되고 있으며, 사이버 공격의 추적을 회피할 목적으로 제3국등을 활용해 발신지를 우회하는 방법을 사용하고 있어 그 사례는 더욱 많을 것으로 추정된다(성용은 2020).

북한의 사이버 테러 수준으로 평가되고 있으며 북한의 사이버 능력은 지속될 것으로 예상된다(Nakasone and Sulmeyer 2020.). 특히 북한은 이메일을 통해 악성프로그램 유포하는 사례가 많아지고 있으며 북한은 핵실험으로 인한 경제 제재 이후 외화벌이 목적이 두드러지고 있는데 대표사례로는 2017년 컴퓨터 파일을 암호화한 후 복호화 대가로 금전을 요구했던 '워너크라이(Wanna Cry)'가 있다.

2. 미국의 '워너크라이'(WannaCry)' 대응: 사이버안보 거버넌스

워너크라이(WannaCry)의 사이버 공격의 시작은 2017년 5월부터 전세계 100여개 국가에서 무차별적으로 확산되었다(김수진 2017). 특히 일부 정부 기관과 병원, 기업과 가정에 있는 컴퓨터를 암호화하고 사용을 불가능하게 만들었다. 이는 악성프로그램의 일종인 '랜섬웨어'(Ransomware)에 감영된 컴퓨터들이 작동을 멈추고 중요 파일을 암호화했으며 이를 푸는 대가로 금전을 요구하는 악성 프로그램이었지만 대가를 지불해도 컴퓨터 잠금은 해제되지 않았다. 러시아, 우크라이나, 대만, 영국 등이 주요 공격 대상으로 삼았다. 또한 FEDEX, Renault, Telefonica 및 Deutsche Bahn을 포함한 다양한 회사가 영향을 받았으나 가장 큰 타격을 입은 것은 영국의 국립 보건 서비스 (NHS England)로 영국의 의료 시스템을 마비시켜 그 피해는 심각했다(Schmitt and Fahey 2017).

민간과 공공기관 그리고 국제적 협력체계를 통한 거버넌스 대응은 워너크라이의 확산을 약화시키고 그 피해를 최소화할 수 있었다. 특히 사이버보안 전문가가 워너크라이 랜섬웨의 킬스위치를 발견하며 랜섬웨어의 전파를 중단할 수 있었다(고현실 2017). 국토안보부(DHS)는 5월 12일 아시아·태평양 지역을 시작으로 유럽으로 이어지는 사이버 공간내 비정상적 활동이 있음을 파악했다. 국토안보부는 민간 및 국제 파트너십을 활성화하기 시작했으며, 연방 CIO와의 IT 및 사이버 보안 업계의 파트너에 도움을 요청했다.

미국 정부는 IT 기업들과 협조체계를 구축하여 사이버 공격의 근원을 추적했다. Microsoft, Google, Facebook 등의 미국의 IT 기업들은은 워너크라이 확산의 진원지를 북한으로 파악하고 북한의 사이버 체계를 비활성화 및 운영을 중단 시키는 조치와 함께, 북한의 해커로 추정되는 계정을 폐쇄했다. 이와 함께 미국 정부는 영국, 호주, 캐나다, 뉴질랜드 그리고 일본과 분석을 공유하며 워너크라이에 대한 국제적 대응을 보였다.

한편 미국 국가안보국(NSA)는 워너크라이 랜섬웨어 공격의 배후로 북한을 지목했다(이광빈 2017). 북한이 워너크리아 공격의 배우라는 정황은 공격에 사용된 IP 주소가 중국에서 정찰총국이 사용해오던 범주로 알려졌다(Nakashima and Rucker 2017). 한편 해커들은 비트코인 형태로 14만 달러를 모았다고도 밝혔다(Nakashima. 2017). 또한 워너크라이의 일부 코드가 과거 '라자루스(Lazarus)'가 사용한 악성프로그램과 코드가 공유되어 있어 워너크라이의 배후로 '라자루스'를 지목했다(성용은 2020).

미국의 국토안보부는 워너크라이와 같은 사이버 공격에 대하여 미국에 대한 공격으로 이해하기 보다는 전지구적 위협으로 인식했다. 특히 국토안보부는 사이버 공격에 대응하기 위해서 국내적으로는 민간과 공공이 함께 하는 집단 방어 그리고 국제적 파트서십을 통한 통한 공동

대응의 필요성을 강조했다. 특히 사이버 공간에서 이루어지는 경제 및 커뮤니케이션 서비스는 민간 영역으로서 정부와 민간의 파트너십, 다시 말해 사이버안보에 대한 거버넌스적 대응은 절대적임을 강조했다.

V. 결 론

코로나19 확산에 따라 북한 해커가 영국 제약사 아스트라제네카(AstraZeneca)의 시스템에 침입하려 했다는 사실이 알려졌다(Stubbs 2020). 해커들은 LinkedIn과 WhatsApp 등을 통해 채용 담당자로 위장해 아스트라제네카 직원에게 구인을 제안하거나 이들에게 악성코드가 포함된 메일을 발송하는 등의 해킹을 시도했다. 이들에 대한 실질적인 피해는 나타나지 않았지만 북한의 사이버 공간에서의 해킹의 움직임은 지속적으로 나타나고 있다.

미국은 사이버 공간에서의 사이버 위협이 증대되고 이 같은 위협이 현실 공간에서 시민과 민간 그리고 국가적 차원의 위협으로 이어짐을 인지하고 이에 대한 대응책을 준비해 왔다. 이를 위해 오바마 행정부는 백악관 주도의 거버넌스 체계의 움직임을 보였지만 스노든(Snowden)이 국가 안보 관련 문서를 폭로하면서 사이버안보 위협에 대한 논쟁에 부딪히며 거버넌스 체계 구축에는 제한적이었다. 이후 트럼프 행정부는 오바마 행정부 시기의 '사이버안보조정관'을 폐지하고 보다 적극적으로 국토안보부를 중심으로 하는 사이버안보 거버넌스 체계를 구축했다. 이는 국토안보부를 중심으로 정부의 사이버안보네트워크를 구축하고 이를 바탕으로 민간의 기업들과 협조 체계를 구축하며 사이버 위협에 대한 적극적인 대응의 움직임을 보였다. 2017년 5월 워너크라이 대응에 있어서도 미국의 사이버안보 거버넌스 체계는 위협에 적극적으로 대응하며 위기의 확산을 최소화할 수 있었다.

북한의 한국에 대한 사이버 공격은 지속적으로 이루어지는 것으로 알려져 있다(성용은 2020). 특히 북한 정부의 후원을 받는 것으로 추정되는 김수키· 라자루스·금성121·코니 등은 블록체인, 첨단 산업, 코로나 바이러스 대응 그리고 청와대 등 불특정 다수를 대상으로 무차별적으로 테러를 가하는 것으로 보고되고 있다. 특히 북한은 정치자금 확보를 목적으로 외화벌이 목적으로 관련 기관을 집중 공격하고 있으며 관련 관료 및 전문가들에 대한 해킹을 확대하고 있다(이철재 2020). 사이버 공간에서 해킹에 대한 대응은 개인이 선제적으로 대응해야 하는 문제이지만 불특정 다수를 대상으로 하는 무차별적 테러는 민관 그리고 국제적 차원의 안보 거버넌스 구축을 통한 대응이 효율적일 수 있다.

참고문헌

고현실.2017.“'우연히 탄생한 영웅'이 랜섬웨어 확산 저지…'킬스위치' 작동” (05.13) <출처: https://www.yna.co.kr/view/AKR20170513050600017?input=1195m>

김귀근.2017.““北, 사이버전략사령부 창설 추진” 주장 나와“ 『연합뉴스』 (11.16) <출처: https://www.yna.co.kr/view/AKR20171116050200014>

김근혜.2019.“트럼프 행정부의 주요기반시설 사이버보안 정책분석에 관한 연구.”『정보보호학회논문지』29(4), 907-918.

김상배, “트럼프 행정부의 사이버안보 전략: 국가지원 해킹에 대한 복합지정학적 대응,”『국제·지역연구』27(4), 2018. pp. 1-35.

김수진.2017.“사상최대 랜섬웨어 공격에 전세계 ‘혼돈’...피해국 100개국 육박” (05.13) <https://www.yna.co.kr/view/AKR20170513049800009?input=1195m>

김윤영.양철호.2020.“북한의 사이버 테러에 대비한 법·제도 개선방안 연구.”『유럽헌법연구』33: 355-384.

김진광.2020.“북한의 사이버조직 관련 정보연구(조직 현황 및 주요 공격 사례를 중심으로)”『한국컴퓨터정보학회 학술발표논문집』28(2): 111-114.

김형수.2013.“김정은 ”사이버전은 만능의 보검“ 3대 전쟁수단 운용.”『중앙일보』

박차오름, 부승찬.2020.“중국의 사이버안보전략과 북한에의 적용: 정체성과 인식을 중심으로.”『아시아리뷰』10(1): 53-79.

배영자.“사이버안보 국제규범에 관한 연구.”『21세기 정치학회보』27(1), 105-128.

성용은.2002.“북한 사이버 테러의 특성 분석 및 시사점”『한국융합과학회지』9(3): 265-279.

심인성.2017. “[트럼프정부 6대 국정기조] 세계 최강 미군 표방-시퀘스터 폐지”『연합뉴스』(01.21). <출처: https://www.yna.co.kr/view/AKR20170121017600071>

안용현.2011. “북한 전자전 능력은?” 『조선일보』 2011.03.07. https://news.chosun.com/site/data/html_dir/2011/03/07/2011030702345.html

이광빈.2017.“NSA "워너크라이 랜섬웨어 공격에 北 정보당국 관여"”『연합뉴스』(06.15) <출처: https://www.yna.co.kr/view/AKR20170615115700009?input=1195m>

이귀원.2019.“유엔 대북제재위 "北 사이버해킹, 한국이 最多 피해국"”(08.31).<출처: https://www.yna.co.kr/view/AKR20190813014900072?input=1195m>

장노순.2017. “랜섬웨어와 북한의 사이버위협” JPI Research Series, 40, 73-77

정구연·이기대.2016.『과학기술발전과 북한의 새로운 위협: 사이버위협과 무인기 침투』KINU 연구총서 16-4. 서울: 통일연구원. 3

정영애.2019.“북한의 사이버 공격 역량의 진화: 사이버 공격 사례 분석을 중심으로.”『평화학연구』20(4): 125-143

조선인민군,“조성된 정세의 요구에 맞게 자기 부문의 싸움준비를 빈틈없이 완성할데 대하여,”『학습제강』(군관, 장령용) (평양: 조선인민군출판사, 2006), pp. 26-27.

주문화, 권헌영, 임종인, “주요국 사이버보안 거버넌스 분석과 정책적 시사점,”『정보보호학회논문지』5, 2018. 1259-1277

최병각.“인터넷 거버넌스와 사이버안보”『비교형사법연구』제19권 제4호 (2018), 457-480.

Choucri, Nazhi, Stuart Madnick and Jeremy Ferwerda, 2014.“Institutional for Cyber Security: International Responses and Global Imperatives,” Information Technology for Development Vol. 20, No. 2.

Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts May 15, 2018 https://www.dhs.gov/news/2018/05/15/department-homeland-security-unveils-strategy-guide-cybersecurity-efforts

Donald J. Trump, Crippled America: How to Make America Great Again (New York: Simon & Shuster, 2015)

Ellen Nakashima and Philip Rucker.2017.“U.S. declares North Korea carried out massive WannaCry cyberattack” Washington Post (Dec. 19) <출처: https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html>

Ellen Nakashima. 2017.“The NSA has linked the WannaCry computer worm to North Korea” Washington Post (Juen 14) <출처: https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.2cf52911d0f8>

Excutive Order 13636 – Improving Critical Infrastructure Cybersecurity

Froomkin,, A. Michael. 1997.“The Internet as a Source of Regulatory Arbitrage,” in Brian Kahin and Charles Nesson(eds.), Borders in Cyberspace: Information Policy and the Global Information Infrastructure. Cambridge, MA: MIT Press.

Goldsmith, Jack.2011. "Cybersecurity treaties: a skeptical view." in Peter Berkowtiz. Future challenges in national security and law 6.

https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

ITU. “TUNIS AGENDA FOR THE INFORMATION SOCIETY.” WSIS-05/TUNIS/DOC/6(Rev. 1)-E. 18 November 2005 https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

Jack Stubbs.2020.“Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca – sources” REUTERS (NOVEMBER 27) <출처: https://www.reuters.com/article/idUSKBN2871A2>

JOSEPH MARKSOCTOBER 24, 2017 Trump Administration Plans a New Cybersecurity Strategy https://www.nextgov.com/cybersecurity/2017/10/trump-administration-plans-new-cybersecurity-strategy/142014/

Kanti Bajpai, “The Idea of Human Security,” International Studies, Vol. 40, No. 3(2003), p.

Mauer, Cyber Norm Emergence at the United States, Belfer Center for Science and International Affairs, Harvard Schoold, 2011, p. 25; 장노순,“사이버안보와 국제규

범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로," p. 19.
Michael Schmitt and Sean Fahey.2017."WannaCry and the International Law of Cyberspace." Just Security. (Dec. 22). <출처: https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/>
Michael Schmitt and Sean Fahey.2017."WannaCry and the International Law of Cyberspace." Just Security. (Dec. 22). <출처: https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/>
Nastasiu, Catalin-Ionut. 2016. "Cyber Security Strategies in the Internet Era," Scientific Research and Education in the Air Force NO. 2.
National Cyber Strategy of the United States of America
Nye, Joseph S.2011."Nuclear lessons for cyber security?." Strategic Studies Quarterly Vol. 5.4: 18-38.
Obama's cybersecurity legacy: good Intentions, good efforts, limited result, " CSO, https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html, Apr. 2,2017.
Paul M. Nakasone and Michael Sulmeyer. 2020. "How to Compete in Cyberspace Cyber Command's New Approach" Foreign Affairs (25 Aug.) <출처: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>
Segal, Adam. 2016. The Hacked World Order: Elements of Cyber Power, Council on Foreign Relations, February 23. https://www.cfr.org/blog/hacked-world-order-elements-cyber-power
Shahan, Travis D. "The World Summit of the Information Society and the Future of Internet Governance." Computer L. Rev. & Tech. J. 10 (2005): 325.
Sidetracked: Obama's cybersecuritylegacy," World Politics Review,https://www.worldpoliticsreview.com/articles/17468/sidetracked-obama-s-cybersecurity-legacy,Dec. 15, 2015
The White House, "FACT SHEET: Cyber Threat Intelligence Integration Center" February 25, 2015 https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center
The White House, "The Comprehensive National Cybersecurity Initiative" https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf
Trump administration plans a new cybersecurity strategy," Boan New, https://www.boannews.com/media/viewasp?idx =57811, Nov. 1, 2017. [Retrieved from 12th July, 2019]
U. S. Department of Homeland Security, "U. S. department of homeland security cybersecurity strategy," The Department of Homeland Security: Washington, DC., 2018.
U.S. Department of Defense, Instruction No. 5205.13: Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities 10 (Jan. 29, 2010), at

http://www.dtic.mil/whs/directives/corres/pdf/520513p.pdf. More recent U.S. definitions have become unwieldy. See “cybersecurity,” Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies, A Glossary of Common Cybersecurity Terminology, at https://ics-cert.us-cert.gov/sites/default/files/documents/Common%20Cyber%20Language_S508C.pdf

U.S. Department of Homeland Security Cybersecurity Strategy, 2018

United Nation Security Council.2019.Resolution 1874 (2009)(S/2019/691).(30 August) <출처 : https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf>

Unity of effort key to DHS’ new cybersecurity strategy," Federal News Net work, https://federalnewsnetwork.com/hearings-oversight/2018/05/unity-of-effort-key-to-dhs-new-cybersecurity-strategy/, May. 15, 2018. [Retrieved from 8th March, 2019]

WGIG, Report of the Working Group on Internet Governance, 2005, p. 4. https://www.wgig.org/docs/WGIGREPORT.pdf

White House Issues Cybersecurity Order” May 11, 2017 https://www.dataprotectionreport.com/2017/05/white-house-issues-cybersecurity-order/

White House. “Briefing on the Attribution of the WannaCry Malware Attack to North Korea” <출처: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>

Williams, Paul D. 2008. Security Studies-an Introduction, London and New York: Routledge.